

ANAYA  
MULTIMEDIA

# EL ARTE DE LA INVISIBILIDAD

El hacker más famoso del mundo enseña  
seguridad en la era Big Brother y Big Data



**KEVIN MITNICK**  
con Robert Vamosi

## Copyright

de copyright © 2017 por Kevin Mitnick copyright de Prólogo © 2017 por Mikko Hypponen diseño de Portada por fotografía de Autor de Lee de Julianna por Tolga Katas copyright de Portada © 2017 por Hachette Grupo de Libro, Inc.

Hachette Grupo de Libro apoya el derecho a expresión libre y el valor de copyright. El propósito de copyright es para fomentar escritores y artistas para producir las obras creativas que enriquece nuestra cultura.

El barrido, cargando, y distribución de este libro sin permiso es un robo del autor's hacienda intelectual. Si te gustaría permiso para utilizar material del libro (otro que para propósitos de reseña), complacer contacto [permissions@hbgusa.com](mailto:permissions@hbgusa.com). Gracias para vuestro apoyo de los derechos del autor.

Poco, Brown y Empresa Hachette Grupo de Libro 1290 Avenida de la América, Nueva York, NY 10104 [littlebrown.com](http://littlebrown.com) [twitter.com/littlebrown](https://twitter.com/littlebrown) [facebook.com/littlebrownandcompany](https://facebook.com/littlebrownandcompany)

Primer ebook edición: febrero 2017

Poco, Brown y Empresa is una reparto de Hachette Grupo de Libro, Inc. El Poco, Brown nombre y el logotipo son marcas de Hachette Grupo de Libro, Inc.

El editor no es responsable para sitios web (o su contenido) aquello no es poseído por el editor.

El Hachette Agencia de Altavoces proporciona una gama ancha de autores para hablar casos. Para descubrir más, va a [hachettespeakersbureau.com](http://hachettespeakersbureau.com) o llamada (866) 376- 6591.

ISBN 978-0-316-38049-2 E3-20161223-JV-Página

*de Título de Portada de PC Prólogo de Dedicación del Copyright por Mikko Hypponen*

Tiempo | de Introducción para Desaparecer

## Contenidos

Capítulo Uno | Vuestra Contraseña Puede Ser Agrietada! Capítulo Dos | Quién Más está Leyendo Vuestro Email? Capítulo Tres | Wiretapping 101 Capítulo Cuatro | Si Te Don't Encripta, eres Unequipped Capítulo Cinco | Ahora Me Veo, Ahora Tú no Capítulo Seis | Cada Clic de Ratón Haces, Seré Mirar Te Capítulo Siete | Paga Arriba o Más!

Capítulo Ocho | Cree Todo, Confía en Nada Capítulo Nueve | no Tienes Ninguna Intimidad? Coge Encima Lo! Capítulo Diez | Te Puede Correr pero No Esconder Capítulo Once | Hey, KITT, no Comparte Mi Capítulo de Ubicación Doce | El Internet de Capítulo

de Vigilancia Trece | Cosas Vuestro Jefe no Te Quiere para Saber Capítulo Catorce | Obteniendo el anonimato Es Capítulo de Trabajo duro Quince | El FBI Siempre Coge Su Capítulo de Hombre Dieciséis | Mastering el Arte de Invisibilidad

*Acknowledgments Sobre los Libros de Autores por Kevin Mitnick Notas Newsletters*

*A mi madre amorosa, Shelly Jaffe, y mi abuela Reba Vartanian*

## **Prólogo por Mikko Hypponen**

Un par de hace meses, cumplí arriba con un amigo viejo quién no había visto desde entonces instituto. Fuimos para una taza de café para coger arriba en qué cada cual de nosotros

había sido haciendo para las décadas pasadas. Me dije aproximadamente su obra de distribuir y apoyando varios tipos de aparatos médicos modernos, y expliqué cómo he pasado el último twenty-cinco años que obran con seguridad de Internet e intimidad. Mi amigo dejado fuera de un chuckle cuándo mencioné intimidad on-line. “Aquello suena todo bien y dandy,” dijo, “pero no soy realmente se preocupó. Después de todo, no soy un delincuente, y no estoy haciendo cualquier cosa malo. No me preocupo si alguien mira en qué I estoy haciendo on-line.”

Escuchando a mi amigo viejo, y su explicación encima por qué la intimidad no importa a él, estuve entristecido. Estuve entristecido porque yo've oyó estas riñas antes, muchas veces. Les oigo de personas quiénes piensan que

tienen nada para esconder. Les oigo de personas quiénes piensan necesidad de delincentes únicos para los proteger. Les oigo de personas quiénes piensan encriptación de uso de terroristas única. Les oigo de personas quiénes piensan nosotros don't necesidad de proteger nuestros derechos. Pero necesitamos para proteger nuestros derechos. Y la intimidad no sólo afecta nuestros derechos, *es un derecho humano*. De hecho, la intimidad está reconocida como derecho humano fundamental en las 1948 Naciones Unidas Universal Declaration de Derechos humanos.

Si nuestra intimidad protección necesitada en 1948, seguramente lo necesita mucho más hoy. Después de todo, somos la primera generación en historia humana que puede ser controlado en un nivel tan preciso. Podemos ser controlados digitalmente durante nuestras vidas. Casi todo de nuestro communications puede ser visto una manera u otro. Incluso llevamos pequeños siguiendo aparatos encima nos todo el tiempo—sólo no les llamamos siguiendo aparatos, les llamamos smartphones.

El control on-line puede ver lo que libros compramos y lo que prendas noticiosas leímos—incluso cuál separa de las prendas son más interesantes a nosotros. Puede ver donde viajamos y quién viajamos con. Y el control on-line sabe si eres sick, o triste, u horny. Mucho del controlando que está hecho hoy compila este dato para ganar dinero. Empresas que oferta los servicios libres de alguna manera convierten aquellos servicios libres a miles de millones de dólares de ingresos—amablemente ilustrando sólo qué valiosos es a usuarios de Internet del perfil en escala de masa. Aun así, allí ha también control más apuntado: la clase de controlar hecho por agencias de gobierno, domésticos o extranjeros.

La comunicación digital lo ha hecho posible para gobiernos para hacer bulk vigilancia. Pero ha también nos habilité para prpers proteger mejor. Prpers podemos proteger con a herramientas les gusta la encriptación, por almacenar nuestro dato en maneras seguras, y por principios básicos siguientes de seguridad de operaciones (OPSEC). Sólo necesitamos una guía encima cómo para hacerlo bien.

Bien, la guía necesitas es aquí mismo en vuestras manos. Yo'm Kevin realmente feliz tomó el tiempo para escribir abajo su conocimiento en el arte de invisibilidad. Después de todo, sabe una cosa o dos aproximadamente quedándose invisible. Esto es un recurso sumo. Leído lo y utilizar el conocimiento a vuestro advantage. Te protege y proteger vuestros derechos.

Atrás en el cafeteria, después de que había acabado café con mi amigo viejo, separamos maneras. Le deseé bien, pero todavía a veces pienso sobre sus palabras: “no me preocupo si alguien mira en qué I estoy haciendo on-line.” No podrías tener cualquier cosa para esconder, mi amigo. Pero tienes todo para proteger.

*Mikko Hypponen Es el agente de búsqueda del jefe de F-Seguro. Él's la persona viviente única quién ha hablado en ambos DEF CON y TED conferencias.*

## Tiempo

### de INTRODUCCIÓN para Desaparecer

Casi dos años al día después Edward Joseph Snowden, un contratista para Booz Allen Hamilton, primero reveló su cache del material secreto tomado de la Agencia de Seguridad Nacional (NSA), HBO comedian John Oliver fue a Plaza de Tiempo en Ciudad de Nueva York a personas de estudio al azar para un segmento de su espectáculo encima intimidad y vigilancia. Sus cuestiones eran claras. Quién es Edward Snowden? Qué hace?<sup>1</sup>

En los clips de entrevista Oliver aireó, nadie parecía para saber. Incluso cuándo las personas dijeron que retiraron el nombre, ellos couldn't dice exactamente lo que Snowden había hecho (o por qué). Después de acaecer un contratista para el NSA, Edward Snowden copió miles de secreto superior y documentos clasificados que posteriormente dio a reporteros tan les podrían hacer públicos alrededor del mundo. Oliver podría haber acabado el segmento de su espectáculo aproximadamente vigilancia en una nota de deprimir —después de años de cobertura de medios de comunicación, nadie en América realmente parecía para preocuparse sobre doméstico espiando por el gobierno—pero el comedian escogió otro tack. Voló a Rusia, donde Snowden ahora vidas en exilio, para un un-encima-un inter vista.<sup>2</sup>

La primera cuestión Oliver puso a Snowden en Moscú era: Qué esperas cumplir? Snowden Contestó que quiso asomar el mundial lo que el NSA hacía—dato de coleccionismo encima casi everyone. Cuándo Oliver le asomó las entrevistas de Plaza de Tiempo, en cuál persona después de que otro professed no para saber quién Snowden era, su respuesta era, “Bien, no puedes tener todo el mundo bien informó.”

Por qué no es nosotros más informados cuándo viene a la intimidad emite que Snowden y otros han criado? Por qué don't parecemos para preocuparse que una agencia de gobierno es wiretapping nuestras llamadas de teléfono, nuestros emails, e incluso nuestros mensajes de texto? Probablemente porque el NSA, en general, no directamente afectar las vidas de la mayoría de nosotros—al menos no en una manera tangible, como una intrusión que podemos *sentir*.

Pero como Oliver también descubierto en los tiempos Cuadran que día, los americanos se preocupan aproximadamente intimidad cuándo pega casa. Además de pedir preguntas sobre Snowden, pidió cuestiones generales aproximadamente intimidad. Por ejemplo, cuándo pidió cómo sentían sobre un secreto (pero hecho-arriba) programa de gobierno que imágenes de récords de personas en cueros siempre que las imágenes están enviadas sobre el Internet, la respuesta unmong New Yorkers era también universal—excepto este tiempo todo el mundo opposed lo, enfáticamente. Una persona incluso admitida a tener recientemente envió tal foto.

Todo el mundo entrevistado en el Tiempo el segmento Cuadrado acordado que las personas en los Estados Unidos tendrían que ser capaces de compartir cualquier cosa—incluso una foto de un pene— en privado sobre el Internet. Cuál era Snowden punto básico.

Resulta que el programa de gobierno de la falsificación que récords los cuadros en cueros es menos lejos-fetched que podrías imaginar. Tan Snowden explicado a Oliver en su entrevista, porque a empresas les gusta Google tiene los servidores físicamente localizados en todo el mundo, incluso un mensaje sencillo (quizás incluyendo nudity) entre un marido y mujer dentro de la misma ciudad de EE.UU. primero podría botar de un servidor extranjero. Desde entonces que datunas hojas los Estados Unidos, incluso para un nanosecond, el NSA podría, gracias a la Ley de Patriota, recoge y archivo que texto o email (incluyendo la foto indecente) porque técnicamente introdujo los Estados Unidos de una fuente extranjera en el momento cuándo estuvo captado. Snowden punto: los americanos medianos están siendo cogidos arriba en un poste-9/11 dragnet aquello era inicialmente diseñado para parar terroristas extranjeros pero que ahora espia encima prácticamente todo el mundo.

Pensarías, dado el constante noticioso sobre los datos incumple y campañas de vigilancia por el gobierno, que nosotros'd ser mucho más indignados. Creerías que dado qué rápidamente esto pasado—en justo un handful de años— seríamos devanar del shock y marching en las calles. De hecho, el opuesto es cierto. Muchos de nosotros, incluso muchos lectores de este libro,

ahora aceptar a al menos algún grado el hecho que todo nosotros —todo nuestras llamadas de teléfono, nuestros textos, nuestro e- correos, nuestros medios de comunicación sociales—pueden ser vistos por otros.

Y aquello está decepcionando.

Quizás te ha roto ninguna ley. Vives wsombrero piensas es una vida mediana y tranquila, y sientes tú es inadvertido entre las multitudes de otros on-line hoy. Me confío en: incluso no eres invisible. Al menos no todavía.

Gozo mágico, y algunos podrían discutir que sleight de la mano es necesaria para el ordenador que corta. Uno el truco mágico popular es para hacer un objeto invisible. El secreto, aun así, es que el objeto no físicamente desaparece o de hecho acaecer invisible. El objeto siempre restos en el fondo, detrás de una cortina, arriba de una manga, en un bolsillo, whether lo podemos ver o no.

El mismo es cierto de los muchos detalles personales sobre cada y cada uno de nosotros aquello actualmente está siendo recogido y almacenado, a menudo sin nuestro notando. La mayoría de nosotros sencillamente no saben qué fáciles es para otros para ver este detalles aproximadamente nos o incluso dónde para mirar. Y porque *no vemos esta información, podríamos creer que somos invisibles a nuestro exes, nuestros padres, nuestras escuelas, nuestros jefes, e incluso nuestros gobiernos.*

El problema es que si sabes dónde para mirar, toda aquella información es disponible a sólo aproximadamente cualquiera.

Siempre que hablo antes de multitudes grandes—ningún asunto la medida de la sala—I normalmente tener una persona quién me desafío encima este hecho. Después de que uno tal caso estuve desafiado por un reportero muy escéptico.

Recuerdo estuvimos sentar en una mesa privada en una barra de hotel en una ciudad de EE.UU. grande cuándo el reportero dijo ella'd nunca sido una víctima de una ruptura de dato. Dado su juventud, dijo que hubo relativamente pocas ventajas a su nombre, por ello pocos récords. Ella nunca detalles personales puestos a cualquier de sus historias o sus medios de comunicación sociales personales— lo mantuvo profesional. se consideró invisible. Así que pedí su para permiso para encontrar su número de Seguridad Social y cualquiera otros detalles personales on-line. A regañadientes acordó.

Con su sentado cercano I logged en a un sitio, uno aquello está reservado para detectives privados. Capacito como el último a través de mi obra que

investiga cortando incidentes globalmente. Ya supe su nombre, así que pedí dónde vivió. Esto podría haber encontrado en el Internet también, on otro sitio, si no había dicho me.

En un par de minutos supe su número de Seguridad Social, su ciudad de nacimiento, e incluso su madre's nombre virginal. También supe todos los sitios ella casa llamada nunca y todos los números de teléfono nunca utilizó. Staring En la pantalla, con un cariz sorprendido en su cara, confirmó que toda la información era más o menos cierta.

El sitio utilicé está restringido a vetted empresas o personaje. Cobra un coste bajo por mes más costes adicionales para cualquier información lookups, y de vez en cuando me auditará para descubrir si tengo un propósito legítimo para dirigir una búsqueda particular.

Pero información similar aproximadamente cualquiera puede ser encontrado para un pequeño lookup coste. Y es perfectamente legal.

Te tienes nunca llenado fuera de una forma on-line, información entregada a un escolar u organización que pone su información on-line, o tuvo un caso legal posted al Internet? Si tan, has volunteered información personal a una tercera fiesta que puede hacer con la información qué complace. Las casualidad son que algunos—si no todo—de aquel dato es ahora on-line y disponible a empresas que lo hace su empresarial de recoger cada bit de información personal del Internet. Los Derechos de Intimidad Clearinghouse listas más de 130 empresas que recoge información personal (si o no es cuidadoso) aproximadamente te.<sup>3</sup>

Y entonces hay el dato que tú no el voluntario on-line pero aquello empero está siendo cosechado por empresas y governments—información aproximadamente quien nosotros email, texto, y llamada; qué buscamos on-line; qué compramos, cualquiera en un ladrillo-y-mortero o una tienda on-line; y donde viajamos, a pie o por automovilísticos. El volumen de datos recogió sobre cada y cada uno de nosotros está creciendo exponentially cada día.

Te puedes pensar don't necesidad de preocuparse sobre este. Me confío en: haces. Espero que por el fin de este libro serás ambos bien-informado y preparó bastante para hacer algo aproximadamente lo.

El hecho es que vivimos con una ilusión de intimidad, y probablemente hemos sido viviendo de este modo para décadas.

En un punto seguro, prpers podríamos encontrar incómodos con cuánto acceso nuestro gobierno, nuestros empresarios, nuestros jefes, nuestros



profesores, y nuestros padres tienen a nuestras vidas personales. Pero desde aquel acceso ha sido obtenido gradualmente, desde entonces nosotros've abrazó cada comodidad digital pequeña sin resistir su impacto en nuestra intimidad, acaece cada vez más duro de girar atrás el reloj. Además, quién entre nosotros quiere dar arriba de nuestros juguetes?

El peligro de viviente dentro de un estado de vigilancia digital no es tanto que el dato está siendo recogido (allí's poco podemos hacer sobre aquel) pero *qué está hecho con el dato* una vez está recogido.

Imaginar lo que un overzealous prosecutor podría hacer con el dossier grande de dato crudo señala disponible encima te, quizás volviendo varios años. Dato hoy, a veces recogido fuera de contexto, vivirá para siempre. Even EE.UU. justicia de Corte

Suprema Stephen Breyer acuerda que es “difícil para cualquiera para saber, por adelantado, sólo cuándo un conjunto particular de las declaraciones más tarde podrían parecer (a un prosecutor) para ser pertinentes a algunos tal investigación.”<sup>4</sup> En otras palabras,, un cuadro de ti bebido que alguien posted encima Facebook podría ser el menos de vuestras preocupaciones.

Puedes pensar que tienes nada para esconder, pero sabes que seguro? En una opinión bien discutida pieza en *seguridad Alambrada*, respetada investigador Moxie Marlinspike puntos fuera que algo como sencillito como siendo en la posesión de una langosta pequeña es de hecho un delito federal en los Estados Unidos.<sup>5</sup> “Lo doesn't asunto si compraste él en un grocery tienda, si alguien más lo dio a ti, si es muerto o vivo, si lo encontraste después de que murió de causas naturales, o incluso si lo mataste mientras obrando en defensa propia. Puedes ir a prisión debido a una langosta.”<sup>6</sup> El punto aquí es hay mucho menor, unenforced leyes que te podría ser romper sin conocerlo. Exceptúa ahora hay una estela de dato para probarlo sólo unos cuantos grifos fuera, disponibles a cualquier persona quién lo quiere.

La intimidad es compleja. No es un un-medida-acceso-toda proposición. Nosotros todos tienen razones diferentes para compartir alguna información aproximadamente nosotros libremente con desconocidos y manteniendo otras partes de nuestras vidas privadas. Quizás tú sencillamente don't querer vuestro significativo otro leyendo vuestro material personal. Quizás no quieres vuestro empresario para saber sobre vuestra vida privada. O quizás te realmente teme que una agencia de gobierno está espiando encima te.

Estos son escenarios muy diferentes, así que nadie la recomendación ofreció aquí está yendo a cabido les todo. Porque aguantamos complicados y por tanto actitudes muy diferentes hacia intimidad, guiaré tú a través de qué es

importante— qué está pasando hoy con colección de dato subrepticio—y dejado decides lo que obras para vuestra vida propia.

Si cualquier cosa, este libro te hará consciente de maneras de ser privadas dentro del mundo digital y soluciones de oferta que te poder o no puede escoger adoptar. Desde entonces la intimidad es una elección personal , grados de invisibilidad, también, variará por individual.

En este libro haré el caso que cada cual y cada uno de nosotros está siendo mirado, en casa y fuera en el mundial—como andas abajo la calle, sienta en una cafetería, o paseo abajo la carretera. Vuestro ordenador, vuestro teléfono, vuestro coche, vuestro sistema de alarma de la casa, incluso vuestro refrigerador es todos los puntos potenciales de acceso a vuestra vida privada.

El bueno noticioso es, además de asustarte, también te voy a asomar qué para hacer sobre la carencia de intimidad—una situación aquello ha estado a la orden del día. En este libro, aprenderás cómo a:

encripta y enviar un email seguro protege vuestro dato con gestión de contraseña buena esconde vuestra alocución de IP cierta de sitios visitas ocultar vuestro ordenador de ser seguido defender vuestro anonimato y mucho más

Ahora, apareja a maestro el arte de invisibilidad.

## CAPÍTULO UNO

### **Vuestra Contraseña Puede Ser Agrietada!**

Jennifer Lawrence era habiendo un fin de semana de Día de Trabajo áspero. El ganador de Premio de la Academia era uno de varias celebridades quién despertó una mañana en 2014 para encontrar que sus la mayoría de cuadros privados—muchos del cual les asomó en el desnudo—era splashed aproximadamente en el Internet.

Toma un momento a mentalmente escanear todas las imágenes que unre actualmente almacenados en vuestro ordenador, teléfono, y email. Seguro, muchos de ellos son perfectamente benignos. Tú'd ser bien con el entero mundial viendo los ocasos, el lindos familiares snapshots, quizás incluso el jokey malos-cabello-día selfie. Pero ser cómodo sharing cada cual y cada uno de ellos? Cómo sientes si ellos de repente todo pareció on-line? Quizás no todas nuestras fotos personales son salacious, pero ellos're récords quietos

de momentos privados. Tendríamos que ser capaces de decidir si, cuándo, y cómo para compartirles, todavía con servicios de nube la elección puede no siempre ser el nuestro.

La historia de Lawrence de la Jennifer dominó el fin de semana de Día de Trabajo lento ciclo noticioso en 2014. Era parte de un caso llamó theFappening, una filtración enorme de fotografías desnudas y casi desnudas de Rihanna, Kate Upton, Kaley Cuoco, Adrianne Curry, y casi trescientos otras celebridades, la mayoría de ellos mujeres, cuya celda-imágenes de teléfono de alguna manera habían sido remotely accedidos y compartió. Mientras algunas personas eran, previsiblemente, interesados en ver estas fotos, para muchos el incident era un unsettling recordatorio que la misma cosa podría haber pasado a ellos.

Tan qué hizo alguien coge acceso a aquellas imágenes privadas de Jennifer Lawrence y otros?

Desde entonces todas las celebridades utilizaron iPhones, la especulación temprana centrada en una ruptura de dato masiva que afecta Manzana iCservicio fuerte, una nube-opción de almacenamiento para usuarios de iPhone. Como vuestras carreras de aparato físicas fuera de memoria, vuestras fotos, limas nuevas, música, y los juegos son en cambio almacenados en un servidor en Apple, normalmente para un coste mensual pequeño. Google ofrece un servicio similar para Android.

Apple, el cual casi nunca comentarios en los medios de comunicación encima asuntos de seguridad, negó cualquier falta en su fin. La empresa emitió una declaración que llama el incidente un “ataque muy apuntado encima nombres de usuario, contraseñas, y cuestiones de seguridad” y añadió que “ninguno de los casos hemos investigado ha resultado de cualquier ruptura en cualquier de los sistemas de Apple incluyendo iCloud o Encontrar mi iPhone.”<sup>1</sup>

Las fotos primero empezaron parecer en un hacker el foro bien sabido para posting compromised fotos.<sup>2</sup> Dentro de aquel foro puedes encontrar las discusiones activas de las herramientas forenses digitales utilizaron para surreptitiously obteniendo tales fotos. Investigadores, detectives, y aplicación de ley utiliza estas herramientas para acceder dato de aparatos o la nube, normalmente siguiendo un crime. Y naturalmente las herramientas tienen otros usos también.

Uno de las herramientas abiertamente habladas en el foro, Elcomsoft Rompiente de Contraseña del Teléfono, o EPPB, está pretendido para

habilitar aplicación de ley y agencias de gobierno para acceder iCloud cuentas y está vendido públicamente. Es sólo uno de muchas herramientas allí, pero aparece para ser el más popular en el foro. EPPB Requiere que los usuarios tienen el objetivo's iCloud username e información de contraseña primero. Para las personas que utilizan este foro, aun así, obteniendo iCloud usernames y palabrasde pase no es un problema. Lo Tan pasado que sobre aquel fin de semana de vacaciones en 2014, alguien posted a un repositorio de código on-line popular (Github) una herramienta llamó iBrute, un mecanismo que corta contraseña específicamente diseñado para adquirir iCloud credentials de justo aproximadamente cualquiera.

Utilizando iBrute y EPPB junto, alguien podría impersonate una víctima y descargar una copia de seguridad llena de aquella víctima's nube-dato de iPhone almacenado a otro aparato. Esta capacidad es útil cuándo tú upgrade vuestro teléfono, por ejemplo. Es también valioso a un atacante, quiénes entonces pueden ver todo tú've nunca hecho en vuestro aparato móvil. Esto cede mucho más información que sólo logging en a una víctima iCloud cuenta.

Jonathan Zdziarski, un forensics asesor e investigador de seguridad, dijo *Alambrado* que su examen del filtró fotos de Kate Upton, por ejemplo, era compatible con el uso de iBrute y EPPB. Teniendo el acceso a una copia de seguridad de iPhone restaurada da un atacante mucha información personal que más tarde podría ser útil para chantaje.<sup>3</sup>

En octubre 2016, Ryan Collins, una persona de treinta y seis años de Lancaster, Pensilvania, estuvo sentenciado a dieciocho meses en prisión para “acceso no autorizado a un ordenador protegido para obtener la información” narró al tajo. Estuvo cobrado con acceso ilegal a encima cien Apple y cuentas de email del Google.<sup>4</sup>

para proteger vuestro iCloud y otras cuentas on-line, tienes que poner una contraseña fuerte. Aquello's obvio. Todavía en mi experiencia como penetración tester (bolígrafo tester)—alguien quién está pagado para cortar a redes de ordenador y encontrar vulnerabilidades— encuentro que muchas personas, incluso ejecutivos en empresas grandes, es perezoso cuándo viene a contraseñas. Considera que el CEO de Sony Diversión, Michael Lynton, utilizó “sonym13” como su contraseña de cuenta del ámbito. Es ninguna maravilla holas los emails estuvieron cortados y extendidos a través del Internet desde los atacantes tuvo acceso administrativo a más todo dentro de la empresa.

Allende vuestra obra-narró las contraseñas son aquellas contraseñas que protege vuestras la mayoría de cuentas personales. Escogiendo un duro-a-contraseña de suposición ganada't impide cortar herramientas como oclHashcat (una herramienta que agrieta contraseña que gráfico de apalancamientos que procesa unidades—o GPUs—para altos-acelera agrietar) de posiblemente agrietando vuestra contraseña, pero hará el proceso bastante lento para fomentar un atacante de mover encima a un objetivo más fácil.

Él's una suposición justa que algunos de las contraseñas expuestas durante el julio 2015 Ashley Madison el tajo ciertamente está siendo utilizado en otro lugar, incluyendo encima cuentas de banco e incluso ordenadores de obra. De las listas de 11 millones de Cenizaley Madison contraseñas posted on-line, la mayoría de común era “123456,” “12345,” “contraseña,” “DEFAULT,” “123456789,” “qwerty,” “12345678,” “abc123,” y 1234567.

“”<sup>5</sup> Si ves uno de vuestras contraseñas propias aquí, las casualidad eres es vulnerable a una ruptura de dato, como estos plazos comunes están incluidos en la mayoría de cajas de herramienta que agrietan contraseña disponibles on-line. Siempre puedes comprobar el sitio [www.haveibeenpwned.com](http://www.haveibeenpwned.com) para ver si vuestra cuenta ha sido compromised antiguamente.

En el veinte-primer siglo, podemos hacer mejores. Y significo *mucho mejor*, con configuraciones más largas y mucho más complejas de letras y números. Aquello puede sonar duro, pero te asomará tanto un automático y una manera manual de hacer

este. La aproximación más fácil es a forgo la creación de vuestras contraseñas propias y sencillamente

automate el proceso. Hay varias gerente de contraseña digitales allí. No sólo almacenan vuestras contraseñas dentro de una bóveda cerrada y dejar acceso de un clics cuándo les necesitas, también generan nuevos y realmente fuertes, contraseñas únicas para cada sitio cuándo les necesitas.

Ser consciente, aun así, de dos problemas con esta aproximación. Uno es que gerente de contraseña utilizan uno contraseña maestra para acceso. Si alguien pasa para infectar vuestro ordenador con malware aquello roba la base de datos de contraseña y vuestra contraseña maestra a través de keylogging—cuándo el malware récorde cada keystroke lo—haces's juego encima. Aquella persona entonces tendrá acceso a todas vuestras contraseñas. Durante mis compromisos que prueban bolígrafo, a veces reemplazo la gerente de contraseña con una versión modificada que transmite la contraseña maestra a nosotros (cuándo la gerente de contraseña es abierta-

fuelle). Esto está hecho después de que obtenemos admin acceso al cliente's red. Entonces vamos después de todo las contraseñas privilegiadas. En otras palabras,, utilizaremos gerente de contraseña como puerta posterior para coger los tonos al reino.

El otro problema es clase de obvio: Si pierdes la contraseña maestra, pierdes todas vuestras contraseñas. Finalmente, esto es vale, como siempre puedes actuar una reinicialización de contraseña en cada sitio, pero aquello sería un enorme hassle si tienes cuentas muchísimas.

A pesar de estos defectos, las puntas siguientes tendrían que ser más de adecuados de mantener vuestras contraseñas aseguran.

Primero, fuerte passphrases, no contraseñas, tendría que ser mucho tiempo—al menos veinte a veinticinco caracteres. Caracteres aleatorios—ek5iogh#skf&skd—obra más. Desafortunadamente la mente humana tiene problema recordando secuencias aleatorias. Tan uso una gerente de contraseña. Utilizando una gerente de contraseña es lejos mejor que escogiendo vuestro propio. Prefiero a gerente de contraseña de fuente abierta les gusta la contraseña Seguro y KeePass que dato de tienda única locally en vuestro ordenador.

Otra regla importante para las contraseñas buenas nunca es utilizar la misma contraseña para dos cuentas diferentes. Aquello's duro. Hoy tenemos contraseñas en justos aproximadamente todo. Así que tiene una gerente de contraseña genera y almacenar contraseñas fuertes , únicas para ti.

Incluso si tienes una contraseña fuerte, la tecnología todavía puede soler derrotarte. hay programas que adivinan contraseña como John el Ripper, un programa de fuente abierta libre que cualquiera puede descargar y que obras dentro parámetros de configuración set por el usuario.<sup>6</sup> Por ejemplo, un usuario podría especificar

cuántos caracteres para probar, si para utilizar símbolos especiales, si para incluir conjuntos de lengua extranjera, y tan encima. John el Ripper y otra contraseña hackers es capaz a permute las letras de contraseña que utilizan rule conjuntos que es extremadamente eficaz en agrietar contraseñas. Esto sencillamente significa prueba cada combinación posible de números, letras, y símbolos dentro de los parámetros hasta que es exitoso en agrietar vuestra contraseña. Afortunadamente, la mayoría de nosotros aren't arriba en contra nación-estados con virtualmente unlimited tiempo y recursos. Más probablemente somos arriba contra un cónyuge, un pariente, o alguien nosotros realmente meados fuera quién, cuándo afrontado con una contraseña

de veinticinco caracteres, ganando tener el tiempo o recursos a exitosamente agrietarlo.

Dejado es decir quieres crear vuestras contraseñas la manera anticuada y que te've escogido algunas contraseñas realmente fuertes. Suposición qué? Es vale para escribirles abajo. Sólo no escribe "Banco de América: 4thel1sttimein4ever\*." Aquello sería demasiado obvio. InsteEl anuncio reemplaza el nombre de vuestro banco (por ejemplo) con algo cryptic, como "Bote de Galleta" (porque algunas personas una vez escondieron su dinero en botes de galleta) y seguir él con 4thel1st. "" Aviso no completé la frase. Te don't Necesidad a. Sabes el resto de la frase. Pero alguien más puede no.

Cualquiera encontrando este imprimido-fuera la lista de contraseñas incompletas tendría que ser suficientemente confundido—al menos al principio. Historia interesante: era en la casa de un amigo—un muy Microsoft bien sabido empleado—y durante cena hablábamos la seguridad de contraseñas con su mujer y niño. En uno señala mi amigo's la mujer levantada y fue al refrigerador. Había escrito abajo todas sus contraseñas en una hoja de papel sola y lo enganchó a la puerta del electrodoméstico con un imán. Mi amigo sólo sacudió su jefa, y yo grinned ampliamente. Escribiendo abajo las contraseñas no podrían ser una solución perfecta, pero tampoco está olvidando que raramente contraseña fuerte utilizada.

Algunos sitios web—como vuestra cerradura de sitio web—bancaria fuera de usuarios después de varias contraseña fallada untttempts, normalmente tres. Muchos sitios, aun así, todavía no esto. Pero incluso si un sitio cierra una persona fuera después de que tres falló intentos, aquel isn't cómo el uso de tipos malo John el Ripper u oclHashcat. (Adicionalmente, oclHashcat distribuye el proceso de cortar sobre múltiple GPUs y es mucho más poderoso que John el Ripper.) También, hackers don't de hecho probar cada contraseña posible sola en un sitio vivo.

Dejado es decir ha habido una ruptura de dato, e incluido dentro del vertedero de dato es usernames y contraseñas. But Las contraseñas recuperaron de la ruptura

de dato es mera gibberish. Qué hace aquella ayuda cualquiera rompe a vuestra cuenta? Siempre que escribes en una contraseña, si es a unlock vuestro portátil o un

servicio on-line—que la contraseña está puesta a través de un un-manera algorithm sabido como hash función. No es igual tan encriptación. La encriptación es dos-manera: puedes encriptar y decrypt mientras tienes un tono. Un hash es un fingerprint representando una serie particular de



caracteres. En teoría, algoritmos de una maneras pueden't ser revocados—o al menos no fácilmente.

Qué está almacenado en la base de datos de contraseña en vuestro PC tradicional, vuestro aparato móvil, o vuestra cuenta de nube no es `MaryHadALittleLamb123$` pero su hash valor, el cual es una secuencia de números y letras. La secuencia es un token aquello representa vuestra contraseña.<sup>7</sup>

es la contraseña hashes, no las contraseñas ellos, aquello está almacenado en la memoria protegida de nuestros ordenadores y puede ser obtenido de un compromise de apuntó sistemas o filtrados en los datos incumple. Una vez un atacante ha obtained esta contraseña hashes, el hacker puede utilizar una variedad de públicamente herramientas disponibles, como John el Ripper u oclHashcat, para agrietar el hashes y obtener la contraseña real, cualquiera a través de brute fuerza (probando cada combinación alfanumérica posible) or probando cada palabra en una lista de palabra, como un diccionario. Las opciones disponibles en John el Ripper y oclHashcat dejar el atacante de modificar las palabras probaron contra conjuntos de regla numerosa, por ejemplo el conjunto de regla llamó leetspeak—un sistema para reemplazar letras con números, como en “k3v1n m17n1ck.” Esta regla cambiará todas las contraseñas a varios leetspeak permutaciones. Utilizando estos métodos para agrietar las contraseñas es mucho más eficaces que sencillos brute fuerza. Las contraseñas más sencillas y más comunes son fácilmente agrietadas primero, entonces contraseñas más complejas están agrietadas con el tiempo. La periodo de cronometra toma depende en varios factores. Utilizando una herramienta que agrieta contraseña junto con vuestro incumplido username y hashed contraseña, hackers puede ser capaz de acceder uno o más de vuestra cuentas por probar que la contraseña en sitios adicionales conectó a vuestra alocución de email u otro identificador.

En general, el más caracteres en vuestra contraseña, el más largo lo tomará programas que adivinan contraseña como John el Ripper para correr a través de todas las variaciones posibles. Como procesadores de ordenador cogen más rápidos, la periodo de cronometra toma para calcular todo el posible seis-carácter e incluso contraseñas de ocho caracteres está acaeciendo mucho más cortas, también. Aquello's por qué recomiendo utilizar contraseñas de veinticinco caracteres o más.

Después de que creas contraseñas fuertes—y muchos de ellos—nunca les dan



fuera. Aquello parece dolorosamente obvio, pero estudio en Londres y otras ciudades importantes asoman que las personas han comerciado sus contraseñas en cambio para algo como trivial como bolígrafo o una pieza de chocolate.<sup>8</sup>

Un amigo de la mina una vez compartió su Netflix contraseña con una novia. Hizo sentido en el tiempo. había el inmediato gratificatiencia de dejar su escoger una película para ellos para mirar junto. Pero atrapado dentro de Netflix sección de película recomendable era todo su “porque miraste...” Películas, incluyendo películas había mirado con novias pasadas. *La Hermandad de los Pantalones Ambulantes*, para caso, no es una película se habría ordenado, y su novia supo esto.

Naturalmente, todo el mundo ha exes. Incluso podrías ser sospechoso si dataste alguien quién didn't. Pero ninguna novia quiere ser afrontada con evidencia de quienes han ido antes de su.

Si te contraseña-proteger vuestros servicios on-line, tienes que también contraseña- proteger vuestros aparatos individuales. La mayoría de nosotros tiene portátiles, y muchos de nosotros todavía han desktops. Puedes ser en casa sólo ahora, pero qué sobre aquellos huéspedes de cena que vienen later? Por qué tomar una casualidad que uno de ellos podría acceder vuestras limas, fotos, y juegos sólo por sentar en vuestro escritorio y moviendo el ratón? Otro Netflix cautionary cuento: atrás en los días cuándo Netflix principalmente enviados fuera de DVDs, supe un par quién cogía pranked. During una fiesta en su casa, habían dejado su navegador abre a su Netflix cuenta. Después, el par encontrado que todas las clases de raunchy B-y películas de C listas habían sido añadidas a su queue—pero sólo después de que ellos'd recibidos más de uno de estas películas en el correo.

Es aún más importante de proteger tú con contraseñas en la oficina. Piensa de todo aquel tiempo tú're llamado fuera de vuestro escritorio a un impromptu reunión. Alguien podría andar por vuestro escritorio y ver el spreadsheet para el presupuesto del barrio próximo. O todos los emails que sientan en vuestra bandeja de entrada. O peor, a no ser que tienes una contraseña-ahorrativo de pantalla protegida que chuts en después de que unos cuantos segundos de inactividad, siempre que eres fuera de vuestro escritorio para un periodo extendido—fuera para comer o en una reunión larga—alguien podría sentar y escribir un email y enviarlo tan te. O incluso alterar el presupuesto del barrio próximo.

Hay métodos nuevos creativos a impedir este, gusta software que cierra pantalla que usos Bluetooth para verificar si eres cercano vuestro ordenador.

En otras palabras,, si vas al baño y vuestro teléfono celular sale de Bluetooth gama del ordenador, la pantalla es inmediatamente cerró. hay también versiones que uso un Bluetooth aparato como un wristband o smartwatch y hará

la misma cosa.

Creando contraseñas para proteger servicios y cuentas on-line es una cosa , pero él's no yendo para ayudarte si alguien obtiene posesión física de vuestro aparato, especialmente si has dejado aquellas cuentas on-line abren. Tan si te contraseña- proteger sólo uno puesto de aparatos, tendría que ser ynuestros aparatos móviles, porque estos son el más vulnerables a coger perdido o robado. Aún así *Informes de Consumidor* encontraron que 34 por ciento de los americanos no protegen sus aparatos móviles con cualesquier medidas de seguridad en absoluto, como cerrar la pantalla con un sencillo ALFILER de cuatro dígitos.<sup>9</sup>

En 2014 un Martinez, California, el agente policial confesó a robar fotos desnudas del teléfono celular de un DUI sospechoso, una vulneración clara de la Cuarta Enmienda, el cual es parte de la factura de la Constitución de Derechos.<sup>10</sup> Específicamente, el Cuarto Unmendment prohíbe unreasonable búsquedas y ataque sin un warrant emitidos por un juez y apoyado por aplicación de ley—de causa probable los agentes tienen que declarar por qué quieren acceso a vuestro teléfono, para caso.

Si has no ya contraseña-protegió vuestro aparato móvil, toma un momento ahora y hacer tan. Seriamente.

Hay tres maneras comunes para cerrar vuestro teléfono—si es un Androide o iOS o algo más. El más familiar es un passcode—una secuencia de números que introduces en un orden concreto a unlock vuestro teléfono. No resuelve para el número de dígitos el teléfono recomienda. Va a vuestros encuadres y manualmente configurar el passcode para ser más fuerte—siete dígitos si quieres (como un número de teléfono viejo de vuestra niñez.) Ciertamente uso más de justo cuatro.

Algunos los aparatos móviles te dejan para escoger un texto-basó passcode, como los ejemplos creamos [aquí](#). Otra vez, escoge al menos siete caracteres. Los aparatos móviles modernos muestran ambos número y tonos de letra en la misma pantalla, haciéndolo más fácil de cambiar atrás y adelante entre ellos.

Otra opción de cerradura es visual. Desde entonces 2008, teléfonos de Androide han sido equipados con algo patrones de cerradura de Androide

llamados (Alpes). Nueve puntos parecen en la pantalla, y les conectas en cualquier orden que quieras; aquello conectando la secuencia acaece vuestro passcode. Podrías pensar este ingenioso y que el sheer la gama de combinaciones posibles hace vuestra secuencia unbreakable. Pero en el Passwords-Con conferencia en 2015, los investigadores informaron que—la carácter humana siendo qué es participantes— en un estudio availed ellos de justo unos cuantos patrones posibles fuera de las 140,704 combinaciones posibles en ALP.<sup>11</sup> Y qué era aquellos patrones previsibles? Often La primera letra del nombre del usuario. El estudio también encontrado que las personas tendieron para utilizar los puntos en el medios y no en el remotos cuatro esquinas. Considera que el tiempo próximo pusiste un ALP.

Finalmente hay el biometric cerradura. Apple, Samsung, y otro popular los fabricantes actualmente dejan clientes la opción de utilizar un fingerprint escáner a unlock sus teléfonos. Ser consciente que estos no son foolproof. Después de la emisión de Tacta ID, investigadores—quizás esperando Manzana para tener mejorada a la cosecha actual de fingerprint escáners ya en la lonja—estuvo sorprendida para encontrar que varios métodos viejos de derrotar fingerprint escáners obra quieta en el iPhone. Estos incluyen captar un fingerprint fuera de una superficie limpia que utiliza polvo de criatura y cinta adhesiva clara.

Otros teléfonos utilizan el contruidos-en cámara para reconocimiento facial del dueño. Esto, también, puede ser derrotado por aguantar arriba de una fotografía de resolución alta del dueño delante del cámara.

En general, biometría por ellos es vulnerable a ataques. Idealmente la biometría tendría que ser utilizada tan sólo uno autenticando factor. Golpe vuestra yema o sonrisa para el cámara, entonces introducir un ALFILER o passcode. Aquello tendría que mantener vuestro aparato móvil seguro.

Qué si creaste una contraseña fuerte pero no lo escribió abajo? Reinicializaciones de contraseña son un godsend cuándo absolutamente puedes't acceso un infrequently cuenta utilizada. Pero también pueden ser que cuelgan abajo fruta para -ser atacantes. Utilizando las pistas dejamos en la forma de perfiles de medios de comunicación sociales por todas partes el Internet, hackers puede obtener acceso a nuestro email—y otros servicios— sencillamente por resetting nuestras contraseñas.

Uno ataca aquello ha sido en la prensa implica obtener el objetivo's últimos cuatro dígitos de su o su número de carta del crédito, y entonces utilizando que como prueba de identidad cuándo llamando en a un servproveedor de hielo para cambiar la alocución de email autorizada. Aquella manera, el

atacante puede reinicialización la contraseña en su o su propio sin el dueño legítimo que sabe.

Atrás en 2008 un estudiante en la Universidad de Tennessee, David Kernell, decidido para ver si él could acceso entonces candidato a la presidencia de vicio Sarah Palin personal Yahoo cuenta de email.<sup>12</sup> Kernell podría haber adivinado varias contraseñas, pero el acceso a la cuenta podría haber sido cerrado después de que unos cuantos fallado prueba. En cambio utilizó la función de reinicialización de la contraseña, un proceso él más tarde descrito como “fácil.”<sup>13</sup>

I soy seguro nosotros've todo recibió emails extraños de amigos y asocia contener enlaces a sitios de porno en países extranjeros sólo para aprender más tarde que nuestros amigos' cuentas de email habían sido tomadas encima. Este email takeovers a menudo ocurrir porque las contraseñas guarding las cuentas no son fuertes. Cualquiera alguien aprendió la contraseña—a través de una ruptura de dato—o el atacante utilizaron la función de reinicialización de la contraseña.

Cuando primer encuadre arriba de una cuenta como un email o incluso una cuenta de banco, puedes haber sido pedido qué es normalmente labeled tan cuestiones de seguridad. Típicamente hay tres de ellos. A menudo hay gota-abajo listado de cartas sugirió cuestiones, así que puedes escoger cuál unos quieres respuesta. Normalmente son realmente obvionos.

Dónde fuiste nato? Dónde vas a instituto? O universidad? Y el favorito viejo, vuestra madre's nombre virginal, el cual aparentemente ha sido en uso como cuestión de seguridad desde entonces al menos 1882.<sup>14</sup> Como hablaré abajo, lata de empresas y escanea el Interred y recoger información personal que las marcas que contestan esta seguridad básica cuestiona una pieza de pastel. Una persona puede pasar unos cuantos minutos en el Internet y tener una casualidad buena de ser capaz de contestar todas las cuestiones de seguridad de una personaje dada.

Sólo recientemente tener estas cuestiones de seguridad mejoraron un poco. Por ejemplo, “Qué es el estado donde vuestro hermano-en-la ley nació?” Es bastante distinto, aunque contestando estas “cuestiones” buenas correctamente pueden llevar sus riesgos propios, el cual cogeré a en un minuto. Pero muchos tan-cuestiones de seguridad llamada son todavía demasiado fáciles, como “Qué es la ciudad natal de vuestro padre?”

En general, cuándo poniendo estas cuestiones de seguridad, intenta evitar las sugerencias más obvias disponibles de la gota-abajo carta. Incluso si el sitio incluye enly cuestiones de seguridad básica, ser creativos. Nadie dice que

tienes que proporcionar respuestas sinceras. Puedes ser listo aproximadamente lo. Por ejemplo, según lo que vuestro streaming servicio de vídeo está concernido, quizás tutti-frutti es vuestro color favorito nuevo. Quién adivinaría aquello? Es un color, bien? Qué proporcionas como la respuesta acaece la respuesta “” correcta a aquella cuestión de seguridad.

Siempre que proporcionas respuestas creativas, ser seguro para escribir abajo tanto la cuestión y la respuesta y puesto les en un sitio seguro (o sencillamente utilizar una gerente de contraseña para almacenar vuestras cuestiones y respuestas). Puede haber una ocasión más tardía cuándo necesitas hablar a apoyo técnico, y un representante te podría pedir uno de las cuestiones de seguridad. Tiene un binder manejable o mantener una carta en vuestra cartera (o memorize y coherentemente utilizar el mismo conjunto de respuestas) para ayudar recuerdas que “En un hospital” es la respuesta correcta a la cuestión “Dónde

fuiste nata?” Este sencillo obfuscation thwart alguien quién más tarde hizo su búsqueda de Internet encima te y probó una respuesta más razonable, como “Colón, Ohio.”

Hay riesgos de intimididad adicional en contestar seguridad muy concreta cuestiones honestamente: estás dando fuera información más personal que es ya allí. Por ejemplo, la respuesta sincera a Qué “estado era vuestro hermano-en-la ley nata en?” Entonces puede ser vendido por el sitio diste que respuesta a y quizás combinado con otra información o utilizado para llenar en información desaparecida. Por ejemplo, del hermano-en-la ley contesta uno puede inferir que eres o nosotrosre casados y que vuestro socio, o vuestro ex, tiene un sibling quién es tampoco un hombre o casado a un hombre nato en el estado proporcionaste. Aquello es información adicional muchísima de una respuesta sencilla. Por otro lado, si te don't tener un hermano-en-ley, va adelante y contestar la cuestión creativamente, quizás por contestar “Puerto Rico.” Aquello tendría que confundir cualquiera intentando construir un perfil encima te. Los arenques más rojos proporcionas, el más acaeces invisible on-line.

Cuándo contestando estos relativamente uncommon questions, siempre considerar qué valioso el sitio es a ti. Por ejemplo, podrías confiar en vuestro banco para tener esta información personal adicional pero no vuestro streaming servicio de vídeo. También considerar lo que el sitio's la política de privacidad podría ser: busca lengua que dice o sugiere que podría vender la información recoge a terceras fiestas.

La reinicialización de contraseña para Sarah Palin Yahoo cuenta de email requirió su cita de nacimiento, código de cremallera, y la respuesta a la cuestión de seguridad “¿Dónde cumplen vuestro marido?” La cita de nacimiento de Palin y código de cremallera fácilmente podría ser encontrado on-line (en el tiempo, Palin era el gobernador de Alaska). La cuestión de seguridad tomó un poco más de obra, pero también, era accesible a Kernell. Palin dio muchas entrevistas en qué declaró repetidamente que su marido era su instituto sweetheart. Aquello, resulta, era la respuesta correcta a su cuestión de seguridad: “Instituto.”

Por adivinar la respuesta a Palin's cuestión de seguridad, Kernell era capaz de reinicializar su Yahoo contraseña de Correo a un que controló. Esto le dejó para ver todo su personal Yahoo emails. Un screenshot de su bandeja de entrada era posted en un hacker sitio web. Palin ella estuvo cerrado out de su email hasta que ella reinicializó la contraseña.<sup>15</sup>

Qué Kernell era ilegal, una vulneración del Fraude de Ordenador y Ley de Abuso. Específicamente, estuvo encontrado culpable encima dos cuentas: anticipatory obstrucción de justicia por destrucción de récords, un felony, y obteniendo acceso no autorizado

a un ordenador, un misdemeanor. Estuvo sentenciado en 2010 a un año y un día en plus de prisión tres años de emisión supervisada.<sup>16</sup>

Si vuestra cuenta de email ha sido tomada encima, como Palin es era, primero necesitarás cambiar vuestro password utilizando (sí, adivinaste él) la opción de reinicialización de la contraseña. Marca esta contraseña nueva una contraseña más fuerte, como sugerí encima. Segundo, control la caja Enviada para ver exactamente qué estuvo enviado vuestro nombre. Podrías ver un spam mensaje que estuvo enviado a múltiples parties, incluso vuestra lista de contactos entera. Ahora sabes por qué vuestros amigos han sido enviándote spam para todos estos años—alguien cortó sus cuentas de email.

También comprobar para ver si cualquiera se ha añadido a vuestra cuenta. Más temprano hablamos aproximadamente correo forwarding respecto a cuentas de email múltiple. Bien, un atacante quién obtiene acceso a vuestro servicio de email también podría tener todo vuestro email envió a su cuenta. Todavía verías vuestro email normalmente, pero el atacante lo vería también. Si alguien se ha añadido a vuestra cuenta, eliminar este email de enviar alocución inmediatamente.

Las contraseñas y Los Alfileres son parte de la solución de seguridad, pero nosotros've sólo vistos que estos pueden ser adivinados. Incluso mejor que las contraseñas complejas son autenticación de dos factores methods. De

hecho, en respuesta a Jennifer Lawrence y otras celebridades habiendo sus fotos desnudas escayolaron sobre el Internet, Manzana instituyó autenticación de dos factores, o 2FA, para su iCloud servicios.

Qué es 2FA?

Cuándo intentando para autenticar un usuario, sites o las aplicaciones buscan al menos dos de tres cosas. Típicamente estos son algo tienes, algo sabes, y algo eres. Algo tienes puede ser una raya magnética o chip-embedded crédito o carta de débito. Algo sabes es a menudo un ALFILER o una respuesta a una cuestión de seguridad. Y algo eres abarca biometría — fingerprint barrido, reconocimiento facial, reconocimiento de voz, y tan encima. El más de estos tienes, el más seguro te puede ser que el usuario es quién dice que es.

Si estos sonidos como tecnología nueva, no es. Para más de cuarenta años la mayoría de nosotros ha sido actuando 2FA sin prpers prpers darse.

Siempre que utilizas un ATM, actúas 2FA. Cómo es que posible? Tienes un banco-carta emitida (aquello es algo tienes) y un ALFILER (aquello es algo sabes). Cuándo les pusiste junto, el unmanned ATM fuera en la calle sabe que quieres acceso a la cuenta identificada en la carta. En algunos países, hay medio adicional de autenticación en ATMs, como reconocimiento facial y una huella de palma. Esto se apellida multifactor autenticación (MFA).

Algo similar es posible on-line. Muchos financieros y salud-instituciones de cuidado, así como email comercial y cuentas de medios de comunicación sociales, dejarte para escoger 2FA. En este caso, el something sabes es vuestra contraseña, y el algo tienes es vuestro teléfono celular. Utilizando el teléfono para acceder estos sitios está considerado “fuera de banda” porque el teléfono no es conectado al ordenador estás utilizando. Pero si tienes 2FA habilitado, un atacante no tendría que ser capaz de acceder vuestro 2FA- protegió cuentas sin habiendo vuestro aparato móvil a mano.

Dice utilizas Gmail. Para habilitar 2FA te será pedido a entrada vuestra celda- número de teléfono en el Gmail sitio. Para verificar vuestra identidad, Google entonces enviará un código de SMS de seis dígitos a vuestro teléfono. Por posteriormente inputting que código en el Gmail sitio, has sólo verificó que este ordenador y que celda-número de teléfono está conectado.

Después de que aquello, si alguien intenta cambiar la contraseña en vuestra cuenta de un nuevo computar o aparato, un mensaje de texto será enviado a vuestro teléfono. Sólo cuándo el código de verificación correcto está



introducido en el sitio web cualesquiera cambian a vuestra cuenta ser salvado.

hay un wrinkle a aquello, aun así. Según investigadores en Symantec, si envías un SMS para confirmar vuestra identidad, alguien quién pasa para saber vuestra celda-número de teléfono puede hacer un poco de ingeniería social y robar vuestro 2FA- código de reinicialización de contraseña protegido si no estás pagando atención cercana.<sup>17</sup>

Dice quiero tomar sobre vuestra cuenta de email y no sabe vuestra contraseña. Sé vuestra celda-número de teléfono porque tú're fácil de encontrar a través de Google. Puedo ir a la página de reinicialización para vuestro servicio de email y pedir una reinicialización de contraseña, el cual, porque habilitaste autenticación de dos factores, resultará en un código de SMS que es enviado a vuestro teléfono. Tan lejos, tan bien, bien? Cuelga encima.

Un ataque reciente en un teléfono utilizado por activista político DeRay Mckesson asomado cómo los tipos malos podrían burlar vuestro operador móvil para hacer un SIM intercambio.<sup>18</sup> En otras palabras,, el atacante podría hijack vuestro servicio celular y entonces recibir vuestros mensajes de SMS—por ejemplo, el código de SMS de Google a reinicialización Mckesson's Gmail cuenta que estuvo protegido con autenticación de dos factores. Esto es mucho más probablemente que fooling alguien a leer de su o su mensaje de SMS con una contraseña nueva. A pesar de que aquello es todavía posible, e implica ingeniería social.

Porque no veré el código de verificación enviado por vuestro proveedor de email a vuestro teléfono, I'll necesidad de fingir para ser alguien más para coger él de ti. Segundos justos antes de que recibes el SMS real de, dice, Google, I como el atacante puede enviar un SMS de un tiempos, uno aquello dice: “Google ha detectado actividad inusual en vuestra cuenta. Complacer responder con el código envió a vuestro aparato móvil para parar actividad no autorizada.”

Verás que sí, de hecho, sólo cogías un texto de SMS de Google que contiene un código de verificación legítimo, y tan puedes, si no estás siendo prudente, sencillamente responder a mí en un mensaje e incluir el código. Entonces tendría menos de sesenta segundos para introducir el código de verificación. Ahora tengo qué I necesidad para introducir en la página de reinicialización de la contraseña y, después de cambiar vuestra contraseña, toma sobre vuestro e-maqueja cuenta. O cualquiera otra cuenta.



Desde entonces códigos de SMS no son encriptados y puede ser obtenido en la manera I sólo descrito, un aún más asegurar 2FA el método es para descargar el Google Authenticator aplicación de Juego de Google o la tienda de aplicación del iTunes para uso con un iPhone. Esta aplicación generará un código de acceso único en la aplicación él cada vez quieres visitar un sitio que requiere 2FA—tan hay ningún SMS para ser enviado. Esta aplicación-generó código de seis dígitos es synced con el sitio's mecanismo de autenticación utilizó para conceder acceso al sitio. Aun así, Google Authenticator tiendas vuestra contraseña de un tiempos semilla en la Manzana Keychain con un encuadre para “Este Aparato Sólo.” Aquello significa si tú atrás arriba de vuestro iPhone y restaurar a un *aparato* diferente porque eres upgrading o reemplazando un teléfono perdido, vuestro Google Authenticator los códigos no serán transferidos y es un enorme hassle a reinicialización les. Él's siempre una idea buena de imprimir fuera de los códigos de emergencia en caso acabas cambiar aparatos físicos. A Otras aplicaciones les gusta 1 Contraseña te dejas para recular arriba y restaurar vuestra contraseña de un tiempos siembra tan no tienes este problema.

Una vez te ha registrado un aparato, mientras continúas a registro en al sitio de aquel aparato, serás apuntado para un código de acceso nuevo a no ser que específicamente compruebas la caja (si available) para confiar en el ordenador para treinta días, incluso si tomas vuestro portátil o teléfono a otra ubicación. Aun así, si utilizas otro aparato—dice, tomas prestado el ordenador de vuestro cónyuge—entonces serás autenticación adicional pedida. Needless Para decir, si estás utilizando 2FA, siempre tener vuestro teléfono celular manejable.

Dado todas estas precauciones, te podrías preguntar qué consejo doy a personas quiénes están dirigiendo cualquier tipo de la transacción financiera on-line.

Para aproximadamente \$100 un año puedes coger antivirus y firewall protección para hasta

tres ordenadores bajo vuestro control. El problema es que cuándo tú're surfing la Web, podrías cargar a vuestro navegador un anuncio de pancarta que contiene malware. O quizás abres vuestro email, y uno de los emails contiene malware. Una manera u otro you va a coger vuestro ordenador infectado si asiduamente toca el Internet, y vuestro antivirus el producto no puede coger todo aquello es allí.

Así que recomiendo que pasas alrededor \$200 para te coger un Chromebook. Me gusta iPads, pero son caros. El Chromebook es tan cercano a un fácil-a-pastilla de uso como un iPad es, y cuesta mucho menos.

Mi punto es que necesitas tener un aparato secundario que utilizas exclusivamente para material financiero—quizás incluso material médico también. Ninguna aplicación puede ser instalada a no ser que tú primero registro con un Gmail cuenta—esto te limitará a abrir el navegador a surf el Internet.

Entonces, si no has hecho ya tan, activa 2FA en el sitio de modo que reconoce el Chromebook. Una vez tú've completado vuestro bancario o salud- negocio de cuidado, puesto el Chromebook fuera hasta el tiempo próximo tienes que equilibrar vuestro talonario de cheques o arreglar la cita de un doctor.

Esto parece como un hassle. Es. Reemplaza la comodidad de en cualquier momento amontonando con casi en cualquier momento amontonando. Pero el resultado es que eres lejos menos probable de tener alguien messing alrededor con vuestro bancario e información de crédito. Si utilizas el Chromebook sólo para el dos o tres aplicaciones instalas, y si te marcador el bancario o salud-sitios web de cuidado y visitar ningún otros, es muy improbable que tendrás un Troyano o algunos otra forma de malware residiendo en vuestra máquina.

Así que hemos establecido que necesitas crear contraseñas fuertes y no compartirles. Necesitas girar encima 2FA siempre que posible. En el próximo pocos capítulos miraremos en cómo día común-a-interacciones de día pueden dejar digitales fingerprints en todas partes y qué puedes hacer para proteger vuestra intimidad.

## CAPÍTULO DOS

### Quién Más está Leyendo Vuestro Email?

Si eres me gusto, uno de las primeras cosas por la mañana es control vuestro email. Y, si eres me gusto, también te preguntas quién más ha leído vuestro email. Aquello no es un paranoid preocupación. Si utilizas una Web-servicio de email basado como Gmail o Perspectiva 365, la respuesta es clase de obvio y asustando.

Incluso si eliminas un email el momento lo leíste encima vuestro ordenador o teléfono celular, aquello no necesariamente borra el contenido. Allí quieto una copia de él a algún lugar. Correo de web es nube -basado, tan para ser

capaz de acceder él de cualquier aparato anywhere, en cualquier tiempo, tiene que haber copias redundandas. Si utilizas Gmail, por ejemplo, una copia de cada email enviado y recibido a través de vuestro Gmail la cuenta está retenida en varios servidores en todo el mundo en Google. Este es también cierto si utilizas sistemas de email proporcionados por Yahoo, Manzana, AT&T, Comcast, Microsoft, o incluso vuestro workplace. Cualesquier emails envías también puede ser inspeccionado, en cualquier tiempo, por el hosting empresa. Presuntamente esto es para filtrar fuera de malware, pero la realidad es tsombrero tercera lata de fiestas y accede nuestros emails para otro, más siniestros y self-sirviendo, razones.

En principio, la mayoría de nosotros nunca estand para cualquiera excepto el pretendido recipient leyendo nuestro correo. Hay leyes protegiendo el correo imprimido entregó through los EE.UU. Servicio Postal, y las leyes que protegen contenido almacenado como e- correo. Todavía en práctica, normalmente sabemos y probablemente aceptar que hay un seguro

Comercio-fuera implicado en la facilidad de email de comunicación proporciona. Sabemos que Yahoo (entre otros) ofrece una Web libre-servicio de correo, y sabemos que Yahoo marcas la mayoría de su dinero de publicitario. Quizás nosotros've no dados cuenta exactamente cómo el dos podría ser conectado y cómo aquello podría afectar nuestra intimidad.

Un día, Stuart Diamond, un residente de California Del norte, . se dio cuenta que los anuncios vio en el superior-esquina derecha de su Yahoo cliente de Correo no fue aleatorio; estuvieron basados en los contenidos of los emails había sido enviando y recibiendo. Por ejemplo, si mencioné en un email un upcoming hablando viaje a Dubai, los anuncios podría ver en mi cuenta de email sugeriría aerolíneas, hoteles, y cosas para hacer mientras en los Emiratos árabes Unidos.

Esta práctica es normalmente cuidadosamente deletreado fuera en los plazos de servicio que la mayoría de nosotros apalabrados pero probablemente nunca leídos. Nadie quiere ver anuncios que tiene nada para hacer con nuestros intereses individuales, bien? Y mientras el e- viajes de correo entre Yahoo actitulares de cuenta, parece razonable que la empresa sería capaz de escanear los contenidos de aquellos emails para anuncios de objetivo a nosotros y quizás bloquear malware y spam, el cual es email indeseado .

Aun así, Diamante, junto con David Sutton, también de Del norte California, empezó para notar que los contenidos de emails enviaron a y recibidos de alocuciones *fuera de Yahoo* también influyó la selección de anuncio presentó

a ellos. Aquello sugirió que la empresa interceptaba y leyendo *todo* su e-correo, no sólo aquellos sent a y de sus servidores propios.

Basado en los patrones observaron, el dos archivó una clase-pleito de acción en 2012 contra Yahoo en behalf de su 275 millones de cuenta titulares, citando preocupaciones alrededor de qué es esencialmente equivalente a ilegal wiretapping por la empresa.

Hizo aquel fin el barrido? Núm.

En una clase-traje de acción, hay un periodo de descubrimiento y respuesta de ambas fiestas. En este caso que la fase inicial duró casi tres años. En junio de 2015, un juez en San Jose, California, gobernado que el men tuvo tierras suficientes para su clase-traje de acción para proceder y que personas quién enviado o recibido Yahoo Correo desde entonces octubre 2, 2011, cuándo los hombres archivaron su petición inicial, podría unir en el pleito bajo el Almacenó Ley de Comunicaciones. Además, una clase de no-Yahoo titulares de cuenta del Correo que viven en California también puede demandar bajo la invasión de aquel estado de Ley de Intimidación. Aquel caso es todavía pendiente.

En lo defender contra otro pleito que escanea email, esto uno archivó temprano en 2014, Google accidentally información publicada sobre su proceso

de barrido del email en un oído de corte, entonces deprisa intentado y fallado para tener aquella información redacted o sacó. El caso implicó la cuestión de precisamente qué estuvo escaneado o leído por Google. Según el plaintiffs en el caso, el cual incluido varias empresas de medios de comunicación grandes, incluyendo los dueños de EE.UU. *Hoy*, Google se dio cuenta en algún punto que por escanear sólo los contenidos de la bandeja de entrada, faltaron muchísimos potencialmente contenido útil. Este traje alegad aquel Google movió de escanear único archived email, el cual reside en el servidor de Google, a escanear todo Gmail todavía en transit, si estuvo enviado de un iPhone o un portátil mientras el usuario sentaba en Starbucks.

A veces empresas haber incluso tried a en secreto emails de escáner para sus propósitos propios. Uno caso bien sabido de este pasado en Microsoft, el cual padeció un enorme backlash cuándo reveló que había escaneado la bandeja de entrada de un Hotmail usuario quién estuvo sospechado de haber pirateado una copia del company software. A raíz de esta revelación, Microsoft lo ha dicho dejará aplicación de ley maneja tales investigaciones en el futuro.

Estas prácticas no son limitadas a vuestro email privado. Si envías email a través de vuestra red de obra, vuestra empresa IT el departamento también puede ser escaneando y archiving vuestras comunicaciones. Es hasta el LO personal o sus gerente si para dejar cualquier flagged pase de email a través de sus servidores y redes o implicar aplicación de ley. Esto incluye emails que contiene secretos de comercio o material cuestionable como pornografía. También incluye escanear email para malware. Si vuestro LO el personal está escaneando y archiving vuestros emails, te tendrían que acordar cada vez te el registro en qué su póliza es—a pesar de que la mayoría de empresas no.

While La mayoría de nosotros puede tolerar habiendo nuestros emails escanearon para malware, y quizás algunos de nosotros toleran escaneando para propósitos publicitarios, la idea de terceras fiestas que leen nuestra correspondencia y obrando en los contenidos concretos encontrados dentro de los emails concretos es hacerwnright perturbando. (Exceptúa, naturalmente, cuándo viene a pornografía de niño.<sup>1</sup>)

Así que siempre que escribes un email, ningún asunto cómo intrascendente, e incluso si eliminas él de vuestra bandeja de entrada, recuerda que allí's una casualidad excelente que una copia de aquellas palabras y las imágenes serán escaneadas y se mantendrá a base de—quizás no para siempre, pero para un bueno mucho tiempo mientras. (Un poco las empresas pueden tener pólizas de retención corta, pero él's seguro de asumir que la mayoría de empresas mantienen email para un tiempo largo.)

Ahora que sabes el gobierno y las empresas están leyendo vuestro e-correos, el menos puedes hacer es marca él mucho más duro para ellos para hacer tan.

La mayoría de web-uso de servicios de email basado encriptación cuándo el email es en transit. Aun así, cuando algunos servicios transmiten correo entre Agentes de Traslado del Correo (MTAs), they no puede ser utilizando encriptación, por ello vuestro mensaje es en el abierto. Por ejemplo, dentro del workplace un jefe puede tener acceso a la empresa e- sistema de correo. Para acaecer invisible te necesitará encriptar vuestros mensajes— que es, les cierra de modo que sólo el recipients puede unlock y leído les. Qué es encriptación? Es un código .

Una encriptación muy sencilla ejemplo—un Caesar cipher, dice—sustituye cada letra para otro un número seguro de puesto fuera en el alfabeto. Si aquel número es 2, por ejemplo, entonces utilizando un Caesar cipher, *un* acaece *c*,

$c$  acaece  $e$ ,  $z$  acaece  $b$ , y tan adelante. Utilizando este offset-por-dos esquema de encriptación, “Kevin Mitnick” acaece “Mgxkp Okvpkem.”<sup>2</sup>

La mayoría de sistemas de encriptación utilizaron hoy es, naturalmente, mucho más fuerte que cualquier básico Caesar cipher. Therefore Tendrían que ser mucho más duros de romper. Una cosa aquello's cierto aproximadamente todas las formas de encriptación es que requieren un tono, el cual está utilizado como contraseña para cerrar y abrir el mensaje encriptado. La encriptación simétrica significa que el mismo tono está utilizado ambos para cerrar y unlock el mensaje encriptado. Los tonos simétricos son duros de compartir, aun así, cuándo dos fiestas son desconocidas a cada cual otro o físicamente lejos aparte, como son en el Inter red.

La mayoría de encriptación de email de hecho utiliza qué está llamado asymmetrical encryption. Aquello significa genero dos tonos: un tono privado que estancias en mi aparato, el cual yo nunca acción, y un tono público que I poste libremente en el Internet. Los dos tonos son diferentes todavía matemáticamente narró.

Por ejemplo: Bob quiere enviar Alice un email seguro. Encuentra Alice's tono público en el Internet o lo obtiene directamente de Alice, y cuándo enviando un mensaje a su encripta el mensaje con su tono. Este mensaje se quedará encriptado hasta que Alice—y Alice única—utiliza un passphrase a unlock su tono privado und unlock el mensaje encriptado.

Así que cómo encriptando los contenidos de vuestra obra de email?

El método más popular de encriptación de email es PGP, el cual está para “Intimididad Buena Bonita.” No es gratis. Es un producto del Symantec Empresa. Pero su creator, Phil Zimmermann, también authored una versión de fuente abierta, OpenPGP, el cual es libre. Y una tercera opción, GPG (GNU Guardia de Intimididad), creado por Werner Koch, es también libre. El bueno noticioso es que todo tres es interoperational. Aquello significa que ningún asunto qué versión de PGP utilizas, las funciones básicas son igual.

Cuándo Edward Snowden primero decidido para revelar el dato sensible él'd copiado del NSA, necesitó la asistencia de gustar-importó las personas esparcieron alrededor del mundo. Paradójicamente, necesitó marchar la verja mientras todavía quedando activo en el Internet. Necesitó acaecer invisible.

Incluso si no tienes secretos estatales para compartir, podrías ser interesado en mantener vuestros emails privados. Snowden's Experiencia y que de otros

ilustran que no es fácil de hacer que, pero es posible, con diligencia apropiada.

Snowden Utilizado su cuenta personal a través de una empresa llamó Lavabit para comunicar con otros. Pero e-el correo no es señalar-a-punto, significando que un email solo podría pegar varios servidores alrededor del mundiales antes de aterrizar en el pretendido recipient's bandeja de entrada. Snowden Supo que cualquier cosa escribió podría ser leído por cualquiera quién interceptó el email anywhere a lo largo de su viaje.

Así que tuvo que actuar una maniobra complicada para establecer un verdaderamente seguro, anónimo, y medio encriptado plenamente de la comunicación con intimidad defiende y filmmaker Laura Poitras, quién hubo recientemente acabó un documental sobre las vidas de pito-blowers. Snowden Quiso establecer un cambio encriptado con Poitras, excepto único unas cuantas personas supieron su tono público. No hizo su tono público muy público.

Para encontrar su tono público, Snowden tuvo que lograr fuera a una tercera fiesta, Micah Lee del Electrónica Fundación de Frontera, un grupo que intimidad de apoyos on-line. El tono público de Lee era disponible on-line y, según la cuenta publicada en el *Interceptar*, una publicación on-line, hubo Poitras's tono público, pero él primero necesitado para comprobar para ver si le permitiría para compartirlo. Ella .<sup>3</sup>

Al llegar a este punto ni Lee ni Poitras tuvo cualquier idea quién quiso su tono público; sólo supieron que alguien hizo. Snowden Había utilizado una cuenta diferente, no su cuenta de email personal, para lograr fuera. Pero si no utilizas PGP a menudo, puedes olvidar para incluir vuestro PGP tono en emails importantes de vez en cuando, y aquello es qué pasado a Snowden. Había olvidado para incluir su tono público propio así que Lee podría responder.

Sin manera segura para contactar esta persona de misterio, Lee quedó sin elección pero para enviar un sencillo-texto, unencrypted email atrás a Snowden pidiendo su tono público, el cual proporcionó.

Una vez más Lee, un confiado en tercera fiesta, tuvo que ser traído a la situación. Puedo decir tú de experiencia personal que es muy importante de verificar la identidad de la persona con quien te es habiendo una conversación segura, preferentemente a través de un amigo mutuo—y marca seguro estás comunicando

con aquel amigo y no alguien más disfrazado. Sé qué importante esto es porque he sido el posar antes de que, en una situación donde obró a mi ventaja que la otra fiesta no cuestionó mi identidad real o el tono público envié. Una vez quise comunicar con Neill Clift, un estudiante de posgrado en química orgánica en la Universidad de Leeds, en Inglaterra, quién era muy especializado en encontrar vulnerabilidades de seguridad en el Equipamiento Digital Corporation VMS sistema operativo. Quise Clift para enviarme todos los agujeros de seguridad que había informado al dic. Para aquel I le necesitó para creer que I de hecho obrado para Dic.

empecé por posar tan alguien nombró Dave Hutchins y enviando Clift un spoofed message de él. Anteriormente había llamado Clift fingiendo ser Derrell Piper de VMS ingeniería, así que yo (posando tan Hutchins) escribí en mi e- correo que Piper quiso intercambiar emails con Clift sobre un proyecto. En pasar por DEC's sistema de email, ya supe que Clift y la Piper real hubo anteriormente e-mailed cada cual otro, así que esta petición nueva no sonaría todo aquel extraño. Entonces envié un email spoofing la alocución de email real de Piper.

A más allá convencer Clift esto era todo en el arriba-y-arriba, incluso sugerí que utiliza PGP encriptación de modo que a alguien le gusta Kevin Mitnick wouldn't ser capaz de leer los emails. Pronto Clift y Piper “” intercambiaba tonos públicos y encriptando comunicaciones—de comunicaciones que I, como Piper, podría leer. Clift la equivocación era en no questioning la identidad de Piper él. De modo parecido, cuándo recibes un unsolicited llamada de teléfono de vuestro banco que pide vuestro número de Seguridad Social o información de cuenta, siempre tendrías que colgar y llamar el banco tú—nunca sabes quién es por otro lado de la llamada de teléfono o email.

Dado la importancia de los secretos estuvieron a punto de acción, Snowden y Poitras no podría utilizar sus alocuciones de email regulares. Por qué no? Sus cuentas de email personales contuvieron asociaciones únicas—como intereses concretos, listas de contactos—que podría identificar cada cual de ellos. En cambio Snowden y Poitras decidido para crear alocuciones de email nuevo.

El problema único era, cómo saben cada cual otro es alocuciones de email nuevo? En otras palabras,, si ambas fiestas eran totalmente anonymous, cómo saben quién era quién y quien podrían confiar en? Cómo podría Snowden, por ejemplo, regla fuera de la posibilidad que el NSA o alguien



más no posaba tan Poitras cuenta de email nuevo? Los tonos públicos son mucho tiempo, así que puedes't sólo elegir arriba de un teléfono seguro y leído fuera de los caracteres a la otra persona. Necesitas un cambio de email seguro.

Por enlisting Micah Lee una vez más, ambos Snowden y Poitras podría anclar su confianza en alguien cuando poniendo arriba de su email nuevo y anónimo cuentas. Poitras Primero compartió su tono público nuevo con Lee. Pero PGP tonos de encriptación ellos es bastante mucho tiempo (no bastante pi periodo, pero son largos), y, otra vez, qué si alguien miraba su cuenta de email también? Así que Lee no utilizó el tono real pero en cambio un cuarenta-character abreviatura (o un fingerprint) de Poitras tono público. Esto él posted a un Twitter de sitio—público.

A veces para acaecer invisible tienes que utilizar el visible.

Ahora Snowden podría anónimamente el tweet de vista Lee y comparar el acertado clave al mensaje recibió. Si el dos didn't partido, Snowden sabría no para confiar en el email. El mensaje podría haber sido compromised. O podría ser hablar en cambio al NSA.

En este caso, el dos emparejó.

Ahora muchos ordena sacados de quién eran on-line—y donde eran en el mundiales—Snowden y Poitras era casi a punto para empezar su comunicación de email anónima segura. Snowden Finalmente envió Poitras un email encriptado que identifica él sólo tan “Citizenfour.” Esta firma acaecía el título de su Premio de Academia—documental ganador sobre su campaña de derechos de la intimidad.

Aquello podría parecer como el fin—ahora podrían comunicar securely vía email encriptado—pero lo wasn't. Era sólo el comienzo.

En el despertar de los 2015 ataques terroristas en Paris, había discusión de varios gobiernos aproximadamente construyendo en puertas posteriores u otras maneras para aquellos en gobierno a decrypt email encriptado, texto, y mensajes de teléfono—aparentemente de terroristas extranjeros. Esto, naturalmente, derrota el propósito de encriptación. Pero los gobiernos de hecho no necesitan para ver el encriptó contenidos de vuestro email para saber quien te está comunicando con y qué a menudo, como veremos.

Como mencioné antes, el propósito de encriptación es para codificar vuestro mensaje de modo que sólo alguien con el tono correcto más tarde lo puede descodificar. Ambos la fuerza de la operación matemática y la periodo del

tono de encriptación determina qué fácil es para alguien sin una clave de agrietar vuestro código.

Algoritmos de encriptación en utilizar hoy es público. Quieres aquello.<sup>4</sup> Ser temeroso de algoritmos de encriptación que es propietario y no público. Los algoritmos públicos han sido vetted para la debilidad que—significa las personas han sido expresamente intentando romperlos. Siempre que uno de los algoritmos públicos parece débil o está

agrietado, está retirado, y algoritmos más nuevos, más fuertes están utilizados en cambio. Los algoritmos más viejos todavía existen, pero su uso es fuertemente desalentado.

Los tonos son (más o menos) bajo vuestro control, y tan, como podrías adivinar, su gestión es muy importante. Si tú generó un tono de encriptación, tú—y nadie más—tendréis la clave almacenado en vuestro aparato. Si dejaste una empresa actuar la encriptación, dice, en la nube, entonces que la empresa también podría mantener la clave después de que él o ella comparte él contigo. La preocupación real es que esta empresa también puede ser obligada por orden judicial para compartir el tono con aplicación de ley o una agencia de gobierno, con o sin un warrant. Necesitarás leer la política de privacidad para cada servicio que utilizas para encriptación y entender quién posee los tonos.

Cuando encriptas un mensaje—un email, texto, o fin de uso—de llamada de teléfono-a- encriptación de fin. Aquello significa vuestro mensaje se queda ilegible hasta que logra su pretendido destinatario. Con fin-a-encriptación de fin, sólo te y vuestro destinatario tener los tonos para descodificar el mensaje. No El transportista de telecomunicaciones, dueño de sitio web, o desarrollador de aplicación—las fiestas que aplicación de ley o el gobierno pedirán para girar encima información aproximadamente te. Cómo sabes si el servicio de encriptación que estás utilizando es fin-a-encriptación de fin? Hacer un Google busca “fin-a-llamada de voz de encriptación de fin.” Si la aplicación o el servicio no utiliza fin-a-encriptación de fin, entonces escoger otro.

Si todos estos sonidos complicaron, aquello es porque es. Pero hay PGP tapón- ins para el Chrome y Firefox navegadores de Internet de encriptación de marca del sombrero más fácil. Uno es Mailvelope, el cual pulcramente maneja la encriptación pública y privada tonos de PGP. Sencillamente tipo en un passphrase, el cual soler generar los tonos públicos y privados. Entonces siempre que escribes una Web-email basado, seleccionar un

recipient, y si el recipient tiene un público clave disponible, entonces tendrás la opción para enviar aquella persona un mensaje encriptado.<sup>5</sup>

Incluso si encriptas vuestros mensajes de email con PGP, un pequeños pero información- la parte rica de vuestro mensaje es todavía legible by sólo aproximadamente cualquiera. En lo defender del Snowden revelations, el gobierno de EE.UU. declaró repetidamente que lo doesn't captura los contenidos reales de nuestros emails, el cual en este caso sería ilegible con PGP encriptación. En cambio, el gobierno dijo que recoge sólo el email metadata.

Qué es email metadata? Es la información en el A y De campos así como las alocuciones de IP de los varios servidores que mango el email de origen a recipient. También incluye la línea subject, los cuales a veces pueden ser muy revelando tan al encriptó contenidos del mensaje. Metadata, un legado de los días tempranos del Internet, es todavía incluido en cada email enviado y recibido, pero lectores de email moderno esconden esta información de exposición.<sup>6</sup>

PGP, ningún asunto qué “sabor” utilizas, no encripta el metadata—el A y De campos, la línea subject, y el tiempo-información de sello. Estos restos en texto sencillo, si es visible a ti o no. Terceras fiestas todavía serán capaces de ver el metadata de vuestro mensaje encriptado; ellos'll sabe que en tal-y-tal cita enviaste un email a alguien, aquello dos días más tarde enviaste otro email a aquella persona misma, y tan encima.

Aquello podría sonar vale, desde las terceras fiestas no son de hecho leyendo el contenido, y tú probablemente don't cuidado sobre la mecánica de cómo aquellos emails viajaron—las varias alocuciones de servidor y los sellos de tiempo—pero tú serían sorprendidos por cuánto puede ser aprendido de la ruta de email y la frecuencia de emails sólo.

Atrás en el '90s, antes de que fui en el corrido del FBI, actué qué I llamó un metadata análisis en varios records de teléfono. Empecé este proceso por cortar a PacTel Celular, un proveedor celular en Los Ángeles, para obtener los records de detalle de la llamada (CDRs) de anyone quién llamó un informante quien el FBI utilizaba para obtener información sobre mis actividades.

CDRs Es mucho como el metadata I'm hablando aproximadamente aquí; asoman el tiempo una llamada de teléfono estuvo hecha, el número dialed, la periodo de la llamada, y el número de tiempo un número particular se apellidó—todo información muy útil.

Por buscar a través de las llamadas que era colocado a través de PacTel Celular al informante's landline, era capaz de obtener una lista de la celda-números de teléfono de las personas quién le llamó. A análisis de las visitas' enunciando records, era capaz de identificar aquellas visitas como miembros del FBI's equipo de delito de cuello blanco, operando fuera de la oficina de Los Ángeles. Efectivamente, algunos de los números cada individuales dialed era interno a la oficina de Los Ángeles del FBI, el abogado de EE.UU.'s oficina, y otras oficinas de gobierno. Algunos de aquellas llamadas eran bastante mucho tiempo. Y bastante frecuente.

Siempre que movieron el informante a una casa segura nueva, era capaz de obtener el landline número del seguro house porque los agentes lo llamarían después de probar para lograr el informante en su pager. Una vez tuve el landline número para el informante, era también capaz de obtener la alocución física a través de ingeniería social—que es, por fingir para ser alguien en Pacific Timbre, la empresa que proporcionó el servicio en la casa segura.

La ingeniería social es una técnica de cortar que manipulación de usos, engaño,

e influencia para coger un objetivo humano a comply con una petición. A menudo las personas están burladas a dar arriba de información sensible. En este caso, supe los números internos en la empresa de teléfono, y fingí ser un técnico de campo quién habló la terminología correcta y lingo, el cual era instrumental en obtener información sensible.

Tan mientras grabando el metadata en un email no es igual tan captando el contenido real, es empero intruso de una perspectiva de intimidad.

Si miras en el metadata de cualquier email reciente tú'll ver las alocuciones de IP de los servidores que pasó vuestro email alrededor del mundial antes de que logró su objetivo. Cada servidor—como cada persona quién accede el Internet— tiene una alocución de IP única, un valor numérico que está calculado utilizando el país donde estás localizado y quién vuestro proveedor de Internet es. Los bloques de alocuciones de IP están puestos aside para varios países, y cada proveedor tiene su propio sub-bloque, y esto es más allá subdivided por tipo de dial—de servicio-arriba, cable, o móvil. Si adquiriste una IP estática lo dirige será asociado con vuestra cuenta de suscriptor y domicilio particular, otherwise vuestra alocución de IP externa será generada de un grupo de alocuciones asignó a vuestro proveedor de servicio del Internet. Por ejemplo, un sender—alguien enviándote un email—

podría tener la alocución de IP 27.126.148.104, el cual está localizado en Victoria, Australia.

O podría ser 175.45.176.0, el cual es uno de Corea del Norte's alocuciones de IP. Si es el último, entonces vuestra cuenta de email podría ser flagged para reseña de gobierno. Alguien en el gobierno de EE.UU. podría querer saber por qué estás comunicando con alguien de Corea del Norte, incluso si la línea subject lee “Cumpleaños Feliz.”

Por él, todavía no podrías pensar la alocución de servidor es muy interesante. Pero la frecuencia de contacto te puede decir mucho. Además, si identificas cada elemento—el sender y el auricular y sus ubicaciones— puedes empezar para inferir qué es realmente yendo en. Por ejemplo, el metadata asociado con el teléfono llama —la duración, el tiempo de día están hechos, y tan encima—te puede decir mucho sobre una persona's salud mental. Un 10:00 p.m. llamar a un doméstico violence hotline duradero diez minutos o una llamada de medianoche de la Brooklyn Puente a una prevención de suicidio hotline duradero veinte minutos pueden ser muy revelando. Una aplicación desarrollada en Dartmouth patrones de partidos Universitarios de estrés, depresión, y loneliness en dato de usuario. Esta actividad de usuario también ha sido correlativa con notas estudiantiles.<sup>7</sup>

Quieto don't ver el peligro en habiendo vuestro email metadata expuesto? Un programa creado en MIT Inmersión llamada visually mapa las relaciones entre el senders y auriculares de unll el email has almacenado en vuestro e-cuenta de correo sólo por utilizar el metadata. La herramienta es una manera a visually cuantificar quién importa a ti más. El programa incluso incluye una escala de tiempo corredera, así que puedes ver cómo las personas sabes aumento y caída en importance a ti con el tiempo. A pesar de que podrías pensar que entiendes vuestras relaciones, viéndoles graphically representados puede ser un sobering experiencia. No te podrías dar cuenta qué a menudo te email alguien te don't realmente saber o qué poco te email alguien sabes muy bien. Con la herramienta de Inmersión puedes escoger si para cargar el dato, y también puedes eliminar la información una vez lo ha sido graphed.<sup>8</sup>

Según Snowden, nuestro email, texto, y telefonar metadata está siendo recogido por el NSA y otras agencias. Pero el gobierno puede't recoger metadata de todo el mundo—o puede él? Técnicamente, núm. Aun así, ha habido un aumento agudo en “colección” legal desde entonces 2001.

Autorizado bajo los EE.UU. Ley de Vigilancia de Inteligencia Extranjera de 1978 (FISA), los EE.UU. Extranjeros Entelligence Corte de Vigilancia (sabido como FISC, o el FISA Corte) oversees todas las peticiones para

vigilancia warrants contra personaje extranjeras dentro de los Estados Unidos. En la superficie parece razonable que una orden judicial estaría entre ley enforcement y una personaje. La realidad es un poco diferente. En 2012 sólo, 1,856 peticiones estuvieron presentadas, y 1,856 peticiones estuvieron aprobadas, sugiriendo que el proceso hoy es en gran parte una goma-operación de aprobación del sello para el gobierno de EE.UU..<sup>9</sup> Después del FISA Court becas una petición, aplicación de ley puede obligar empresas privadas para girar encima todo su dato encima tú—aquello es, si no han hecho ya tan.

Para acaecer verdaderamente invisible en el mundo digital necesitarás hacer más de encriptar vuestros mensajes. Necesitarás a:

**Sacar vuestra alocución de IP cierta:** Esto es vuestro punto de conexión al Internet, vuestro fingerprint. Puede asomar donde eres (abajo a vuestra alocución física) y qué proveedor utilizas.

**Oscuro vuestro hardware y software:** Cuando conectas a un sitio web on-line, un snapshot del hardware y software tú're utilizando puede ser recogido por el sitio. hay burla que puede soler descubrir si tienes el software particular instalado, como Adobe Centellea. El software de navegador dice un sitio web qué sistema operativo estás utilizando, qué versión de aquel sistema operativo tienes, y a veces lo que otro

software tienes correr en vuestro desktop en el tiempo. **Defender vuestro anonimato:** la atribución on-line es duro. Probando que eras en el teclado cuándo un caso ocurrió es difícil. Aun así, si andas delante de un cámara antes de ir on-line en Starbucks, o si sólo compraste un latte en Starbucks con vuestra carta de crédito, estas acciones pueden

ser enlazadas a vuestra presencia on-line unos cuantos momentos más tarde.

Como hemos aprendido, cada vez conectas al Internet, hay una alocución de IP asociado con aquella conexión.<sup>10</sup> Esto es problemático si estás intentando ser

invisible on-line: podrías cambiar vuestro nombre (o no darlo en absoluto), pero vuestra IP address todavía revelará donde eres en el mundo, qué proveedor utilizas, y la identidad de la persona que paga para el servicio de Internet (cuál puede o no puede ser tú). Todas estas piezas de información están incluidas dentro del email metadata y más tarde puede soler identificarte singularmente. Cualquier comunicación, si es email o no, puede soler identificarte basado en el Protocolo Interno (IP) dirige aquello

está asignado al router estás utilizando mientras eres en casa, obra, o el sitio de un amigo.

Alocuciones de IP en los emails naturalmente pueden ser forjados. Alguien podría utilizar un proxy alocución—no su o su alocución de IP real pero alguien más es—de modo que un e- el correo parece para originar de otra ubicación. Un proxy es como un traductor de lengua extranjera— hablas al traductor, y el traductor habla al altavoz de lengua extranjera—sólo los restos de mensaje exactamente igual. El punto aquí es que alguien podría utilizar un proxy de China o incluso Alemania para evadir detección en un email que realmente proviene Corea del Norte.

En vez de hosting vuestro propio proxy, puedes utilizar un servicio sabido como un anónimo remailer, el cual enmascarará vuestro email's alocución de IP para ti. Un anónimo remailer sencillamente cambia la alocución de email del sender antes de enviar el mensaje a su pretendido recipient. El recipient puede responder vía el remailer. Aquello es la versión más sencilla .

hay también variaciones. Algún tipo I y tipo II remailers no te deja para responder a emails; son sencillamente correspondencia de una maneras. Tipo III, o Mixminion, remailers hacer de ferun lleno suite de servicios: respondiendo, enviando, y encriptación. Necesitarás descubrir qué servicio vuestro remailer suministros si escoges este método de correspondencia anónima.

Una manera para enmascarar vuestra alocución de IP es para utilizar la cebolla router (Tor), el cual es lo que Snowden y Poitras hizo.

Desarrollado por los EE.UU. Laboratorio de Búsqueda Naval en 2004 como manera para personal militar para dirigir búsquedas sin exponer sus ubicaciones físicas, el Tor programa de fuente abierta desde entonces ha sido expandido. Tor Está diseñado para ser utilizado por las personas que viven en regímenes duros como manera de evitar censura de servicios y medios de comunicación populares y para impedir cualquiera de seguir qué plazos de búsqueda utilizan. Tor Los restos libres y puede ser utilizado por cualquiera, anywhere—incluso te.

Qué hace Tor obra? Él upends el modelo habitual para acceder un sitio web.

Normalmente cuándo vas on-line abres un navegador de Internet y tipo en el nombre del sitio quieres visita. Una petición sale a aquel sitio, y milisegundos más tarde una respuesta vuelve a vuestro navegador con la página de sitio web. El sitio web sabe—basado en la IP dirige—who el proveedor de servicio es, y a veces incluso dónde en el mundo estás localizado, basó encima dónde el proveedor de servicio está localizado o la

latencia del hops de vuestro aparato al sitio. Por ejemplo, si vuestro aparato dice que es en los Estados Unidos, pero el tiempo y número de hops vuestra petición toma para lograr su destino sugiere que eres a algún lugar más en el mundo, algunos sitios—gaming sitios, en particular—detectará que fraude tan posible.

Cuándo utilizas Tor, la línea directa entre ti y vuestro sitio web de objetivo está ocultado por nodos adicionales, y cada diez segundos la cadena de los nodos que te conectan a cualquier sitio estás mirando en cambios sin interrupción a ti. El various nodos que te conectas a un sitio es como capas dentro de una cebolla. En otras palabras,, si alguien era para retroceder del sitio web de destino e intentar encontrarte, ellos'd ser incapaces a porque la ruta sería constantemente cambiando. A no ser que vuestro punto de entrada y vuestro punto de salida acaecen asociados de alguna manera, vuestra conexión está considerada anónima.

Cuándo utilizas Tor, vuestra petición para abrir una página—dice, mitnicksecurity.com —no es enviado directamente a aquel servidor pero primero a otro Tor nodo. Y sólo para hacer las cosas aún más complicadas, aquel nodo entonces pasa la petición a otro nodo, el cual finalmente conecta a mitnicksecurity.com. Tan allí's un nodo de entrada, un nodo en el medio, y un nodo de salida. Si era para mirar en quién visitaba mi sitio de empresa, sólo vería la alocución de IP e información del nodo de salida, el último en la cadena, y no el primero, vuestro nodo de entrada. Puedes configurar Tor tan utiliza nodos de salida en un país particular, como España, o incluso un nodo de salida concreto, quizás en Honolulu.

Para utilizar Tor you necesitará el modificado Firefox navegador del Tor sitio (torproject.org). Siempre buscar legítimo Tor navegadores para vuestro sistema operativo

del Tor sitio web de proyecto. No utiliza un tercer-sitio de fiesta. Para sistemas operativos de Androide, Orbot es un legitimate libre Tor aplicación de Juego de Google que ambos encripta vuestro tráfico y oculta vuestra alocución de IP.<sup>11</sup> En iOS aparatos (iPad, iPhone), instalar el Navegador de Cebolla, una aplicación legítima de la tienda de aplicación del iTunes.

Podrías ser pensamiento , por qué no alguien sólo construye un servidor de email dentro de Tor? Alguien hizo. Tor El correo era un servicio hosted en un sitio accesible único a Tor navegadores. Aun así, el FBI cogió que servidor en un caso no relacionado y acceso obtenido por tanto a todo el email encriptado almacenado en Tor Correo. Esto es un cautionary el cuento



que asoma que incluso cuándo piensas que vuestra información es seguro, foolproof, probablemente no es.<sup>12</sup>

A pesar de que Tor usas una red especial, todavía puedes acceder el Internet de él, pero las páginas son mucho más lentos de cargar. Aun así, además de allowing te a surf el searchable Internet, Tor da accedes a un mundo de sitios que no es normalmente searchable—qué está llamado la Web Oscura. Estos son sitios que don't resuelve a nombres comunes como Google.com y en cambio fin con el .Prórroga de cebolla. Algunos de esta oferta de sitios escondida, vende, o proporcionar elementos y servicios que puede ser ilegal. Algunos de ellos son sitios legítimos mantuvo por personas en oppressed partes del mundo.

Tendría que ser notado, aun así, que hay varias debilidades con Tor: no tienes ningún control sobre los nodos de salida, los cuales pueden ser bajo el control de gobierno o aplicación de ley<sup>13</sup> Te todavía puede ser profiled y posiblemente identificó<sup>14</sup> Tor es muy lento

Que siendo dicho, si todavía decides utilizar Tor te tener que no corrido él en el same aparato físico que te uso para explorar. En otras palabras,, tiene un portátil para explorar la Web y un aparato separado para Tor (para caso, una Frambuesa Pi el miniordenador que corre Tor software). La idea aquí es que si alguien es capaz a compromise vuestro laptop todavía no serán capaces de pelar de vuestro Tor capa de transporte como está corriendo en una caja física separada.<sup>15</sup>

En el caso de Snowden y Poitras, como dije, sencillamente conectando a cada cual otro email encima encriptado wasn't bastante bueno. Después de Poitras creado un público nuevo

Tono para su cuenta de email anónima, lo podría haber enviado a Snowden's alocución de email anterior, pero si alguien miraba que cuenta, entonces su identidad nueva sería expuesta. Una regla muy básica es que tienes que mantener vuestras cuentas anónimas completely separados de cualquier cosa aquello podría narrar atrás a vuestra identidad cierta.

Para ser invisible te necesitará para empezar un limpio slate para cada contacto seguro nuevo haces. Cuentas de email del legado podrían ser conectadas en varias maneras a otras partes de vuestros amigos—de vida, hobbys, obra. Para comunicar en clandestinidad, necesitarás crear cuentas de email nuevo que utilizan Tor de modo que el encuadre de alocución de la IP

arriba de la cuenta no es asociada con vuestra identidad real en cualquier manera.

Creando alocuciones de email anónimo está desafiando pero posibles.

Hay servicios de email privado puedes utilizar. Desde entonces dejarás una estela si pagas para aquellos servicios, tú're de hecho mejor fuera utilizando un Servicio web libre. Un menor hassle: Gmail, Microsoft, Yahoo, y otros te requerís para suministrar un número de teléfono para verificar vuestro identificar. Evidentemente puedes't uso vuestra celda real- número de teléfono, desde entonces puede ser conectado a vuestro nombre real y alocución real. Podrías ser capaz de poner arriba de un Skype número de teléfono si apoya autenticación de voz en vez de SMS authentication; aun así, todavía necesitarás un email de existir cuenta y un prepaid carta de regalo para poner arriba de un Skype número.<sup>16</sup> Si piensas utilizar un prepaid teléfono celular en y de él protegerá vuestro anonimato, eres mal. Si tú've nunca utilizó un prepaid teléfono para hacer las llamadas asociaron con vuestra identidad real, es niño juego para descubrir quién eres.

En cambio tú'll quiere utilizar un disposable teléfono. Algunas personas piensan de teléfonos de quemador como aparatos utilizaron sólo por terroristas, pimps, y traficante de droga, pero hay plenty de perfectamente usos legítimos para ellos. Por ejemplo, un reportero empresarial, después de que habiendo su basura pasada por por los detectives privados contrataron por Hewlett-Packard, quién era ansioso de descubrir quién podría ser filtrar junta crítica -de-información de directores, switched encima a teléfonos de quemador de modo que los detectives privados tendrían un tiempo más duro que identifica sus llamadas. Después de aquella experiencia sólo habló a su fuente en aquel teléfono de quemador.<sup>17</sup>

De modo parecido, una mujer quién está evitando un abusivo ex podría obtener una poca paz de mente por utilizar un teléfono que doesn't requerir un contrato o, para aquel asunto, un Google o una cuenta de Manzana. Un teléfono de quemador típicamente tiene pocos o Internet muy limitado capacidades. Teléfonos de quemador mayoritariamente proporcionan voz, texto, y servicio de email, y aquello's aproximadamente todo alguna necesidad de personas. Tú, aun así, también tendría que coger dato porque puedes tether este teléfono de quemador a vuestro portátil y utilizarlo a surf el Internet. ([Aquí](#) te dices cómo para cambiar el control de acceso de los medios de comunicación—MAC— alocución en vuestro portátil de modo que cada time te tether con un teléfono de quemador aparece para ser aparato nuevo.)

Aun así, adquiriendo un teléfono de quemador anónimamente será delicado. Las acciones tomadas en el mundo real puede soler identificar tú en el mundo virtual. Seguro, podría andar a Walmart y pagar en metálico for un teléfono de quemador y cien minutos de airtime. Quién sabría? Bien, muchas personas .

Primero, cómo cojo a Walmart? Tomo un Uber coche? Tomo un taxi? Estos récords pueden todo ser subpoenaed.

Podría conducir mi coche propio, pero ley enforcement usos reconocimiento de plato de licencia automático tecnología (ALPR) en parcelas de aparcamiento públicas grandes para buscar vehículos desaparecidos y robados así como personas encima quien hay excepcionales warrants. El ALPR los récords pueden ser subpoenaed.

Incluso si anduve a Walmart, encimace introduje la tienda mi cara sería visible en varios cámaras de seguridad dentro de la tienda él, y que el vídeo puede ser subpoenaed.

Vale, así que dejado es dice envío alguien más a la tienda—alguien no sé, quizás un homeless persona contraté en la algo. TPaseos de persona del sombrero en y compra el teléfono y varias cartas de recambio del dato con dinero efectivo. Aquello sería la aproximación más segura . Quizás arreglas para cumplir esta persona más tarde fuera de la tienda. Esto ayudaría físicamente distancia tú de las ventas reales tramitanión. En este caso el enlace más débil todavía podría ser la persona enviaste—qué fidedigno es? Si le pagas más del valor del teléfono, probablemente será feliz de entregar el teléfono como prometió.

Activación del prepaid el teléfono requiere tampoco llamando el operador móvil's departamento de servicio del cliente o activándolo encima el sitio web del proveedor. Para evitar siendo grabado para “garantía de calidad,” es más seguro de activar sobre la Web. Utilizando Tor sobre una red inalámbrica abierta después de que tú've cambiado vuestro MAC la alocución tendría que ser el mínimo safeguards. Tendrías que hacer arriba toda la información de suscriptor introduces en el sitio web. Para vuestra dirección, Google justo la alocución de un hotel importante y utilizar aquello. Marca arriba de una cita de nacimiento y ALFILER que te'll recordar en caso necesitas contactar servicio de cliente en el futuro.

Hay servicios de email que no requiere verificación, y si te don't necesidad de preocuparse sobre potestades, Skype los números obran bien para inscripción de cuenta del Google y material similar, pero por el bien de

ilustración, dejado es dice que después de utilizar Tor a randomize vuestra alocución de IP, y después de crear un Gmail cuenta

que tiene nada para hacer con vuestro número de teléfono real, Google envía vuestro teléfono un código de verificación o una llamada de voz. Ahora tienes un Gmail cuenta que es virtualmente untraceable.

Así que tenemos una alocución de email anónima estableció utilizar servicios familiares y comunes. Podemos producir razonablemente emails seguros cuya alocución de IP —gracias a Tor—es anónimo (a pesar de que te don't tiene control sobre los nodos de salida) y cuyos contenidos, gracias a PGP, no puede ser leído exceptúa por el pretendido recipient.

Nota que para mantener esta cuenta anónima te sólo puede acceder la cuenta de dentro de Tor de modo que vuestra alocución de IP nunca será asociada con él. Más allá, nunca tendrías que actuar cualesquier búsquedas de Internet mientras logged en a aquel anónimos Gmail cuenta; puedes inadvertently buscar algo aquello está narrado a vuestro cierto identidad. Incluso buscando información de tiempo podría revelar vuestra ubicación.<sup>18</sup>

Como puedes ver, acaeciendo invisible y manteniendo tú invisible requiere disciplina enorme y diligencia perpetua. Pero merece la pena para ser invisible.

El más important takeaways es: primero, ser consciente de todas las maneras que alguien te puede identificar incluso si emprendes algunos pero no todo de las precauciones I've describió. Y si emprendes todas estas precauciones, sabe que necesitas actuar diligencia prevista cada vez utilizas vuestras cuentas anónimas. Ninguna excepción.

Es también valor reiterando que fin-a-encryptación de fin que—mantiene vuestro mensaje ilegible y seguro hasta que logra el recipient como opposed a sencillamente encryptando —es muy importante. Fin-a-encryptación de fin puede ser utilizada para otros propósitos, como llamadas de teléfono encryptado e instante messaging, el cual nosotros'll hablar en el próximo dos capítulos.

## CAPÍTULO TRES

### Wiretapping 101

pasas horas incontables en vuestro teléfono celular todos los días, charlando, texting, surfing el Internet. Pero de hecho sabes cómo vuestras obras de teléfono celular?

Servicio celular, el cual utilizamos en nuestros aparatos móviles, es cablemenos y confía a torres celulares, o canal de base. Para mantener conectividad, los teléfonos celulares continuamente envían fuera de almenaras minúsculas a la torre o las torres físicamente más cercanas a ellos. La respuesta de señal a aquellas almenaras de las torres traduce al number de barras “” no tienes ninguna barra, ninguna señal.

Para proteger la identidad del usuario un poco, estas almenaras de vuestro teléfono celular utilizan qué está sabido como identidad de suscriptor móvil internacional, o IMSI, un número único asignó a vuestro SIM carta. Esto era originally del tiempo cuándo las redes celulares necesitaron saber cuándo eras en sus torres y cuándo vagabas (utilizando otros transportistas' torres de celda). La primera parte del IMSI el código singularmente identifica el operador de red móvil, y la parte restante identifica vuestro teléfono celular a aquel operador de red.

Aplicación de ley tiene creó aparatos que finge ser canal de base celular. Estos están diseñados para interceptar voz y mensajes de texto. En los Estados Unidos, aplicación de ley y agencias de inteligencia también utilizan otros aparatos para coger IMSIs (ve [aquí](#)). El IMSI está captado instantáneamente, en menos de un segundo, y sin advertir. Típicamente IMSI catchers está utilizado en rallys grandes, dejando aplicación de ley a más tarde identificar quién era en attendance, particularmente si aquellos

Las personaje activamente llamaban otros para unir en. A Aparatos les gustan estos también puede ser utilizado por commuting servicios y aplicaciones para crear informes de tráfico. Aquí el número de cuenta real, o IMSI, no importa, sólo qué rápidamente vuestros movimientos de teléfono celular de torre a torre o geographic región a región geográfica. La cantidad de cronometra toma un teléfono celular para venir e ir de cada torre determina el estado de tráfico: rojo, amarillo, o verde.<sup>1</sup>

Vuestro aparato móvil conecta a una serie de torres celulares siempre que es powered arriba. La torre más cercana de hecho maneja vuestra llamada, texto, o sesión de Internet. Como mueves alrededor, vuestro teléfono pings la torre más cercana y, si es necesario, vuestros movimientos de llamada de torre a torre, todo el mientras manteniendo consistencia. Las otras torres cercanas son todos en standby, de modo que si mueves de señalar Un para señalar B y otra torre viene a gama para una señal mejor, entonces el handoff es liso y no tendrías que experimentar una llamada caída.

Lo basta para decir que vuestro aparato móvil emite una secuencia única que es logged en un número de torres celulares individuales. Así que cualquiera mirando en los registros de una torre concreta verían la identidad de suscriptor móvil provisional (TMSI) de todas las personas en el área general en cualquier momento dado, si hicieron llamadas o no. Lata de aplicación de la ley y pide esta información de transportistas celulares, incluyendo el atrás-identidades de cuenta del fin de titulares concretos.

Normalmente, si miras en justo el registro de una torre de celda, el dato sólo podría asomar que alguien pasaba a través de y que suyo o su aparato contactó una torre de celda concreta como standby. Si una llamada estuvo hecha o si el dato estuvo intercambiado, también habría un récord de aquella llamada y su duración.

Dato de celda múltiple-registros de torre, aun así, puede soler geográficamente pinpoint un usuario. La mayoría de aparatos móviles ping tres o más torres a la vez. Utilizando registros de aquellas torres de celda, alguien puede triangulate, basado en la fuerza relativa de cada ping, una ubicación bastante exacta del usuario del teléfono. Así que el teléfono llevas alrededor todos los días es esencialmente un aparato de seguir.

Cómo puede evitas ser siguió?

Firmando un contrato con una celda-transportista de teléfono requiere un nombre, alocución, y un número de Seguridad Social. Además, allí's un control de crédito para hacer seguro puedes pagar vuestra factura mensual. No puedes evitar esto si vas con un transportista comercial.

Un teléfono de quemador parece como una opción razonable. Un prepaid teléfono celular, quizás uno que reemplazas frecuentemente (dice, semanal o incluso mensual), evita dejar mucho de una estela. Vuestro TMSI aparecerá encima registros de torre de la celda, entonces

desaparecer. Si adquiriste el teléfono discreetly, lo ganado't ser localizable atrás a una cuenta de suscriptor. Prepaid Servicios de celda son cuentas de suscriptor quieto, así que el IMSI siempre será asignado a una cuenta. Por tanto, el anonimato de una persona depende encima cómo él o ella adquirieron el aparato de quemador.

Por el bien de riña, dejado es asumirte ha exitosamente disconnected tú de la compra de un teléfono de quemador. Seguiste los pasos perfilaron [aquí](#) y utilizó una persona no relacionada a ti para adquirir el teléfono para dinero efectivo. Es el uso de aquel disposable teléfono untraceable? La respuesta corta es núm.

Aquí es un cautionary cuento: una tarde en 2007, un \$500 millones de envase loaded con el éxtasis de droga fue perder de un puerto en Melbourne, Australia. El dueño del envase, Pat Barbaro, una traficante de droga sabida, logrado a su bolsillo, estiró fuera uno de sus doce teléfonos celulares, y dialed el número de un reportero local, Nick McKenzie, quién sólo sabría la visita por el nombre Stan. Barbaro Más tarde utilizaría sus otros teléfonos de quemador a texto McKenzie, intentando a anónimamente obtener información del investigative reportero sobre el envase desaparecido. Como veremos, este didn't obra.

Teléfonos de quemador, a pesar de qué muchas personas pueden pensar, no es verdaderamente anónimo. Bajo la Asistencia de Comunicaciones de los EE.UU. para Ley de Aplicación de la Ley (CALEA), todo IMSIs conectado con teléfonos de quemador están informados, tan aquellos suscriptores bajo contrato con major los transportistas son. En otras palabras,, un oficial de aplicación de la ley puede algo un teléfono de quemador de un registro archiva tan fácilmente como puede algo un teléfono de contrato registrado. Mientras el IMSI no identificará quién posee el teléfono, los patrones de uso pueden.

En Australia, donde CALEA no existe, aplicación de ley era todavía capaz de mantener tabuladores en Barbaro's muchos telefona utilizar métodos bastante tradicionales. Para caso, podrían haber notado una llamada hecha con su teléfono personal y entonces unos cuantos segundos más tarde vistos en el registro archiva another llamada o texto de uno de sus teléfonos de quemador en el mismo sitio de celda. Con el tiempo, el hecho que estos IMSIs más a menudo que no parecidos juntos en los mismos sitios de celda podrían sugerir que pertenecieron a una personaje sola.

El problema con Barbaro having muchos teléfonos celulares en su disposición era que ningún asunto qué teléfono utilizó, personal o quemador, siempre y cuando se quedó en la misma algo, la señal pegaría la misma torre celular. El quemador-llamadas de teléfono siempre parecidas luego a sus llamadas de teléfono registrado. El teléfono registrado, listado en su nombre con un transportista, era enteramente ley localizable y ayudada la aplicación le identifica. Estableció un caso sólido en contra le, particularmente porque este patrón estuvo repetido en otras ubicaciones. Esto ayudó australiano authorities condenado Barbaro de orchestrating uno del éxtasis más grande shipments en la historia de Australia.

Mckenzie concluyó, "Nunca desde el teléfono buzzed que día en mi bolsillo, y Stan' 'brevemente introdujo mi vida, I've sido especialmente consciente

aproximadamente cómo las comunicaciones de una persona dejan una estela, ningún asunto cómo prudente son.”<sup>2</sup>

Te podría, naturalmente, haber sólo un teléfono de quemador. Esto significaría que necesitarías adquirir minutos adicionales anónimamente utilizando prepaid cartas o Bitcoin de vez en cuando, el cual you puede hacer por utilizar un Wi-Fi abierto sin incidentes después de cambiar vuestro control de acceso de los medios de comunicación (MAC) alocución en vuestra carta inalámbrica (ve [aquí](#)), y siendo fuera de cualquier vista de cámara. O podrías, como sugerido en el capítulo anterior, alquilar un más extraño de pagar en metálico en la tienda para adquirir el prepaid teléfono y varias cartas de recambio.<sup>3</sup> Esto añade costado y quizás inconveniencia, pero tendrías un teléfono anónimo.

A pesar de que puede parecer marca tecnología nueva, celular es más de cuarenta años, y lo, como cobrizos-alambrar sistemas telefónicos, contiene tecnologías de legado que puede compromise vuestra intimidad.

Cada generación de celda-tecnología de teléfono ha ofrecido características nuevas, mayoritariamente pretendidos para mover más datos más efficiently. Primer-teléfonos de generación, o 1G, tuvo la tecnología telefónica disponible en el 1980s. Estos temprano 1redes de G y handsets era analógico-basado, y utilizaron una variedad de ahora niveles móviles interrumpidos. En 1991, el segundo-generación (2G) la red digital estuvo presentada. Esto 2red de G ofreció dos niveles: sistema global para comunicaciones móviles (GSM) y reparto de código acceso múltiple (CDMA). Él también servicio de mensaje corto presentado (SMS), unstructured supplementary dato de servicios (USSD), y otros protocolos de comunicaciones sencillos que sigue en uso hoy. Somos actualmente en medio de 4G/LTE y en el camino hacia 5G.

Ningún asunto qué generación de tecnología un transportista dado está utilizando (2G, 3G, 4G, o 4G/LTE), hay un protocolo de señal internacional subyacente sabido como el sistema de señalización. El protocolo de sistema de la señalización (actualmente en versión 7), entre otras cosas, mantiene las llamadas móviles conectadas cuándo conduces a lo largo de una autopista y cambio de torre de celda a torre de celda. También puede ser utilizado para vigilancia. Sistema de señalización 7 (SS7) básicamente todo necesario a ruta una llamada, como:

Encuadre arriba de una conexión nueva para una llamada que Desgarra abajo que conexión cuándo la llamada acaba Enunciar la fiesta apropiada que hace la llamada que Dirige características extras como que envían



llamada, llamando nombre de fiesta y exposición de número, tres-la manera que llama, y otra Red Inteligente (EN) Peaje de servicios-libre (800 y 888) así como peaje (900) llama

servicios Inalámbricos, incluyendo identificación de suscriptor, transportista, y móvil vagando

Hablando en el Congreso de Comunicación del Caos, un ordenador anual hacker la conferencia aguantada en Berlín, Alemania, Tobias Engel, fundador de Sternraute, y Karsten Nohl, científico de jefe para Laboratorios de Búsqueda de la Seguridad, explicaed que podrían no sólo localizar celda-visitas de teléfono anywhere en el mundo, también podrían escuchar en en sus conversaciones de teléfono. Y si no podrían escuchar en tiempo real, podrían grabar el encriptó llamadas y textos para más tardíos decryption.

En security, eres sólo tan seguro como el enlace más débil. Qué Engel y Nohl funda era que mientras los países desarrollados en América del Norte y Europa han invertido miles de millones en crear relativamente seguro y privado 3G y 4redes de G, tienen que todavía señalización de uso system 7 (SS7) como un protocolo subyacente.

SS7 Mangos el proceso para llamada-establecimiento, enunciando, encaminamiento, e información-funciones de cambio. Cuál significa si puedes tocar a SS7, puedes manipular la llamada. SS7 Deja un atacante de utilizar un transportista pequeño en, dice, Nigeria para acceder las llamadas hicieron en Europa o los Estados Unidos. “ Es gusta aseguras la puerta de frente de la casa, pero la puerta posterior es de par en par,” dijo Engel.

Los dos investigadores probaron un método en qué unos usos atacantes un teléfono función que envía llamada y SS7 a adelante un objetivo's outgoing llamadas a él antes de conferencing (tres-la manera que llama) en su pretendido recipient. Una vez el atacante se ha establecido, puede escuchar a todas las llamadas hicieron por la personaje apuntada de cualquier sitio encima tierra.

Otra estrategia sería para el atacante de poner arriba de antenas radiofónicas para recoger todas las llamadas celulares y textos dentro de una área dada. Para cualquier encriptado 3llamadas de G, el atacante podría pedir SS7 para proporcionarle con el apropiado decryption tono.

“ Es todo automatizó, en el empujón de un botón,” Nohl dijo. “ Me atacaría como perfecto espiondo capacidad, a récord y decrypt bastante cualquier

Red... Cualquier red hemos probado, obra.”<sup>4</sup> Él entonces enumerado casi cada transportista importante en América del Norte y Europa, alrededor veinte en todo.

Nohl Y Engel también encontrado que podrían localizar cualquier celda-usuario de teléfono por utilizar un SS7 la función llamó un en cualquier momento consulta de interrogatorio. Aquello es, podrían hacer tan hasta la función estuvo cerrada abajo temprano en 2015. Aun así, desde entonces todos los transportistas tienen que seguir sus usuarios para proporcionar servicio, SS7 proporciona otras funciones que todavía dejar algunos vigilancia remota. Tendría que ser notado que los defectos concretos identificaron por Nohl y Engel ha sido mayoritariamente mitigado por los transportistas desde su búsqueda fueron públicos.

Podrías creer que la encriptación sólo ayudaría mantener celda-el teléfono llama private. Comienzo con 2G, GSM-llamadas de teléfono basado han sido encriptadas. Aun así, los métodos iniciales utilizaron para encriptar las llamadas en 2G eran débiles y finalmente rompió abajo.

Desafortunadamente, el coste de upgrading las redes celulares a 3G probaron prohibitive para muchos carriers, así que un debilitados 2G quedado en utilizar hasta que alrededor 2010 o tan.

En el verano de 2010, un equipo de investigadores dirigió por Nohl dividido toda la encriptación posible los tonos utilizaron por 2G GSM redes entre ellos y crunched los números para producir qué está llamado un rainbow mesa, una lista de precomputed tonos o contraseñas. Publicaron la mesa para asomar transportistas alrededor del mundiales sólo qué insecure 2encriptación de G que utiliza GSM es. Cada paquete —o unidad de datos entre fuente y destino— de voz, texto, o el dato envió encima 2G GSM podría ser decrypted en justo unos cuantos minutos utilizando la mesa publicada de tonos.<sup>5</sup> Esto era un ejemplo extremo, pero el equipo lo consideró necesario; cuándo Nohl y otros hubieron anteriormente presentó sus hallazgos a los transportistas, sus avisos cayeron en sordos ears. Por demostrar cómo podrían agrietar 2G GSM encriptación, más o menos forzaron los transportistas para hacer el cambio.

Es importante de notar que 2G todavía existe hoy, y los transportistas están considerando vendiendo acceso a su viejo 2redes de G para uso en Internet de aparatos de Cosas (aparatos otro que ordenadores que conecta al Internet, como vuestra televisión y refrigerador), el cual sólo necesita transmisión de dato ocasional. Si esto pasa, necesitaremos hacer seguro los aparatos ellos

tiene fin-a-acabar encryptiencima porque sabemos que 2G no proporcionará fuerte bastante encriptación por él.

Naturalmente eavesdropping existido antes de los aparatos móviles realmente tomaron fuera. Para Anita Busch, la pesadilla empezó la mañana de junio 20, 2002, cuándo despertó al golpe urgente de un vecino en su puerta. Alguien había puesto un agujero

de bala en el windshield de su automovilístico como sentó en el vado. No sólo que, alguien hubo también dejó Busch una rosa, un pez muerto, y una nota de una palabras —“Parón”—en el capote del coche.<sup>6</sup> Más tarde aprendería que su teléfonos había sido tocado, y no por aplicación de ley.

El hecho que la escena con un agujero de bala y un pez muerto era reminiscent de un Hollywood malo gangster la película hizo algún sentido. Busch, un reportero condimentado, era en el tiempo sólo unas cuantas semanas a un freelance tarea chronicling delito organizado's creciendo influencia en Hollywood para el *Tiempo de Los Ángeles*. Investigaba Steven Seagal y su socio empresarial anterior, Julius R. Nasso, quién había sido indicted para conspirar con la Mafia de Nueva York para extorsionar dinero de Seagal.<sup>7</sup>

Qué siguió encontrar la nota en su coche era una serie de mensajes de teléfono. La visita aparentemente quiso compartir alguna información sobre Seagal. Mucho más tardó Busch aprendido que la visita había sido contratada por Anthony Pellicano, un anterior alto-profile Los Ángeles detective privado quién en el tiempo Busch el coche era tampered con era ya sospechado por el FBI de ilegal wiretapping, bribery, robo de identidad, y obstrucción de justicia. Busch's Teléfono de cable cobrizo había sido tocado por Pellicano, quién supo por eavesdropping en sus llamadas que escribía una historia de diario sobre sus clientes. El pez de frente su coche era un intento de advertirle fuera.

Típicamente wiretapping es sólo asociado con llamadas de teléfono, pero wiretapping leyes en los Estados Unidos también pueden cubrir eavesdropping encima email y mensajes de instante. De momento enfocaré en wiretapping uso tradicional, en cobrizo-alambrar landlines.

Landlines Es el hardwired teléfonos en vuestra casa o negocio, y wiretapping implica literalmente tocando al cable vivo. Atrás en el día, empresas de teléfono cada bancos físicos tenidos de cambios encima cuál actuaron una versión de wiretapping. Qué aquello significa es que la empresa de teléfono tuvo electrodomésticos especiales que las tecnologías de marco hooked hasta el número de teléfono del objetivo en el mainframe en la oficina central. hay

adicional wiretapping equipamiento que dio a este electrodoméstico y suele monitor el objetivo. Hoy, aquella manera de eavesdropping está retirado: empresas de teléfono son todos requirió para implementar el técnico requirements mandated por CALEA.

A pesar de que un número de crecer de las personas hoy han movido a teléfonos celulares, muchos todavía retienen su landlines para su cobrizos-alambrar dependability. Otros utilizan qué está llamado Voz encima Protocolo de Internet (VoIP) tecnología, el cual es telephony sobre el Internet y normalmente bundled en la casa u oficina con vuestro

cable o servicio de Internet. Si él's un cambio físico en la empresa de teléfono o un cambio digital, aplicación de ley tiene la capacidad a eavesdrop en llamadas. El 1994 CALEA requires fabricantes de telecomunicaciones y transportistas para modificar su equipamiento para los propósitos de dejar aplicación de ley a wiretap la línea. Tan debajo CALEA, cualquier landline la llamada en los Estados Unidos es teóricamente subject a interceptación. Y bajo CALEA, todo acceso de aplicación de la ley requiere un Título III warrant. Aquello dijo, él's quieto ilegal para un ciudadano normal para dirigir un wiretap, el cual es qué Anthony Pellicano hizo a covertly monitor Anita Busch y otros. Su lista de eavesdropping las víctimas pasa para incluir celebridades de Hollywood como Sylvester Stallone, David Carradine, y Kevin

Nealon, entre otros. Su lista de wiretap las víctimas también incluye mi amigo Erin Finn, porque su

ex-el novio estuvo obsesionado con su y le quiso seguir cada movimiento. Porque su línea de teléfono había sido tocada, I, también, estuvo controlado cuándo le llamé. La parte más fresca de la saga es que AT&T me pagué miles de dólares como parte de una clase-poblamiento de acción debido a Pellicano's wiretapping de mis llamadas a finlandés. Cuál es un poco irónico, porque en otra ocasión, era el haciendo el tocando. Pellicano's Propósito en wiretapping las personas era quizás más malicious que mina; intentaba intimidar testigos a cualquier no atestiguando o atestiguando en una manera segura.

Back En el mid-1990s, un wiretap tuvo que ser instalado por técnicos. Tan Pellicano, o uno de sus personas, tuvo que contratar alguien quién obró en PacBell para tocar Busch es y Finn's líneas telefónicas. Los técnicos eran capaces de poner arriba de prórrogas de los teléfonos de objetivo en Pellicano's oficina, en Beverly Cerros. En este caso no había ningún grifo

hecho en la caja de cruce, o el terminal al lado de la casa o complejo de apartamento, a pesar de que aquello es también posible.<sup>8</sup>

Como puedes retirar de leer mi Fantasma de libro *anterior en los Cables*, una vez conduje abajo de mi padre's apartamento en Calabasas a Playa Larga para poner arriba de un físico wiretap en una línea de teléfono utilizada por Kent, un amigo de mi hermano tardío. Había muchos cuestiona rodear la muerte de mi hermano, de una sobredosis de droga, y yo believed tuvo una parte en aquella muerte, aunque más tarde aprendí no fue implicado. En el espacio de utilidad dentro del complejo de apartamento donde Kent vivió, utilicé ingeniería social para fingir para ser un técnico de línea que llama una unidad particular dentro de GTE (Electrónica y Teléfono Generales) para encontrar donde el cable y el par asignaron al teléfono de Kent estuvo localizado. Resultó que Kent's cables de teléfono corrieron a través de un apartamento completamente separado edificio. Y tan en un segundo espacio de utilidad, era finalmente capaz a clip mi voz-activado

microcassette la cinta registradora a su línea de teléfono en la caja terminal (el sitio donde técnicos de empresa del teléfono conectan las líneas a cada apartamento).

Después de que aquello, en cualquier momento Kent hizo una llamada, podría grabar ambos lados de la conversación sin su conociendo hacía tan— aun así tendría que notar que mientras los registros eran en tiempo real, mi escuchando a ellos no fue. Todos los días sobre el próximo diez días I tuvo que hacer el paseo de sesenta minutos a Kent's apartamento, después escuchando al recuperó cintas para cualquier mencionar de mi hermano. Desafortunadamente, nada nunca vino de él. Años más tarde aprendí que mi tío probablemente había sido responsable para la muerte de mi hermano.

Given Qué fácil era para Pellicano y me para tocar a conversaciones de teléfono privado, te puedes preguntar cómo puedes acaecer invisible con un cobrizo- alambrar landline teléfono que es aparentemente abrir a vigilancia? Puedes't, sin comprar equipamiento especial. Para el verdaderamente paranoid, hay landline teléfonos que encriptará todas vuestras conversaciones de voz sobre cables cobrizos.<sup>9</sup> Estos teléfonos solucionan el problema de interceptación de llamadas de teléfono privado, pero sólo si ambos fines de la encriptación de uso de la llamada; otherwise pueden ser fáciles de controlar.<sup>10</sup> Para el resto de nosotros, hay algunas elecciones telefónicas básicas podemos hacer para evitar siendo eavesdropped encima.

El movimiento hacia telefonía digital ha hecho la vigilancia más fácil, no más duro. Hoy, si un grifo es necesario en una línea de teléfono digital,

puede ser hecho remotely. El ordenador de cambiar sencillamente crea un segundo, corriente paralela de datos; ningún equipamiento de control adicional está requerido. Esto también lo hace mucho más duro de determinar si una línea dada ha sido tocada. Y en más casos tales grifos son only descubiertos por accidente.

Poco después Grecia hosted la 2004 olimpiada de Verano, ingenieros en Vodafone-Panafon sacados algún rogue software que había sido descubierto para ser corriendo en la red celular de la empresa para más de un año. En práctica, ley enforcement intercepta toda voz y dato de texto enviado sobre cualquier red celular a través de un remoto-el sistema controlado llamó RES (subsistema de equipamiento de control remoto), el equivalente digital de un analógico wiretap. Cuándo un subject debajo la vigilancia hace un móvil call, el RES crea una segunda corriente de dato que alimenta directamente a un agente de aplicación de la ley.

El rogue el software descubierto en Grecia tocó a Vodafone's RES, significando que alguien otro que un agente de aplicación de ley legítimo escuchaba a las conversaciones dirigieron sobre su red celular; en este caso, el wiretapper estuvo interesado en oficiales de gobierno. Durante la olimpiada, algunos

países—como los Estados Unidos y Rusia—proporcionaron sus sistemas de comunicaciones privados propios para estatales-nivelar conversations. Otros jefes de estado y ejecutivos empresariales de alrededor del mundo utilizó el compromised Vodafone sistema.

Una investigación asomó que las comunicaciones del primer ministro griego y su mujer—así como aquellos del alcalde de Atenas, el comisario de Unión europeo griego, y los ministerios de defensa nacional, asuntos extranjeros, el marine mercantil, y la justicia—había sido controlada durante la olimpiada. Otro interceptado telefona pertenecido a miembros de organizaciones de derechos civiles, antiglobalization groups, la fiesta de Democracia Nueva gobernanta, el helénico Navy personal general, así como activistas de paz y un griegos-empleado americano en la embajada de Estados Unidos en Atenas.<sup>11</sup>

El espiando podría haber continuado más largo hubo Vodafone no llamado en el vendedor de hardware fo su RES sistema, Ericsson, mientras investigando una queja separada—que sus mensajes de texto padecían fallos de entrega en un más altos que tasa normal. Después de diagnosticar el problema, Ericsson notificó Vodafone que había encontrado rogue software.

Desafortunadamente, más de una década después, nosotros todavía don't saber quién esto. O por qué. O incluso qué común esta actividad podría ser. Para hacer los asuntos peores, Vodafone aparentemente mishandled la investigación.<sup>12</sup> Para una cosa, el registro clave archiva cubrir el caso faltó. Y en vez de dejar el rogue el programa corrido después de que descubrimiento—una práctica común en ordenador investigaciones criminales—Vodafone abruptamente sacó él de su sistema, los cuales pueden haber vertido del perpetrators y les dejó a más allá cubrir sus pistas.

El Vodafone el caso es un unsettling recordatorio de cómo vulnerable nuestros teléfonos celulares son a interceptación. Pero hay maneras todavía puedes ser invisible con un teléfono digital.

Además teléfonos celulares y anticuados landlines, una tercera opción de telefonía, como yo mentioned más temprano, es Voz encima Protocolo de Internet (VoIP). VoIP Es sumo para cualquier aparato inalámbrico que carencias un medio nativo de hacer una llamada de teléfono, p. ej., un Tacto de iPod de la Manzana; él's más gustar surfing el Internet que haciendo una llamada de teléfono clásica. Landlines Requiere cable cobrizo. Torres de celda de uso de teléfonos celulares. VoIP Sencillamente está transmitiendo vuestra voz sobre el Internet—tampoco utilizando Internet alambrado o inalámbrico servicios. VoIP También obras en aparatos móviles, como portátiles y pastillas, si o no tienen servicio celular.

Para ahorrar dinero, muchas casas y las oficinas han cambiado al VoIP los sistemas que

son ofrecidos por proveedores de servicio nuevo y existiendo empresas de cable. VoIP Usos el mismo cable coaxial que trae streaming vídeo y alto-Internet de velocidad a vuestra casa.

El bueno noticioso es que VoIP sistemas de teléfono utilizan encriptación; específicamente, algo protocolo de descripción de sesión llamado descripciones de seguridad, o SDES. El malo noticioso es que en su propio, SDES no es muy seguro.

Parte del problema con SDES es el tono de encriptación no es compartido sobre SSL/TLS (una red cryptographic protocolo), el cual es seguro. Si el vendedor no utiliza SSL/TLS, aun así, entonces el tono está enviado el claro. En vez de encriptación asimétrica, utiliza symmetric encriptación, el cual significa que el clave generado por el sender mosto de alguna manera ser pasado al recipient en orden para la llamada para ser unscrambled.

Dejado es dice Bob quiere hacer una llamada a Alice, quién es en China. Bob's SDES- encriptado VoIP el teléfono genera un tono nuevo para aquella



llamada. De alguna manera Bob tiene que coger que tono nuevo a Alice así que su VoIP el equipamiento puede decrypt su llamada de teléfono y ellos pueden dialogar. La solución SDES las ofertas es para enviar el clave al transportista de Bob, el cual entonces lo pasa al transportista de Alice, el cual entonces comparte él con su.

Ves el defecto? Recordar qué dije aproximadamente fin-a-criptación de fin en el capítulo anterior? Las estancias de conversación aseguran hasta el recipient abre él en el otro fin. Pero SDES acciones el tono de Bob a Bob cargador y, si Alice's el transportista es diferente, la llamada está encriptada de Alice cargador a Alice. Si el vacío es significativo es discutible. Algo así también pasa con Skype y Voz de Google. Los tonos nuevos están generados siempre que una llamada está inicializada, pero aquellos tonos son entonces dados encima a Microsoft y Google. Tanto para queriendo tener una conversación privada.

Afortunadamente, hay maneras de encriptar móviles VoIP de acabar para acabar.

Señal, una aplicación de Sistemas de Murmullo Abierto, es un libre, abierto-fuente VoIP sistema para teléfonos celulares que proporciona fin cierto-a-criptación de fin para ambos iPhone y Androide.<sup>13</sup>

La ventaja principal de utilizar la señal es que la gestión clave está manejada sólo entre las fiestas de llamar, not a través de cualquier tercera fiesta. Aquello significa que, como en SDES, los tonos nuevos están generados con cada llamada; aun así, las copias únicas de los tonos están almacenadas en los usuarios' aparatos. Desde CALEA deja acceso a cualquier récord de una llamada concreta, aplicación de ley en este caso sólo ve el tráfico encriptado a través del transportista móvil's línea, el cual sería ininteligible. Y Sistemas de Murmullo Abierto, el nonprofit organización que

Señal de marcas, no tiene los tonos, así que un warrant sería inútil. Los tonos existen sólo en los aparatos en cualquier fin de la llamada. Y una vez los fines de llamada, aquellos tonos de sesión están destruidos.

Actualmente CALEA no extiende para acabar usuarios o sus aparatos.

Podrías creer que habiendo la encriptación en vuestro teléfono celular drenaría vuestra batería. Él , pero no por mucho. Notificaciones de empujón de usos de señal, tan hacer las aplicaciones WhatsApp y Telegrama. Por ello sólo ves una llamada cuándo es incoming, el cual corta abajo encima uso de batería mientras tú're escuchando para llamadas nuevas. El Androide e iOS aplicaciones también audio de uso codecs y buffer los algoritmos nativos a la



red móvil, tan otra vez la encriptación no está drenando poder muchísimo mientras estás haciendo una llamada.

Además de utilizar fin-a-encriptación de fin, la señal también utiliza clandestinidad de delantero perfecto (PFS). Qué es PFS? Es un sistema que usa una encriptación ligeramente diferente tono para cada llamada, de modo que incluso si alguien dirige para conseguir vuestra llamada de teléfono encriptada y el clave aquello solió lo encripta, vuestras otras llamadas quedarán seguras. Todo PFS los tonos están basados en un tono original solo, but la cosa importante es que si alguien compromises uno clave, no significa vuestro potencial adversary tiene acceso a vuestras comunicaciones más lejanas.

## CAPÍTULO CUATRO

### **Si no Encriptas, eres Unequipped**

Si alguien era para elegir arriba de vuestro unlocked teléfono celular ahora mismo, aquella persona podría obtener acceso a vuestro email, vuestra cuenta de Facebook, y quizás

incluso vuestra cuenta de Amazona. En nuestros aparatos móviles, nosotros ya no registro en individualmente a servicios, como hacemos en nuestros portátiles y desktops; tenemos aplicaciones móviles, y, una vez nosotros're logged en, quedan abiertos. Además vuestras fotos y vuestra música, hay otras características únicas en vuestro teléfono celular, como mensajes de texto del SMS. Estos, también, acaecer expuesto si alguien obtiene acceso físico a vuestro unlocked aparato móvil.

Considera esto: en 2009 Daniel Lee de Longview, Washington, estuvo arrestado encima sospecha de vender drogas.<sup>1</sup> Mientras era en custodia la policía pasó por su no-contraseña-teléfono celular protegido e inmediatamente descubrió varias droga-mensajes de texto narrado. Uno tal hilo era de una personaje llamó Z-Jon.

Leyó, “tengo cien y treinta para el-sesenta I debe tú de anoche.” Según testimonio de corte, el Longview policía no sólo leído Z- los mensajes de Jon a Lee, ellos también activamente respondidos, arreglando su trato de droga propio. Posando como Lee, la policía envió Z-Jon un mensaje de texto en respuesta, pidiéndole si “necesitó más.” Z-Jon respondió, “Yeah, aquello sería fresco.” Cuando Z-Jon (de quién nombre real es Jonathan Roden) apareció para aquella reunión, el Longview la policía le arrestó para intentado heroin posesión.

La policía también notó otro hilo de mensajes de texto encima el teléfono de Lee y 75

Shawn arrestado Daniel Hinton bajo circunstancias similares.<sup>2</sup> Tanto los hombres apelaron, y en 2014, con la ayuda de la Unión de Libertades Civil americana, el Washington Corte Suprema Estatal overturned Roden es e Hinton's condenas por una corte más baja, afirmando que la policía había violado el defendants' expectativa de intimidad.

El Washington las justicias Estatales dijeron que tuvo Lee visto los mensajes de Roden y Hinton primero o instruyó los agentes policiales para responder por decir “Daniel no es aquí,” aquello habría cambiado el fundamentals en ambos casos. “Mensajes de texto pueden abarcar los mismos temas íntimos como llamadas de teléfono, selló letras y otras formas tradicionales de comunicación aquello históricamente ha sido fuertemente protegido debajo ley de Washington,” Justice Steven Gonzalez escribió en Hinton's caso.<sup>3</sup>

Las justicias gobernadas que la expectativa de intimidad tendría que extender del papel-era de letra a la edad digital. En los Estados Unidos, aplicación de ley no es permitted para abrir una letra físicamente sellada sin el recipient's permiso. La expectativa de intimidad es una prueba legal. Suele determinar si las protecciones de intimidad dentro de la Cuarta Enmienda a the Constitución de Estados Unidos aplica. Queda para ser visto cómo las cortes deciden casos futuros y si incluyen esta prueba legal.

Tecnología de texto—también sabida como servicio de mensaje corto, o SMS—ha sido alrededor desde entonces 1992. Teléfonos celulares, incluso teléfonos de característica (i.e., no-smartphones), deja para enviar mensajes de texto breve. Mensajes de texto no son necesariamente punto- a-punto: en otras palabras,, los mensajes no literalmente viaje de telefonar para telefonar. Como un email, el mensaje escribes fuera en vuestro teléfono está enviado unencriptado, en el claro, a centro de servicio de mensaje a escaso (SMSC), la parte de la red móvil diseñó para almacenar, adelante, y entregar el SMS—a veces horas más tarde.

Mensajes de texto móviles nativos—aquellos iniciados de vuestro teléfono y no un pase—de aplicación a través de un SMSC en el transportista, donde pueden o no puede ser no almacenado. Los transportistas declaran retienen textos para únicos unos cuantos días. Después de aquel tiempo ha expirado, los transportistas insisten que vuestros mensajes de texto están almacenados sólo en los teléfonos que envía y recibirles, y el número de mensajes almacenó varía por el modelo de teléfono. A pesar de estas reclamaciones,

pienso todos los operadores móviles en los Estados Unidos retienen mensajes de texto a toda costa de qué dicen el público.<sup>4</sup>

hay algunos duda rodear esta reclamación por los transportistas. Documents Expuesto por Edward Snowden sugerir una relación estanca entre el NSA y al

menos uno de los transportistas, AT&T. Según *Alambrado*, empezando en 2002— poco después 9/11—el NSA AT&T acercada y les pidió para empezar construyendo salas secretas en algunos del cargadores's facilidades. Uno era para ser localizado en Bridgeton, Misuri, y otro en Folsom Calle en San Francisco céntrico. Finalmente otras ciudades estuvieron añadidas, incluyendo Seattle, San Jose, Los Ángeles, y San Diego. El propósito de estas salas secretas era a canal todo el Internet, email, y tráfico de teléfono a través de un filtro especial que buscaría palabras clave. Es unclear si mensajes de texto estuvieron incluidos, a pesar de que parece razonable de pensar eran. Es también unclear si esta práctica todavía existe en AT&T o cualquiera otro poste cargador-Snowden.<sup>5</sup>

Una pista sugiere que esta práctica no continúa.

En el 2015 AFC juego de campeonato, dirigiendo hasta Super Bol XLIX, los Patriotas de Inglaterra Nuevos controversia incendiada con su victoria sobre el Indianapolis Colts, 45–7. En el fondo de la controversia era si el equipo de Inglaterra Nuevo hubo deliberadamente underinflated sus pelotas de fútbol. La Liga de Fútbol Nacional tiene reglas estrictas alrededor de la inflación apropiada de sus pelotas de fútbol, y después de aquel juego de play off estuvo determinado que las bolas contribuyeron por el equipo de Inglaterra Nuevo no cumplió los criterios. Central a la investigación era mensajes de texto envió por los Patriotas' estrella quarterback, Tom Brady.

Públicamente Brady negó implicación. Asomando detectives el text mensajes envió y recibido antes de que y durante el juego haber quizás confirmó esto. Desafortunadamente, el día cumplió con detectives claves, Brady abruptamente cambió teléfonos celulares, discarding el había utilizado entre noviembre 2014 y approximately Marcha 6, 2015, a una marca-teléfono nuevo. Brady más tarde dijo el comité que había destruido su teléfono original y todo el dato encima lo, incluyendo sus mensajes de texto almacenados. Como resultado Brady recibió una suspensión de cuatro juegos del NFL, el cual era más tarde lifted por orden judicial.<sup>6</sup>

“Durante los cuatro meses que el teléfono celular era en uso, Brady había intercambiado casi 10,000 mensajes de texto, ninguno de los cuales ahora pueden ser recuperados de aquel aparato,” la liga dijo. “Siguiendo el oído de

apelación, los representantes de Señor Brady provided una letra de su cellphone cargador confirmando que los mensajes de texto enviaron de o recibidos por el destruidos cellphone ya no podría ser recuperado.”<sup>7</sup>

Así que si Tom Brady tuvo una nota de su cargador diciendo que sus mensajes de texto eran todos destruyó, y los transportistas ellos dice ellos don't retenerles, la manera única de prolongar la vida de un texto es para recular arriba de vuestro aparato móvil a la nube. Si utilizas un servicio de vuestro transportista, o incluso de Google o Manzana,

aquellas empresas pueden tener acceso a vuestros mensajes de texto.

Aparentemente Tom Brady didn't tiene tiempo para recular arriba de los contenidos de su teléfono viejo a la nube antes de su emergencia upgrade.

El congreso no ha dirigido el asunto de retención de datos en general y teléfonos celulares en particular. De hecho, el congreso ha debatido en años recientes si para requerir todos los transportistas móviles a mensajes de texto del archivo para hasta dos años. Australia decidió hacer este en 2015, así que queda para ser visto si esto obra allí.

Así que cómo puede mantienes vuestros mensajes de texto privados? Ante todo, don't uso el texto nativo messaging servicio que pasa por vuestro transportista inalámbrico. En cambio utilizar un tercer-aplicación de fiesta. Pero cuál?

Para enmascarar nuestras identidades on-line—para gozar el Internet anónimamente— necesitaremos confiar en *algún* software y servicios de software. Aquella confianza es dura de verificar. En general, abierto-fuente y nonprofit las organizaciones proporcionan quizás el software más seguro y servicios porque hay literalmente miles de ojos poring sobre el código y flagging cualquier cosa aquello mira sospechoso o vulnerable. Cuándo utilizas software propietario, más o menos tienes que tomar la palabra del vendedor.

Reseñas de software, por su carácter, sólo te puede decir tanto—como cómo unas obras de característica de interfaz particulares. El reviewers pasa unos cuantos días con el software y escribir sus impresiones. Ellos don't de hecho utilizar el software, ni puede informan en qué pasa sobre el plazo largo. Sólo graban sus impresiones iniciales.

Además, reviewers no te dice si puedes confiar en el software. Ellos no vet la seguridad y aspectos de intimidad del producto. Y sólo porque un producto proviene una marca bien sabida nombre doesn't malo es seguro. De hecho tendríamos que ser cautos de nombres de marca popular porque nos pueden

engañar a un sentido falso de seguridad. No tendrías que tomar el vendedor en su palabra.

Atrás en el 1990s, cuándo necesité encriptar mi Windows 95 portátil, escogí una utilidad ahora interrumpida producto de Norton llamado Norton Diskreet. Peter Norton es un genio. Su primera utilidad de ordenador automatizó el proceso de undeleting una lima. Fue en para crear utilidades de sistema sumas muchísimas atrás en el 1980s, a la vez cuándo pocas personas podrían entender una orden puntual. Pero entonces vendió la empresa a Symantec, y alguien más empezó escribir el software en su nombre.

En el tiempo adquirí Diskreet, un producto que es ya no disponible, 56-mordió

DES encriptación (DES estands para “nivel de encriptación de los datos”) era un trato grande. Era la encriptación más fuerte podrías esperar para. Para darte un poco contexto, hoy utilizamos AES 256-mordió encriptación (AES estands para “nivel de encriptación adelantada”). Cada cual añadió mordió de la encriptación añade exponentially más tonos de encriptación y por tanto más seguridad. DES 56-mordió la encriptación estuvo considerada estatal-de-el-el arte seguro hasta que estuvo agrietado en 1998.<sup>8</sup>

En todo caso, I quiso ver si el Diskreet el programa era bastante robusto para esconder mi dato. También quise desafiar el FBI si nunca cogieron mi ordenador. Después de adquirir el programa corté a Symantec y localizó el código de fuente del programa.<sup>9</sup> Después de que analicé qué hizo y cómo él, descubrí que Diskreet sólo utilizó treinta bits del 56-mordió clave—el resto sólo acolchaba con ceros.<sup>10</sup> Aquello's menos aún seguro que los cuarenta bits que estuvo dejado para ser exportado fuera de los Estados Unidos.

Qué aquello significado en los plazos prácticos era que alguien—el NSA, aplicación de ley, o un enemigo con un ordenador muy rápido—podría agrietar el Diskreet producto mucho más fácilmente que anunciado, desde entonces él no realmente uso 56-mordió encriptación en absoluto. Aún así la empresa era marketing el producto como habiendo 56-mordió encriptación. Decidí utilizar algo más en cambio.

Cómo el público sabe esto? Ellos no.

A pesar de que redes sociales como Facebook, Snapchat, e Instagram fila en la copa cuándo viene a popularidad entre adolescentes, texto messaging los reinados supremos en general, según los datos suministraron por

Niche.com.<sup>11</sup> Un estudio reciente encontrado que 87 por ciento de texto de adolescentes diariamente, comparado al 61 por ciento quienes dicen que utilizan Facebook, el luego elección más popular. Las chicas envían, en medianos, aproximadamente 3,952 mensajes de texto por mes, y los chicos envían más cercanos a 2,815 mensajes de texto por mes, según el estudio.<sup>12</sup>

El bueno noticioso es que hoy todo el popular messaging las aplicaciones proporcionan alguna forma de encriptación cuándo enviando y recibiendo vuestros textos—que es, protegen qué está llamado “dato en movimiento.” El malo noticioso es aquello no toda la encriptación que es utilizado es fuerte. En 2014, investigador Paul Jauregui de la seguridad firme Praetorian encontrado que era posible a circumvent la encriptación utilizada por WhatsApp y comprometer en un hombre-en-el-medio (MitM) ataque, en qué el atacante intercepta mensajes entre la víctima y su recipient y es capaz de ver cada mensaje. “Esto es la clase de embutir el NSA querría,” Jauregui observó.<sup>13</sup> Como de esta escritura, la encriptación utilizada en WhatsApp ha sido

actualizado y fin de usos-a-encriptación de fin en ambos iOS y aparatos de Androide. Y la empresa de padre para WhatsApp, Facebook, ha añadido encriptación a su 900 millones de Mensajero usuarios, a pesar de que es un optar-en, significándote tiene que configurar “Conversaciones Secretas” para obrar.<sup>14</sup>

El peor noticioso es qué pasa a dato aquello es archived, o dato “en resto.” La mayoría de aplicaciones de texto móviles no encriptan archived dato, cualquiera en vuestro aparato o en un tercer-sistema de fiesta. Aplicaciones como OBJETIVO, Mensajero de Mora, y Skype todos almacenan vuestros mensajes sin encriptarles. Aquello significa el proveedor de servicio puede leer el contenido (si él's almacenado en la nube) y uso él para publicitario. También significa que si aplicación de ley—o criminal hackers—era para obtener acceso al aparato físico, podrían también leídos aquellos mensajes.

Otro asunto es retención de dato, el cual mencionamos encima—cuánto tiempo hace datos en estancia de resto en resto? Si aplicaciones como OBJETIVO y Skype arcoive vuestros mensajes sin encriptación, cuánto tiempo les mantienen? Microsoft, el cual posee Skype, ha dicho que “Skype los usos automatizaron escanear dentro Mensajes de Instante y SMS a (un) identifica sospechado spam y/o (b) identifica URLs aquello ha sido anteriormente flagged como spam, fraude, o phishing enlaces.” Tan lejos estos sonidos como el anti-malware actividad de barrido que las empresas actúan en nuestros emails. Aun así, la política de privacidad continúa en para



decir: “Skype retendrá vuestra información para mientras es necesario a: (1) cumple cualquiera de los Propósitos (como definidos en prenda 2 de esta Política de privacidad) o (2) comply con legislación aplicable, peticiones reguladoras y órdenes pertinentes de cortes competentes.”<sup>15</sup>

Aquello no suena tan bueno. Cuánto tiempo es “mientras es necesario”?

Mensajero de Instante del AOL (OBJETIVO) puede haber sido el primer mensaje de instante servicio que cualquiera de nosotros utilizó. Él's sido alrededor de un largo mientras. Diseñado para desktop o tradicional PCs, el OBJETIVO originalmente tomó la forma de un poco pop-arriba ventana que parecido en la esquina de mano derecha más baja del desktop. Hoy es disponible como aplicación móvil también. Pero en plazos de intimidad, el OBJETIVO cria algunos banderas rojas. Primero, el OBJETIVO mantiene un archivo de todos los mensajes envió a través de su servicio. Y, como Skype, también escanea los contenidos de aquellos messages. Una tercera preocupación es aquel AOL mantiene récords de los mensajes en la nube en caso nunca quieres acceder una historia de chat de cualquier terminal o el aparato diferente del donde tuviste vuestra última sesión.<sup>16</sup>

Desde vuestro dato de chat del AOL no es encriptado ei s disponible de cualquier terminal porque vive en la nube, es fácil para aplicación de ley y criminal hackers para coger una copia. Por ejemplo, mi cuenta de AOL estuvo cortada por un guión kiddie cuyo mango on-line es Virus —su nombre real es Michael Nieves.<sup>17</sup>

Él was capaz a social-ingeniero (en otras palabras,, subir el teléfono y dulce-charla) AOL y acceso de beneficio a su cliente interno-sistema de base de datos, llamó Merlin, el cual le dejó para cambiar mi alocución de email a uno asociado con una cuenta separada bajo su control. Una vez él que era capaz a reinicialización mi contraseña y acceso de beneficio a todos mis mensajes pasados. En 2007 Nieves estuvo cobrada con cuatro felonies y un misdemeanor para, según la queja, cortando a redes “de ordenador de AOL internas y bases de datos, incluyendo el cliente que enuncia récords, alocuciones y carta de crédito información.”

Como la Fundación de Frontera Electrónica ha dicho, “ningún registro es registros buenos.” AOL tiene registros.

Texto no nativo las aplicaciones pueden decir que tienen encriptación, pero no podría ser bueno o fuerte encryption. Qué tiene que buscas? Una aplicación de texto que proporciona fin-a- encriptación de fin, significando que ningún tercer-la fiesta tiene acceso a los tonos. Los tonos tendrían que existir en cada aparato sólo. Nota, también, si cualquier aparato es

compromised con malware, entonces utilizando cualquier tipo de encriptación es worthless.

Hay tres sabores “básicos” de aplicaciones de texto:

Los que no proporcionan ninguna encriptación en absoluto—significando que cualquiera puede leer vuestros mensajes de texto. Los que proporcionan encriptación, pero no de acabar para acabar—significando que la comunicación puede ser interceptada por terceras fiestas como el proveedor de servicio, el cual tiene conocimiento de los tonos de encriptación.

Los que proporcionan encriptación de acabar para acabar—significando que la comunicación puede't ser leído por terceras fiestas porque los tonos están almacenados en los aparatos individuales.

Desafortunadamente el texto más popular-messaging a aplicaciones—les gusta el OBJETIVO—no es muy privado. Even Murmullo y el secreto no pueden ser totalmente privado. El murmullo está utilizado por millones y lonjas él como anónimos, pero los investigadores tienen poked agujeros en estas reclamaciones. El murmullo sigue sus usuarios, mientras las identidades de usuarias Secretas son a veces reveló.

El telegrama es otro messaging aplicación que encriptación de ofertas, y está considerado una alternativa popular a WhatsApp. Corre encima Androide, iOS, y aparatos de Ventanas. Los investigadores tienen, aun así, encontrados un adversary puede

compromise Servidores de telegrama y coger acceso a dato crítico.<sup>18</sup> Y los investigadores lo han encontrado fáciles de recuperar mensajes de Telegrama encriptado, incluso después de que han sido eliminados del aparato.<sup>19</sup>

Tan ahora que hemos eliminado algunas elecciones populares, lo que restos? Abundancia. Cuándo tú're en la tienda de aplicación o Juego de Google, buscar aplicaciones que uso algo llamó extraoficial messaging, u OTR. Es un más alto-fin estándar-a-protocolo de encriptación del fin utilizado para mensajes de texto, y puede ser encontrado en un número de productos.<sup>20</sup>

Vuestra aplicación de mensaje de texto ideal también tendría que incluir clandestinidad de delantero perfecto (PFS). Recuerda que esto emplea una sesión aleatoriamente generada tono que está diseñado para ser resilient en el futuro. Aquello significa si uno clave es compromised, puede't soler leído vuestros mensajes de texto futuros.

Hay varias aplicaciones que uso tanto OTR y PFS.



ChatSecure Es un texto seguro-messaging aplicación que obras en ambos Androide e iPhones.<sup>21</sup> Lo también proporciona algo el certificado llamado que clava. Aquello significa incluye una prueba-de-certificado de identidad, el cual está almacenado en el aparato. A cada contacto con los servidores en ChatSecure, el certificado dentro de la aplicación en vuestro aparato está comparada con el certificado en el motsu barco. Si el certificado almacenado no empareja, la sesión no continúa. Otro tacto bueno es que ChatSecure también encripta los registros de conversación almacenaron en el aparato—el dato en resto.<sup>22</sup>

Quizás la opción de fuente abierta mejor es Señal de Sistemas de Murmullo Abierto, el cual obra en ambos iOS y Androide (ve [aquí](#)).

Otro texto-messaging aplicación para considerar es Cryptocat. Es disponible para iPhone y navegadores más importantes en vuestro PC tradicional. No es, aun así, disponible para Android.<sup>23</sup>

Y, en el tiempo de esta escritura, el Tor proyecto, el cual mantiene el Tor navegador (ve [aquí](#)), acaba de liberar Tor Mensajero. Como el Tor navegador, la aplicación anonymizes vuestra alocución de IP, el cual significa que los mensajes son difíciles de localizar (aun así, complacer nota que, gusta con el Tor navegador, nodos de salida no son por default bajo vuestro control; ve [aquí](#)). Mensajes de instante están encriptados utilizando fin-a-encriptación de fin. Como Tor, la aplicación es un poco difícil para el primer-usuario de tiempo, pero finalmente tendría que obrar para proporcionar verdaderamente mensajes de texto privado.<sup>24</sup>

hay también aplicaciones comerciales que proporciona fin-a-encriptación de fin. El único caveat es que su software es propietario, y sin reseña independiente su seguridad y la integridad no pueden ser confirmadas. Fin de ofertas de Teléfono

silencioso-a-acabar encryption texto messaging. Él , aun así, registro algún dato, pero sólo para mejorar sus servicios. Los tonos de encriptación están almacenados en el aparato. Teniendo los tonos en el aparato significa que el gobierno o aplicación de ley pueden't obliga Círculo Silencioso, su fabricante, para liberar los tonos de encriptación para cualquier de sus suscriptores.

Yo've discutido encriptando dato en moción y dato en descansar así como utilizando fin-a-encriptación de fin, PFS, y OTR para hacer tan. Qué aproximadamente no-aplicación-basó servicios, como correo de Web? Qué sobre contraseñas?

## CAPÍTULO CINCO

### Ahora Me Veo, Ahora Tú no

En abril de 2013, Khairullozhon Matanov, una persona de veintidós años taxista anterior de Quincy, Massachusetts, fue a cena con un par de amigos—un par de hermanos, de hecho. Entre otros temas, los tres hombres hablaron sobre los casos más tempranos en el día que ocurrió cercano la línea de llegada del Maratón de Boston, donde alguien había plantado cocinas de arroz empaquetaron con uñas y pólvora y un temporizador. Las explosiones resultantes alegaron tres vidas y dejados más de doscientas personas hirieron. Los hermanos en Matanov mesa, Tamerlan y Dzhokhar Tsarnaev, más tarde sería identificado como los sospechosos primos.

A pesar de que Matanov dicho más tarde que tuvo no prio conocimiento del bombardeando, presuntamente dejó un poste temprano-bombardeando reunión con agentes de aplicación de la ley y promptly eliminados la historia de navegador de su ordenador personal. Aquella ley sencilla que—borra la historia de navegador de su portátil— resultado en cargos en contra le.<sup>1</sup>

Eliminando historia de navegador era también una de los cargos en contra David Kernell, el universitario estudiantil quién cortó Sarah Palin's cuenta de email. Qué es chilling es que cuándo Kernell aclarado su navegador, corrió un disco defragmenter, y eliminó el Palin fotos había descargado, él wasn't todavía debajo investigación. El mensaje aquí es que en los Estados Unidos no eres dejado para borrar cualquier cosa haces en vuestro ordenador. Prosecutors Quiere ver vuestra historia de navegador entera.

Los cargos nivelaron contra Matanov y Kernell raíz de un casi ley de quince años—la Reforma de Contabilidad de Empresa Pública y Ley de Protección del Inversor (como él's sabido en el Senado), o el Corporativo y Auditando Imputabilidad y Ley de Responsabilidad (como él's sabido en la Casa), más generalmente llamó el Sarbanes-Oxley Ley de 2002. La ley era un resultado directo de corporativo mismanagement en Enron, una empresa gasista natural más tarde encontrada para ser lying y engañando inversores y el gobierno de EE.UU.. Detectives en el Enron el caso descubrió que el dato muchísimo había sido eliminado en el principio de la investigación, impidiendo prosecutors de ver exactamente qué había ido en dentro de la empresa. Como resultado, Senador Paul Sarbanes (D-MD) y G de Michael

del Representante. Oxley (R-OH) Patrocinó legislación que impuso una serie de requisitos apuntó en preservar dato. Uno era que historias de navegador tienen que ser retenidas.

Según una acusación de jurado magnífica, Matanov eliminado su Google Chrome historia de navegador selectively, dejando behind actividad de días seguros durante la semana de abril 15, 2013.<sup>2</sup> Oficialmente era indicted encima dos cuentas: “(1) destruyendo, alterando, y falsificando récords, documentos, y objetos tangibles en una investigación federal, y (2) haciendo un materially falso, fictitious, y declaración fraudulenta en una investigación federal que implica terrorismo internacional y doméstico.”<sup>3</sup> estuvo sentenciado a treinta meses en prisión.

Para datar, el navegador-provisión de historia de Sarbanes-Oxley raramente ha sido invocado—cualquiera contra businesses o personaje. Y sí, Matanov el caso es una anomalía, un alto-perfil caso de seguridad nacional. En su despertar, aun así, prosecutors, consciente de su potencial, ha empezado invocándolo más frecuentemente.

Si no puedes parar alguien de controlar vuestro email, llamadas de teléfono, y mensajes de instante, y si puedes't lawfully eliminar vuestra historia de navegador, qué puede haces? Quizás puedes evitar recoger tal historia en primer lugar.

Navegadores como Mozilla Firefox, Google Chrome, el safari de la manzana, y Microsoft's Explorador de Internet y Borde todos ofrecen un contruidos-en manera alternativa para buscar anónimamente en cualquier aparato prefieres—si utilizas un PC tradicional o un aparato móvil. En cada caso el navegador él abrirá una ventana nueva y no grabar qué tú searched o donde fuiste en el Internet durante aquella sesión abierta. Cerrado abajo la ventana de navegador privada, y todos los rastros de los sitios visitaste desaparecerá de vuestro PC o aparato. Qué intercambias para la intimidad es que a no ser que te marcador un sitio mientras utilizando privado explorando, no puedes volver a él; no hay ninguna historia—al menos no en

vuestra máquina. Tanto como puedes sentir invencible utilizando una ventana privada en Firefox o el

incognito modo en Chrome, vuestra petición para acceso de sitio web privado, como vuestros emails, todavía tiene que viaje a través de vuestro ISP—vuestro proveedor de servicio del Internet, la empresa pagas para Internet o el servicio celular—y vuestro proveedor pueden interceptar cualquier información aquello está enviado sin ser encriptó. Si accedes un

sitio web que usas encryption, entonces el ISP puede obtener el metadata — que visitaste tal y tal sitio en tal y tal cita y tiempo.

Cuándo un navegador de Internet—tampoco en un PC tradicional o un aparato móvil— conecta a un sitio web, primero determina si allí encriptación, y si hay, qué clase. El protocolo para comunicaciones de Web está sabido tan http. El protocolo está especificado antes de la alocución, el cual significa que un típico URL podría parecer esto:

<http://www.mitnicksecurity.com>. Incluso el “www” es superfluous en algunos casos.

Cuándo conectas a un sitio que utiliza encriptación, los cambios de protocolo ligeramente. En vez de http, “” ves “https.” Tan ahora él's <https://www.mitnicksecurity.com>. Esta conexión de https es más segura. Para una cosa, es punto -a-punto, aun así sólo si eres connecting directamente al sitio él. hay también Redes de Entrega de Contenido muchísimas (CDNs) que cache páginas para sus clientes para entregarles más rápidos, ningún asunto donde eres en el mundo, y por tanto venido entre ti y el sitio web deseado.

Mantiene en mente, también, que si eres logged en a vuestro Google, Yahoo, o cuentas de Microsoft, estas cuentas pueden grabar el tráfico de Web en vuestro PC o aparato móvil—quizás construyendo vuestro perfil conductista on-line así que las empresas pueden objetivo mejor los anuncios ves. Una manera para evitar esto es a siempre registro fuera de Google, Yahoo, y cuentas de Microsoft cuándo estás acabado utilizándoles. Puedes registro atrás en a ellos el tiempo próximo necesitas a.

Además, hay default los navegadores construyeron en a vuestros aparatos móviles. Estos no son navegadores buenos. Son caga, porque ellos're mini versiones del desktop y navegadores de portátil y carecer de algunos de la seguridad y protecciones de intimidad las versiones más robustas tienen. Por ejemplo, iPhones barco con Safari, pero también podrías querer considerar going a la tienda de Manzana on-line y descargando la versión móvil de Chrome o Firefox, navegadores que estuvo diseñado para el entorno móvil. Las versiones más nuevas de Androide embarcan con Chrome como el default. Todo los navegadores móviles al menos apoyan privados browsing.

Y si utilizas un Kindle Fuego, tampoco Firefox ni Chrome es opciones de descarga a través de Amazon. En cambio tienes que utilizar unos cuantos trucos manuales para instalar

Mozilla Firefox o Chrome a través del navegador de Seda de la amazona. Para instalar Firefox en el Kindle Fuego, abre el navegador de Seda e ir al

Mozilla FTP sitio. Selecciona “Va,” entonces seleccionar la lima que fines con la prórroga .apk.

Privado explorando doesn't crea limas provisionales, y por eso mantiene vuestra historia de explorar de vuestro portátil o aparato móvil. Podría una tercera fiesta todavía ve vuestra interacción con un sitio web dado? Sí, a no ser que aquella interacción es primero encriptó. Para cumplir esto, la Fundación de Frontera Electrónica ha creado un tapón de navegador-en HTTPS llamado En todas partes.<sup>4</sup> Esto es un tapón -en para el Firefox unnd Chrome navegadores en vuestro PC tradicional y para el Firefox navegador en vuestro aparato de Androide. Allí's ningún iOS versión en el tiempo de esta escritura. Pero HTTPS En todas partes puede conferir una ventaja distinta: considera que en el primeros pocos segundos de conexión, the el navegador y el sitio negocian lo que amable de seguridad para utilizar. Quieres clandestinidad de delantero perfecto, el cual hablé aproximadamente en el capítulo anterior. No todos los sitios utilizan PFS. Y no todo fin de negociaciones con PFS— incluso si está ofrecido. HTTPS En todas partes puede forzar uso de https siempre que posible, incluso si PFS no es en uso.

Aquí's uno más criterio para una conexión segura: cada sitio web tendría que tener un certificado, un tercer-garantía de fiesta que cuándo conectas, dice, al Banco de sitio web de América verdaderamente es el Banco de Unmerica sitio y no algo fraudulento. Obra de navegadores modernos con estas terceras fiestas, sabidos tan potestades de certificado, para mantener actualizó listas. Siempre que conectas a un sitio que no es propiamente credentialed, vuestro navegador tendría que emitir un aviso que pide si confías en el sitio bastante para continuar. Es hasta ti para hacer una excepción. En general, a no ser que sabes el sitio, no hace excepciones.

Además, no hay sólo uno escribe de certificado en el Internet; hay niveles de certificados. El más common certificado, uno ves todo el tiempo, identifica sólo que el nombre de ámbito pertenece a alguien quién pidió el certificado, utilizando verificación de email. Podría ser cualquiera, pero aquello no importa —el sitio tiene un certificado que está reconocido por vuestro navegador. El mismo es cierto de la segunda clase de certificado, un certificado organizativo. Esto significa que el sitio comparte su certificado con otros sitios narró al mismo ámbito—en otras palabras,, todos los subdominios en mitnicksecurity.com compartiría el mismo certificado.

El más stringent nivel de verificación de certificado, aun así, es qué's llamado un certificado de verificación extendido. Encima todos los navegadores, alguna parte del URL verde de turnos (normalmente es gris, como el resto del URL) cuándo un

certificado de verificación extendido ha sido emitido. Clicking Sobre la alocución— <https://www.mitnicksecurity.com>—tendría que revelar detalles adicionales sobre el certificado y su dueño, normalmente la ciudad y estado del servidor que proporciona el sitio web. Este físico-la confirmación mundial indica que la empresa que aguanta el URL es legítimo y ha sido confirmado por un confiado en tercer-potestad de certificado de la fiesta.

Podrías esperar el navegador en vuestro aparato móvil para seguir vuestra ubicación, pero podrías ser sorprendido que el browser en vuestro PC tradicional la misma cosa. Hace. Qué?

Recordar cuándo expliqué que email metadata contiene la alocución de IP de todos los servidores que mango los emails en su manera a ti? Bien, una vez más, la alocución de IP que proviene vuestro explorarr puede identificar cuál ISP estás utilizando y angostar abajo las áreas geográficas posibles donde te podría ser localizado.

El muy primer tiempo accedes un sitio que específicamente pide vuestro dato de ubicación (como un sitio de tiempo), vuestro navegador tendría que pedir whether quieres compartir vuestra ubicación con el sitio. La ventaja de compartir es que el sitio puede personalizar su listado para ti. Por ejemplo, podrías ver anuncios en [washingtonpost.com](http://www.washingtonpost.com) para negocios en la ciudad donde vives más que en la DC área.

Inseguro si contestaste que cuestión de navegador antiguamente? Entonces probar la página de prueba en <http://benwerd.com/lab/geo.php>. Esto es uno de muchos sitios de prueba que te dirá si vuestro navegador está informando vuestra ubicación. Si es y quieres ser invisible, then inutilizar la característica. Afortunadamente, puedes girar fuera ubicación de navegador que sigue. En Firefox, tipo “aproximadamente: config” en el URL barra de alocución. Desplaza hacia abajo a geo “” y cambiar el encuadre para “inutilizar.” Salvar vuestros cambios. En Chrome, va a Opciones>Bajo la Ubicación>de Encuadres de Contenido>de Capote. hay un “no deja cualquier sitio para seguir mi opción de ubicación” física que inutilizará geolocalización en Chrome. Otros navegadores tienen opciones de configuración similar.

También podrías querer fingir vuestra ubicación—si sólo sólo para divertido. Si quieres enviar fuera de las coordenadas falsas—dicen, la Casa Blanca—en Firefox, puedes instalar un tapón de navegador-en llamó Geolocator. En Google Chrome, control el tapón-en está construido-en poner llamado “emula coordenadas de geolocalización.” Mientras en Chrome, prensa Ctrl+Turno+I en Ventanas o Cmd+Opción+I en Mac para abrir el Chrome

Herramientas de Desarrollador. La ventana de Consola abrirá, y puedes clic los tres puntos verticales en el derecho superior de la Consola, entonces seleccionar más

sensores>de herramientas. Un tabulador de sensor abrirá. Esto te deja para definir la latitud exacta y longitud quieres acción. Puedes utilizar la ubicación de un hito famoso o tú pueden escoger un sitio en medio de uno de los océanos. Cualquiera manera, el sitio web ganado't saber donde realmente eres.

Puedes ocultar no sólo vuestra ubicación física pero también vuestra alocución de IP mientras on-line. Más temprano mencioné Tor, el cual randomizes la alocución de IP vista por el sitio web estás visitando. Pero no todos los sitios aceptan Tor tráfico. Hasta que recientemente, Facebook no. Para aquellos sitios que no acepta Tor conexiones, puedes utilizar un proxy.

Un abierto proxy es un servidor que sienta entre ti y el Internet. En [capítulo 2](#) I explicó que un proxy es como un traductor de lengua extranjera— hablas al traductor, y el traductor habla al altavoz de lengua extranjera, pero los restos de mensaje exactamente igual. Utilicé el término para describir la manera someone en un país hostil podría intentar enviar te un email fingiendo ser de una empresa amistosa.

También puedes utilizar un proxy para dejarte para acceder georestricted sitios web— por ejemplo, si vives en un país que acceso de búsqueda de Google de límites. O quizás necesitas esconder vuestra identidad para descargar ilegal o copyrighted contenido a través de BitTorrent.

Proxies No es antibalas, aun así. Cuando utilizas un proxy, recuerda que cada navegador tiene que ser manualmente configurado para señalar al proxy servicio. E incluso el mejor proxy los sitios admiten que listos Centellear o trucos de Javascript todavía pueden detectar vuestra IP subyacente dirige—la alocución de IP utilizas para conectar al proxy en primer lugar. Puedes limitar la efectividad de estos trucos por bloqueadores o restringiendo el uso de Centellear y Javascript en vuestro navegador. Pero la manera mejor de impedir inyección de Javascript de controlar tú vía vuestro navegador es para utilizar el HTTPS En todas partes tapón-en (ve [aquí](#)).

Hay muchos comerciales proxy servicios. Pero ser seguro para leer la intimidad policy de cualquier servicio firmas arriba para. Para atención a la manera maneja encriptación de datos en moción y si lo complies con aplicación de ley y peticiones de gobierno para información.

hay también algunos libres proxies, pero tienes que contender con una corriente de inútil anunciando en cambio para el uso del servicio. Mi consejo

es a beware de libre proxies. En su presentación en DEF CON 20, mi amigo y experto de seguridad conjunto de Alonso del Chema arriba de un proxy como un experimento: quiso atraer tipos malos al proxy, así que anunció la alocución de IP en xroxy.com. Después de que unos cuantos días más de cinco mil personas utilizaban su libres

“Anónimo” proxy. Desafortunadamente la mayoría de ellos lo utilizaba para dirigir estafas.

El lado de dedo, aun así, es que Alonso fácilmente podría utilizar el libre proxy para pulsar malware al tipo malo's navegador y controlar suyo o sus actividades. Hizo tan utilizando qué está llamado un gancho de TERNERA, un marco de explotación del navegador. También utilizó un acuerdo de licencia de usuario de fin (EULA) que las personas tuvieron que aceptar para dejarle para hacerlo. Aquello's cómo era capaz de leer los emails que son enviados a través del proxy y determinar que manejaba el tráfico narró a actividad criminal. El moral aquí es que cuando algo es gratis, coges qué pagas para.

Si utilizas un proxy con protocolo de https, una aplicación de ley o agencia de gobierno sólo verían el proxy's alocución de IP, no las actividades en los sitios web visitas—que la información sería encriptada. Como mencioné, tráfico de Internet de http normal no es encriptado; por eso tienes que también HTTPS de uso En todas partes (sí, esto es mi respuesta a la mayoría de invisibilidad de navegador woes).

Por el bien de comodidad, las personas a menudo sincronizan sus encuadres de navegador entre aparatos diferentes. Por ejemplo, cuándo firmas en al Chrome navegador o un Chromebook, vuestros marcadores, tabuladores, historia, y otras preferencias de navegador son todos synced vía vuestra cuenta de Google. Estos encuadres cargan automáticamente every tiempo utilizas Chrome, si en tradicional PCs o aparatos móviles. Para escoger qué información tendría que ser synced a vuestra cuenta, va a la página de encuadres en vuestro Chrome navegador. El Salpicadero de Google te das el control lleno tiene que nunca quieres sacar synced información de vuestra cuenta. Asegura que la información sensible no es coche-synced. Mozilla es Firefox también tiene un sync opción.

El downside es que todas unas necesidades atacantes para hacer es señuelo tú a firmar en a vuestra cuenta de Google en un Chrome o Firefox browser, entonces toda vuestra historia de búsqueda cargará en su aparato. Imaginar vuestro amigo que utiliza vuestro ordenador y escogiendo a registro en al



navegador. La historia de vuestro amigo, marcadores, etc., ahora será synced. Aquello significa que vuestro amigo's surfing historia, entre otra información, es ahora viewable en vuestro ordenador. Plus, si firmas en a una cuenta de navegador sincronizada que utiliza una terminal pública y olvidar para firmar fuera, todo vuestro navegador's los marcadores y la historia serán disponibles al usuario próximo. Si estás firmado en a Google Chrome, entonces incluso vuestro calendario de Google, YouTube/Youtube, y otros aspectos de vuestra cuenta de Google acaecen expuestos. Si tienes que utilizar una terminal pública, ser vigilant aproximadamente firmando fuera antes de que dejas.

Otro downside de syncing es que todo interconectó los aparatos asomarán el mismo contenido. Si vives sólo, aquello puede ser bien. Pero si compartes un iCloud cuenta, las cosas malas pueden pasar. Padres quiénes dejan sus niños para utilizar el iPad familiar, por ejemplo, involuntariamente les podría exponer a contenido de adulto.<sup>5</sup>

En una tienda de Manzana en Denver, Colorado, Elliot Rodriguez, un ejecutivo de cuenta local, registró su pastilla nueva con su existiendo iCloud cuenta. Instantáneamente todas sus fotos, textos, y música y descargas de vídeo eran disponibles a él encima la pastilla nueva. Este convenience le salvó tiempo; no tiene que manualmente copia y salvar todo aquel material a aparatos múltiples. Y le dejó acceso a los elementos ningún asunto qué aparato escogió utilizar.

En algún punto más tarde encima Elliot pensó que era una idea buena de dar su pastilla de tecnología vieja a su hija de ocho años. El hecho que estuvo conectada a sus aparatos era plus de plazo a escaso. Ocasionalmente en su pastilla Elliot notaría una aplicación nueva su hija había descargado a su pastilla. A veces incluso compartirían family fotos. Entonces Elliot tomó un viaje a Ciudad de Nueva York, donde viajó a menudo para empresarial.

Sin pensar, Elliot tomó fuera de su iPhone y captó varios momentos con su Nueva York–basaron mistress, algunos de ellos bastante... Íntimo. Las imágenes de su iPhone synced automáticamente a su hija's iPad atrás en Colorado. Y naturalmente su hija pidió su madre sobre la mujer quién era con Papá. Needless Para decir, Elliot tuvo algún serio explicando para hacer cuando cogía en casa.

Y entonces hay el cumpleaños-preproblema enviado. Si compartes aparatos o synced cuentas, vuestras visitas a sitios podrían verter regalo recipients fuera a qué ellos'll estar cogiendo para sus cumpleaños. O, peor, qué podrían

haber cogido. Aún así otra razón por qué compartiendo un PC familiar o la pastilla pueden presentar un problema de intimidad.

Una manera para evitar esto es para poner arriba de usuarios diferentes, un paso relativamente fácil en Ventanas. Mantener los privilegios de administrador para tú de modo que puedes añadir software al sistema y puesto arriba de casa o familia adicionales miembros con theredero cuentas propias. Todos los usuarios registro en con sus contraseñas propias y tener acceso a sólo su contenido propio y sus marcadores de navegador propios e historias.

Apple deja para reparto similares dentro de su OSX sistemas operativos. Aun así, no muchas personas remember a segmento su iCloud espacio. Y a veces, según parece a través de ninguna falta de nuestro propio, la tecnología sencillamente nos traiciono.

Después de que años de datar varias mujeres, Dylan Monroe, un LA-productor de televisión

basada, finalmente encontrado “el” y decidido para sentar cabeza. Su prometidóe movido en, y, como parte de su vida nueva junta, inocentemente conectó su mujer futura a su iCloud cuenta.

Cuándo quieres empezar una familia, hace sentido para conectar todo el mundo a una cuenta. Haciendo así que te dejas para compartir todos vuestros vídeos, textos, y música con los quieres. Exceptúa aquello es en el presente tenso. Qué sobre vuestro pasado digitalmente almacenado?

A veces teniendo un servicio de copia de seguridad de nube automático como iCloud significa que acumulamos muchos años' valor de fotos, textos, y música, algunos del cual tendemos para olvidar, tan olvidamos los contenidos de cajas viejas en el ático.

Las fotos son la cosa más cercana tenemos que memorias. Y sí, los cónyuges han sido encontrando cajas de zapato de fotografías y letras viejas para generaciones ahora. Pero un medio digital que te dejas para tomar literalmente miles de fotos de definición alta sin demasiado esfuerzo crea problemas nuevos. De repente Dylan's memorias viejas—algún de ellos muy privados de hecho—volvió para perseguirle en la forma de fotos que era ahora en su prometidóe iPhone e iPad.

Había elementos de mobiliario aquello tuvo que ser sacado de la casa porque otras mujeres habían actuado leyes íntimas en aquel sofá, table, o cama. Había restaurantes donde su prometidóe rechazado para ir a porque había

visto fotos de otras mujeres allí con él, en aquella mesa por la ventana o en aquella cabina de esquina.

Dylan obligó su prometido amorosamente, incluso cuándo le pidió para hacer el sacrificio definitivo que—vende su casa una vez el dos de ellos estuvo casado. Todo porque había conectado su iPhone al suyo.

La nube crea otro problema interesante. Incluso si eliminas vuestra historia de navegador en vuestro desktop, portátil, o aparato móvil, una copia de vuestros restos de historia de la búsqueda en la nube. Almacenado en la empresa de motor de búsqueda's servidores, vuestra historia es un poco más dura de eliminar y más duro a no ha almacenado en primer lugar. Esto es sólo un ejemplo de cómo colección de dato subrepticio sin el contexto apropiado puede ser fácilmente misinterpreted en una cita más tardía y tiempo. Él's fácil de ver cómo un conjunto inocente de búsquedas puede ir awry.

Una mañana en el verano tardío de 2013, semanas justas después del Maratón de Boston que bombardea, Michele Catalano's el marido vio dos negro SUVs atracción arriba delante de su casa en Isla Larga. Cuándo fue exterior de saludar los agentes, le pidieron para confirmar su identidad y pidió su permiso para

buscar la casa. Habiendo Nada para esconder, a pesar de que incierto por qué eran allí, les dejó para introducir. Después de un cursory control de las salas, los agentes federales bajaron a negocio.

“Tiene cualquiera en esta casa información buscada en ollas de presión?”

“Tiene cualquiera en esta casa información buscada en mochilas?”

Aparentemente el familiar's las búsquedas on-line a través de Google habían provocado un preemptive investigación por el Departamento de Seguridad de Patria. Without Sabiendo la carácter exacta del Catalano investigación familiar, uno podría imaginar que en las semanas que siguen el Maratón de Boston que bombardea búsquedas on-line seguras, cuándo combinados, sugirió el potencial para terrorismo y así que era flagged. Dentro dos hel nuestro el Catalano la casa estuvo aclarada de cualquier potencial wrongdoing. Michele más tarde escribió sobre la experiencia para *Medio*—si sólo como advertir que qué buscas hoy podría volver para perseguirte mañana.<sup>6</sup>

En su prenda, Catalano apuntado fuera que los detectives tienen que haber descontado su busca “Lo que el infierno hago con quinoa?” Y Es “Un- Rod suspendió todavía?” Dijo su presión-consulta de cocina era

aproximadamente nada más de hacer quinoa. Y la consulta de mochila? Su marido quiso una mochila.

Al menos una empresa de motor de búsqueda, Google, ha creado varias herramientas de intimidad que te dejass para especificar qué información sientes cómodo manteniendo.<sup>7</sup> Por ejemplo, puedes girar del anuncio personalizado que sigue de modo que si miras arriba de Patagonia (la región en América Del sur) te don't el inicio que ve anuncios para viaje americano Del sur. Puedes también turno de vuestra historia de búsqueda altogether. O podrías no registro en a Gmail, YouTube/Youtube, o cualquiera de vuestras cuentas de Google mientras buscas on-line.

Incluso si no eres logged en a vuestro Microsoft, Yahoo, o cuentas de Google, vuestra alocución de IP es todavía ligada a cada petición de motor de búsqueda. Una manera para evitar este un-a-un partido es para utilizar el Google-proxy startpage.com o el motor de búsqueda DuckDuckGo en cambio.

DuckDuckGo Es ya un default opción dentro de Firefox y Safari. Google diferente, Yahoo, y Microsoft, DuckDuckGo tiene ninguna provisión para cuentas de usuario, y la empresa dice vuestra alocución de IP no es logged por default. La empresa también mantiene su propio Tor relé de salida, significado que te puede buscar DuckDuckGo mientras utilizando Tor sin mucho de una actuación lag.<sup>8</sup>

Porque DuckDuckGo no sigue vuestro uso, vuestros resultados de búsqueda no serán

filtrados por vuestras búsquedas pasadas. La mayoría de personas no se lo dan cuenta, pero los resultados ves dentro Google, Yahoo, y Bing está filtrado por todo buscaste en aquellos sitios antiguamente. Por ejemplo, si el motor de búsqueda ve que tú're buscando los sitios narraron a asuntos de salud, empezará para filtrar los resultados de búsqueda y pulsar los resultados narraron a asuntos de salud al muy superiores. Por qué? Porque muy pocos de nosotros molestan para adelantar a la segunda página de un resultado de búsqueda. Allí's un chiste de Internet que dice que si quieres saber el sitio mejor para enterrar un ente muerto, prueba [aquí](#) de los resultados de búsqueda.

A Algunas personas les podría gustar la comodidad de no teniendo que rollo a través de según parece resultados no relacionados, pero al mismo tiempo es patronizing para un motor de búsqueda para decidir qué puedes o no puede ser interesado en. Por más medidas, aquello es censura . DuckDuckGo

Regresa relevant resultados de búsqueda, pero filtrados por tema, no por vuestra historia pasada.

En el capítulo próximo I'll la charla sobre sitios web de maneras concretas lo hace dura para ti para ser invisible a ellos y qué puedes hacer a surf la Web anónimamente.

## CAPÍTULO SEIS

# Cada Clic de Ratón Haces, Seré Mirar Te

Ser muy prudente qué buscas en el Internet. Él's no motores de búsqueda justos que pista vuestros hábitos on-line; cada sitio web visitas hace también. Y

creerías que algunos de ellos sabrían mejores que para exponer asuntos privados a otros. Por ejemplo, un 2015 informe encontrado que “70 por ciento de sitios de salud' URLs contiene información exponiendo afecciones concretas, tratamientos, y enfermedades.”<sup>1</sup>

En otras palabras,, si soy en WebMD y buscando “el pie del atleta,” el unencrypted el pie de atleta *de palabras* parecerá dentro del URL visible en la barra de alocución de mi navegador. Esto significa que cualquiera—mi navegador, mi ISP, mi transportista celular—puede ver que estoy buscando información sobre atleta pie. Teniendo HTTPS En todas partes habilitado en vuestro navegador encriptaría los contenidos del sitio estás visitando, asumiendo el https de apoyos del sitio, pero lo doesn't encriptar el URL. Tan incluso las notas de Fundación de Frontera Electrónicas, https nunca fue diseñado para encubrir la identidad de los sitios visitas.

Además, el estudio encontrado que 91 por ciento de salud-narró peticiones de marca de los sitios a terceras fiestas. Estas llamadas son embedded en las páginas ellos, y hacen peticiones para imágenes minúsculas (cuál puede o no puede ser visible en la página de navegador), el cual informa estos otro tercer-sitios de fiesta que estás visitando una página particular. Hacer un buscar “atleta pie,” y como muchos como veinte

entidades diferentes que—varían de pharmaceuticals empresas a Facebook, Pinterest, Twitter, y Google—está contactado apenas la carga de resultados de la búsqueda en vuestro navegador. Ahora todas aquellas fiestas te conocen ha sido buscando información sobre atleta pie.<sup>2</sup>

Estas terceras fiestas utilizan esta información para apuntar tú con on-line anunciando. Unlso, si te logged en a la salud-sitio de cuidado, podrían ser capaces de obtener vuestra alocución de email. Afortunadamente puedo ayudar impides estas entidades de aprender más aproximadamente te.

En la salud-sitios de cuidado analizaron en el 2015 estudio, la copa diez terceras fiestas eran Google , comScore, Facebook, AppNexus, AddThis, Twitter, Quantcast, Amazona, Adobe, y Yahoo. Algunos—comScore, AppNexus, y Quantcast— tráfico de Web de la medida, tan hace Google. De las terceras fiestas listaron encima, Google, Facebook, Twitter, Amazona, Adobe, y Yahoo está espiando en vuestra actividad para razones comerciales, así que pueden, por ejemplo, anuncios de carga para atletas's remedios de pie en búsquedas futuras.

También mencionado en el estudio era las terceras fiestas Experian y Axioma, los cuales son sencillamente almacenes de dato—ellos collect tanto dato sobre una persona como posiblemente pueden. Y entonces lo venden. Recordar las cuestiones de seguridad y las respuestas creativas sugerí que utilizas? A menudo empresas como Experian y el axioma recoge, proporciona, y utilizar aquellas cuestiones de seguridad a build perfiles on-line. Estos perfiles son valiosos a marketers aquello quiere apuntar sus productos a seguros demographics.

Qué hace aquella obra?

Si escribes el URL en manualmente o utilizar un motor de búsqueda, cada sitio en el Internet tiene ambos un hostname y una alocución de IP numérica (un poco los sitios existen sólo alocuciones tan numéricas). Pero casi nunca ves la alocución numérica. Vuestro navegador lo esconde y utiliza un servicio de nombre del ámbito (DNS) para traducir un sitio hostname el nombre—dice, Google—en a una alocución concreta, en https de caso de Google://74.125.224.72/.

DNS Es como un libro de teléfono global, cruz-referencing el hostname con la alocución numérica del servidor del sitio sólo pediste. Tipo “Google.com” a vuestro navegador, y el DNS contactos su servidor en https://74.125.224.72. Entonces ves la pantalla blanca familiar con el día's Google Doodle por encima de un campo de búsqueda del espacio. Aquello, en teoría, es qué toda obra de navegadores de la Web. En practicar hay más a él.

Después del sitio ha sido identificado a través de su alocución numérica, enviará información atrás a vuestro navegador de Web de modo que puede empezar “construir” la Página web

ves. Cuando la página está regresada a vuestro navegador, ves los elementos esperarías—la información quieres recuperado, cualquiera narró imágenes, y maneras a navigate a otras partes del sitio. Pero a menudo hay elementos que está regresado a vuestro navegador que llamada fuera a otros sitios web para guiones o imágenes adicionales. Algunos, si no todo, de estos guiones son para seguir propósitos, y en más casos tú simply no les necesita.

Casi cada tecnología digital produce metadata, y, como tú've sin duda ya adivinado, los navegadores son no diferentes. Vuestro navegador puede revelar información sobre la configuración de vuestro ordenador si queried por el sitio estás visitando. Por ejemplo, qué versión de qué navegador y sistema operativo tú're utilizando, qué añade-ons tienes para aquel navegador, y lo que otros programas estás corriendo en vuestro ordenador (como Adobe productos) mientras buscas. Incluso puede revelar detalles de vuestro ordenador's hardware, como la resolución de la pantalla y la capacidad del onboard memoria.

Podrías pensar después de leer este lejos que te ha tomado zancadas sumas en acaecer invisible on-line. Y tienes. Pero allí's más obra para ser hecha.

Toma un momento y surf encima a Panopticlick.com. Esto es un sitio construido por la Fundación de Frontera Electrónica que determinará sólo qué común o único vuestra configuración de navegador está comparada a otros, basados en qué's corriendo en vuestro PC o el sistema operativo del aparato móvil y el tapón-ins te puede haber instalado. En otras palabras,, tienes cualquier tapón-ins que puede soler límite u otherwise proteger la información que Panopticlame puede glean de vuestro navegador sólo?

Si los números en el lado izquierdo, los resultados de Panopticlick, es alto — decir, un número de seis dígitos—entonces eres un poco único, porque vuestros encuadres de navegador están encontrados en menos que uno en cien ordenadores de millar. Felicitaciones. Aun así, si vuestros números son abajo—decir, menos de tres dígitos—entonces vuestros encuadres de navegador son bastante comunes. Eres sólo uno en unos cuantos centenar. Y aquello significa si voy a apuntar tú—con anuncios o malware—I don't tiene que obrar muy duro, porque tienes una configuración de navegador común.<sup>3</sup>

Te podría creer que habiendo una configuración común te puede ayudar acaecida invisible—te're parte de la multitud; tú blend en. Pero de una perspectiva técnica, esto abre tú hasta malicious actividades. Un criminal hacker doesn't quiere expend esfuerzo muchísimo. Si una casa tiene una puerta abierta y la casa luego a él ha una puerta cerró, el cual piensas que un ladrón atracaría? Si un criminal

hacker sabe que tienes encuadres comunes, entonces quizás también careces de protecciones seguras que podría realzar vuestra seguridad.

Entiendo yo sólo saltado de hablar marketers intentando seguir qué ves on-line a criminal hackers quién puede o no puede utilizar your información personal para robar vuestra identidad. Estos son muy diferentes. Marketers Recoge información para crear anuncios que mantiene los sitios web provechosos. Sin publicitario, algunos sitios sencillamente no podrían continuar. Aun así, marketers, criminal hackers, y, para aquel asunto, los gobiernos son todos intentando coger información que te no puede querer dar, y tan, por el bien de riña, son a menudo lumped juntos en discusiones sobre la invasión de intimidad.

Una manera para ser común todavía también seguro de on-line eavesdropping es para utilizar una máquina virtual (VM; ve [aquí](#)), un sistema operativo como Mac OSX corriendo como huésped arriba de vuestro sistema operativo de Ventanas. Puedes instalar VMware en vuestro desktop y utilizarlo para correr otro sistema operativo. Cuándo estás hecho, tú sencillamente cerrado lo abajo. El sistema operativo y todo tú dentro desaparecerá. Las limas salvas, aun así, quedará wherever te les salvó.

Algo más para mirar fuera para es que marketers y criminal hackers igualmente aprender algo sobre visitantes a un sitio web a través de qué's sabido como uno- lima de imagen del píxel o bug de web. Como un pop de navegador del espacio-arriba ventana, esto es un 1 × imagen de 1 píxeles colocada a algún lugar en una Página web que, a pesar de que invisible, empero llama atrás al tercer-sitio de fiesta que plo abrochó allí. El backend el servidor graba la alocución de IP que probado a render que imagen. Una imagen de un píxeles colocada en una salud-sitio de cuidado podría decir un pharmaceuticals empresa que estuve interesado en atleta remedios de pie.

El 2015 estudio mencioné a principios de este capítulo encontrado que casi a medias de tercer-peticiones de fiesta sencillamente pop abierto-arriba de las ventanas que contienen ningún contenido cualquier cosa. Estas “ventanas” de espacio generan peticiones de http silencioso a tercer-anfitriones de fiesta que está utilizado sólo para seguir propósitos. Puedes evitar estos por instruir vuestro navegador no para dejar pop-arriba de ventanas (y esto también eliminará aquellos anuncios molestos también).

Casi un tercer del tercio restante-peticiones de fiesta, según el estudio, líneas pequeñas constadas de de código, limas de Javascript, el cual normalmente sólo ejecuta animaciones en una Página web. Un sitio web puede identificar



el ordenador que accede al sitio, mayoritariamente por leer la IP dirige aquello está pidiendo la lima de Javascript.

Incluso sin una imagen de un píxeles o un pop de espacio-arriba ventana, vuestra Web surfing todavía puede ser seguido por los sitios visitas. Por ejemplo, la amazona podría

saber que el último sitio visitaste era una salud-sitio de cuidado, así que hará recomendaciones para salud-productos de cuidado para ti encima su sitio propio. La Amazona de manera podría hacer este es a de hecho ver el último sitio visitaste en vuestra petición de navegador.

La amazona cumple esto por utilizar tercer-fiesta referrers—texto en la petición para una Página web que dice la página nueva donde la petición originó. Por ejemplo, si estoy leyendo una prenda encima *Alambrada* y contiene un enlace, cuándo clic que enlace el sitio nuevo sabrá que era anteriormente en una página dentro de Wired.com. Puedes ver cómo este tercer-la fiesta que sigue puede afectar vuestra intimidad.

Para evitar esto, siempre puedes ir a Google.com primero, así que el sitio quieres la visita no sabe donde eras anteriormente. I don't cree tercer-fiesta referrers es un trato tan grande, exceptuar cuándo estás intentando enmascarar vuestra identidad. Esto es uno más ejemplo de un comercio-fuera entre comodidad (sencillamente yendo al sitio de webpróximo) e invisibilidad (siempre empezando de Google.com).

Mozilla Firefox ofrece uno de los defensas mejores en contra tercer-la fiesta que sigue a través de un tapón-en llamó NoScript.<sup>4</sup> Esto añade-encima eficazmente bloquea sólo aproximadamente todo consideró lesivo a vuestro computer y navegador, concretamente, Centellea y Javascript. Añadiendo tapón de seguridad-ins cambiará el cariz y sentir de vuestra sesión de explorar, a pesar de que puedes cereza-elegir y habilitar características concretas o permanentemente confiar en algunos sitios.

Uno resulta de habilitante NoScript is que la página visitas tendrá ningún anuncio y ciertamente ningún tercer-fiesta referrers. A raíz del bloqueador, los carices de Página web ligeramente duller que la versión sin NoScript habilitó. Aun así, tener que quieres ver aquello Centellea-vídeo codificado en el upper esquina izquierda de la página, específicamente puedes dejar que un elemento a render mientras continuando bloquear todo más. O, si te sientes puede confiar en el sitio, puedes temporalmente o permanentemente dejar todos los elementos en aquella página para cargar— algo podrías querer hacer en un sitio bancario, por ejemplo.

Para su parte, Chrome ha ScriptBlock,<sup>5</sup> cuál te dejas a defensivamente bloque el uso de guiones en una Página web. Esto es útil para niños quién puede surf a un sitio que deja pop-arriba anuncios de diversión del adulto.

Bloqueando potencialmente lesivo (y ciertamente intimidad-compromising) los elementos en estas páginas mantendrán vuestro ordenador de ser invadido con que genera anuncio malware. Por ejemplo, puedes haber notado que los anuncios parecen en vuestra página de casa del Google. De hecho, tú should tiene ningún anuncio de centellear en vuestra página de casa del Google. Si les ves, vuestro ordenador y el navegador pueden haber sido compromised (quizás hace algún tiempo), y como resulta estás viendo

tercer-anuncios de fiesta que puede contener caballos Troyanos—keyloggers, los cuales graban cada keystroke te marca, y otro malware—si te clic encima les. Incluso si los anuncios no contienen malware, el advertisers' los ingresos proviene el número de clics reciben. El más personas engañan a clicking, el más dinero hacen.

Tan bien como son, NoScript y ScriptBlock don't bloque todo. Para protección completa en contra amenazas de navegador, podrías querer instalar Adblock Plus. El problema único es que Adblock graba todo: esto es otra empresa que pistas vuestro surfing historia, despite vuestro uso de privado explorando. Aun así, en este caso el bueno—bloqueando potencialmente anuncios peligrosos— outweighs el malos: saben donde has sido on-line.

Otro tapón útil-en es Ghostery, disponible para ambos Chrome y Firefox. Ghostery Identifica todo the rastreadores de tráfico de la Web (como DoubleClick y Google AdSense) que uso de sitios para seguir vuestra actividad. Como NoScript, Ghostery te das control granular sobre qué rastreadores quieres dejar en cada página. El sitio dice, “Bloqueando los rastreadores impedirán them de correr en vuestro navegador, los cuales pueden ayudar control cómo vuestro dato conductista está seguido. Mantiene en importar que algunos rastreadores son potencialmente útiles, como la red social alimenta widgets o navegador-basó juegos. Bloqueando puede tener un unintended efecto en los sitios visitas.” Significando que algunos sitios ya no obra con Ghostery instalado. Afortunadamente, lo puedes inutilizar encima un sitio-por-base de sitio.<sup>6</sup>

Además de utilizar tapón-ins para bloquear sitios de identificarte, podrías querer confundir potencial hackers más allá por utilizar una variedad de email dirige tailored para propósitos individuales. Por ejemplo, en [capítulo 2](#) I maneras discutidas de crear cuentas de email anónimo para comunicar sin

detección. De modo parecido, para día sencillo-a-el día que explora, es also una idea buena de crear cuentas de email múltiple—no para esconder pero para te hacer menos interesando a terceras fiestas en el Internet. Teniendo perfiles de personalidad on-line múltiples diluye el impacto de intimidad de habiendo sólo uno alocución identificable. Lo hace más duro para cualquiera para construir un perfil on-line de ti.

Dejado's dice quieres adquirir algo on-line. Podrías querer crear una alocución de email que utilizas exclusivamente para compra. También podrías querer tener cualquier cosa adquieres con esta alocución de email envió a vuestra gota de correo en vez de vuestro domicilio particular.<sup>7</sup> Además, podrías querer utilizar una carta de regalo para vuestra compra, quizás uno te reload de vez en cuando.

De este modo la empresa que te vende los productos sólo tendrán vuestro

nonprimary Alocución de email, vuestro nonprimary real-alocución mundial, y vuestro más-o-menos throwaway carta de regalo. Si allí's nunca una ruptura de dato en aquella empresa, al menos los atacantes no tendrán vuestra alocución de email real, real-alocución mundial, o número de carta del crédito. Esta clase de desconexión de un on-line adquiriendo el caso es práctica de intimidad buena .

También podrías querer crear otro nonprimary alocución de email para redes sociales. Esta alocución podría acaecer vuestra “alocución” de email pública, el cual desconocidos y meros acquaintances puede utilizar para entrar tacto contigo. La ventaja a esto es que, una vez más, las personas ganadas't aprende mucho aproximadamente te. Al menos no directamente. Más allá te puedes proteger por dar cada nonprimary alocución un nombre único, cualquiera una variación en vuestro nombre real u otro nombran enteramente.

Ser prudente si vas con la opción anterior. No podrías querer listar un nombre medio—o, si siempre pasas de largo vuestro nombre medio, no podrías querer listar vuestro primer nombre. Incluso algo inocente como Johnqdoe@xyz.com sólo nos vertí fuera que tienes un nombre medio y que empieza con Q . TSuyo es un ejemplo de dar fuera de información personal cuándo no es necesario. Recuerda que estás probando a blend al fondo, no llamar atención a tú.

Si utilizas una palabra o la frase no relacionada a vuestro nombre, lo hace tan unrevealing como posible. Si vuestra alocución de email es snowboarder@xyz.com, no podemos saber vuestro nombre, pero sabemos

uno de vuestros hobbies. Mejor de escoger algo genérico, como silverfox@xyz.com.

Tú'll naturalmente también quiere tener una alocución de email personal. Sólo tendrías que compartir esto uno con familia y amigos cercanos. Y las prácticas más seguras a menudo venidas con bonificaciones buenas: tú'll encontrar aquello no utilizando vuestra alocución de email personal para on-line adquiriendo impedirá tú de recibir una tonelada de spam.

Los teléfonos celulares no son inmunes de corporativos siguiendo. En el verano de 2015, una águila-eyed investigador AT&T cogida y Verizon anexando código adicional a cada petición de Página web hecha a través de un navegador móvil. Esto no es el IMSI—identidad de suscriptor móvil internacional— hablé aproximadamente en [capítulo 3](#) (ve [aquí](#)); bastante, es un código de identificación único enviado con cada petición de Página web. El código, sabido como encabezamiento de identificador único, o UIDH, es un provisional serial número que advertisers puede utilizar para identificarte encima la Web. El investigador descubrió qué iba en porque configuró su teléfono celular a registro todo tráfico de web (cuál no muchas personas ). Entonces notó el dato adicional tacked encima a Verizon customers y, más tarde, AT&T

Clientes.<sup>8</sup> El problema con este código adicional es que los clientes no fueron dichos aproximadamente

lo. Para caso, aquellos who había descargado el Firefox aplicación móvil y tapón utilizado-ins para aumentar su intimidad era, si utilizaron AT&T o Verizon, empero siendo seguido por el UIDH códigos.

Gracias a estos UIDH códigos, Verizon y AT&T podría tomar el tráfico asociado con vuestras peticiones de Web y cualquiera lo utilizan para construir un perfil de vuestra presencia on-line móvil para futuro publicitario o sencillamente vender el dato crudo a otros.

AT&T ha suspendido la operación—por ahora.<sup>9</sup> Verizon lo ha hecho todavía otra opción para el usuario de fin para configurar.<sup>10</sup> Nota: por *no* optando fuera, das Verizon permiso para continuar.

Incluso si giras fuera Javascript, un sitio web todavía puede pasar una lima de texto con datos llamó una galleta de http atrás a vuestro navegador. Esta galleta podría ser almacenada para un tiempo largo. La galleta *de plazo* es corta para *galleta mágica*, una pieza de texto que está enviado de un sitio web y almacenado en el navegador para mantener del usuario pista de cosas,

como elementos en un carro de compra, o incluso para autenticar un usuario. Las galletas eran primero utilizadas en la Web por Netscape y era aliado de origen pretendió ayudar con crear carros de compra virtual y funciones de comercio electrónico. Las galletas son típicamente almacenadas en el navegador en un PC tradicional y tener citas de expiración, a pesar de que estas citas podrían ser décadas en el futuro.

Es las galletas peligrosas? Ningún—al menos no por ellos. Aun así, las galletas proporcionarían terceras fiestas con información sobre vuestra cuenta y vuestras preferencias concretas, como vuestras ciudades favoritas en un sitio de tiempo o vuestras preferencias de aerolínea en un sitio de viaje. El tiempo próximo vuestro browser conecta a aquel sitio, si una galleta ya existe, el sitio te recordará y quizás decir “Hola, Amigo.” Y si es un sitio de comercio electrónico, también puede recordar vuestro últimas pocas compras.

Las galletas no de hecho almacenan esta información en vuestro traditional PC o aparato móvil. Como teléfonos celulares que uso IMSIs como proxies, la galleta contiene un proxy para el dato que se mantiene a base de el fin posterior en el sitio. Cuando vuestro navegador carga una Página web con una galleta adosó, el dato adicional está estirado del sitio que es concreto a ti.

No sólo hacer las galletas almacenan vuestras preferencias de sitio personales, también proporcionan valiosos siguiendo dato para el sitio provinieron. Por ejemplo, si eres un cliente probable de una empresa y tú han anteriormente introdujo vuestro e-

alocución de correo u otra información para acceder un papel blanco, las casualidad son hay una galleta en vuestro navegador para aquella empresa's sitio que partidos, en el fin posterior, información aproximadamente tú en un cliente gestión récord (CRM) el sistema—dice, Salesforce o HubSpot. Ahora cada vez accedes que empresa's sitio, serás identificado a través de la galleta en vuestro navegador, y que la visita será grabada dentro del CRM.

Las galletas son segmented, significando que sitio web Un puede no necesariamente ver los contenidos de una galleta para sitio web B. Ha Habido excepciones, pero generalmente la información es separada y razonablemente seguro. De una perspectiva de intimidad, aun así, las galletas no te hacen muy invisibles.

Puedes sólo galletas de acceso en el mismo ámbito, un conjunto de recursos asignó a un specific grupo de personas. Agencias de anuncio cogen alrededor esto por cargar una galleta que puede seguir vuestra actividad en varios sitios que es parte de sus redes más grandes. En general, aun así, las galletas no

pueden acceder otro sitio's galletas. Los navegadores modernos proporcionan una manera para el usuario para controlar galletas. Por ejemplo, si tú surf la Web que utiliza incognito o privado explorando características, no retendrás un récord histórico dentro del navegador de vuestra visita a un sitio dado, ni adquieres una galleta nueva para aquella sesión. Si you tuvo una galleta de una visita más temprana, aun así, todavía aplicará en modo privado. Si estás utilizando el normal explorando característica, por otro lado, puedes de vez en cuando quiere manualmente sacar algunos o todo de las galletas adquiriste a lo largo de los años.

Tendría que notar que sacando todas las galletas no pueden ser aconsejables. Selectively Sacando las galletas que está asociado con uno-de visitas a sitios no te preocupas aproximadamente ayudará sacar rastros de tú del Internet. Sitios tú revisit ganado't ser capaz de verte, por ejemplo. Pero para algunos sitios, como un sitio de tiempo, podría ser tedioso de mantener escribiendo en vuestro código de cremallera cada vez visitas cuándo una galleta sencilla podría bastar.

Sacando las galletas pueden ser cumplidas por utilizar un añadir-encima o por ir a los encuadres or sección de preferencias de vuestro navegador, donde hay normalmente una opción para eliminar uno o más (incluso todo) de las galletas. Puedes querer determinar el destino de vuestras galletas en un caso-por-base de caso.

Algunos advertisers galletas de uso para seguir cuánto tiempo pasas en los sitios donde ellos've colocados sus anuncios. Algunos incluso graban vuestras visitas a sitios anteriores, qué está sabido como el referrer sitio. Tendrías que eliminar estas galletas inmediatamente. Reconocerás algunos de ellos porque sus nombres no contendrán los nombres del sites te visitó. Por ejemplo, en vez de CNN, “” un referrer la galleta se identificará como “Ad321.” También puedes querer considerar utilizando una galleta

herramienta de software más limpio, como el en [piriform.com/ccleaner](http://piriform.com/ccleaner), para ayudar dirigir vuestras galletas fácilmente.

hay, aun así, algunas galletas que es impervious a cualesquier decisiones haces en el lado de navegador. Estos se apellidan super galletas porque existen en vuestro ordenador, exterior de vuestro navegador. Super Las galletas acceden las preferencias de un sitio y siguiendo dato ningún asunto qué navegador utilizas (Chrome hoy, Firefox mañana). Y tendrías que eliminar super galletas de vuestro navegador, otherwise vuestro PC tradicional intentará para recrear galletas de http de memoria el tiempo próximo vuestro browser accesos el sitio.

hay dos concreto super galletas que vivos fuera de vuestro navegador que te puede eliminar—Centellear, de Adobe, y Silverlight, de Microsoft. Tampoco de estos super las galletas expira. Y es generalmente seguro de eliminarles.<sup>11</sup>

Entonces allí's la galleta más dura de ellos todo. Samy Kamkar, una vez famoso para crear el rápidamente extendiendo Myspace el gusano llamó Samy, ha creado algo llama Evercookie, el cual es sencillamente un muy, galleta muy persistente.<sup>12</sup> Kamkar conseguido esta persistencia por storing el dato de galleta en tan muchos sistemas de almacenamiento del navegador como posibles durante el sistema operativo de Ventanas. Mientras uno de los sitios de almacenamiento queda intacto, Evercookie intentará para restaurar la galleta en todas partes más.<sup>13</sup> Por ello sencillamente eliminando un Evercookie del almacenamiento de galleta del navegador cache no es bastante. Como los niños' juego whack-un-topo, Evercookies mantendrá reventar arriba. Necesitarás eliminar les completamente de vuestra máquina para ganar.

Si consideras cuántas galletas puedes ya have en vuestro navegador, y si multiplicas que por el número de áreas de almacenamiento potencial en vuestra máquina, puedes ver que serás en para una tarde larga y tarde.

No es sitios web justos y transportistas móviles que quiere seguir vuestras actividades on-line. Facebook ha acaecido ubiquitous—una programa allende medios de comunicación sociales justos. Puedes firmar en a Facebook y entonces utiliza que registro de Facebook mismo-en para firmar en a varias otras aplicaciones.

Qué popular es esta práctica? Al menos un informe de marketing encuentra que 88 por ciento de consumidores de EE.UU. haber logged en a un sitio web o la aplicación móvil que utiliza un existiendo identidad digital de una red social como Facebook, Twitter, y Plus de Google.<sup>14</sup>

hay pros y cons a esta comodidad—sabida como OAuth, un protocolo de autenticación que deja un sitio para confiarte en incluso si te don't introducir una

contraseña. Por un lado, él's un atajo: deprisa puedes acceder los sitios nuevos que utilizan vuestro existiendo contraseña de medios de comunicación sociales. Por otro lado, esto deja el sitio de medios de comunicación social a glean información sobre you para sus perfiles de marketing. En vez de justo sabiendo sobre vuestra visita a un sitio solo, sabe aproximadamente todos los sitios, todas las marcas utilizas su registro-en



información para. Cuando utilizamos OAuth, nosotros're dando arriba de intimidad muchísima por el bien de comodidad.

Facebook es quizás el más “pegajoso” de todas programa de medios de comunicación sociales. Logging Fuera de Facebook puede deauthorize vuestro navegador de acceder Facebook y sus Aplicaciones web. Además, Facebook añade rastreadores para controlar actividad de usuario que función incluso después de que tú're logged fuera, pidiendo información como vuestra ubicación geográfica, el cual sitios visitas, qué te clic encima dentro de sitios individuales, y vuestro Facebook username. Grupos de intimidad han expresado preocupación aproximadamente Facebook's intent para empezar siguiendo información de algunos de los sitios web y aplicaciones sus usuarios están visitando para mostrar anuncios más personalizados.

El punto es aquel Facebook , gusta Google, quiere dato aproximadamente te. No puede venir derecho fuera y pedir, pero encontrará maneras de cogerlo. Si enlazas vuestra cuenta de Facebook a otros servicios, la programa tendrá información aproximadamente te y *que* otro servicio o aplicación. Quizás utilizas Facebook para acceder vuestra cuenta de banco —si tú , sabe lo que institución financiera utilizas. Utilizando sólo una autenticación significas que si alguien coge a vuestra cuenta de Facebook, aquella persona tendrá el acceso a cada otro sitio web enlazó a aquella cuenta—incluso vuestra cuenta de banco. En el negocio de seguridad, habiendo qué llamamos un punto solo del fallo nunca es una idea buena. A pesar de que toma unos cuantos segundos más, él's fichaje de valor en a Facebook sólo cuándo necesitas a y firmando en a cada aplicación utilizas por separado.

Además, Facebook intencionadamente ha escogido no a honor el “no sigue” la señal enviada por Explorador de Internet en las tierras que hay “ningún consenso de industria” detrás lo.<sup>15</sup> Los rastreadores de Facebook entran las formas clásicas: galletas, Javascript, imágenes de un píxeles, e iframes. Esto deja apuntó advertisers para escanear y acceder galletas de navegador concreto y rastreadores para entregar productos, servicios, y anuncios, tanto encima y fuera Facebook.

Afortunadamente hay prórrogas de navegador que servicios de Facebook del bloque encima tercer-sitios de fiesta, p. ej., Facebook Disconnect para Chrome<sup>16</sup> y Lista de Intimidad del Facebook para Adblock Plus (cuál obra con ambos Firefox y Chrome).<sup>17</sup> Finalmente el gol de todo de este tapón-en las herramientas es para darte control sobre qué compartes con Facebook y cualquiera otras redes sociales como opposed a forzarte



para tomar un backseat y dejando el servicio estás utilizando para regir estas cosas para ti.

Dado que Facebook sabe sobre sus 1.65 miles de millones suscriptores, la empresa ha sido bastante benévola—tan lejos.<sup>18</sup> Él has una tonelada de datos, pero lo, gusta Google, ha escogido no para obrar encima todo de él. Pero aquello no lo significa no.

Más overt que galletas—e igualmente parásitos—es toolbars. El adicional toolbar ves en la copa de vuestro navegador de PC tradicional podría ser labeled YAHOO o MCAFEE o PEDIR . O puede llevar el nombre de cualquier número de otras empresas. Las casualidad eres don't recordar cómo el toolbar cogido allí. Ni nunca lo utilizas. Ni sabes cómo para sacarlo.

Toolbars Así dibujar vuestra atención fuera del a olbaraquello vino con vuestro navegador. El nativo toolbar te dejass para escoger qué motor de búsqueda para utilizar como el default. El parásito uno te tomará a su sitio de búsqueda propio, y los resultados pueden ser llenados con contenido patrocinado. Esto pasó a Gary Más, un residente de Hollywood Del oeste, quiénes lo fundan con el Ask.com toolbar y no manera clara para sacarlo. “Es como un malo houseguest,” dicho Más. “No dejará.”<sup>19</sup>

Si tienes un segundo o tercer toolbar, puede ser porque has descargado software nuevo o tuvo que actualizar existiendo software. Por ejemplo, si has Java instalado en vuestro ordenador, Oráculo, el fabricante de Java, automáticamente incluirá un toolbar a no ser que específicamente lo dices no a. Cuándo eras clicking a través de la descarga o actualizar screens, probablemente no notaste la caja de control minúscula que por default indicado vuestro consentimiento a la instalación de un toolbar. Hay nada ilegal sobre este; diste consentimiento, incluso si significa que te didn't optar fuera de tener instala automáticamente. Pero que toolbar deja otra empresa para seguir vuestros hábitos de Web y quizás cambiar vuestro default motor de búsqueda a su servicio propio también.

La manera mejor de sacar un toolbar es a uninstall lo la manera tú uninstall cualquier programa en vuestro PC tradicional. Pero algunos del más persistentes y parásitos toolbars te puede requerir para descargar una herramienta de traslado, y a menudo el proceso de uninstalling puede dejar detrás bastante información para dejar los agentes publicitarios narraron al toolbar a reinstall lo.

Cuándo instalando software nuevo o actualizando existiendo software, para atención a todas las cajas de control. Puedes evitar muchísimo hassle si te don't apalabrar la instalación de estos toolbars en primer lugar.

¿Qué si utilizas privado explorando, ha NoScript, HTTPS En todas partes, y periódicamente eliminas vuestro navegador's galletas y ajenos toolbars? Tendrías que ser seguro, bien? Nope. Todavía *puedes* ser seguido on-line.

Los sitios web son coded utilizando algo llamó Hypertext Markup Lengua, o HTML. Hay muchos las características nuevas disponibles en la versión actual, HTML5. Algunos de las características han acuciado la defunción del super galletas Silverlight y Centellear—cuál es una cosa buena . HTML5 Tiene, aun así, habilitado nuevo siguiendo tecnologías, quizás por accidente.

Uno de estos es aleta de telagerprinting, un on-line siguiendo herramienta que es fresco en un muy creepy manera. Tela fingerprinting usos el HTML5 elemento de tela para dibujar una imagen sencilla. Aquello's lo. El dibujo de la imagen tiene lugar dentro del navegador y no es visible a ti. Toma sólo una fracción de un segundo. Pero el resultado es visible al sitio web de pedir.

La idea es que vuestro hardware y software, cuándo combinado como recursos para el navegador, render la imagen singularmente. La imagen—podría ser una serie de variously colored las formas—es entonces convertidas a un número único, aproximadamente las contraseñas de manera son. Este número es entonces emparejado a casos anteriores de aquel número visto en otros sitios web alrededor del Internet. Y de aquel—el número de sitios donde aquello el número único está visto—un profile de sitios web visitas puede ser construido arriba. Este número, o tela fingerprint, puede soler identificar vuestro navegador siempre que regresa a cualquier sitio web particular que lo pidió, incluso si has sacado todas las galletas o galletas futuras bloqueadas de installing, porque utiliza un elemento construido a HTML5 él.<sup>20</sup>

Tela fingerprinting es un paseo-por proceso; no te requiere a clic o cualquier cosa pero sencillamente ver una Página web. Afortunadamente hay tapón-ins para vuestro navegador que lo puede bloquear. Para Firefox allí ha CanvasBlocker.<sup>21</sup> Para Google Chrome allí's CanvasFingerprintBlock.<sup>22</sup> Incluso el Tor el proyecto ha añadido su propio anticanvas tecnología a su navegador.<sup>23</sup>

Si utilizas este tapón-ins y seguir todo mis otras recomendaciones, podrías creer que que eres finalmente libres de on-line siguiendo. Y tú'd ser incorrecto.

Empresas como Drawbridge y Tapad, y Oráculo Crosswise, toma on-line siguiendo un paso más allá. Alegan para tener tecnologías que puede seguir vuestros intereses a través de aparatos múltiples, incluyendo sitios visitas sólo en vuestros teléfonos celulares y pastillas.

Algunos de este siguiendo es el resultado de aprendizaje de máquina y lógica difusa. Para example, si un aparato móvil y un PC tradicional tanto contactar un sitio que utiliza la misma alocución de IP, es muy posible que están poseídos por una persona sola. Por ejemplo

, dice buscas un elemento particular de ropa en vuestro teléfono celular, entonces cuándo coges home y es en vuestro PC tradicional, encuentras que elemento mismo de ropa en la sección “recientemente” vista del sitio web del detallista. Mejor todavía, dejado's dice compras el elemento de la ropa que utiliza vuestro PC tradicional. El más los partidos crearon entre distintos devices, el más probablemente es que una personaje sola está utilizando tanto de ellos. Drawbridge Reclamaciones solas enlazó 1.2 miles de millones usuarios a través de 3.6 miles de millones aparatos en 2015.<sup>24</sup>

Google, naturalmente, la misma cosa, tan hacer Manzana y Microsoft. Teléfonos de androide requieren t utiliza de una cuenta de Google. Aparatos de manzana utilizan una Manzana ID. Si un usuario tiene un smartphone o un portátil, el tráfico de Web generado por cada está asociado con un usuario concreto. Y los sistemas operativos de Microsoft más tardíos requieren una cuenta de Microsoft en ordenar to aplicaciones de descarga o para almacenar fotos y documenta utilizar el servicio de nube de la empresa.

La diferencia grande es aquel Google, Manzana, y Microsoft te dejas para inutilizar algunos o todo de esta actividad de colección del dato y retroactively eliminar dato recogido. Drawbridge, Crosswise, y Tapad marca el proceso de inutilizar y deletion menos claro. O puede sencillamente no ser disponible.

A pesar de que utilizando un proxy servicio o Tor es una manera conveniente de ocultar vuestra ubicación cierta cuándo accediendo el Internet, este enmascaramiento puede crear problemas interesantes o incluso backfire encima te, porque a veces on-line siguiendo puede ser justificado—especialmente cuándo una empresa de carta del crédito está intentando luchar fraude. Por ejemplo, vísperas justas Edward Snowden fue público, quiso crear un sitio web a support derechos on-line. Tuvo problema, aun así, pagando la empresa anfitriona para la inscripción con su carta de crédito.

En el tiempo, todavía utilizaba su nombre real, alocución de email real, y cartas de crédito personal—este era sólo antes de que caecía un pito - blower. También utilizaba Tor, el cual a veces provoca avisos de fraude de empresas de carta del crédito cuándo quieren verificar vuestra identidad y puede't reconciliar algunos de la información proporcionaste con qué han encima lima. Si, dice, vuestra cuenta de carta del crédito dice que vives en

Nueva York, por qué hace vuestro Tor nodo de salida dice que eres en Alemania? Una discrepancia de geolocalización así a menudo banderas un intento de adquirir abuso tan posible e invita escrutinio adicional.

Empresas de carta del crédito ciertamente nos siguen on-line. Saben todas nuestras compras. Saben donde tenemos suscripciones. Saben cuándo dejamos el país. Y saben siempre que utilizamos una máquina nueva para hacer una compra on-line.

Según Micah Lee del EFF, en uno señala Snowden era en su disco de habitación de hotel de Hong Kong ussing secretos de gobierno con Laura Poitras y Glenn Greenwald, un reportero del *Guardián*, y al propio tiempo era encima control con el departamento de apoyo del cliente en DreamHost, un proveedor de Internet basado en Los Ángeles. Aparentemente Snowden explicado to DreamHost que era en el extranjero y no confió en el servicio de Internet local, por ello su uso de Tor. Finalmente DreamHost aceptado su carta de crédito sobre Tor.<sup>25</sup>

Una manera para evitar este hassle con Tor es para configurar el torrec config lima para utilizar nodos de salida located en vuestro país de casa. Aquello tendría que mantener las empresas de carta del crédito felices. Por otro lado, constantemente utilizando los mismos nodos de salida finalmente podrían revelar quién eres. Hay algunos especulación seria que agencias de gobierno podrían controlar algunos salen nodas, así que utilizando diferentes unos hace sentido.

Otra manera de pagar sin dejar un rastro es para utilizar Bitcoin, una moneda virtual. Gusta más monedas, fluctúa en valorar basado en las personas de confianza tienen en él.

Bitcoin Es un algoritmo que deja personas para crear—o, en Bitcoin terminología, mina—su moneda propia. Pero si era fácil, todo el mundo lo haría. Así que no es. El proceso es computacionalmente intensivo, y toma un largo mientras sólo para crear uno Bitcoin. Así hay una cantidad finita de Bitcoin en existencia en cualquier día dado, y que, además de confianza de consumidor, influye su valor.

Cada Bitcoin tiene un cryptographic firma que lo identifica tan original y único. Las transacciones hicieron con aquel cryptographic la firma puede ser localizada atrás a la moneda, pero el método por qué obtienes la moneda puede ser ocultada—por ejemplo, por poner arriba de un rock-alocución de email anónima sólida y utilizando que alocución de email para poner arriba de un anónimo Bitcoin la cartera que utiliza el Tor red.

Compras Bitcoin en person, o anónimamente on-line utilizando prepaid cartas de regalo, o encontrar un Bitcoin ATM sin vigilancia de cámara. Según qué factores de vigilancia potencialmente podrían revelar vuestra identidad cierta, cada necesidades de riesgo para ser tomados a cuenta cuándo escogiendo qué purchasing método para utilizar. Puedes entonces puesto estos Bitcoins a qué's sabido como tumbler. Un tumbler toma algunos Bitcoins de mí, algunos de ti, y algunos de otras personas escogidas al azar y les mezcla junto. Mantienes el valor de las monedas minus el tumbling coste—él's sólo que el cryptographic la firma de cada moneda puede ser diferente después de que está mezclado con otros. Aquello anonymizes el sistema un poco.

Una vez les tienes, cómo almacenas Bitcoins? Porque hay no Bitcoin bancos, y porque Bitcoin no es moneda física, necesitarás utilizar un Bitcoin la cartera pone arriba anónimamente utilizando el detalló las instrucciones describieron más tarde en este libro.

Ahora que te've comprado y lo almacenó, cómo utilizas Bitcoin? Los cambios te dejan para invertir en Bitcoin y cambio él a otras monedas, como dólares de EE.UU., o bienes de compra en sitios como Amazon. Dice tienes uno Bitcoin, valorado en \$618. Si sólo necesitas alrededor \$80 para una compra, entonces retendrás un porcentaje seguro del valor original, según el tipo de cambio, después de la transacción.

Las transacciones están verificadas en un públicos ledger sabidos como blockchain e identificados por alocución de IP. Pero como nosotros have vistos, alocuciones de IP pueden ser cambiadas o fingió. Y a pesar de que los mercaderes han empezado aceptando Bitcoin, los costes de servicio, típicamente pagados por el mercader, ha sido transferido al comprador. Además, cartas de crédito diferente, Bitcoin permisos ningún reembolso or reimbursements.

Puedes acumular tanto Bitcoin como tú moneda dura. Pero a pesar de su éxito global (el Winklevoss hermanos, famosos para Marca desafiante Zuckerberg sobre el fundando de Facebook, es inversores importantes en Bitcoin), el sistema ha tenido algunos fallos monumentales también. En 2004, Mt. Gox, un basado en Tokyo Bitcoin cambio, bancarrota declarada después de anunciar que su Bitcoin había sido robado. Ha Habido otros informes de robo entre Bitcoin cambios, el cual, diferente la mayoría de EE.UU. amontonan accounts, no es asegurado.

Todavía, a pesar de que ha habido varios intentos en moneda virtual antiguamente, Bitcoin ha acaecido el Internet's moneda anónima estándar.

Una obra en progreso, sí, pero una opción para cualquiera buscando intimidad.

Podrías sentir invisible ahora mismo—ocultando vuestra alocución de IP con Tor; encriptando vuestro email y mensajes de texto con PGP y Señal. He no, aun así, habló mucho aproximadamente hardware—cuáles pueden soler ambos te encontráis y esconderte encima el Internet.

## CAPÍTULO SIETE

### **Paga Arriba o Más!**

La pesadilla empezó on-line y acabada con agentes federales storming una casa en Blaine suburbano, Minnesota. Los agentes hubieron sólo una alocución

de IP asociada con descargas de pornografía del niño e incluso una amenaza de muerte en contra Vicepresidente Joe Biden. Por contacting el proveedor de servicio del Internet asociado con aquella alocución de IP, los agentes adquirieron el usuario's alocución física. Aquella clase de seguir era espalda muy exitosa en los días cuándo todo el mundo todavía tuvo una conexión alambrada a sus módems o routers. En aquel tiempo, cada alocución de IP podría ser físicamente localizada a una máquina dada.

Pero hoy más las personas utilizan conexiones inalámbricas dentro de sus casas. Inalámbrico deja todo el mundo dentro para mover alrededor de la casa con aparatos móviles y quedar conectado al Internet. Y si tú're no prudente, también deja vecinos para acceder que señal misma. En este caso los agentes federales stormed la casa incorrecta en Minnesota. Realmente quisieron la casa puerta próxima a él.

En 2010, Barry Vincent Ardolf abogado culpable a cargos de cortaring, robo de identidad, posesión de pornografía de niño, y haciendo amenazas en contra Vicepresidente Biden. Réconds de corte asoman que el problema entre Ardolf y su vecino empezó cuándo el vecino, quién era de hecho un abogado y no fue nombrado, archivó un informe policial que dice que Ardolf presuntamente “inappropriately tocado y dio un beso” el abogado toddler en la boca.<sup>1</sup>

Ardolf entonces utilizó la alocución de IP de la casa inalámbrica de su vecino router a 75

Abierto Yahoo y Myspace cuentas en el nombre de su víctima. Era de estas cuentas de falsificación que Ardolf lanzados una campaña para avergonzar y causar problemas legales para el abogado.

Muchos ISPs ahora proporcionar su casa routers con las capacidades inalámbricas construyeron en.<sup>2</sup> Algún ISPs, como Comcast, es creating un segundo Wi-Fi abierto servicio encima que te ha limitado control. Por ejemplo, puedes ser capaz de cambiar unos cuantos encuadres, como la capacidad de girarlo fuera. Tendrías que ser consciente de él. Alguien en una furgoneta aparcada delante de vuestra casa podría ser utilizar vuestro libre inalámbrico. A pesar de que no tienes que extra de paga para aquel, todavía podrías notar una degradación leve en velocidad de Wi-Fi si hay uso pesado de la segunda señal. Puedes inutilizar Comcast Xfinity Casa Hotspot si te don't pensarte nunca necesitará dar visitantes a vuestra casa acceso de Internet libre.<sup>3</sup>

Mientras construido-en inalámbrico es sumo para cogerte arriba y corriendo con un servicio nuevo, a menudo estos de banda ancha routers no es configurado propiamente y puede crear problemas cuándo no son asegurados. Para una cosa, unsecured el acceso inalámbrico podría proporcionar un punto digital de entrada a vuestra casa, como hizo para Ardolf. Mientras los intrusos no podrían ser después de vuestras limas digitales, podrían ser mirar para causar problemas empero.

Ardolf Era ningún genio de ordenador. Confesó en cortejar que él didn't saber la diferencia entre WEP (intimidad equivalente alambrada) encriptación, el cual era lo que el vecino router utilizado, y WPA (Wi-Fi protegió acceso) encriptación, el cual es mucho más seguro. Era sólo enojado. Esto es sólo uno más razón por qué tendrías que tomar un momento para considerar la seguridad de vuestra casa propia red inalámbrica. Nunca sabes cuándo un vecino enojado podría intentar utilizar vuestra red de casa en contra te.

Si alguien algo malo en vuestra red de casa, hay algunos protection para el router dueño. Según el EFF, los jueces federales han rehusado BitTorrent los pleitos trajeron por titulares de copyright porque el defendants exitosamente alegó que alguien más descargó las películas que utilizan sus redes inalámbricas.<sup>4</sup> El EFF states que una alocución de IP no es una persona, significando que los suscriptores inalámbricos no pueden ser responsables para las acciones de otros utilizando sus redes inalámbricas.<sup>5</sup>



A pesar de que ordenador forensics aclarará una persona inocente de quién Wi-Fi estuvo utilizado en la comisión de un felony—como hizo en el caso del abogado de Minnesota—por qué pasa por todo aquello?

Incluso si utilizas un telefónico-dial basado-arriba módem o un cable-basó ASM (cualquier- fuente multicast) router (disponible de Cisco y Belkin, entre otros), estos aparatos han tenido su acción de software y problemas de configuración.

En primer lugar, descarga el más tardío firmware (el software instalado en un aparato de hardware). Puedes hacer que por acceder el router's pantalla de configuración (ve abajo) o por visitar el sitio web del fabricante y buscando actualizaciones para vuestra marca particular y modelo. Hacer este tan a menudo tan posible. Uno manera fácil para actualizar vuestro router's firmware es para comprar un nuevo uno cada año. Esto puede coger caro, pero asegurará que tienes el más tardío y más sumo firmware. Segundo, actualización vuestro router encuadres de configuración. No quieres el default encuadres.

Pero primero: qué's en un nombre? Más de piensas. Común a ambos el ISP- proporcionados router y un router te comprados en Mejores Compra es el nombrando. Todo inalámbrico routers emisión por default qué está llamado un identificador de conjunto del servicio (SSID).<sup>6</sup> El SSID es generalmente el nombre y modelo de vuestro router, p. ej., “Linksys WRT54GL.” Si miras en las conexiones inalámbricas disponibles en vuestra área, verás qué I malo.

Retransmitiendo el default SSID fuera al mundo puede enmascarar el hecho que la señal de Wi-Fi de hecho está proviniendo una casa concreta, pero también deja alguien en la calle para saber la marca exacta y modelo del router te propio. Por qué es que malo? Aquella persona puede also saber las vulnerabilidades de aquella marca y modelo y ser capaz de explotarles.

Tan qué cambias el nombre del router y actualizar su firmware?

Accediendo el router es fácil; haces tan de vuestro navegador de Internet. Si no tienes las instrucciones para vuestro router, allí's una lista on-line de URLs aquello te dices qué para escribir a vuestra ventana de navegador así que puedes conectar directamente al router en vuestra red de casa.<sup>7</sup> después de escribir en el local URL (tú're justo hablando al router, recuerda, no al Internet en grande), tendrías que ver un registro-en pantalla. Tan qué es el username y contraseña para el registro-en?



Resulta que hay una lista de default registro-ins publicado en el Internet también.<sup>8</sup> En el Linksys ejemplo encima, el username es el espacio y la contraseña es “admin.” Needless Para decir, una vez eres dentro del router's pantalla de configuración, inmediatamente tendrías que cambiar su default contraseña, siguiendo el consejo te diste más temprano aproximadamente creando contraseñas únicas y fuertes (ve [aquí](#)) o utilizando una gerente de contraseña.

Recuerda para almacenar esta contraseña en vuestra gerente de contraseña o escribirlo abajo, como tú probablemente ganado't necesidad de acceder vuestro router muy a menudo. Tener que

olvidas la contraseña (realmente, qué a menudo eres yendo para ser en la pantalla de configuración para vuestro router?), don't preocupación. Hay un botón de reinicialización físico que restaurará el default encuadres. Aun así, en dirigir un físico, o duro, reinicialización, también tienes que reenter todos los encuadres de configuración I'm aproximadamente para explicar abajo. Así que escribe abajo el router encuadres o tomar screenshots e imprimirles fuera siempre que estableces router encuadres que es diferente del default. Estos screenshots será valioso cuándo necesitas a reconfigure vuestro router.

Sugiero que cambias “Linksys WRT54GL” a algo inocuo, como “HP Inkjet,” así que lo ganado't ser obvio a desconocidos qué casa la señal de Wi-Fi podría ser provenir. A menudo utilizo un nombre genérico, como el nombre de mi complejo de apartamento o incluso el nombre de mi vecino.

hay también una opción para esconder vuestro SSID enteramente. Aquello significa otros no serán capaces a fácilmente verlo listado como conexión de red inalámbrica.

Mientras tú're dentro de vuestro básico router encuadres de configuración, hay varios tipos de seguridad inalámbrica para considerar. Estos son generalmente no habilitados por default. Y no toda encriptación inalámbrica está creada igual, ni es apoyado por todos los aparatos.

La forma más básica de encriptación inalámbrica, intimidad equivalente alambrada (WEP), es inútil. Si lo ves como una opción, don't incluso considerarlo. WEP Ha sido agrietado para años, y es por tanto ya no recomendado. Único viejo routers y aparatos oferta quieta él como opción de legado. En cambio, escoge uno de la encriptación más nueva, más fuerte niveles, como Wi-Fi protegió acceso, o WPA. WPA2 Es aún más seguro.

Girando encima encriptación en el router significa que los aparatos que conectan a él también necesitará emparejar encryption encuadres. La mayoría de aparatos nuevos automáticamente notan el tipo de ser de encriptación

utilizó, pero los modelos más viejos todavía te requieren para indicar manualmente qué nivel de encriptación estás utilizando. Siempre utilizar el nivel más alto posible. Tú're sólo tan seguro como vuestro enlace más débil, así que marca seguro a max fuera del aparato más viejo en plazos de su encriptación disponible.

Habilitante WPA2 significa que cuándo conectas vuestro portátil o aparato móvil, también necesitarás poner lo a WPA2, a pesar de que algunos los sistemas operativos nuevos reconocerán el tipo de encriptación automáticamente. Sistemas operativos modernos en vuestro teléfono o el portátil identificarán el Wi-Fi disponible en vuestra área. Vuestro SSID emisión (ahora “HP Inkjet”) tendría que parecer en la lista en o cerrar hasta arriba. Iconos de candado dentro de la lista de conexiones de Wi-Fi disponible (normalmente

overlaid a la fuerza de cada conexión) indica qué conexiones de Wi-Fi requieren contraseñas (el vuestro ahora tendría que tener un candado).

De la lista de conexiones disponibles, clic por tu cuenta SSID. Tendrías que ser apuntado para introducir una contraseña—ser seguro para hacerlo al menos quince caracteres. O utilizar una gerente de contraseña para crear una contraseña compleja. Para conectar a vuestra contraseña-Wi-Fi protegido, tendrás que tipo en aquella contraseña al menos una vez en cada aparato para connect, así que una gerente de contraseña no podría obrar en todos los casos, particularmente cuándo tienes que recordar la contraseña compleja y tipo él en más tardío tú. Cada aparato que—incluye vuestro “refrigerador” listo y televisión digital— todos utilizan el router contraseña has escogido cuándo pusiste la encriptación en vuestro router. Necesitarás hacer este una vez para cada aparato que accesos vuestra casa o Wi-Fi de oficina, pero te ganado't tiene que él otra vez a no ser que cambias vuestra contraseña de red de la casa o adquirir un aparato nuevo.

También puedes ir uno da un paso más allá y conexiones de Wi-Fi del límite sólo a los aparatos específicas. Esto está sabido como whitelisting. Con este proceso concedes acceso a (whitelist) algunos aparatos y prohibir (blacklist) todo más. Esto te requerirá para introducir vuestro devla alocución de control de acceso de medios de comunicación del hielo, o MAC alocución. También significará que cuándo tú luego upgrade vuestro teléfono celular, lo tendrás que añadir al MAC alocución en vuestro router antes de que conectará.<sup>9</sup> Esta alocución es única a cada aparato; de hecho, los primeros tres conjuntos de caracteres (octetos) es el fabricante's código, y la final tres es único al producto. El router rehusará cualquier aparato cuyo hardware MAC no ha sido anteriormente almacenó. Aquello dijo, un hacker la herramienta llamó

aircrack-ng puede revelar el autorizado MAC dirección de un usuario actualmente conectado y entonces una lata atacante spoof el MAC dirección para conectar al inalámbrico router. Sólo gustar escondido inalámbrico SSIDs, es trivial a bypass MAC la dirección que filtra.

Encontrando el MAC la dirección en vuestro aparato es relativamente fácil. En Ventanas, va al botón de Inicio, tipo “CMD,” Orden “de clic Puntual,” y en el inverted caret, tipo “IPCONFIG.” La máquina regresará una lista larga de datos, pero el MAC la dirección tendría que ser allí, y constará de doce hexadecimal characters con cada dos caracteres separaron por un colon. Para productos de Manzana es incluso más fácil. Va al icono de Manzana, selecciona “Preferencias de Sistema,” e ir a Red. “” Entonces clic el aparato de red en la panel izquierda e ir a Hardware>Adelantado, y verás el MAC dirección. Para algunos productos de Manzana más viejos, el procedimiento es: Preferencias de Sistema>de icono de Manzana>las redes>Construidas-en Ethernet. Puedes encontrar el MAC dirección para

vuestro iPhone por seleccionar General>de Encuadres>Aproximadamente y mirando debajo “Dirección de Wi-Fi.” Para un Android teléfono, va a Encuadres>Aproximadamente Estado>de Teléfono, y cariz debajo “Wi-Fi MAC dirección.” Estas direcciones pueden cambiar basadas en el aparato y modelo estás utilizando.

Con estos doce-dígito MAC direcciones a mano, ahora necesitarás decir el router para dejar sólo else aparatos y bloquear todo más. hay unos cuantos downsides. Si un huésped viene encima y quiere conectar a vuestra red de casa, tendrás que decidir si para dar uno de vuestros aparatos y su contraseña a aquella persona o sencillamente turno de MAC dirección filtering por reentering el router pantalla de configuración. También, hay tiempo cuándo podrías querer cambiar el MAC dirección de un aparato (ve [aquí](#)); si te don't cambio él atrás, no podrías ser capaz de conectar a vuestro MAC-red de Wi-Fi restringido en casa u obra. Afortunadamente, rebooting el aparato restaura el original MAC dirección en más casos.

Para hacer conectando cualquier aparato nuevo a una casa router fácil, la Alianza de Wi-Fi, un grupo de vendedores ansiosos de extender el uso de tecnologías de Wi-Fi, creados Wi-Fi protegidos setup (WPS). WPS Estuvo anunciado como manera para cualquiera—I malo cualquiera—a securely conjunto arriba de un aparato móvil en casa o en la oficina. En realidad, aun así, no es muy seguro.

WPS Es típicamente un botón que te empujón en el router. Otros métodos incluyen uso de un ALFILER y comunicación de campo cercano (NFC).

Sencillamente puesto, activas el WPS característica, y comunica con cualesquier aparatos nuevos tienes en vuestra casa u oficina, automáticamente sincronizándoles para obrar con vuestra red de Wi-Fi.

Los sonidos sumos. Aun así, si el router es fuera en público “”—decir, en vuestro salón—entonces cualquiera puede tocar el WPS botón y unir vuestra red de casa.

Incluso sin acceso físico, un atacante on-line puede utilizar brute fuerza para adivinar vuestro WPS ALFILER. Podría tomar varias horas, pero él's todavía un método de ataque viable, uno te tendrías que proteger en contra por inmediatamente girando de WPS en el router.

Otro WPS método de ataque está sabido como Pixie Polvo. Esto es un ataque off-line y afecta sólo unos cuantos fabricantes de chip, incluyendo Ralink, Realtek, y Broadcom. Pixie Obras de polvo por ayudar hackers acceso de beneficio a las contraseñas en inalámbricos routers. Básicamente la herramienta es muy sincera y puede obtener acceso a un aparato en segundos u horas según la complejidad del escogido o generado WPS ALFILER.<sup>10</sup> Para example, uno tal programa, Reaver, puede agrietar un

WPS-habilitó router dentro de varias horas. En general, es una idea buena de girar de WPS. Sencillamente puedes conectar cada aparato móvil nuevo a vuestra red por escribir en cualquier contraseña has asignado para acceso.

Así que has impedido, a través del uso de encriptación y contraseñas fuertes, el uso de vuestra casa inalámbrica router red por otros. Hace aquel malo que nadie puede coger dentro de vuestra red de casa o incluso digitalmente ver dentro de vuestra casa? No enteramente.

Cuándo instituto sophomore Blake Robbins se apellidó al principal's oficina de su escuela de Filadelfia suburbana, no tuvo ninguna idea estuvo a punto de ser reprimanded para “comportamiento impropio”—en casa. El más Bajo Merion Distrito Escolar, Filadelfia exterior, había dado todo su alumnado de instituto, incluyendo Robbins, nuevo MacBooks para utilizar para su obra de curso. Qué el distrito escolar didn't decir el alumnado era que el software diseñó para recuperar los aparatos en el caso estuvieron perdidos también podría soler monitor todo 2,300 alumnado' comportamiento mientras eran en vista de los portátiles' webcams.

Robbins's Alegó offense? La píldora que revienta. El Robbins familia, a través de su abogado, mantuvo todo a lo largo de aquel el chico sencillamente comía Mike y caramelo de Ike mientras haciendo sus deberes.

Por qué era esto incluso un asunto?

El distrito escolar mantiene activó el software que sigue robo sólo después de que uno de sus portátiles estuvo robado. Obras de software que siguen robo así: cuándo alguien utilizando el software informa que suyo o su portátil ha sido robado, la escuela puede registro encima a un sitio web y ver imágenes del portátil robado's webcam así como oye sonidos del micrófono. Un administrador escolar entonces podría controlar el portátil y tomar cuadros como necesitó. De este modo el aparato puede ser localizado y returned y la fiesta culpable puede ser identificada. Aun así, en este caso estuvo alegado que los oficiales escolares giraban en esta característica para espiar en el alumnado mientras eran en casa.

La webcam en Robbins escolar-emitado Mac el portátil grabó centenares de fotos, incluyendo algún del chico dormido en su cama. Para otro alumnado era peor. Según testimonio de corte, la escuela hubo aún más cuadros de algún alumnado, unos cuantos de quien era “parcialmente desnudó.” Esto podría haber continuado inadvertido por el alumnado hubo Robbins no sido reprimanded para algo presuntamente hizo en casa.

Robbins, junto con un estudiante anterior, Jalil Hasan—quién hubo casi cincocientas

imágenes tomadas de él y cuatrocientas imágenes de su pantalla de ordenador captaron, revelando su actividad on-line y los sitios visitó—demandado el distrito escolar. Robbins Recibió \$175,000 y Hasan \$10,000.<sup>11</sup> El distrito también pagado casi medio un millón de dólares para cubrir los chicos' gastos legales. En total el distrito escolar tuvo que pagar fuera, a través de su asegurador, unaronda \$1.4 millones.

Él's fácil para malicious software para activar la webcam y micrófono en un PC tradicional sin el usuario que lo conoce. Y esto es cierto en un aparato móvil también. En este caso era una acción deliberada . Pero todo demasiado a menudo no es. Uno rápidamente fija es para poner cinta sobre la webcam en vuestro portátil hasta que pretendes utilizarlo otra vez.

En la caída de 2014, Sophie Curtis, un reportero para el *Telégrafo basado en Londres*, recibió una petición de conexión del LinkedIn en un email que parecido para provenir alguien quién obró en su diario. Era la clase de email que Sophie recibió todo el tiempo, y como cortesía profesional ella didn't piensa dos veces aproximadamente aceptando él de un colega. Un par de semanas más tarde recibió un email que parecido para ser de un pito anónimo-blower organización que estuvo a punto de emisión documentos sensibles. Como reportero quién había cubierto agrupa como Anónimo y

WikiLeaks, hubo received emails así antes de que, y era curiosa sobre la petición. El anexo de lima pareció una lima estándar, así que ella clicked para abrirlo.

Inmediatamente se dio cuenta algo era mal. Defensor de Windows, la seguridad programa aquello viene con cada copia de Ventanas, empezó emitir avisos en su desktop. Y los avisos mantuvieron piling arriba en la pantalla.

Curtis, como personas muchísimas hoy, había sido burlado a clicking en un anexo que pensó era una lima normal. Mientras fingiendo tener information quiso ver, la lima descargada y desempaquetó una serie de otras limas que dejó el atacante remoto para tomar control completo sobre su ordenador. El malicious el software incluso tomó un cuadro de su con su webcam propia. En él su cara aguanta un lovale de sheer frustración como intenta entender cómo alguien podría haber tomado sobre su ordenador.

De hecho Curtis supo lleno bien quién había tomado sobre su ordenador. Como un experimento, unos cuantos meses más tempranos había contratado una penetración tester, o bolígrafo tester. A Alguien le gusto. Las personaje y las empresas contratan profesionales hackers para probar para romper a la red de ordenador de una empresa para ver donde necesitan fortificación. En el caso de Curtis, el proceso estuvo extendido fuera sobre varios meses.

En el inicio de trabajos así, siempre intento coger tanta información sobre el cliente como puedo. Paso aprendizaje de tiempo sobre su o su vida y hábitos on-line. Sigo el cliente's postes públicos a Twitter, Facebook, y, sí, incluso LinkedIn. Cuál es exactamente qué Sophie Curtis bolígrafo tester hizo. Entre todos sus emails era uno mensaje construido cuidadosamente— el primer un enviado por su bolígrafo tester. El bolígrafo tester supo que obró como reportero y supo que era abierta a e- correo solicitations de anteriormente personaje desconocidas. En aquel primer case Curtis más tarde escribió que no hubo bastante contexto para su para ser interesado en entrevistar una persona particular para una historia futura. Pero estuvo impresionada por la cantidad de investigar el hacker y sus colegas en la empresa de seguridad hicieron.

Curtis dijo: “eran capaces de utilizar Twitter para descubrir mi alocución de email de la obra, así como algunos de mis ubicaciones recientes y el nombre de una noche social regular atiendo con otros periodistas. De objetos en el fondo de uno de las fotos hube posted encima Twitter eran capaces de descubrir qué teléfono celular utilicé para utilizar, y el hecho que mi prometido utilizó para fumar corro-ups (era una foto vieja), así como el

hecho le gusta el ciclismo.”<sup>12</sup> Cualquiera de estos detalles podría haber sido la base para otro email.

Allí ha también una Inteligencia Artificial nueva—la herramienta basada anunciada en el DEF CON 2016 conferencia que analizará los tweets de un objetivo. Entonces construirá una lanza-phishing el email basado en sus intereses personales.<sup>13</sup> Así que ser prudente cuándo clicking enlaces dentro de un tweet.

De hecho, a menudo es las pocas cosas —el comentario extraño posted aquí o allí, el único knickknack en la balda detrás tú en una foto, la camiseta de un campamento una vez atendiste—aquello proporciona información personal crucial que te nunca habría pretendido para compartir públicamente. Podemos considerar estos un-de momentos harmless, pero el más detalles un atacante puede aprender aproximadamente te, el mejor puede burlar tú a opening arriba anexos de email, y tomar sobre vuestro mundo on-line.

Curtis señala fuera que el bolígrafo-equipo de prueba acabó su ataque allí. Tuvo ellos ser reales criminales hackers, el divertidos y los juegos podrían haber continuado para algún tiempo, quizás con los tipos malos que obtienen acceso a sus cuentas de medios de comunicación sociales, su red de oficina en el *Telégrafo*, incluso sus cuentas financieras. Y más probablemente lo habrían hecho de tal manera que Curtis no podría haber sabido su ordenador había sido compromised; la mayoría de ataques no inmediatamente Defensor de Ventanas del gatillo o antivirus software. Algunos atacantes entran y persistir para los meses o los años antes del usuario tiene cualquier pista que él o ella ha sido cortados. Y no es sólo vuestro portátil: un email-el ataque provocado también podría ser lanzado

de un jailbroken iPhone o un Androide aparato móvil.

Mientras Google y otros proveedores de email escanean vuestros mensajes para impedir la transmisión de malware y la propagación de pornografía on-line—y para recoger dato publicitario—ellos no necesariamente escáner para fraude. Gusta intimidad, el nivel para qué, como he dicho, es diferente para todo el mundo, el fraude es duro de cuantificar. Y no siempre lo reconocemos, incluso cuándo él's staring nos en la cara.

Dentro del ente del email de Linkedin de la falsificación de Curtis era un un-por-píxel de una pulgadas, un tiny punto de una imagen, invisible al ojo, como aquellos I dichos podría ser encontrado en sitios web y utilizados para seguirte on-line. Cuándo aquellas llamadas de punto minúsculas fuera, dice un servidor de seguir en una ubicación remota, el cual podría ser anywhere en el mundo, qué cronometra abriste el email, cuánto tiempo quedó en la



pantalla, y en qué aparato lo abriste. También puede decir si salvaste, enviado, o eliminó el mensaje. Además, si el escenario utilizado por el bolígrafo- equipo de prueba había sido real, el atacante podría tener incluíd un enlace a través de qué Curtis podría haber visitado una página de LinkedIn de la falsificación. Esta página se parecería a un real uno en todos los respetos exceptúa que sería hosted en un servidor diferente, quizás en otro país.

Para un advertiser, este bug de Web puede soler gatsu información aproximadamente (y por eso perfil) el recipient. Para atacantes, puede soler obtener los detalles técnicos necesitan diseñar su ataque próximo, el cual incluiría una manera de coger dentro de vuestro ordenador. Por ejemplo, si estás corriendo una versión vieja de un navegador, puede haber bugs que puede ser explotado.

Así que el segundo email Curtis recibió del bolígrafo testers incluído un anexo, un documento comprimido puesto para explotar una vulnerabilidad en el software que solió abre la lima (p. ej., Adoes Acróbata ). Cuando hablamos de malware, más las personas piensan de los virus de ordenador del tempranos 2000s, cuando un email infectado solo podría extender adicional infectó emails a todo el mundo en una lista de contacto. Estos tipos de masa-ataques de infección son menos common hoy, en parte debido a cambios a software de email él. En cambio el más peligroso malware hoy es mucho más sutil y a menudo apuntado y tailored a una personaje. Como era en el caso de Sophie Curtis. El bolígrafo testers utilizado una forma especial de phishing lanza llamada phishing, diseñado para apuntar una persona concreta.

Phishing Es el criminally proceso fraudulento de probar para obtener información sensible como usernames, contraseñas, y carta de crédito o información

de banco. Ha sido utilizado contra CFOs quiénes están engañados a alambrar sumas grandes de dinero porque el “CEO” ha autorizado el traslado. Normalmente, el phishing email o mensaje de texto incluye un elemento de acción como clicking un enlace o abriendo arriba de un anexo. En el caso de Curtis el intent era para plantar malware en su ordenador para el propósito de ilustrar qué fácil es para alguien para hacer este.

Uno del más famoso phishing los esquemas era Operación Aurora , en qué un phishing el email estuvo enviado a empleados chinos de Google. La idea era para infectar sus máquinas en China para acceso de beneficio a la red interna en Google's sede mundial, en Vista de Montaña, California. Esto los



atacantes , cogiendo peligrosamente cerrar al código de fuente para el motor de búsqueda de Google. Google no fue sólo. Empresas como Adobe intrusiones similares informadas. Como Google de resultado brevemente estiró sus operaciones de China.<sup>14</sup>

Siempre que cogemos un LinkedIn o petición de Facebook, nuestro guardia es abajo. Quizás porque confiamos en aquellos sitios, también confiamos en sus mensajes de email. Y todavía, como hemos visto, cualquiera puede oficio un mensaje que los carices legitiman. En persona, normalmente podemos notar cuándo alguien está llevando una falsificación mustache o implantes de cabello o hablando en una voz falsa; tenemos siglos' valor de instintos evolutivos para ayudarnos detectar engaño sin pensar aproximadamente lo. Aquellos instintos don't aplica on-line, al menos no para la mayoría de nosotros. Sophie Curtis era una reportera ; era su trabajo para ser curioso y escéptico, para seguir ventajas y hechos de control. Podría haber mirado a través del *Telégrafo* employee lista para ver quién la persona encima LinkedIn era y aprendió que el email era probablemente falsificación. Pero ella no. Y la realidad es que la mayoría de nosotros es igualmente unguarded.

Un atacante quién es phishing tendrá algunos pero no todo de vuestra información personal—the poco mordió tiene sirve como su cebo. Por ejemplo, un phisher te podría enviar un email que incluye los últimos cuatro dígitos de vuestro número de carta del crédito para establecer confianza, entonces ir en para pedir aún más información. A veces los cuatro dígitos son incorrect, y el phisher pedirá que haces cualesquier correcciones necesarias en vuestra respuesta. No él. En corto, don't interaccionar con un phisher. En general no responde a cualesquier peticiones para información personal, incluso si parecen fidedignos. En cambio, contacto el requester en un email separado (si tienes la alocución) o texto (si tienes la celda-número de teléfono).

El más respecto de phishing el ataque es uno aquello's utilizado para burlar un objetivo a hacer un elemento de acción que directamente explota su o su ordenador, dando el control lleno atacante. Aquello es qué hago en compromisos de ingeniería social.

Credential Cosechando es también una línea popular de ataque, donde una persona's username y la contraseña está captada, pero el peligro real de lanza phishing está obteniendo acceso al sistema de ordenador del objetivo y red.

Qué si interaccionaste con un phisher y como resultar perdido todo el dato—todas las fotografías personales y documentos privados—en vuestro PC

infectado o aparato móvil? Aquello es qué pasado a autor Alina la madre de Simone. Escritura en el *New York Times*, Simone describió qué era gusta para su madre—quién no fue tecnológicamente inclinado—para ser arriba contra un enemigo sofisticado quién utilizaba algo llamó ransomware.<sup>15</sup>

En 2014 una ola de extortionist malware pegado el Internet, targeting personaje y empresas igualmente. Cryptowall Es un ejemplo: encripta vuestro paseo duro entero, cerrando tú fuera de cada lima hasta que pagas el atacante de darte el clave a unlock vuestras limas. A no ser que tienes una copia de seguridad llena, los contenidos de vuestro traditional PC o aparato de Androide serán inaccesibles hasta que pagas el rescate.

Don't quiere paga? La letra de extorsión que parece en la pantalla de exposición declara que el clave a unlock las limas serán destruidas dentro de una cantidad segura de tiempo. A menudo hay un reloj de cuenta atrás incluido. Si te don't paga, la fecha límite es a veces extendida, a pesar de que los aumentos de precio con cada retraso.

En general tendrías que evitar clicking encima anexos de email (a no ser que les abres en Google Google o Vista Rápidos Docs). Todavía, hay otras maneras en qué Cryptowall anuncios—de pancarta de las propagaciones en sitios web, por ejemplo. Sólo viendo una página con un anuncio de pancarta infectado puede infectar vuestro PC tradicional—esto se apellida un paseo-por porque te didn't activamente clic en el anuncio. Aquí es donde teniendo anuncio-tapón de traslado-ins como Adblock el plus en vuestro navegador es realmente eficaz.

En los primeros seis meses de 2015, el FBI's Centro de Queja de Delito de Internet (IC3) grabó casi mil casos de Cryptowall 3.0, con las pérdidas estimaron para ser alrededor \$18 million. Esta cifra incluye rescate que estuvo pagado, el coste a ÉL departamentos y tiendas de reparación, y productividad perdida. En algunos casos el encriptó las limas contienen personalmente información identificable como números de Seguridad Social, los cuales pueden capacitar el attack como ruptura de datos y así incurrir más costes.

A pesar de que el clave a unlock las limas siempre pueden ser adquiridas para un coste plano de 500 \$a 1000, \$quienes están infectados típicamente probar otro medio—como romper la encriptación ellos—para sacar el ransomware. Aquello es qué

Simone la madre probó. Cuándo finalmente llamó su hija, eran casi fuera de tiempo.

Casi todo el mundo quién intenta romper el ransomware la encriptación falla. La encriptación es realmente fuerte y requiere ordenadores más poderosos y más tiempo para romperlo que más las personas tienen en su disposición. Así que las víctimas normalmente paga. Según Simone, el Dickson Condado, Tennessee, sheriff's la oficina pagada en noviembre 2014 un Cryptowall rescate a unlock 72,000 informes de autopsia, declaraciones de testigo, fotografías de escena del delito, y otros documentos.

El hackers a menudo pago de demanda en Bitcoin, significando que muchos las personas medianas tendrán un tiempo duro que paga.<sup>16</sup> Bitcoin, como mencioné, es un descentralizado, peer-a-peer moneda virtual, y más las personas no tienen Bitcoin las carteras disponibles para retirada.

Durante la pieza de Tiempo, Simone acuerda lectores que nunca tendrían que pagar el rescate—aún así ella sólo que al final. De hecho el FBI ahora asesora personas cuyos ordenadores están infectados con ransomware a sencillamente paga arriba. Joseph Bonavolonta, el ayudante agente especial en cargo del FBI cyber y programa de contrainteligencia en Boston, dicho, “para ser sincero, a menudo asesoramos personas sólo para pagar el rescate.” Dijo ni siquiera el FBI es capaz de agrietar el ultrasecure la encriptación utilizada por el ransomware autores, y añadió que porque tantas personas han pagado los atacantes, el \$500 coste ha quedado bastante compatible a lo largo de los años.<sup>17</sup> El FBI más tarde salió para decirlo's hasta las empresas individuales para decidir si para pagar o contactar otros profesionales de seguridad.

La madre de Simone, quién hubo nunca adquirió una aplicación en su vida, llamó su hija en la undécima hora sólo porque necesitó a figure fuera cómo para pagar con la moneda virtual. Simone dijo que encontró un Bitcoin ATM en Manhattan de qué, después de un software glitch y una llamada de servicio al ATM dueño, finalmente hizo el pago. En aquel día's tipo de cambio, cada Bitcoin era un poco más de 500. \$

Si estos extortionists recibir su pago en Bitcoin o en efectivo, quedan anónimos, a pesar de que técnicamente hay maneras de localizar ambas formas de pago. Las transacciones dirigieron on-line utilizando Bitcoin puede ser conectado al comprador—pero no fácilmente. La cuestión es, quién va a poner adelante el tiempo y esfuerzo para perseguir estos delincuentes?

En el capítulo próximo describiré qué puede pasar cuándo conectas al Internet vía Wi-Fi público. De una perspectiva de intimidad quieres el

anonimato de un Wi-Fi público pero al mismo tiempo necesitarás tomar precauciones.

## CAPÍTULO OCHO

### Cree Todo, Confía en Nada

Cuando el teléfono era todavía una novedad, era físicamente alambrado a la casa y quizás colocado en un recoveco construido a la muro. Cogiendo una segunda línea

estuvo considerada un símbolo de estado . De modo parecido, cabinas de teléfono público estuvieron construidas para intimidad. Even bancos de teléfonos de paga en hotel lobbies estuvo equipado con el sonido desconcierta entre ellos para dar la ilusión de intimidad.

Con teléfonos celulares, aquel sentido de intimidad ha bajado de punto enteramente. Es común de andar abajo la calle y oír personas ruidosamente compartiendo alguna obra personal o peor——recitando su número de carta del crédito dentro de earshot de todo quiénes pasan de largo. En el midst de esta cultura de transparencia y compartiendo, necesitamos pensar cuidadosamente sobre la información somos voluntariado al mundo.

A veces el mundo está escuchando. Soy refrán justo .

Supone te gusta obrar en la cafetería alrededor del corner de vuestra casa, como a veces hago. Tiene Wi-Fi libre. Aquello tendría que ser vale, bien? Odio para romperlo a ti, pero núm. Wi-Fi Público no fue creado con on-line bancario o comercio electrónico en mente. Es meramente conveniente, y él's también increíblemente insecure. No toda aquella inseguridad es técnica. Algunos de él empieza—y, I esperanza, fines—contigo.<sup>1</sup>

Cómo puede dices si eres en Wi-Fi público? Para una cosa, te ganado't ser pedido a entrada una contraseña para conectar al punto de acceso inalámbrico. Para demostrar qué visible eres en Wi-Fi público, investigadores del

antivirus Empresa F-Seguro construido su punto de acceso propio, u hotspot. Dirigieron su experimento en dos ubicaciones diferentes en Londres céntrico—una cafetería y un espacio público. Los resultados eran ojo - inaugurales.

En el primer experimento, los investigadores puestos arriba en una cafetería en una parte ocupada de Londres. Cuándo patrons considerado las elecciones

de redes disponibles, el F-Seguros hotspot vino arriba como ambos fuerte y libre. Los investigadores también incluyeron una pancarta que parecía en el navegador del usuario declarando los plazos y afecciones. Quizás has visto una pancarta así en vuestra tienda de café local que estipula qué puedes y puede no mientras utilizando su servicio. En este experimento, aun así, los plazos para el uso de este Wi-Fi libre requirieron la rendición del usuario firstborn niño o mascota amada. Seis personas consintieron a aquellos plazos y afecciones.<sup>2</sup> Para ser justos, más las personas no toman el tiempo para leer la huella fina— sólo quieren cualquier cosa es en el otro fin. Todavía, tienes que al menos skim los plazos y afecciones. En este caso, F-Seguro dicho más tarde que tampoco lo ni sus abogados quisieron cualquier cosa para hacer con niños o mascotas.

El asunto real es qué puede ser visto por terceras fiestas mientras eres en Wi-Fi público. Cuando tú're en en casa, vuestra conexión inalámbrica tendría que ser encriptada con WPA2 (ve [aquí](#)). Aquello significa si cualquiera es snooping, él o ella no pueden ver qué estás haciendo on-line. Pero cuando tú're utilizando Wi-Fi abierto, público en una tienda de café o aeropuerto, aquel tráfico de destino está puesto bare.

Otra vez podrías pedir, qué es el problema con todo este? Bien, ante todo, no sabes quién's en el otro fin de la conexión. En este caso el F-equipo de búsqueda Segura éticamente destruyó el dato recogieron, pero delincuentes probablemente no. Venderían vuestra alocución de email a empresas que send te spam, tampoco para cogerte para comprar algo o para infectar vuestro PC con malware. E incluso podrían utilizar los detalles en vuestro unencrypted emails a lanza de oficio-phishing ataques.

En el segundo experimento, el equipo puso el hotspot en un balcón en cercano proximity a las Casas de Parlamento, la sede de las fiestas Laborales y Conservadoras, y la Agencia de Delito Nacional. Dentro treinta minutos un total de 250 personas conectó al experimental libre hotspot. La mayoría de estos era conexiones automáticas made por cualquier aparato era utilizó. En otras palabras,, los usuarios no conscientemente escogen la red: el aparato que para ellos.

Un par de asuntos aquí. Dejado primer cariz en cómo y por qué vuestros aparatos móviles automáticamente unen una red de Wi-Fi.

Vuestro traditional PC y todos vuestros aparatos móviles recuerdan vuestro últimas pocas conexiones de Wi-Fi, ambos públicos y privados. Esto es bien porque te salvas el problema de continuamente reidentifying un Wi-Fi frecuentemente utilizado punto de acceso— como vuestra casa u oficina.

Esto es también malo porque si andas a una marca- cafetería nuevá, un sitio tú've nunca sido antes, de repente podrías encontrar que tienes conectividad inalámbrica allí. Por qué es que malo? Porque podrías ser conectado a algo otro que la red inalámbricá de la cafetería.

Las casualidad son vuestro aparato móvil detectó un punto de acceso que partidos un perfil ya en vuestra la mayoría de conexión reciente lista. Puedes notar algo amiss sobre la comodidad de automáticamente conectando a Wi-Fi en un sitio tú've nunca sido antes, pero también puedes ser en medio de un primer-persona shooter juego y no quiere pensar mucho allende aquel.

Qué hace obra de conexión de Wi-Fi automática? Como expliqué en el último capítulo, quizás te ha Comcast servicio de Internet en en casa, y si tú puedes unlso tener un libre, nonencrypted público SSID llamó Xfinity tan parte de vuestro plan de servicio. Vuestro Wi-Fi-el aparato habilitado puede haber conectado a él una vez antiguamente.<sup>3</sup> Pero cómo sabes que el tipo con un portátil en la mesa de esquina no está retransmitiendo un spoofed punto de acceso inalámbrico llamó Xfinity?

Dejado es dice *estás* conectado a aquel tipo sombrío en la esquina y no a la cafetería's red inalámbrica. Primero, todavía serás capaz a surf la Red. Así que puedes continuar tocar vuestro juego. Aun así, cada paquete de unencrypted dato envías y recibir sobre el Internet será visible a este carácter sombrío a través de su spoofed laptop punto de acceso inalámbrico.

Si está tomado el problema para poner arriba de una falsificación punto de acceso inalámbrico, entonces él's probablemente captando aquellos paquetes con una aplicación libre como Wireshark. Utilizo esta aplicación en mi obra como bolígrafo tester. Me dejo para ver la actividad de red aquello's yendo en alrededor me. Puedo ver las alocuciones de IP de personas de sitios están conectando a y cuánto tiempo están visitando aquellos sitios. Si la conexión no es encriptada, es legal de interceptar el tráfico porque es generalmente disponible al public. Por ejemplo, como un LO admin, querría saber la actividad en mi red.

Quizás el tipo sombrío en la esquina sólo está husmeando, viendo donde vas y no influyendo el tráfico. O quizás activamente está influyendo vuestro tráfico de Internet. Esto serviría propósitos múltiples.

Quizás él's redirigiendo vuestra conexión a un proxy que implantes un javascript keylogger en vuestro navegador tan cuando visitas Amazona vuestro keystrokes será captado como interaccionas con el sitio. Quizás coge pagado para

cosechar vuestro credentials—vuestro username y contraseña. Recuerda que vuestra carta de crédito puede ser asociada con Amazona y otros detallistas.

Cuándo entregando mi keynote, doy una demostración que espectáculos cómo puedo interceptar una víctima's username y contraseña cuándo accediendo sitios una vez él o ella está conectado a mi spoofed punto de acceso. Porque estoy sentando en medio de la interacción entre la víctima y el sitio web, puedo inyectar Javascript y falsificación de causa Adobe actualizaciones para reventar arriba en su o su pantalla, el cual, si instalado infectará la víctima's ordenador con malware. El propósito es normalmente para burlar tú a instalar la actualización de falsificación para obtener control de vuestro ordenador.

Cuándo el tipo en la mesa de esquina está influyendo el tráfico de Internet, aquello's llamado un hombre-en-el-ataque medio. El atacante es proxying vuestros paquetes a través de a el sitio real, pero interceptando o inyectando dato a lo largo de la manera.

Sabeing que involuntariamente podrías conectar a un punto de acceso de Wi-Fi sombrío, cómo puede lo impides? En un portátil el aparato pasará por el proceso de buscar una red inalámbrica preferida y entonces conectar a él. Pero algunos portátiles y los aparatos móviles automáticamente escogen qué red para unir. Esto estuvo diseñado para hacer el proceso de tomar vuestro aparato móvil de una ubicación a otro tan indoloro como posible. Pero como mencioné, hay downsides a esta comodidad.

Según Apple, sus varios productos automáticamente conectarán a redes en este orden de preferencia:

1. La red privada el aparato más recientemente unido,
2. Otra red privada, y
3. Un hotspot red.

Portátiles, afortunadamente, proporcionar el medio para eliminar conexiones de Wi-Fi obsoleto—por ejemplo, aquel Wi-Fi de hotel te conectado a último verano en un viaje empresarial. En un portátil de Ventanas, puedes uncheck el “Conectar Automáticamente” campo luego al nombre de red antes de que conectas. O dirigirse a Red de Panel>del Control y Compartiendo Center y clic en el nombre de red. Clic en “Haciendas Inalámbricas,” entonces uncheck “Conecta automáticamente cuándo esta red es en gama.” En un Mac, se dirige a Preferencias de Sistema, va a Red, Wi-Fi de punto destacado en la panel izquierda, y el clic “Adelantó.” Entonces uncheck “Recordar redes este ordenador ha unido.” Puedes también individualmente sacar redes por seleccionar el nombre y pulsando el minus botón



debajo lo. Androide e iOS los aparatos también tienen instrucciones para eliminar Wi-Fi

utilizado anteriormente conexiones. En un iPhone o iPod, va a vuestros encuadres, selecciona “Wi-Fi,” clic el “i” icono luego al nombre de red, y escoger “Olvidar Esta Red.” En un teléfono de Androide, puedes ir a vuestros encuadres, escoge “Wi- Fi,” mucho tiempo-prensas el nombre de red, y seleccionar “Olvidar Red.”

Seriamente, si realmente tienes algo sensible de hacer fuera de vuestra casa, entonces recomiendo utilizar la conexión celular en vuestro aparato móvil en vez de utilizar la red inalámbrica en el aeropuerto o tienda de café. Puedes también tether a vuestro aparato móvil personal que utiliza USB, Bluetooth, o Wi-Fi. Si utilizas Wi-Fi, entonces hace seguro configuras WPA2 seguridad como mencionado más temprano. La otra opción es para adquirir un portátil hotspot para utilizar cuándo viajando. Nota, también, este ganado't te haces invisible, pero es una alternativa mejor que utilizando Wi-Fi público. Pero si necesitas proteger vuestra intimidad de la operadora móvil—dice, para descargar un sensible spreadsheet—entonces sugiero que utilizas HTTPS En todas partes o un Protocolo de Traslado de Lima Seguro (SFTP). SFTP se mantiene utilizar el Transmitir aplicación en Mac y el Tunnelier aplicación en Ventanas.

Una red privada virtual (VPN) es un túnel “seguro” que extiende una red privada (de vuestra casa, oficina, o un VPN proveedor de servicio) a vuestro aparato en una red pública. Puedes buscar Google para VPN proveedores y servicio de compra para aproximadamente \$60 un año. La red tú'll encontrar en la tienda de café local o el aeropuerto o en otros sitios públicos no es para ser confiados en— es público. Pero por utilizar un VPN te puede túnel a través del público network atrás a una red privada y segura. Todo haces dentro del VPN está protegido por encriptación, como todo vuestro tráfico de Internet es ahora asegurado sobre la red pública. Es por eso que es importante de utilizar un VPN proveedor lo puedes—confiar en puede ver vuestro tráfico de Internet. Cuándo utilizas un VPN en la tienda de café, el sketchy tipo en la esquina sólo puede ver que te ha conectado a un VPN servidor y nada más —vuestras actividades y los sitios visitas es todo completamente escondido detrás de duro- a-encriptación de grieta.

However, todavía tocarás el Internet con una IP dirige aquello es localizable directamente a ti, en este caso la alocución de IP de vuestra casa u oficina. Así que eres todavía no invisible, incluso utilizando un VPN. No olvida—vuestro VPN el proveedor sabe vuestra IP de originar alocución. Más tarde hablaremos cómo para hacer esta conexión invisible (ve [aquí](#)).



Muchas empresas proporcionan VPNs para sus empleados, dejándoles para conectar de una red pública (i.e., el Internet) a una red corporativa interna privada. Pero qué sobre el resto de nosotros?

Hay muchos comerciales VPNs disponibles. Pero cómo sabes si para confiarles en? El subyacente VPN tecnología, IPsec (seguridad de protocolo del Internet), automáticamente incluye PFS (clandestinidad de delantero perfecto; ve [aquí](#)), pero no todos los servicios—incluso corporativos unos—de hecho molestan para configurarlo. OpenVPN, un proyecto de fuente abierta, incluye PFS, así que podrías inferir que cuándo un producto dice que utiliza OpenVPN lo también utiliza PFS, pero esto no es siempre el caso. El producto no podría tener OpenVPN configurado properly. Marca seguro el servicio específicamente incluye PFS.

Una desventaja es que VPNs es más caro que proxies.<sup>4</sup> Y, desde comercial VPNs está compartido, también pueden ser lentos, o en algunos casos sencillamente no puedes coger un disponible VPN para vuestro personal use y tendrás espera hasta que uno acaece disponible. Otra molestia es que en algún Google de casos reventará arriba de un CAPTCHA petición (cuál te pides para escribir en los caracteres ves en la pantalla) antes de que puedes utilizar su motor de búsqueda porque quiere make seguro eres un humano y no un bot. Finalmente, si vuestro particular VPN el vendedor mantiene registros, leídos la política de privacidad para hacer seguro que el servicio no retiene vuestro tráfico o registros de conexión—incluso encriptados—y que lo doesn't marca el dato fácil de compartir con aplicación de ley. Puedes imaginar esto fuera en los plazos de servicio y política de privacidad. Si pueden informar actividades a aplicación de ley, entonces ellos registro VPN conexiones.

Pasajeros de aerolínea quiénes utilizan un en-servicio de Internet del aire como GoGo corrido el mismo risk como hacen yendo on-line mientras sentando en un Starbucks o aeropuerto lounge, y VPNs no es siempre soluciones sumas. Porque quieren impedir Skype u otra voz-aplicaciones de llamada, GoGo y otro en-servicios de aire throttle UDP paquetes—cuál hará más VPN servicios muy despacio tan UDP es el protocolo la mayoría de uso por default. Aun así, escogiendo un VPN servicio que usos el TCP protocolo en vez de UDP, como TorGuard o ExpressVPN, mucho puede mejorar actuación. Ambos de estos VPN los servicios dejan el usuario para poner cualquier TCP o UDP como su protocolo preferido.

Otra consideración con un VPN es su política de privacidad. Si utilizas un comercial VPN o un corporativo-proporcionó VPN, vuestros viajes de tráfico

sobre su red, el cual es por qué él es importante de utilizar https así que el VPN el proveedor puede't ver los contenidos de vuestras comunicaciones.<sup>5</sup>

Si obras en una oficina, las casualidad son vuestra empresa proporciona un VPN de modo que puedes obrar remotely. Dentro de una aplicación en vuestro PC tradicional, escribes en vuestro

username y contraseña (algo sabes). La aplicación también contiene un certificado de identificar colocado allí por vuestro LO departamento (algo ya tienes), o te puede enviar un texto en vuestra empresa-teléfono emitido (también algo tienes). La aplicación puede emplear todo tres técnicas en qué's sabidos como multifactor autenticación.

Ahora puedes sentar en un Starbucks o un aeropuerto lounge y negocio de conducta como si utilizabas un servicio de Internet privado. Aun así, no tendrías que dirigir negocio personal, como banca remota, a no ser que la sesión real is encriptó utilizar el HTTPS En todas partes prorroga.

La manera única de confiar en un VPN el proveedor es para ser anónimo del inicio. Si realmente quieres ser completamente anónimo, nunca utilizar una conexión de Internet que podría ser enlazado a ti (i.e., uno originando de vuestra casa, oficina, amigos' casas, una habitación de hotel reservada en vuestro nombre, o cualquier cosa más conectado a tú). Estuve cogido cuándo el FBI localizó una celda-señal de teléfono a mi guarida en Raleigh, Carolina del Norte, atrás en el 1990s. Tan nunca acceder personal information utilizando un aparato de quemador en la misma ubicación si tú're intentando para evitar potestades gubernamentales. Cualquier cosa haces en el aparato de quemador tiene que ser completamente separar para quedar invisible. Significando que no metadata del aparato puede ser enlazado a vuestra identidad real.

También puedes instalar un VPN en vuestro aparato móvil. Apple proporciona instrucciones para hacer tan,<sup>6</sup> y puedes encontrar instrucciones para aparatos de Androide también.<sup>7</sup>

Si has sido siguiendo mi consejo en el libro tan lejos, tú probablemente boleteo mucho mejor que la media Joe. La mayoría de vuestro uso de Internet probablemente será seguro de eavesdropping o manipulación por un atacante.

Así que vuestros medios de comunicación sociales. Https de usos del Facebook para todas sus sesiones.

Comprobando vuestro email? Google también ha cambiado over a https sólo. La mayoría de servicios de correo de la Web han seguido, como tiene

instante más importante messaging servicios. De hecho, sitios más importantes—Amazona, eBay, Dropbox—todo ahora https de uso.

Para ser invisible, es siempre más a capa vuestra intimidad. Vuestro riesgo de habiendo vuestro traffic visto por otros en unas disminuciones de red públicas con cada capa adicional de seguridad empleas. Por ejemplo, de una red de Wi-Fi pública, acceso vuestro pagado VPN servicio, entonces acceder Tor con el HTTPS En todas partes la prórroga instalada por default en el Abetoefox navegador.

Entonces cualquier cosa tú on-line será encriptado y duro de localizar.

Te dices sólo quiere comprobar el tiempo y no cualquier cosa financiero o personal, y estás utilizando vuestro portátil personal propio fuera de vuestra red de casa—que tendría que ser seguro, bien? Una vez más, no realmente. Hay unas cuantas precauciones todavía necesitas tomar.

Primero, turno fuera Wi-Fi. Seriamente. Muchas personas dejan Wi-Fi en sus portátiles giró encima incluso cuándo ellos don't lo necesita. Según los documentos liberaron por Edward Snowden, el Establecimiento de Seguridad de las Comunicaciones Canadá (CSEC) puede identificar los viajeros que pasan through aeropuertos canadienses sólo por captar su MAC alocuciones. Estos son legibles por cualquier ordenador que está buscando cualquier petición de sonda enviada de aparatos inalámbricos. Incluso si no conectas, el MAC la alocución puede ser captada. Tan si te don't lo necesita, turno de vuestro Wi-Fi.<sup>8</sup> Como hemos visto, la comodidad a menudo obra en contra intimidad y seguridad.

Tan lejos hemos skirted alrededor de un asunto importante—vuestro MAC alocución. Esto es único a cualquier aparato estás utilizando. Y no es permanente; lo puedes cambiar.

Dejado me darte un ejemplo.

En el segundo capítulo, te dijiste aproximadamente encriptando vuestro email que utiliza PGP (Intimidad Buena Bonita; ve [aquí](#)). Pero qué si te don't quiere pasar por el hassle, o qué si el recipient no tiene un público PGP tono para ti para utilizar? hay otro clandestine manera de intercambiar mensajes vía email: uso la carpeta de borradores en una cuenta de email compartida.

Esto es CIA qué anterior General de director David Petraeus información intercambiada con su mistress, Paula Broadwell—su biógrafo. El escándalo desdoblado después de Petraeus acabado la relación y notó que alguien había sido enviando emails amenazantes a un amigo de su. Cuándo el FBI

investigó, encontraron no sólo que las amenazas habían provenido Broadwell pero que también había sido dejando romántico messalvias para Petraeus.<sup>9</sup>

Qué's interesante es que los mensajes entre Broadwell y Petraeus no fue transmitido sino dejado en la carpeta de borradores del “anónimo” e- cuenta de correo. En este escenario el email no pasa a través de otros servidores en un intento de lograr el recipient. Hay menos oportunidades para interceptaciones. Y si alguien coge acceso a la cuenta más tarde encima, no habrá ninguna evidencia si eliminas los emails y vacíos la basura por adelantado.

Broadwell También logged en a su “cuenta” de email anónima que utiliza un ordenador dedicado. No contactó el sitio de email de su alocución de IP de la casa. Aquello habría sido demasiado obvio. En cambio fue a varios hoteles para dirigir sus comunicaciones.

A pesar de que Broadwell había tomado dolores considerables para esconder, todavía no fue invisible. Según el *New York Times*, “porque el sender's la cuenta había sido registrada anónimamente, los detectives tuvieron que utilizar las técnicas forenses que— incluyen un control de qué otras cuentas de email había sido accedido de la misma alocución de ordenador—para identificar quién escribía los emails.”<sup>10</sup>

proveedores de Email como Google, Yahoo, y Microsoft retiene registro-en récords para más de un año, y estos revelan la IP particular dirige un consumidor ha logged en de. Para examenple, si utilizaste un Wi-Fi público en Starbucks, la alocución de IP revelaría la ubicación física de la tienda. Los Estados Unidos actualmente permite agencias de aplicación de la ley para obtener este registro-en récords de los proveedores de email con un meros subpoena—ningún juez requirió.

Aquello significa los detectives tuvieron la ubicación física de cada IP dirige aquello contactó que cuenta de email particular y entonces podría emparejar Broadwell aparato MAC alocución en el router registro de conexión en aquellas ubicaciones.<sup>11</sup>

Con el autor llenoy del FBI detrás les (esto era un trato grande , porque Petraeus era el director de CIA en el tiempo), los agentes eran capaces de buscar todo el router limas de registro para cada hotel y ver cuándo Broadwell's MAC la alocución aparecida en limas de registro del hotel. Además, eran capaces de asomar que en las citas en cuestión Broadwell era un huésped registrado. Los detectives notaron que mientras ella logged en a estas cuentas de email, nunca de hecho envió un email.

Cuándo conectas a una red inalámbrica, el MAC alocución en vuestro computer es automáticamente grabado por el inalámbrico networking equipamiento. Vuestro MAC la alocución es similar a un número de serial asignó a vuestra carta de red. Para ser invisible, con anterioridad a conectar a cualquier red inalámbrica necesitas cambiar vuestro MAC alocución a uno not asociado contigo.

Para quedarse invisible, el MAC la alocución tendría que ser cambiada cada vez conectas a la red inalámbrica así que vuestras sesiones de Internet pueden no fácilmente ser correlativos a ti. Es también importante no para acceder cualquiera de vuestras cuentas on-line personales durante este proceso, como puede compromise vuestro anonimato.

Instrucciones para cambiar vuestro MAC la alocución varía con cada sistema operativo—i.e., Ventanas, Mac OS, Linux, incluso Androide e iOS.<sup>12</sup> Cada vez conectas a un público (o privado) red, podrías querer recordar para cambiar vuestro MAC alocución. Después de un reboot, el original MAC regresos de alocución.

Dejado es dice no posees un portátil y tener ninguna elección pero para utilizar una terminal de ordenador pública, ser él en una cafetería, una biblioteca, o incluso un centro empresarial en un hotel de fin alto. Qué puede haces para te proteger?

Cuándo voy acampar observo el “dejar ningún rastro” gobierna—aquello es, el camping tendría que mirar tan hizo cuando primero llegué. El mismo es cierto con terminales de PC público. Después de que dejas, nadie te tendría que conocer era allí.

Esto es especialmente cierto en espectáculos de comercio. Era en el Espectáculo de Electrónica de Consumidor anual un año y vio un banco de público PCs conjunto fuera de modo que attendees podría comprobar su email mientras andando el piso de convención. Incluso vi esto en el anual security-conferencia de RSA consciente, en San Francisco. Teniendo una fila de las terminales genéricas fuera en público es una idea mala para un número de razones.

Uno, estos son arrendó ordenadores, reused de caso a caso. Pueden ser limpiados, el OS reinstalled, pero entonces otra vez no podrían ser.

Dos, tienden para correr admin derechos, el cual significa que la conferencia attendee puede instalar cualquier software él o ella quiere. Esto incluye malware como keyloggers, los cuales pueden almacenar vuestro username e información de contraseña. En la seguridad business, hablamos del principio

de menos “privilegio,” el cual significa que una máquina concede un usuario sólo los privilegios mínimos él o ella necesita coger el trabajo hecho.

Logging En a una terminal pública con sistema admin privilegios, el cual es el default puesto en some terminales públicas, viola el principio de menos privilegio y sólo aumenta el riesgo que estás utilizando un aparato anteriormente infectado con malware. La solución única es a de alguna manera ser seguro que estás utilizando una cuenta de huésped, con privilegio limitados, el cual la mayoría de

personas no sabrán cómo para hacer. En general recomiendo nunca confiando en una terminal de PC pública. Asumir la persona

quién último utilizado lo instalado malware—tampoco conscientemente o unconsciously. Si te registro en a Gmail en una terminal pública, y hay un keylogger en aquella terminal pública, algunos tercera fiesta remota ahora tiene vuestro username y contraseña. Si te registro en a vuestro banco—lo olvida. Recuerda, tendrías que habilitar 2FA en cada sitio accedes tan un atacante armado con vuestro username y la contraseña puede no impersonate te. Autenticación de dos factores mucho mitigará las casualidad de vuestra cuenta que es cortado si alguien obtiene conocimiento de vuestro username y contraseña.

El número de personas quiénes utilizan quioscos públicos en ordenador-basó conferencias como CES y RSA me asombro. Línea inferior, si tú're en un espectáculo de comercio, uso vuestro celular-pastilla o teléfono habilitados, vuestro personales hotspot (ve [aquí](#)), o espera hasta que vuelves a vuestra sala.

Si tienes que utilizar el Internet fuera de vuestra casa u oficina, uso vuestro smartphone. Si absolutamente tienes que utilizar una terminal pública, entonces no por cualquier signo de medio en a cualquier cuenta personal, incluso correo de Web. Si estás buscando un restaurante, por ejemplo, acceso sólo aquellos sitios web que no *requiere* autenticación, como Yelp. Si utilizas una terminal pública en un semiregular base, entonces puesto arriba de una cuenta de email para utilizar sólo en terminales públicas, y email de delantero único de vuestras cuentas legítimas a este “throwaway” alocución cuándo eres en la carretera. La parón que envía una vez regresas casa. Esto minimiza la información que es findable bajo aquella alocución de email.

Luego, marca seguro los sitios accedes de la terminal pública tiene https en el URL. Si te don't ve https (o si lo ves pero sospechoso que alguien lo ha puesto allí para darte un sentido falso de seguridad), entonces quizás



tendrías que reconsiderar acceder información sensible de esta terminal pública.

Dejado es dice coges un https legítimo URL. Si eres en un registro-en página, buscar una caja que dice “Mantenerme logged en.” Uncheck Aquello. La razón es clara: esto no es vuestro PC personal. Está compartido por otros. Por te mantener logged en, estás creando una galleta en aquella máquina. Te don't Querer la persona próxima en el terminal de ver vuestro email o ser capaz de enviar email de vuestra dirección, tú?

Como notado, don't registro en a sitios financieros o médicos de una terminal pública. Si tú registro en a un sitio (si Gmail u otherwise), marca seguro te registro fuera cuándo estás hecho y quizás considera cambiar vuestra contraseña de vuestro propio computer o aparato móvil después sólo para ser seguro. Puedes no siempre

registro fuera de vuestras cuentas en en casa, pero tienes que siempre esto cuando utilizando alguien más ordenador.

Después de que has enviado vuestro email (o mirado en cualquier quisiste mirar en) y registred fuera, entonces intentar borrar la historia de navegador así que la persona próxima no puede ver donde has sido. También eliminar cualesquier galletas si puedes. Y marca seguro te didn't descarga limas personales al ordenador. Si tú, entonces intentar eliminar la lima o limas del desktop o carpeta de descargas cuándo estás acabado.

Desafortunadamente, aun así, sólo eliminando la lima no es bastante. Luego necesitarás a vacío la basura. Aquel quieto doesn't plenamente sacar el material eliminado del ordenador— puedo recuperar la lima después de que dejas si quiero. Afortunadamente, más las personas no tienen la capacidad de hacer que, y normalmente eliminando y emptying la basura bastará.

Todos estos pasos son necesarios de ser invisibles en una terminal pública.

## CAPÍTULO NUEVE

### **no Tienes Ninguna Intimidación? Coge Encima Lo!**

En algún punto durante el tiempo que anterior antivirus creador de software John McAfee pasado como fugitivo de potestades en Belice, empezó un blog. Toma él de mí: si estás intentando marchar la verja y totalmente desaparecer, te don't quiere empezar un blog. Para una cosa, estás atado para equivocarse.



McAfee Es un hombre listo. Hizo su fortuna en los días tempranos de Valle de Silicio por pioneering antivirus búsqueda. Entonces vendió su empresa, vendido todas sus ventajas en los Estados Unidos, y para alrededor cuatro años, de 2008 a 2012, vivió en Belice, en una propiedad privada de la costa. Hacia el fin de aquel periodo, el gobierno de Belice had le debajo cercano-vigilancia constante, raiding su hacienda y acusándole de reunir un ejército privado además de comprometer en narcotráfico.

McAfee Negó hacer tampoco. Alegó luchaba los señores de droga en la isla. Dijo, para example, que había ofrecido una televisión de pantalla plana a una traficante de marihuana de tiempo pequeño en la afección que la parón de hombre que trata. Y estuvo sabido para estirar sobre coches que sospechó llevaba traficante de droga.<sup>1</sup>

McAfee de hecho tuvo un laboratorio de droga, pero no necesariamente para drogas recreativas. Alegó creaba una generación nueva de drogas “” útiles. Por ello su sospecha de crecer que los coches llenos de los hombres blancos fuera de su hacienda eran espías de pharmaceuticals empresas como GlaxoSmithKline. Más allá alegó que las redadas por la policía local eran instigated por estos mismos pharmaceuticals empresas.

Guarding Su hacienda era varios hombres con pistolas y once perros. Un vecino dos casas al del sur, Greg Faull, renegó asiduamente a las potestades sobre los perros que ladran tarde en la noche. Entonces una noche en noviembre de 2012, algunos de McAfee's los perros estuvieron envenenados. Y más tarde que semana misma, Faull estuvo disparado, encontró facedown en un grupo de sangre en su casa.

Las potestades de Belice naturalmente consideraron McAfee una persona de interés en su investigación. Tan McAfee narra en su blog, cuándo oyó de su housekeeper que la policía quiso hablar a él, fue a esconder. Acaecía un fugitivo .

Pero no fue el blog que ley dirigida finalmente aplicación a McAfee. Era una foto . Y no fue incluso su propio.

Un investigador de seguridad nombró Mark Loveless (mejor sabido en círculos de seguridad como Nómada Sencillo) notó un cuadro de McAfee publicado encima Twitter por revista de Vicio en diciembre temprano de 2012. La foto el editor del vicio *asomado estando luego a McAfee en una ubicación tropical—quizás en Belice, quizás a algún lugar más.*

Loveless Supo que las fotos digitales captan información muchísima sobre when, dónde, y cómo están tomados, y quiso ver lo que información digital esta foto podría contener. Las fotos digitales almacenan qué está sabido como lima de imagen intercambiable, o EXIF, dato. Esto es foto metadata, y contiene detalles mundanos como el amount de saturación de color en la imagen de modo que la foto puede ser con exactitud reproducida en una pantalla o por una impresora. Puede también, si el cámara está equipado para hacer tan, incluir la longitud exacta y latitud del sitio donde la foto estuvo tomada.

Aparentemente la foto de McAfee con el *editor* de revista del Vicio estuvo tomado con un iPhone 4S cámara. Algún barco de teléfonos celulares con la geolocalización automáticamente habilitó. Loveless Cogido afortunado: la imagen posted en la lima on-line incluida la geolocalización exacta de John McAfee, quién era, resultó, en neighboring Guatemala.

En un blog subsiguiente McAfee dijo fingió el dato, pero aquello parece improbable. Más tarde dijo que pretendió revelar su ubicación. Más probablemente cogía perezoso.

La historia larga corta, la policía guatemalteca detuvo McAfee y wouldn't dejado le dejar el país. Entonces padeció una afección de salud, era hospitalized, y era finalmente dejado para regresar a los Estados Unidos.

El asesinato de Greg Faull los restos no resueltos. McAfee Ahora vidas en Tennessee, y en 2015 decidió estar en cartelera presidente para defender para más cyberfriendly pólizas en el gobierno de EE.UU.. No bloguea casi tan a menudo

hoy en día.

Dejado es dice eres un ambicioso joven jihadist, y eres orgulloso de ser posted a una sede militar recientemente establecida de Daesh, o ISIL. Qué es la primera cosa haces? Estiras fuera de vuestro teléfono celular y tomar un selfie. Peor, además de la foto de ti y vuestro nuevo cava, te poste unas cuantas palabras sobre el equipamiento sofisticado disponible en esta facilidad particular.

A medias un mundial fuera, reconnaissance aviadores en Florida Hurlburt el campo está peinando medios de comunicación sociales y ver la foto. “Cogíamos un en,” uno de ellos dice. Efectivamente, unas cuantas horas más tarde tres JDAMs (junta ataque directo munitions) toma fuera de aquel edificio militar nuevo reluciente.<sup>2</sup> Todo debido a un selfie.<sup>3</sup>

no siempre consideramos qué *más* mentiras dentro del marco de un selfie nosotros've sólo tomados. En película y teatro esto se apellida el *mise-en-scène*, aproximadamente traducido del francés como “qué es en la escena.” Vuestro cuadro podría asomar un crowded ciudad skyline, incluyendo la Torre de Libertad, fuera de vuestra ventana de apartamento. Incluso un cuadro de tú en un encuadre rural—quizás un prairie extendiendo fuera al horizonte plano—me doy información valiosa aproximadamente dónde vives. Estos visuals proporciona pistas de ubicación minúscula que podría verter fuera alguien quién es ansioso de encontrarte.

En el joven jihadist caso, qué era en la escena era un militar headquarter s. Embedded En el metadata del selfie era la longitud precisa y latitud, o geolocalización, del sitio donde la foto estuvo tomada. General Hawk Carlisle, la jefa de la Orden de Combate de Aire de EE.UU., estimó era un mero veinticuatro horas del tiempo que selfie era primero posted en medios de comunicación sociales a la destrucción completa de aquella sede.

Ciertamente el metadata dentro de vuestras limas de imagen pueden soler localizarte. EXIF El dato en una imagen digital contiene, entre otras cosas, la cita y tiempo cuándo el cuadro estuvo chasqueado, la marca y número de modelo del cámara, y, si tienes la geolocalización activada en el deal vicio que toma la foto, la longitud y latitud del sitio donde tomaste la imagen. Es esta información, dentro de la lima, que el ejército de EE.UU. utilizó para encontrar el Daesh sede en el desierto, tan Marca Loveless utilizado EXIF dato para identificar John McAfee ubicación. Cualquiera puede utilizar esta herramienta—es indígena en el inspector de lima encima Manzana OSX y en herramientas descargables como FOCA para Ventanas y Metagoofil para Linux—para obtener acceso al metadata almacenado en fotos y documentos.

A veces no es una foto pero una aplicación que da arriba de vuestra algo. En el verano

de 2015, señor de droga Joaquin “El Chapo” Guzman huyó de una prisión mexicana e inmediatamente fue de la verja. O él?

Dos meses después de su evasión—de México máximo-seguridad Altiplano prisión—El Chapo's hijo de veintinueve años, Jesus Alfredo Guzman Salazar, posted una imagen a Twitter. A pesar de que los dos hombres sentaron en una mesa de cena con Salazar está ocultado por emoticons, la complexión del hombre en los osos izquierdos un parecido fuerte al Chapo. Más allá, Salazar captioned la imagen: “August aquí, ya sabes con quien.” El tweet también contuvo el dato de ubicación del Twitter—Costa Rica que—

sugiere que El Chapo el hijo falló para cambiar del autotagging función encima la aplicación de smartphone de Twitter.<sup>4</sup>

Incluso si te don't tener un condenado huído en vuestra familia, necesitas ser consciente que la información digital y visual escondida (a veces en vista sencilla) en vuestras fotos pueden revelar mucho a alguien quién no te conoce y puede volver para perseguirte.

Las fotos on-line pueden hacer más de justos revelar vuestra ubicación. Pueden, conjuntamente con programas de software seguro, revela información personal aproximadamente te.

En 2011 Alessandro Acquisti, un investigador de Carnegie Mellon Universidad, posó una hipótesis sencilla: “ quise ver si era posible de ir de una cara en la calle a un número de Seguridad Social,” dijo. Y encontró que era de hecho posible.<sup>5</sup> Por tomar una fotografía de webcam sencilla de un voluntario estudiantil, Acquisti y su equipo tuvo bastante información para obtener información personal sobre aquella personaje.

Piensa sobre aquel. Podrías tomar una foto de una persona fuera en la calle y, utilizando software de reconocimiento facial, intento de identificar aquella persona. Sin la confirmación de aquella persona de su o su identity, puedes coger unos cuantos falso positivos. Pero las casualidad son una mayoría de los “golpes” revelarían uno nombra más de otro.

“ hay un blending de dato on-line y off-line, y vuestra cara es el conduit —el veritable enlace entre estos dos mundos,” Acquisti dijo *Threatpost*. “Pienso que la lección es un bastante melancólico un. Tenemos que afrontar la realidad que nuestro muy la idea de intimidad está siendo erosionó. Tú're ya no privado en la calle o en una multitud. El mashup de todas estas tecnologías desafía nuestra expectativa biológica de intimidad.”

Para su estudio, Acquisti y otros alumnado parado en el Carnegie Mellon campus y les pidió para llenar fuera de una estudio on-line. La webcam en el portátil

tomó un cuadro de cada estudiantil como él o ella tomaba la estudio, y el picture era inmediatamente cruz-referenced on-line utilizando software de reconocimiento facial. En la conclusión de cada estudio, muchos del recuperó las fotos ya habían parecido en la pantalla. Acquisti Dicho que 42 por ciento de las fotos eran positivamente identificados y enlazados al alumnado' perfiles de Facebook.

Si utilizas Facebook, eres quizás ya consciente de su tecnología de reconocimiento facial limitada. Cargar una foto al sitio, y Facebook intentará

a phototag las personas dentro de vuestra red, personas con quien you es ya amigos. Tienes algún control sobre este. Por ir a vuestros encuadres de Facebook puedes requerir el sitio para notificarte cada vez aquello pasa y escoger si para ser identificado en la foto. También puedes escoger a poste la foto a vuestra muro o timeline sólo después de que has sido notificado, si en absoluto.

Para hacer tagged las fotos invisibles en Facebook, abre vuestra cuenta e ir a Encuadres “de Intimidad.” Hay varias opciones, incluyendo limitando las imágenes a vuestro personales timeline. Otro que que, Facebook no ha proporcionado todavía una opción para parar personas de tagging tú sin permiso.

Empresas como Google y Manzana también tienen tecnología de reconocimiento facial construida a algunos de sus aplicaciones, como Foto de Google e iPhoto. Puede valer mirar en los encuadres de configuración para aquellas aplicaciones y servicios de modo que puedes limitar lo que tecnología de reconocimiento facial puede hacer en cada. Google tiene tan lejos aguantado atrás de incluir tecnología de reconocimiento facial en su característica de búsqueda de la imagen (indicado por then icono de cámara pequeño ves en la ventana de búsqueda del Google). Puedes cargar un cuadro de existir, y Google encontrará el cuadro, pero no intentará para encontrar otras fotos que asoman la misma persona o personas dentro de la imagen. Google tiene, en varios public declaraciones, dijo que dejando las personas identifican los desconocidos por cara “cruza el creepy línea.”<sup>6</sup>

Aun así, algunos repressive los gobiernos han hecho sólo aquello. Han tomado fotos de manifestantes en grandes antigovernment rallies y entonces puestos las imágenes en la Web. Esto no está utilizando software de reconocimiento de la imagen tanto como es crowdsourcing el proceso de identificación. También, algunos estados de EE.UU. han utilizado sus departamentos de vehículo del motor' bases de datos de foto para identificar sospechosos en casos criminales. Pero aquellos son elegantes estatales-basó operaciones. Qué podría un solitario académico hacer?

Acquisti Y sus investigadores amigos quisieron ver cuánta imagen-la información derivada sobre una persona podría ser cruz-referenced on-line. Para descubrir utilizaron una tecnología de reconocimiento facial llamó Pittsburgh Reconocimiento de Patrón, o PittPatt,

ahora poseído por Google. Los algoritmos utilizaron en PittPatt ha sido autorizado a varias empresas de seguridad e instituciones de gobierno. Poco después de la adquisición, Google fue en récord sobre sus intenciones:

“Como hemos dicho para over un año, no añadiremos reconocimiento de cara a Google a no ser que podemos imaginar fuera de un modelo de intimidad fuerte para él. No lo hemos imaginado fuera.”<sup>7</sup> Dejado esperanza la empresa se aferra a su palabra.

En el tiempo de su búsqueda, Acquisti era capaz de utilizar PittPatt paired con datos-mined imágenes de Facebook de qué él y su equipo consideraron para ser searchable perfiles, i.e., aquellos en qué el Carnegie Mellon los voluntarios hubieron ya posted fotos de themselves junto con piezas seguras de información personal. Entonces aplicaron este conjunto de caras sabidas a las “caras” anónimas en un sitio de datación on-line popular. Allí los investigadores encontraron que podrían identificar 15 por ciento de estos presuntamente “anónimos” digitales oye tbr eaker s.

El creepiest experimento, aun así, implicó enlazar una persona's cara a su o su número de Seguridad Social. Para hacer que, Acquisti y su equipo buscó perfiles de Facebook que incluidos la cita y la ciudad de la persona de nacimiento. Anteriormente, en 2009, el mismo grupo de investigadores había asomado que esta información por él era bastante para habilitarles para obtener el número de Seguridad Social de una persona (números de Seguridad Social son emitido sequentially por un estatal's fórmula propia, y desde entonces 1989 SSNs ha sido emitido encima o muy cercano la cita de nacimiento, haciéndolo incluso más fácil de adivinar últimos cuatro dígitos de una persona).<sup>8</sup>

Después de que algunos cálculos iniciales, los investigadores entonces enviaron una estudio de seguimiento a cada cual de su CMU los voluntarios estudiantiles que piden si los primeros cinco dígitos de su o su número de Seguridad Social como pronosticado por su algoritmo era correcto. Y una mayoría de ellos era.<sup>9</sup>

apostaré hay algunas fotos que te ahora no quiere on-line. Las casualidad eres ganadas't ser capaces de tomarles todo atrás, incluso si les podrías eliminar de vuestro sitio de medios de comunicación social. Aquello es en separar porque una vez te poste algo a una red social, él's poseído por aquella red y fuera de vuestras manos. Y apalabraste esto en los plazos de servicio.

Si utilizas la aplicación de Fotos de Google popular, incluso eliminando una foto allí no necesariamente significarlo's ido. Los clientes han encontrado que las imágenes son todavía allí incluso después de que eliminan la aplicación de sus aparatos móviles. Por qué? Porque una vez la imagen pega la nube, es aplicación -independiente, significando que otras aplicaciones

pueden tener acceso a él y puede continuar mostrar la imagen eliminaste.<sup>10</sup> Esto tiene real-consecuencias mundiales. Te dices posted algún estúpido caption en una foto de alguien quién ahora obras en el muy empresa que estás aplicando para obrar para. O tú posted una foto de tú con alguien te don't querer vuestro cónyuge actual para saber aproximadamente. A pesar de que puede ser vuestra cuenta de red

social *personal*, es la red social *dato*. Tú've probablemente nunca tomado el problema para leer los condiciones de uso para cualquier

sitio web donde te poste vuestro dato personal, experiencias diarias, pensamientos, opiniones, historias, gripes, quejas, y tan encima, o donde te tienda, juego, aprende, e interaccionar, quizás en un diario o incluso hourly base. La mayoría de social networking los sitios requieren usuarios para apalabrar plazos y conditions antes de que utilizan sus servicios.

Controversially, estos denomina a menudo contener cláusulas permitting los sitios para almacenar el dato obtenido de usuarios e incluso comparte él con terceras fiestas.

Facebook ha atraído atención a lo largo de los años para su almacenamiento de dato policies, incluyendo el hecho que el sitio lo hace difícil de eliminar una cuenta. Y Facebook isn't sólo. Muchos sitios web haber casi lengua idéntica en sus condiciones de uso que muy probablemente asustarte fuera si habías leído los plazos antes de firmar encima. Aquí un ejemplo, de Facebook, como de enero 30, 2015:

*posees todo del contenido e información te poste encima Facebook, y puedes controlar cómo está compartido a través de vuestra intimidad y encuadres de aplicación. Además:*

*1. Para contentar aquello está cubierto por derechos de propiedad intelectual, como*

*fotos y vídeos (contenido de IP), específicamente nos das el permiso*

*siguiente, tema a vuestra intimidad y encuadres de aplicación: nos*

*concedo un no-exclusivo, transferable, sub-licensable, realeza-libre, en todo el mundo*

*autorizar para utilizar cualquier contenido de IP que te poste encima o en conexión con Facebook*

*(Licencia de IP). Estos fines de Licencia de la IP cuándo eliminas vuestro contenido*



*de IP o vuestra cuenta a no ser que vuestro contenido ha sido compartido con otros,*

11

En otras palabras,, la empresa de medios de comunicación social tiene el derecho de utilizar cualquier cosa te poste al sitio en cualquier manera quiere. Incluso puede vender vuestro cuadro, vuestras opiniones, vuestra escritura, o cualquier cosa más te poste, ganando dinero de vuestra contribución sin pagarte un penique. Puede utilizar vuestro posted comentarios,

*y no lo han eliminado.*

Críticas, opiniones, calumnia, calumnia (si eres a aquella clase de cosa), y la mayoría de detalles personales tú've posted sobre vuestros niños, vuestro jefe, o vuestro amante. Y no tiene que él anónimamente: si has utilizado vuestro nombre real, el sitio lo puede utilizar, también.

Todo este medio, entre otras cosas, aquellas imágenes te el poste a Facebook puede acabar en otros sitios. Para descubrir si hay cualesquier fotos embarazosas de ti allí en el mundo, puedes actuar qué's llamado una búsqueda de imagen inversa en Google. Para hacer este, clic en el cámara minúsculo dentro de la ventana de búsqueda del Google y cargar cualquier foto de vuestro paseo duro. En unos cuantos minutos verás cualesquier copias de aquella imagen findable on-line. En teoría, si él's vuestra foto, tendrías que saber todos los sitios que viene arriba en los resultados. Aun así, si encuentras que alguien ha posted vuestra foto en un sitio no te gusta, tienes limitó opciones.

Búsquedas de imagen inversa están limitadas por qué es ya posted. En otras palabras,, si hay una imagen similar on-line pero no la imagen misma exacta, Google no lo encontrará. Encontrará cropped versiones de la imagen buscaste, pero en aquel caso el dato central, o bastante de él, queda igual.

Una vez, para mi birthday, alguien intentó crear un sello con mi imagen encima lo. La empresa, Stamps.com, tiene una póliza estricta en contra utilizando imágenes de condenó personas. Mi imagen estuvo rehusada. Quizás ellos una imagen on-line sear ch.

Era en una base de datos a algún lugar como Kevin Mitnick, condenado de un delito.

El año siguiente mi amigo probó una foto más temprana bajo un nombre diferente, uno tomado antes de que era bien sabido. Razonó que quizás esta foto no había sido cargada on-line. Y adivinar qué? Obró. La segunda foto,

espectáculoing un mucho más joven me, estuvo aprobado. Esto asoma las limitaciones de búsquedas de imagen.

Aquello dijo, si encuentras fotos de tú que bastante no ves on-line, tienes unas cuantas opciones.

Primero, contacto el sitio. La mayoría de sitios tienen un “abuse@nameofthesite.com” e- alocución de correo. También podrías contactar el sitio's webmaster en “admin@nameofthesite.com.” Explicar que posees la imagen y no da permiso para él para ser posted. La mayoría de webmasters apeará la imagen sin mucho descalabro. Aun así, si necesitas a you puede archivar una Ley de Copyright de Milenio Digital, o DMCA, petición por e-mailing “Dmca@nameofthesite.com.”

Ser prudente. Misrepresenting Un DMCA la petición podría coger tú a problema, así que busca asesoría jurídica si coge a este nivel. Si todavía puedes't coger la imagen sacó,

entonces considera ir río arriba y contactando el sitio web ISP (si él's Comcast, GoDaddy, u otra empresa). La mayoría tomará un legítimo DMCA petición seriamente.

Además fotos, qué más es en vuestro perfil de medios de comunicación social? No compartirías todo allí es para saber aproximadamente tú con la persona que sienta luego a ti encima el metro. En la misma manera, no es una idea buena de compartir demasiada información personal en sitios web impersonales. Nunca sabes quién está mirando en vuestro perfil. Y una vez es allí, no lo puedes tomar atrás. Piensa cuidadosamente sobre qué te puesto en vuestro perfil—tú don't tiene que llenar en todos los espacios, como el universitarios te atendidos (o incluso cuándo atendiste). De hecho, llena en el menos cantidad de información posiblemente puedes.

También puedes querer crear un perfil de medios de comunicación social dedicado. Don't mentira, sólo ser intencionadamente impreciso con los hechos. Por ejemplo, si creciste arriba en Atlanta, decirte creció arriba en el “southeastern Estados Unidos” o sencillamente “ soy del Del sur.”

También puedes querer crear un “cumpleaños” de seguridad—un día que no es vuestro cumpleaños real—para enmascarar información personal incluso más allá. Ser seguro para mantener pista de vuestros cumpleaños de seguridad, desde entonces son a veces utilizados para verificar vuestra identidad cuándo telefoneas necesidad o apoyo técnicos a reenter un sitio después de que has sido cerrado fuera.

Después de crear o tweaking vuestros perfiles on-line, toma unos cuantos minutos para mirar en las opciones de intimidad en cada sitio. Por ejemplo, dentro Facebook te tendría que habilitar controles de intimidad, incluyendo reseña de etiqueta. Inutilizar “Sugerir fotos de mí a amigos.” Inutiliza “los amigos me pueden comprobar a sitios.”

Los niños con cuentas de Facebook son quizás el más preocupantes. Tienen para llenar en cada caja de espacio pueden, incluso su estado de relación. O inocentemente revelan el nombre de las escuelas atienden y los profesores tienen así como los números de los autobuses montan cada mañana.

Mientras ellos don't necesariamente decir el mundial específicamente dónde viven, pueden tan bien. Necesidad de padres a amigo sus niños, controlar qué ellos poste, y, idealmente, habla por adelantado qué es aceptable y qué no es.

Siendo invisible no te significa puede't actualizaciones de acción sobre vuestra vida personal securely, pero implica ambos sentido común y visitando y revisiting los encuadres de intimidad de los sitios de medios de comunicación sociales utilizas—porque las políticas de privacidad cambian, y a veces no para el mejores. No muestra vuestro cumpleaños, incluso vuestro cumpleaños de seguridad, o en el muy menos esconde él de los amigos “de Facebook”

no personalmente sabes. Considerar un poste que dice Señora Sanchez es una profesora suma . Otro poste

podría ser sobre una feria de oficios en Alamo Elemental. De Google podemos encontrar aquella Señora Sanchez teaches la quinta nota en Alamo Elemental—y de este podemos asumir el titular de cuenta estudiantil tiene alrededor diez años.

A pesar de avisos de Informes de Consumidor y otras organizaciones a quienes hacen poste información personal, las personas continúan decir todo on-line. Recuerda que es perfectamente legal para tercer parties para venir a lo largo de y para tomar aquella información una vez es fuera en público.<sup>12</sup>

Recuerda también que nadie está obligándote a poste información personal. Puedes poste tanto o tan poco como quieres. En algunos casos estás requerido para llenar en alguna información. Beyond Que, decides cuánto compartiendo es bien para ti. Necesitas determinar vuestro nivel de intimidad personal propio y entender que cualquier información proporcionas no puede ser tomado atrás.

Para ayudar a subir el nivel de todas las elecciones, Facebook lanzó una herramienta de chequeo de intimidad nueva en mayo de 2015.<sup>13</sup> A pesar de que a las herramientas les gustan estos, casi trece millones de Facebook usuarios están en 2012 *Consumidor* *dicho revista* de Informes que nunca habían puesto, o no supo aproximadamente, las herramientas de intimidad de Facebook. Y 28 por ciento compartieron todo, o casi todo, sus postes de muro con una audiencia más ancha que sólo sus amigos. Más tellingly, 25 por ciento de aquellos entrevistados por *Informes de Consumidor* dijeron que falsificaron información en sus perfiles para proteger su identidad, y esta cifra era arriba de 10 por ciento en 2010.<sup>14</sup> Al menos estamos aprendiendo.

Mientras tienes el derecho a información de poste aproximadamente tú aquel isn't estrictamente cuidadoso, ser consciente que en California es ilegal al poste on-line como alguien más. Puedes no impersonate otro personaje viviente. Y Facebook tiene una póliza que no te dejará para crear una cuenta bajo un nombre falso.

Esto de hecho pasado a mí. Mi cuenta estuvo suspendida por Facebook porque Facebook me acusó de impersonating Kevin Mitnick. En el tiempo allí era doce Kevin Mitnicks encima Facebook. La situación estuvo fijada cuando CNET corrió una historia sobre el "Kevin" real Mitnick cogiendo cerrado fuera de Facebook.<sup>15</sup>

hay, aun así, muchos razones por qué las personajes podrían necesitar a poste bajo un nombre diferente. Si es importante a ti, entonces encontrar un servicio de medios de comunicación social que te dejas a poste anónimamente o bajo un nombre diferente. Tales sitios, aun así, no emparejará el breadth y lograr de Facebook.

Ser prudente quien te amigo. Si has cumplido la persona presencial, bien.

O si la persona es una amiga de alguien sabes, quizás. Pero si recibes un unsolicited petición, piensa cuidadosamente. Mientras puedes unfriend que persona en cualquier punto, él o ella empero tendrán una oportunidad de ver vuestro perfil entero—y unos cuantos segundos es todo toma para alguien con malicious intent para interferir con vuestra vida. La recomendación mejor es para limitar toda la información personal compartes encima Facebook, porque ha habido ataques muy personales, *incluso entre amigos*, sobre sociales networking sitios web. Y el dato visible a vuestros amigos todavía pueden ser reposted por ellos en otro lugar sin vuestro consentimiento o control.

Te daré un ejemplo. Un tipo una vez me quiso contratar porque era la víctima de extorsión. Había cumplido una chica asombrosa, bella encima

Facebook y empezó enviar sus fotos desnudas de él. Esto continuado para un tiempo. Entonces un día estuvo dicho para enviar esta mujer—quién podría haber sido algún tipo viviendo en Nigeria que utiliza la foto de una mujer—\$4,000. Él , pero entonces me contacté después de que estuvo pedido para enviar otro \$4,000 o sus fotos desnudas serían enviados a todos sus amigos, incluyendo sus padres, encima Facebook. Era desesperado de fijar esta situación. Le dije su opción real única era para decir holas familia o para esperar y ver si el extortionist pasó por con la amenaza. Le dije para parar pagando el dinero—el extortionist no iba a dejar tan mucho tiempo continuó pagar.

Incluso legitimar las redes sociales pueden ser cortadas: alguien podría amigo tú just para coger acceso a alguien sabes. Un agente de aplicación de la ley podría ser buscar información en una persona de interesar quién pasa para ser parte de vuestra red social. Pasa.

Según la Fundación de Frontera Electrónica, las redes sociales han sido utilizadas para vigilancia pasiva por detectives federales para años. En 2011 el EFF liberado una formación de treinta y ocho páginas curso para IRS empleados (obtenidos a través de la Libertad de Ley de Información) que la fundación dijo estuvo utilizado para dirigir investigaciones vía redes sociales.<sup>16</sup> A pesar de que los agentes federales pueden't legalmente fingir ser alguien más, legalmente pueden pedir para ser vuestro amigo. En hacer tan pueden ver todos vuestros postes (según vuestros encuadres de intimidad) así como aquellos de otros en vuestra red. El EFF continúa estudiar los asuntos de intimidad asociaron con esta forma nueva de vigilancia de aplicación de la ley.

A veces las empresas te siguen, o al menos controlarte, si te poste o tweet algo que encuentran objectionable—algo como inocente como comentario sobre una prueba tomaste en escolar, por ejemplo. Para uno estudiantil, un tweet como aquel problema muchísimo causado.

Cuándo Elizabeth C. Jewett, el superintendent del Watchung Cerros Instituto Regional, en Warren, New Jersey, recibió una comunicación del testing empresa que proporcionó su escuela con un statewide examen, su reacción era sorpresa más que preocupación. Estuvo sorprendida que Pearson la educación miraba un estudiantil's cuenta de Twitter en primer lugar. Los menores están dados una cantidad segura de intimidad y libertad de acción cuándo viene a qué ellos poste en medios de comunicación sociales. Pero alumnado—si son en escuela media, instituto, o necesidad—universitaria para darse cuenta aquello qué están haciendo on-line es público y el ser

miró. En este caso uno de Jewett el alumnado hubo presuntamente tweeted material de una prueba estandarizada.

De hecho el estudiante hubo de hecho posted una cuestión sobre una cuestión—no un cuadro de la página de examen, sólo unas cuantas palabras—en un un-día statewide la prueba dada en New Jersey, la Sociedad para Evaluación de Readiness para Universitario y Carreras, o PARCC, prueba. El tweet era posted alrededor 3:00 p.m.—bien después de los estudiantes en el distrito habían tomado la prueba. Después del superintendent habló con un padre del estudiantil quién posted el tweet, el estudiante lo sacó. no había ninguna evidencia de engañar. El tweet—no revelado al público—era un comentario subjetivo más que un solicitation de una respuesta.

Pero el revelation sobre Pearson unnerved personas. “El DOE [Departamento de Educación] nos informé que Pearson está controlando todo social medios de comunicación durante PARCC testaje,” Jewett escribió a sus colegas en un email que un columnista local hecho público sin su permiso. En aquel email Jewett confirmado que al menos tres más los casos habían sido identificados por Pearson y pasados a lo largo de a el estatales DOE.

Mientras Pearson no es sólo en controlar medios de comunicación sociales para detectar robo de hacienda intelectual, su comportamiento cria cuestiones. Cómo, por ejemplo, la empresa sabe la identidad del estudiantil implicado de su mango de Twitter? En una declaración proporcionada al *New York Times*, Pearson dijo: “Una ruptura incluye cualquier tiempo alguien comparte información sobre una prueba exterior del aula—de conversaciones casuales a postes en medios de comunicación sociales. Otra vez, nuestro gol es para asegurar una prueba justa para todos los estudiantes. Cada estudiante merece su o su casualidad de tomar la prueba en un nivel que toca campo.”<sup>17</sup>

El *Tiempo* lo dijo confirmado a través de oficiales en Massachusetts, el cual también está administrando el PARCC prueba, aquel Pearson cruza-tweets de remisión sobre standardized pruebas con listas de estudiantes quiénes han registrado para tomar las pruebas. En este Pearson declinado para comentar para el *Tiempo*.

Para años el estado de California también los medios de comunicación sociales controlados durante su

anuario Estandarizaron Probar e Informando (ESTRELLA) pruebas. En 2013, el último año las pruebas estuvieron dadas statewide, el Departamento de California de Educación identificó 242 escuelas cuyo alumnado posted en

medios de comunicación sociales durante administración de las pruebas, sólo dieciséis del cual incluido postings de cuestiones de prueba o answers.<sup>18</sup>

“El incidente destacó el grado a qué alumnado es debajo vigilancia, tanto dentro y exterior de entornos escolares tradicionales,” dichos Elana Zeide, un socio de búsqueda de la intimidad en el instituto de Ley de la Información de Universidad de Nueva York. “Los medios de comunicación sociales es generalmente vistos como ámbito separado de escolar. Twitter parece más gusta ‘fuera del campus’ habla—de modo que Pearson’ el control es más gusta espiar en estudiantes’ conversaciones en carpools que escolares hallways.”<sup>19</sup>

Aun así, continúa en para decir, “El conversatiencima también necesita mover de enfocar en daños e intereses individuales para tomar las consecuencias más anchas de prácticas de información a cuenta. Escuelas y necesidad de vendedores para parar rechazando padres como Luddites sencillamente porque pueden’t articular un daño concreto e inmediato a su niño. Padres, en turno, necesidad de entender que las escuelas pueden’t defer a todas sus preferencias de intimidad porque hay también intereses colectivos en juego aquello afecta el sistema educativo entero.”

Twitter, con su icónico límite de 140 caracteres, ha acaecido dominante, recogiendo muchísimo según parece detalles minúsculos sobre nuestras vidas diarias. Su política de privacidad reconoce que recoge—y retiene—información personal a través de sus varios sitios web, aplicaciones, servicios de SMS, APIs (la aplicación que programa interfaces), y otras terceras fiestas. Cuando uso de personas Twitter’s servicio, consienten a la colección, traslado, almacenamiento, manipulación, revelación, y otros usos de esta información. Para crear una cuenta de Twitter, un mosto provide un nombre, username, contraseña, y alocución de email. Vuestra alocución de email no puede ser utilizada para más de una cuenta de Twitter.

Otro asunto de intimidad encima preocupaciones de Twitter filtraron tweets—tweets privados que ha sido hecho público. Esto ocurre cuando amigos de someone con una cuenta privada retweet, o copia y paté, el tweet privado de aquella persona a una cuenta pública. Una vez público, no puede ser tomado atrás.

La información personal todavía puede ser peligrosa de compartir encima Twitter, especialmente si vuestros tweets son público (el default). Evita compartir alocuciones, números de teléfono, números de carta del crédito, y números de Seguridad Social encima Twitter.<sup>20</sup> Si tienes que compartir información sensible, uso la característica de mensaje directa para contactar



una personaje concreta. Pero ser consciente que incluso privado o tweets de mensaje directo pueden acaecer públicos.

Para hoy juventud, tan-Generación llamada Z, Facebook y Twitter son ya viejos. Generación Z's acciones en su centro de aparatos móvil alrededor de WhatsApp (irónicamente, ahora parte de Facebook), Snapchat (no Facebook), e Instagram e Instagram Historias (también Facebook). Todas estas aplicaciones son visuales en aquel te dejáis a fotos de poste y vídeos o principalmente fotos de característica o los vídeos tomados por otros.

Instagram, una foto-y aplicación que comparte vídeo, es Facebook para una audiencia más joven. Yot deja sigue, gusta, y chats entre miembros.

Instagram Tiene plazos de servicio y parece para ser responsive para tomar-abajo peticiones por miembros y titulares de copyright.

Snapchat, quizás porque no es poseído por Facebook, es quizás el creepiest del ramo. Snapchat Anuncia que te dejás para enviar un self- destructing foto a alguien. La vida de la imagen es corta, aproximadamente dos segundos, sólo mucho tiempo bastante para el recipient para ver la imagen. Desafortunadamente, dos segundos es mucho tiempo bastante para alguien a grab un rápidamente screenshot aquello dura.

En el invierno de 2013, dos underage chicas de instituto en New Jersey chasquearon fotos de ellos, en cueros, y les envió a un chico en su escuela sobre Snapchat, naturalmente asumiendo que las imágenes serían automáticamente deleted dos segundos después de que les enviaron. Al menos aquello es lo que la empresa dijo pasaría.

Aun así, el chico supo cómo para tomar un screenshot del Snapchat mensaje y más tarde cargó las imágenes a su Instagram aplicación. Instagram No elimina fotos después de que dos segundos. Needless Para decir las imágenes del en cueros underage las chicas fueron viral, y el escolares superintendent tuvo que enviar una casa de nota a los padres que piden que las imágenes ser eliminados de todos los estudiantes' los teléfonos o ellos arriesgarían el ser arrestó encima cargos de pornografía del niño. En cuanto a los tres estudiantes, como menores ellos couldn't ser cobrados con un delito, pero cada cual estuvo sometido a acción disciplinaria dentro del distrito escolar.<sup>21</sup>

Y él's no las chicas justas que envían fotos desnudas a chicos. En el Reino Unido, un chico de catorce años envió un cuadro en cueros de él a una chica en su escuela vía Snapchat, otra vez pensando la imagen desaparecería después de que unos cuantos segundos. La chica, aun así, tomó un screenshot y... Sabes el resto de la historia. Según la BBC, el chico—y la chica—serán

listados en una base de datos de Reino Unido para delitos de sexo incluso aunque son demasiado jóvenes de ser prosecuted.<sup>22</sup>

Como WhatsApp, con su inconsistent capacidades que empañan imagen, Snapchat,

a pesar de la aplicación's promesas, no realmente eliminar imágenes. De hecho Snapchat acordado en 2014 a un poblamiento de Comisión de Comercio Federal sobre cargos que la empresa tuvo engañó usuarios sobre la carácter de desaparecer de sus mensajes, el cual the la agencia federal alegó podría ser salvado o recuperado en un tiempo más tardío.<sup>23</sup> Snapchat's la política de privacidad también dice que no pide, pista, o acceder cualquier ubicación-información concreta de vuestro aparato en cualquier tiempo, pero el FTC encontrado aquellas reclamaciones para ser falsas también.<sup>24</sup>

es un requisito de todos los servicios on-line que las personaje son trece años de edad o más viejo de suscribir. Aquello es por qué estos servicios pedir vuestra cita de nacimiento. Un usuario podría, aun así, sólo decir, debajo pena de perjurio, “juro que soy sobre la edad de trece”—o veintiún o cualquier cosa. Padres quiénes encuentran que su diez-año-olds ha firmado arriba para Snapchat o Facebook les puede informar y tener aquellas cuentas sacaron. Por otro lado, padres quiénes quieren sus niños para tener una cuenta a menudo altera el niño's cita de nacimiento. Aquel dato acaece parte del perfil del niño. De repente vuestro niño de diez años es catorce, el cual significa que él o ella podrían ser coger los anuncios on-line apuntaron en niños más viejos. También nota que cada alocución de email y foto vuestro niño shares sobre el servicio está grabado.

El Snapchat la aplicación también transmite Wi-Fi-basado y celular-información de ubicación basada de usuarios de Androide' aparatos móviles a su analytics siguiendo proveedor de servicio. Si eres un iOS usuario e introducir vuestro número de teléfono para encontrar amigos, Snapchat recoge los nombres y números de teléfono de todos los contactos en vuestro aparato móvil's libro de alocución sin vuestro aviso o consentimiento, a pesar de que iOS apuntará para permiso el primer tiempo está pedido. Mi recomendación es para probar otra aplicación si quieres intimidad cierta.

En Carolina del Norte, un estudiante de instituto y su novia estuvieron cobrados con poseer fotos en cueros de menores incluso aunque las fotos eran de ellos y había sido tomado y compartió consensually. La novia afrontó dos cargos de explotación sexual de un menor: uno para tomar la foto y otro para poseerlo. Sexting Aparte, aquello significa es ilegal para adolescentes

de Carolina del Norte para tomar o poseer fotos desnudas de ellos . En la policía warrant, la novia está listada como both víctima y delincuente.

El novio afrontó cinco cargos, dos para cada foto tomó de él más uno para poseer una foto de su novia. Si condenó podría hacer frente a diez años en prisión y tiene que registro como infractor de sexo para el resto de su vida. Todo para tomar fotos en cueros de él y manteniendo un que su novia le envió.<sup>25</sup>

Cuándo era en instituto, sencillamente cumplí alguien y le pidió fuera. Hoy tienes que puesto alguna información on-line así que las personas te pueden comprobar fuera primero. Pero ser prudente.

Si estás utilizando un sitio de datación y acceso él de alguien más's ordenador, o tener que pasas para utilizar un ordenador público para accederlo, siempre registro fuera. Seriamente. Te don't Querer alguien para pegar el botón Posterior en el navegador y ver vuestra información de datación. O cambiarlo. También, recuerda a uncheck la caja que dice “Recordarme” encima el registro-en pantalla. No quieres esto—o cualquiera otro—ordenador a automáticamente registro alguien más en a vuestra cuenta de datación.

Dice vas en una primera cita, quizás una segunda cita. Personas don't siempre revelar su cierto selves en un primer o segunda cita. Una vez vuestra cita ha friended te encima Facebook o te seguiste encima Twitter o en cualquier otra red social, él o ella pueden ver todos vuestros amigos, vuestros cuadros, vuestros intereses... Las cosas pueden coger ayuno extraño.

Hemos cubierto servicios on-line: qué sobre aplicaciones móviles? Datando las aplicaciones pueden informar vuestra ubicación, y parte de aquel es por diseño. Dice

ves alguien te gusta en vuestra área: entonces puedes utilizar la aplicación para descubrir si aquella persona es cercana. La aplicación de datación móvil Grindr da ubicación muy precisa información para sus suscriptores... Quizás demasiado preciso.

Investigadores Colby Moore y Patrick Wardle del cybersecurity firm Synack era capaz a spoof peticiones a Grindr para seguir algunos de las personas en su servicio como movieron sobre una ciudad sola. Ellos también encontrados que si tuvieron tres cuentas buscan uno individual, podrían triangulate los resultados para coger una medida mucho más precisa de donde aquella persona era en cualquier momento dado.<sup>26</sup>

Quizás datando aplicaciones aren't vuestra cosa, pero incluso logging en al Yelp servicio para buscar un restaurante bueno da tercer-información de negocios de la fiesta sobre vuestro sexo, edad, y location. Un default el encuadre dentro de la aplicación lo deja para enviar información atrás al restaurante, diciéndolo, por ejemplo, que una mujer, edad treinta y un, de Ciudad de Nueva York miraba en su reseña. Puedes, aun así, va a vuestros encuadres y escoger “Basics,” el cual revela sólo vuestra ciudad (desafortunadamente no puedes inutilizar la característica enteramente).<sup>27</sup> Quizás la manera mejor de evitar esto es a no registro en y sencillamente utilizar Yelp como huésped.

Considerando geolocalización, es una idea buena en general para comprobar si *cualesquier* aplicaciones móviles utilizas retransmitido vuestra ubicación. En más casos puedes girar esta característica fuera, cualquiera en cada aplicación individual o enteramente.<sup>28</sup>

Y antes de apalabrar descarga cualquier aplicación de Androide, siempre leído los permisos primero. Puedes ver estos permisos en Juego de Google por iring a la aplicación, entonces desplazando hacia abajo a la sección encima Juego de Google contenta aquello dice “Permisos.” Si los permisos hacen sientes incómodo, o si piensas que dan el desarrollador de aplicación demasiado control, entonces no descarga la aplicación. Apple no proporciona información similar sobre las aplicaciones en su tienda, y en cambio los permisos están apuntados como están necesitados cuándo utilizando la aplicación. De hecho, prefiero utilizar iOS aparatos porque el sistema operativo siempre apunta antes revelando información privada—como mi dato de ubicación. También iOS es mucho más seguro que Androide si te don't jailbreak vuestro iPhone o iPad. Naturalmente, bien-financió adversaries podría adquirir proezas para cualquier sistema operativo en el mercado, pero iOS las proezas son bastante caras—costando encima un millón de dólares.<sup>29</sup>

## CAPÍTULO DIEZ

### Te Puede Correr pero No Esconder

Si llevas vuestro teléfono celular contigo por todas partes el día, como la mayoría de nosotros, entonces no eres invisible. Estás siendo surveilled—incluso si no tienes

la geolocalización que sigue habilitado en vuestro phone. Por ejemplo, si has iOS 8.2 o más temprano, la manzana girará fuera GPS en modo de avión,

pero si tienes una versión más nueva, como la mayoría de nosotros, restos de GPS encima—incluso si eres en modo de avión—a no ser que tomas pasos adicionales.<sup>1</sup> para descubrir cuánto su mobile el transportista supo sobre su actividad diaria, un político alemán prominente, Malte Spitz, traje archivado contra el transportista, y una corte alemana ordenó la empresa para girar sobre sus records. El sheer el volumen de aquellos records asombraba. Sólo dentro de un seis-month periodo, habían grabado su ubicación 85,000 tiempo mientras también siguiendo cada llamada había hecho y recibido, el número de teléfono de la otra fiesta, y cuánto tiempo cada llamada duró. En otras palabras,, esto era el metadata producido por Spitz's teléfono. Y no fue sólo para comunicación de voz pero para mensajes de texto también.<sup>2</sup>

Spitz teamed arriba con otras organizaciones, pidiéndoles a formato el dato y hacerlo público. Una organización produjo a resúmenes diarios les gusta el abajo. La ubicación de la reunión de Fiesta Verde de aquella mañana estuvo constatada de la latitud y la longitud dada en los records de empresa del teléfono.

*Malte Spitz actividad para octubre 12, 2009*

De este dato mismo, otra organización creó un mapa animado. Asoma Spitz minute-por-movimientos de minuto en todas partes Alemania y muestra un símbolo de centellear cada vez hizo o recibió una llamada. Esto es un nivel asombroso de detallar captado en justo pocos días normales.<sup>3</sup>

El dato en Spitz no es un caso especial, naturalmente, ni es esta situación limitó a Alemania. Él's sencillamente un ejemplo llamativo del dato que *vuestra* celda- transportista de teléfono mantiene. Y puede ser utilizado en una corte de ley.

En 2015, un caso antes de la Corte de Estados Unidos de las apelaciones para el Cuarto Circuito implicaron el uso de celda similar-phone records en los Estados Unidos. El caso concernió dos robbers quién atracó un banco, un 7-Once, varios rápido-restaurantes alimentarios, y una tienda de joyas en Baltimore. Por habiendo mano de Sprint encima información sobre la ubicación de los sospechosos primos' teléfonos para el anteriores 221 días, la policía era capaz de ligar los sospechosos a una serie de delitos, ambos por los delitos' proximity a cada cual otro y por los sospechosos' proximity a las escenas

de delito ellos.<sup>4</sup> Un segundo caso, oído por la Corte de Distrito de los Estados Unidos para el Distrito

Del norte de California, no detalló specifics del delito, pero él también centrado en “información de sitio de celda histórica” disponible de Verizon y AT&T para los objetivos' teléfonos. En las palabras de la Unión de Libertades Civil americana, el cual archivó una escrito amicus en el caso, este dato “genera un cercano-récord continuo de un individual's ubicaciones y movimientos.” Cuándo un juez federal celda mencionada-intimidad de teléfono durante el caso de California, el federal prosecutor sugerido que “cellphone usuarios quiénes están concernidos sobre su intimidad podría tampoco no llevar teléfonos o girarles fuera,” según el récord oficial.

Esto parecería para violar nuestra Cuarta Enmienda derecho de ser protegido contra unreasonable búsquedas. La mayoría de personas nunca equipararían sencillamente automovilísticosrying un teléfono celular con forfeiting su derecho no para ser seguido por el gobierno—pero aquello es qué llevando unas cantidades de teléfono a estos días. Ambos casos notan que Verizon, AT&T, y Sprint don't decir clientes en políticas de privacidad ubicación qué dominante que sigue es. Aparentemente AT&T, en una letra a Congreso en 2011, dijo almacena dato celular para cinco años “en caso de enunciar disputas.”<sup>5</sup>

Y dato de ubicación no es almacenado sólo con el transportista; él's también almacenado con el vendedor. Por ejemplo, vuestra cuenta de Google retendrá toda vuestra geolocalización de Androide dato. Y si utilizas un iPhone, la manzana también tendrá un récord de vuestro dato. Para impedir someone de mirar en este dato en el aparato él y para impedir él de ser reculado hasta la nube, periódicamente tendrías que eliminar dato de ubicación de vuestro smartphone. Encima aparatos de Androide, va a Ubicación de Encuadres>del Google>Elimina historia de ubicación. En un iOS aparato necesitas perforar abajo un poco; Apple no lo hace fácil. Va a Servicios>de Ubicación>de Intimidad de Encuadres, entonces desplazar hacia abajo a Servicios “de Sistema,” entonces desplazar hacia abajo a Ubicaciones “Frecuentes,” entonces “Aclarar Historia Reciente.”

En el caso de Google, a no ser que has turned la característica fuera, el dato de geolocalización disponible on-line puede soler reconstruir vuestros movimientos. Por ejemplo, mucho de vuestro día podría ser pasado en una ubicación sola, pero podría haber una explosión de viajar tan cumple con clientes o grab un mordisco para comer. Mmena que perturba es que si cualquiera nunca obtiene acceso a vuestro Google o cuenta de Manzana, aquella persona puede quizás también pinpoint dónde vives o quién vuestros amigos están basados encima dónde pasas la mayoría de vuestro tiempo. En

el muy menos alguien puede imaginar fuera de wsombrero vuestra rutina diaria podría ser.

Así que él's claro que la ley sencilla de ir para un paseo hoy es fraught con oportunidades para otros para seguir vuestro comportamiento. Sabiendo este, decirte conscientemente dejar vuestro teléfono celular en casa. Aquello tendría que solucionar el problema de ser seguido, bien? Bien, aquello depende.

Llevas un aparato que sigue forma física como Fitbit, Maxilar's ARRIBA brazalete, o el Nike+ FuelBand? Si no, quizás llevas un smartwatch de Apple, Sony, o Samsung. Si llevas uno o ambos de esta—una banda de forma física y/o un smartwatch—te todavía puede ser seguido. Estos aparatos y sus aplicaciones acompañantas están diseñados para grabar vuestra actividad, a menudo con información de GPS, así que si está retransmitido vivo o cargó más tarde, todavía puedes ser seguido.

La palabra *sousveillance*, acuñado por la intimidad defiende Steve Mann, es un juego de la vigilancia *de palabra*. La palabra francesa para “encima” es *sur*; la palabra francesa para “abajo” es *sous*. Tan *sousveillance* significa que en vez de ser mirado de arriba—por otras personas o por cámaras de seguridad, por ejemplo, estamos siendo mirados desde abajo “” por los aparatos pequeños que llevamos alrededor y quizás incluso desgaste en nuestros ente.

Rastreadores de forma física y smartwatches biometría récord como vuestro ritmo cardíaco, el número de pasos tomas, incluso vuestra temperatura de ente. Los apoyos de tienda de la aplicación de Apple mucho independientemente creó aplicaciones para seguir salud y wellness en sus teléfonos y relojes. Mismo con la tienda de Juego del Google. Y sorpresa!—Estas aplicaciones están puestas a casa radiofónica el dato a la empresa, aparentemente sólo para recoger él para reseña futura por el dueño pero también para compartirlo, a veces sin vuestro consentimiento activo.

Por ejemplo, durante el 2015 Amgen Visita de California, los participantes en la raza de bicicleta eran capaces de identificar quién había pasado les y más tarde, mientras on-line, directo-mensaje les. Aquello podría coger un poco creepy cuándo unos inicios más extraños que hablan a ti aproximadamente un movimiento particular hiciste durante una raza, un movimiento puedes ni siquiera remember haciendo.

Una cosa similar pasó a mí. En la autopista, conduciendo de Los Ángeles a Las Vega, había sido cortado fuera por un tipo que conduce un BMW. Ocupado en su teléfono celular, de repente cambió caminos, swerving dentro



de pulgadas de mí, asustando el cagar fuera de mí. Él almost secado fuera del ambos de nosotros.

Yo grabbed mi teléfono celular, llamó el DMV, e impersonated aplicación de ley. Cogía el DMV para correr su plato, entonces me dimos su nombre, alocución, y número de Seguridad Social. Entonces llamé AirTouch Celular, impersonating un empleadode Tacto del Aire, y les tuvo una búsqueda en su número de Seguridad Social para cualesquier cuentas celulares. Aquello es cómo yo era capaz de coger su número

de celda. Difícilmente más de cinco minutos después de la otra motor habían cortado me fuera, llamé

el número y le cogió encima el teléfono. Todavía sacudía, meado y enojado. Grité, “Hey, te idiota, I'm el tipo cortaste fuera hace cinco minutos, cuándo tú casi matado nos ambos. Soy del DMV, y si estiras uno más a truco le gusta que, vamos a anular la licencia de vuestra motor!”

Tiene que ser preguntarse a este día cómo algún tipo en la autopista era capaz de coger su celda-número de teléfono. Yo'd gusta pensar la llamada le asustó a acaecer un más considerate motor. Pero nunca sabes.

Qué va alrededor viene alrededor, aun así. En uno señala mi EN&T la cuenta móvil estuvo cortada por algún guión kiddies (un plazo para unsophisticated wannabe hackers) utilizando ingeniería social. El hackers llamado una tienda de AT&T en el Midwest y posado como un empleado en otra tienda de AT&T. Persuadieron el empleado a reinicialización la alocución de email en mi cuenta de AT&T así que podrían reinicialización mi contraseña on-line y acceso de beneficio a mis detalles de cuenta, incluyendo todo mis records de enunciar!

En el caso del Amgen Visita de California, los jinetes utilizaron el Strava aplicación Flyby característica para compartir, por default, dato personal con otro Strava usuarios. En una entrevista en *Forbes*, Gareth Nettleton, director de marketing internacional en Strava, dicho “Strava es fundamentalmente una programa abierta donde los atletas conectan con una comunidad global. Aun así, la intimidad de nuestras atletas es muy importante a nosotros, y hemos tomado mide para habilitar atletas para dirigir su intimidad en maneras sencillas.”<sup>6</sup>

Strava ofrece una intimidad realzada que pone que te dejas para controlar quiénes pueden ver vuestro ritmo cardíaco. También puedes crear intimidad de aparato califica tan otros no pueden ver donde te vivos o donde obras. En el Amgen Visita de California, los clientes podrían optar fuera del Flyby

característica de modo que sus actividades estuvieron marcadas como “privados” en el tiempo de cargar.

Otros aparatos y servicios que siguen forma física ofrece protecciones de intimidad similar. Podrías creer que desde entonces te don't bici seriamente y probablemente no cortará alguien fuera mientras corriendo en la acera alrededor de vuestro complejo de oficina, no necesitas aquellas protecciones. Qué podría ser el daño ? Pero hay other actividades actúas, algunos en privados, aquello todavía podría ser compartido sobre la aplicación y on-line y por tanto crear asuntos de intimidad.

Por él, grabando acciones como dormir o andando arriba de varios vuelos de escalera, especialmente cuándo hecho para un specific propósito médico, como bajar vuestras primas de seguro de la salud, poder no compromise vuestra

intimidad. Aun así, cuándo este dato está combinado con otro dato, un holistic el cuadro de tú empieza para emerger. Y puede revelar más la información que tú son cómodos con.

Uno wearer de un aparato que sigue salud descubierto a revisar su dato on-line que lo asomó un aumento significativo en su ritmo cardíaco siempre que era habiendo sexo.<sup>7</sup> De hecho, Fitbit como empresa sexo informado brevemente como parte de su lista on-line de routinely logged actividades. A pesar de que anónimo, el dato era empero searchable por Google hasta que era públicamente revelado y deprisa sacado por la empresa.<sup>8</sup>

Algunos de ti podrían pensar, “Así que qué?” Ciertamente: no muy interesante por él. Pero cuándo dato de ritmo cardíaco está combinado con, dice, dato de geolocalización, las cosas podrían coger dicey. *Reportero* de fusión Kashmir el cerro tomó el Fitbit dato a su extremo lógico, preguntándose, “Qué si empresas de seguro combinaron vuestro dato de actividad con dato de ubicación del GPS para determinar no sólo cuándo probablemente pudiste habiendo sexo, pero *donde* eras habiendo sexo? Podría una empresa de seguro de la salud identificar un cliente quién cogía afortunado en ubicaciones múltiples por semana, y dar aquella persona un perfil de riesgo médico más alto, basado en su o su alegado promiscuity?”<sup>9</sup>

En el lado de dedo de aquel, Fitbit el dato ha sido exitosamente utilizado en casos de corte para probar o disprove anteriormente unverifiable reclamaciones. En uno caso extremo, Fitbit el dato solió espectáculo que una mujer hubo lied sobre una violación.<sup>10</sup>

A la policía, la mujer—mientras visitando Lancaster, Pensilvania—dijo ella'd despertado alrededor medianoche con un desconocido arriba de su. Más allá alegó que había perdido le Fitbit en la lucha para su emisión. Cuando la policía encontrada el Fitbit y la mujer les dio su consent para accederlo, el aparato dijo una historia diferente. Aparentemente la mujer había sido despierta y andando alrededor toda la noche. Según una canal de televisión local, la mujer estuvo “cobrada con informes falsos a aplicación de ley, alarmas falsas a seguridad pública, y tampering con evidencia para presuntamente overturning mobiliario y colocando un cuchillo en la escena para hacer aparece había sido violada por un intruso.”<sup>11</sup>

Por otro lado, rastreadores de actividad también pueden soler reclamaciones de incapacidad del apoyo. Una empresa de ley canadiense utilizó unctivity-dato de rastreador para asomar las consecuencias severas de un cliente's daño de obra. El cliente había proporcionado la empresa de dato Vivametrica, el cual recoge dato de wearable aparatos y lo compara a dato sobre la actividad y salud de la población general, con Fitbit el dato que asoma una disminución marcada en su actividad. “Caja ahora siempre hemos tenido que confiar en interpretación clínica,” Simon Muller, de McLeod Ley, LLC, en Calgary, dijo *Forbes*. “Ahora estamos mirando en periodos más largos de tiempo a través del curso de un día, y tenemos dato duro.”<sup>12</sup>

Incluso si te don't tener un rastreador de forma física, smartwatches, como la Tren de Galaxia, por Samsung, puede compromise vuestra intimidad en maneras similares. Si recibes rápidamente-notificaciones de mirada, como textos, emails, y llamadas de teléfono, encima ynuestra muñeca, otros podrían ser capaces de ver aquellos mensajes, también.

Allí's sido crecimiento enorme recientemente en el uso de GoPro, un cámara minúsculo que atas a vuestro casco o al salpicadero de vuestro automovilístico de modo que puede grabar un vídeo de vuestros movimientos. Pero qué pasa si olvidas la contraseña a vuestro GoPro aplicación móvil? Un investigador israelí tomó prestado su amigo's GoPro y la aplicación móvil asociada con él, pero no tuvo la contraseña. Gusta email, el GoPro la aplicación te dejás a reinicialización la contraseña. Aun así, el procedimiento—qué desde entonces ha sido cambiado—era defectuoso. GoPro Enviado un enlace a vuestro email como parte del proceso de reinicialización de la contraseña, pero esto enlaza de hecho dirigido a una CREMALLERA archiva aquello era para ser descargado e insertado al aparato SD carta. Cuando el investigador abreed la lima de CREMALLERA encontró una lima de texto nombró “encuadres” que contuvo el usuario

inalámbrico credentials—incluyendo el SSID y contraseña el GoPro utilizaría para acceder el Internet. El investigador descubrió que si cambió el número en el enlace—8605145—a otro número, dice 8604144, podría acceder otras personas's GoPro dato de configuración, el cual incluido sus contraseñas inalámbricas.

Podrías discutir que Eastman Kodak salto-empezó la discusión de intimidad en América—o al menos lo hizo interesando—en el tardío 1800s. Hasta aquel punto, la fotografía era un serio, que consume tiempo, el arte inconveniente que requiere equipamiento especializado (cámaras, luces, darkrooms) y tramos largos de inmovilidad (mientras los temas posaron en un estudio). Entonces Kodak vino a lo largo de y presentó un portátil, relativamente cámara asequible. El primer de su línea vendida para \$25—alrededor \$100 hoy. Kodak Posteriormente presentó el Brownie cámara, el cual vendió para un mero \$1. Ambos estas cámaras estuvieron diseñados para ser tomados fuera de la casa y oficina. Eran los ordenadores móviles y teléfonos celulares de su día.

De repente las personas tuvieron que tratar el hecho que alguien en la playa o en un parque público podría tener un cámara, y que la persona de hecho te podría incluir dentro el marco de una foto. Tuviste que mirar bueno. Tuviste que obrar responsablemente. “No fue sólo cambiando vuestra actitud hacia fotografía, pero hacia la cosa él que te fotografiaba,” dice Brian Wallis, jefe anterior

curator en el Centro Internacional de Fotografía. “Así que tuviste que escenificar una cena, y escenificar una fiesta de cumpleaños.”<sup>13</sup>

I cree de hecho hacemos behave de manera diferente cuándo estamos siendo miró. La mayoría de nosotros es en nuestro comportamiento mejor cuándo sabemos allí's un cámara encima nos, aun así naturalmente siempre habrá quienes no se podrían preocupar menos.

El advenimiento de la fotografía también influida cómo las personas sentían sobre su intimidad. De repente podría haber un récord visual de alguien behaving mal. De hecho, hoy tenemos pizca cams y cámaras de ente en nuestros agentes de aplicación de la ley tan habrá un recordón de nuestro comportamiento cuándo estamos afrontar con la ley. Y hoy, con tecnología de reconocimiento facial, puedes tomar un cuadro de alguien y tenerlo emparejado a su o su perfil de Facebook. Hoy hemos selfies.

Pero en 1888, aquella clase de exposición constante era todavía una novedad impresionante y desconcertanda. El *Hartford Courant* sonado una alarma: “El sedate el ciudadano puede't indulge en cualquier hilariousness sin

incurrir el riesgo de ser cogido en la ley y teniendo su fotografía pasó alrededor entre su domingo-school niños. Y el joven amigo quién desea a cuchara con su chica mejor mientras navegando abajo el río se tiene que mantener constantemente anidado por su paraguas.”<sup>14</sup>

a Algunas personas no les gustó el cambio. En el 1880s, en los Estados Unidos, un grupo de mujeres smashed un cámara a bordo un tren porque ellos didn't querer su dueño para tomar su cuadro. En el Reino Unido, un grupo de chicos británicos ganged juntos de vagar las playas, amenazantes cualquiera quién intentó tomar cuadros de las mujeres que salen del océano después de un nadar.

Escritura en el 1890s, Samuel Warren y Louis Brandeis—el último de quien posteriormente servido en la Corte Suprema—escribió en una prenda que “diario y fotografías instantáneos la empresa ha invadido el sagrado precincts de vida privada y doméstica.” Propusieron que ley de EE.UU. formalmente tendría que reconocer intimidad y, en separar a raíz la marea de fotografía subrepticia, impone responsabilidad para cualesquier intrusiones.<sup>15</sup> Tales leyes estuvieron pasadas en varios estados.

Hoy varias generaciones han crecido arriba con la amenaza de fotografías instantáneas—Polaroid, cualquiera? Pero ahora tenemos que también contender con la ubicuidad de fotografía. En todas partes vas estás atado para ser captado encima vídeo—si o no das vuestro permiso. Y aquellas imágenes podrían ser accesibles a anyone, anywhere en el mundo.

Vivimos con una contradicción cuándo viene a intimidad. Por un lado lo valoramos intensely, consideración él como derecho, y verlo tan atado arriba en nuestra libertad e independencia: shouldn't cualquier cosa hacemos en nuestra hacienda propia, detrás cerró puertas, queda privado? Por otro lado, los humanos son criaturas curiosas. Y ahora tenemos el medio para cumplir aquella curiosidad en anteriormente unimaginable maneras.

Nunca preguntarse qué es sobre aquella valla a través de la calle, en vuestro vecino's backyard? La tecnología puede ser capaz de contestar aquella cuestión para casi cualquiera. Drone Empresas como 3D Robóticas y CyPhy make lo fáciles hoy para la media Joe para poseer su propio drone (por ejemplo, tengo el DJI Phantom 4 drone). Drones Es remoto-aeronave controlada y significativamente más sofisticado que la clase utilizaste para ser capaz de comprar en Radiofónico Shack. Casi todos vienen with cámaras de vídeo minúsculo. Te dáis la casualidad de ver el mundo en una manera nueva. Algunos drones también puede ser controlado de vuestro teléfono celular.

Personal drones es Peeping Toms en esteroides. Casi nada es fuera de bounds ahora que te puede cercar unos cuantos pies de centenar por encima de la tierra.

Actualmente la industria de seguro utiliza drones para razones empresariales. Piensa sobre aquel. Si eres un seguro adjuster y necesidad de coger un sentido de la afección de una hacienda estás a punto de asegura, puedes volar un drone alrededor lo, ambos a visually inspeccionar áreas no tuviste acceso a antes de que y para crear un récord permanente de qué encuentras. Puedes volar alto y cariz abajo para coger el tipo de ver que anteriormente sólo podrías haber cogido de un helicóptero.

El personal drone es ahora una opción para espiar en nuestros vecinos; sólo podemos volar alto encima alguien's techo y cariz abajo. Quizás el vecino tiene un grupo. Quizás al vecino le gusta bañar en el desnudo. Las cosas han cogido complicó: tenemos la expectativa de intimidad dentro de nuestras casas propias y en nuestra hacienda propia, pero ahora aquello's el ser desafío. Google, por ejemplo, máscaras fuera de caras y platos de licencia y otra información personal encima Vista de Calle del Google y Tierra de Google. Pero un vecino con un privado drone te das ninguno de aquellas garantías—aunque puedes probar pedir le amablemente no para volar sobre vuestro backyard. Un vídeo-equipado drone te das Tierra de Google y Vista de Calle del Google combinaron.

Hay algunos controles. La Administración de Aviación Federal, para caso, tiene directrices declarando que un drone no puede dejar la línea del operador de vista, que lo no puede volar dentro de una distancia segura de aeropuertos, y que lo no puede volar en las cotas que superan niveles seguros.<sup>16</sup> Allí's una aplicación llamó B4UFLY que ayudará determinas dónde para volar vuestro drone.<sup>17</sup> Y, en respuesta a comercial drone uso, varios estados han pasado leyes restringiendo o severamente

limitando su uso. En Texas, los ciudadanos normales no pueden volar drones, a pesar de que hay excepciones—incluyendo un de verdad agentes de propiedad. La actitud más liberal hacia drones es quizás encontrado en Colorado, donde los civiles legalmente pueden disparar drones fuera del cielo.

En un mínimo el gobierno de EE.UU. tendría que requerir drone entusiastas para registrar sus juguetes. En Los Ángeles, donde vivo, alguien chocó un drone a líneas de poder en Hollywood Del oeste, cercano la intersección de Larrabee Calle y Bulevar de Ocaso. Tenido el drone sido registrado, las potestades podrían saber quién inconvenienced sietecientas personas para las



horas encima acaban mientras las docenas de empleadas de empresa del poder obraron into la noche para restaurar poder al área.

Las tiendas minoristas cada vez más quieren coger para saber sus clientes. Un método que de hecho las obras es una clase de celda-telefonar IMSI catcher (ve [aquí](#)). Cuando andas a una tienda, el IMSI catcher grabs información de your teléfono celular y de alguna manera cifras fuera de vuestro número. De allí el sistema es capaz a toneladas de consulta de bases de datos y construir un perfil encima te. Ladrillo-y-detallistas de mortero también están utilizando tecnología de reconocimiento facial. Piensa de él como supersize Walmart greeter.

“Hola, Kevin,” podría ser el saludo estándar cojo de un empleado en el no-demasiado-futuro distante, incluso aunque nunca podría haber sido en aquella tienda antes de que. El personalization de vuestra experiencia minorista es otra, albeit muy sutil, forma de vigilancia. Podemos ya no tienda anónimamente.

En junio de 2015, apenas dos semanas después de apoyar encima Congreso para pasar la Libertad de EE.UU. Obra—una versión modificada de la Ley de Patriota con alguna protección de intimidad añadió—nueve intimidad de consumidor grupos, algunos del cual hubo lobbied heavily a favor de la Ley de Libertad, creció frustrado con varios detallistas grandes y andados fuera de negociaciones para restringir el uso de reconocimiento facial.<sup>18</sup>

En el asunto era si los consumidores tienen que por default tiene que dar permiso antes de que pueden ser escaneados. El sombrero suena razonable, aún así no uno de las organizaciones minoristas importantes implicó en las negociaciones cede este punto. Según ellos, si andas a sus tiendas, tendrías que ser juego justo para escanear e identificación.<sup>19</sup>

Algunas personas pueden querer aquella clase de atención personal cuando andan a una tienda, pero muchos de nosotros lo encontrarán sólo sencillos unsettling. Las tiendas lo ven otra manera. No quieren dar consumidores el derechos de optar fuera porque ellos're intentando coger sabidos shoplifters, quién sencillamente optaría fuera si aquello era una opción. Si el reconocimiento facial automático está utilizado, sabido shoplifters sería

identificado el momento introducen una tienda. Qué los clientes dicen? Al menos en el Reino Unido, siete fuera de diez

encuestados de estudio encuentran el uso de tecnología de reconocimiento facial dentro de una tienda “demasiado creepy.”<sup>20</sup> Y algunos estados de EE.UU., incluyendo Illinois, ha tomado él a ellos



para regular la colección y almacenamiento de biometric dato.<sup>21</sup> Estos controles han dirigido a pleitos. Por ejemplo, un hombre de Chicago está demandando Facebook porque no dio el servicio on-line expresa permiso para utilizar tecnología de reconocimiento facial para identificarle en las fotos de otras personas.<sup>22</sup>

reconocimiento Facial puede soler identificar una persona basó sólo en su o su imagen. Pero qué si ya sabes quién la persona es y sólo quieres hacer seguro es donde tendría que ser? Esto es otro uso potencial de reconocimiento facial.

Moshe Greenshpan es el CEO del Israel-y Las Vega-basaron Cara de empresa de reconocimiento facial-Seis. Su software Churchix está utilizado para—entre otras cosas que—toman attendance en iglesias. La idea es para ayudar las iglesias identifican el congregants quiénes atienden irregularmente con objeto de fomentarles para venir más a menudo y para identificar el congregants quiénes *asiduamente* atienden con objeto de fomentarles para dar más dinero a la iglesia.

Cara-Seis dice hay al menos treinta iglesias alrededor del mundiales utilizando su tecnología. Todas las necesidades de iglesia para hacer es carga alto-fotos de calidad de su congregants. El sistema entonces será en el vigía para ellos en servicios y funciones sociales.

Cuándo pedido si las iglesias dicen su congregants están siendo seguidos, Greenshpan Fusión *dicha*, “I don't pensar las iglesias dicen personas. Les fomentamos para hacer tan pero no pienso hacen.”<sup>23</sup>

Jonathan Zittrain, director de Escuela de Ley del Harvard's Berkman Centro para Internet y Sociedad, ha facetiously sugirió que los humanos necesitan un “nofollow” a etiqueta le gustan los utilizados en sitios web seguros.<sup>24</sup> Esto mantendría personas que quieren optar fuera de aparecer en bases de datos de reconocimiento facial. Hacia aquel fin, el Instituto Nacional de Informatics, en Japón, ha creado una visera “de intimidad comercial.” El eyeglasses, los cuales venden para alrededor \$240, el producto ligero visible único a cámaras. El photosensitive la luz es emitted unaronda los ojos a thwart sistemas de reconocimiento facial. Según temprano testers, los vasos son exitosos 90 por ciento del tiempo. El único caveat parece para ser que no son propio para conducir o ciclismo. No pueden ser todo aquel de moda, either, pero son perfectos para ejercitar vuestro derecho a intimidad en un sitio público.<sup>25</sup>

Sabiendo que vuestra intimidad puede ser compromised cuándo eres fuera en el

abierto, podrías sentir más seguro en la intimidad de vuestro coche, vuestra casa, o incluso vuestra oficina. Desafortunadamente aquello es ya no el caso. En el próximo pocos capítulos explicaré por qué.

## CAPÍTULO ONCE

# Hey, KITT, no Comparte Mis Investigadores

de Ubicación Charlie Miller y Chris Valasek era ningún desconocido a cortar coches. Anteriormente el dos había cortado un Toyota Prius—pero

habían hecho tan mientras físicamente conectados al automovilísticos y sentando en el backseat. Entonces, en el verano de 2015, Molinero y Valasek tenido éxito en tomar sobre los controles principales de un Jeep Cherokee mientras viajaba en setenta millas por hora abajo una autopista en St. Louis. Podrían remotely control un coche sin ser anywhere cercano lo.<sup>1</sup>

El Jeep en cuestión tuvo una motor—*reportero* Alambrado Andy Greenberg. Los investigadores habían dicho Greenberg por adelantado: ningún asunto qué pasa, no pánico. Aquello resultó para ser un orden alto, incluso para un tipo que estuvo a la espera para tener su coche cortó.

“Inmediatamente mi acelerador paró obrar,” Greenberg escribió de la experiencia. “Como frenéticamente pulsé el pedial y miró el RPMs sube, el Jeep perdió a medias su velocidad, entonces retrasado a un crawl. Esto ocurrió tan logré un largo overpass, sin hombro para ofrecer una evasión. El experimento había cesado para ser divertido.”

Después, los investigadores afrontaron alguna crítica para ser “temerario” y peligroso. “” Greenberg's El jeep era en una carretera pública, no en una pista de prueba, así que aplicación de ley del Misuri es, en el tiempo de esta escritura, todavía considerando cargos de prensado en contra Molinero y Valasek—y posiblemente Greenberg.

Cortando conectó coches remotely ha sido hablado aproximadamente para años, pero él

Tomó Molinero y Valasek experimento para coger la industria de automóvil para parar atención. Si fue truco “cortando” o búsqueda legítima, cogía fabricantes automovilísticos para empezar pensando seriamente sobre cybersafety—y aproximadamente si el congreso tendría que prohibir el cortando de automóviles.<sup>2</sup>

Otros investigadores han asomado pueden revocar ingeniero el protocolo que controla vuestro vehículo por interceptar y analizando el GSM o CDMA tráfico de vuestro coche onboard ordenador al automaker's sistemas. Los investigadores eran capaces a spoof el automotive sistemas de control por enviar mensajes de SMS para cerrar y unlock puertas automovilísticas. Algunos haber incluso hijacked capacidades de inicio remoto que utilizan los mismos métodos también. Pero Molinero y Valasek era el primer para ser capaz de tomar control completo de un automovilístico remotely.<sup>3</sup> Y alegan que, por utilizar los mismos métodos, podrían tomar sobre coches en otros estados también.

Quizás el resultado más importante del Molinero-Valasek el experimento era un retirar por Chrysler de más de 1.4 millones de sus coches debido a una programación emiten—el primero retirar de su clase. Como una medida interina, Chrysler también suspendió el afectó coches' conexión a la red de Sprint, el cual los coches habían utilizado para telematics, el dato que los coches recogen y acción con el fabricante en tiempo real. Miller y Valasek dicho una audiencia en DEF CON 23 que se habían dado cuenta podrían hacer aquel—tomar sobre coches en otros estados—pero ellos conocieron no fue ético. En cambio dirigieron su experimento controlado con Greenberg en la ciudad natal de Miller.

En este capítulo hablaré las varias maneras los coches conducimos, los trenes montamos, y las aplicaciones móviles utilizamos a poder nuestro diariamente commute a la obra es vulnerable a cyberattacks, no para mencionar la intimidad numerosa compromises que nuestro conectó los coches presentan a nuestras vidas.

Cuándo Johana Bhuiyan, un reportero para BuzzFeed, llegado en las oficinas de Nueva York de Uber, el servicio que llama automovilístico, en uno de Uber's coches propios, Josh Mohrer, la gerente general, esperaba. “Allí eres,” dijo, aguantando arriba de su iPhone. “Te seguía.” No fue un inicio auspicioso a su entrevista, el cual tocó a, entre otras cosas, intimidad de consumidor.<sup>4</sup>

Hasta Bhuiyan's la historia pareció, en noviembre de 2014, pocos exteriores de Uber era incluso consciente de Vista de Dios, una herramienta con qué

Uber pista la ubicación de sus miles de motor de contrato así como sus clientes, todo en tiempo real.

Como mencioné más temprano, aplicaciones routinely pedir usuarios para varios permisos, incluyendo el derechos de acceder su dato de geolocalización. El Uber la aplicación va incluso más allá: pide vuestro aproximado (Wi-Fi) y preciso (GPS) ubicación, el

derecho de acceder vuestros contactos, y no deja vuestro aparato móvil para dormir (así que puede mantener tabuladores encima dónde eres).

Bhuiyan Presuntamente dijo Mohrer arriba frente que no dio el permiso de empresa para seguirle en cualquier momento y anywhere. Pero ella, a pesar de que quizás no explícitamente. El permiso era en el acuerdo de usuario consintió a a descargar el servicio a su aparato móvil. Después de su reunión, Mohrer e- mailed Bhuiyan registros de algunos de su recent Uber viajes.

Uber Compila un dossier personal para cada cliente, grabando cada viaje solo él o ella hace. Aquello es una idea mala si la base de datos isn't seguro. Sabido en el negocio de seguridad como honeypot, el Uber la base de datos puede atraer todas las clases de snoops, del gobierno de EE.UU. a chino hackers.<sup>5</sup>

En 2015, Uber cambiado algunos de sus políticas de privacidad—en algunos casos en detrimento del consumidor.<sup>6</sup> Uber ahora recoge dato de geolocalización de todo EE.UU.-basó usuarios—incluso si las carreras de aplicación sólo en el de fondo e incluso si el satélite y las comunicaciones celulares están girados fuera. Uber Lo dijo utilizará Wi-Fi y alocuciones de IP para seguir los usuarios “off-line.” Aquello significa el Uber leyes de aplicación como espía silencioso en vuestro aparato móvil. La empresa no, aun así, decir por qué necesita esta capacidad.<sup>7</sup>

Ni ha Uber plenamente explicado por qué necesita Vista de Dios. Por otro lado, según la política de privacidad de la empresa: “Uber tiene una póliza estricta que prohíbe todos los empleados en cada nivel de acceder un jinete o el dato de la motor. La excepción única a esta póliza es para un conjunto limitado de propósitos empresariales legítimos.” El negocio legítimo podría incluir controlar las cuentas sospecharon de fraude y resolviendo asuntos de motor (por ejemplo, perdió conexiones). Probablemente no incluye siguiendo los viajes de un reportero.

Podrías pensar Uber daría sus clientes el derechos de eliminar siguiendo información. Núm. Y si después de que lectura esto tú've eliminado la

aplicación de vuestro teléfono, bien, suposición qué? El dato todavía existe dentro de Uber.<sup>8</sup>

Bajo la intimidad revisada policy, Uber también recoge vuestra información de libro de la dirección. Si tienes un iPhone, puedes ir a vuestros encuadres y cambiar vuestra preferencia para contactar compartir. Si posees un Androide, aquello no es una opción.

Uber Los representantes han alegado que la empresa es not actualmente recogiendo esta clase de dato de cliente. Por incluir colección de dato en la política de privacidad, aun así, el cual existiendo los usuarios ya han apalabrado y qué usuarios nuevos tienen que apalabrar, la empresa asegura que puede rodar fuera de estas características en cualquier time. Y el usuario no tendrá cualquier reparación.

Uber's Vista de dios es quizás bastante para hacerte nostalgic para regular viejo taxicabs. Antiguamente, saltarías a un taxi, estado vuestro destino, y pagar en metálico para el paseo una vez llegaste. En otras palabras,, vuestro viaje sería casi completamente anónimo.

Con el advenimiento de casi aceptación universal de cartas de crédito en el tempranos veinte-primer siglo, las transacciones normales muchísimas han acaecido localizables, y tan probablemente hay un récord de vuestro paseo de taxi a algún lugar—quizás lo doesn't residir con una motor concreta o empresa, pero ciertamente reside con vuestra empresa de carta del crédito. Atrás en el 1990s I utilizado para obrar como detective privado, y podría imaginar fuera de los movimientos de mi objetivo por obtener su carta de crédito transacciones. Uno necesita cariz único en una declaración para saber que última semana montaste un taxi en Ciudad de Nueva York y pagó \$54 para aquel viaje.

Alrededor 2010 taxis empezaron para utilizar dato de GPS. Ahora la empresa de taxi sabe vuestro pickup y gota-fuera ubicación, la cantidad de vuestro boleto, y quizás el número de carta del crédito asociado con vuestro viaje. Este dato está mantenido privado por Nueva York, San Francisco, y otras ciudades que apoyo el movimiento de dato abierto en gobierno, proporcionando investigadores con ricos—y anonymized—conjuntos de dato. Mientras los nombres no son incluidos, qué daño allí podría ser en hacer tal anonymized público de dato?

En 2013, Anthony Tockar, entonces un Northwestern estudiante de posgrado Universitario interning para una empresa llamó Neustar, mirado en el anonymized metadata públicamente liberado por the Taxi de Ciudad de la Nueva York y Comisión de Limusina. Este conjunto de dato contuvo un

récord de cada viaje tomado por los coches en su flota durante el año anterior e incluido el número de taxi, el pickup y gota-de tiempo, las ubicaciones, el boleto y cantidades de punta, y anonymized (hashed) versiones de los taxis' licencia y números de medallón.<sup>9</sup> Por él, este conjunto de dato no es muy interesante. El hash el valor en este caso es desafortunadamente relativamente fácil de deshacer.<sup>10</sup>

Cuándo combinas el dato público puesto con otros conjuntos de dato, aun así, empiezas para coger un cuadro completo de qué's yendo en. En este caso, Tockar era capaz de determinar donde celebridades concretas como Bradley Cooper y Jessica Alba habían tomado sus taxis dentro Ciudad de Nueva York durante el año anterior. Cómo hace este salto?

El geolocalización tenida ya dato, así que supo dónde y cuándo los taxis eligieron arriba y caídos de sus boletos, pero tuvo que ir más allá para determinar

11

quién era dentro del taxi . Así que combinó el Taxi de Ciudad de la Nueva York y Comisión de Limusina metadata con fotos on-line de los sitios web tabloides

normales disponibles on-line. Una base de datos de paparazzi. Piensa sobre aquel. Paparazzi frecuentemente celebridades de fotografía tan

introducen y salir los taxis de Ciudad de Nueva York. En estos casos el número de medallón único del taxi es a menudo visible dentro de la imagen. Está imprimido en el lado de cada taxi. Así que un número de taxi fotografió al lado Bradley Cooper, para caso, podría ser emparejado al dato públicamente disponible con respecto a pickup y gota-de ubicaciones y boleto y cantidades de punta.

Afortunadamente, no todo de nosotros tiene paparazzi en nuestra estela. Aquello no significa allí aren't otras maneras de localizar nuestros viajes, aun así. Quizás no tomas taxis. Es allí otras maneras de determinar vuestra ubicación? hay. Incluso si tomas transporte público.

Si montas un autobús, tren, o transbordador para obrar, tú're ya no invisible entre las masas. Transit Los sistemas son experimenting con utilizar aplicaciones móviles y comunicación de campo cercano (NFC) a jinetes de etiqueta como suben y marchar transporte público. NFC Es a escaso-distancia señal radiofónica que a menudo requiere contacto físico. Sistemas de pago como Paga de Manzana, Paga de Androide, y Samsung Paga todos utilizan NFC para hacer fumbling para barrios una cosa del pasado.

Dejado's dice tienes un NFC-teléfono habilitado con una aplicación de vuestro local transit la potestad instalada. La aplicación querrá una conexión a vuestra cuenta de banco o carta de crédito de modo que siempre puedes entablar cualquier autobús o tren o transbordador sin preocuparse sobre un saldo negativo en vuestra cuenta. Aquella conexión a vuestro número de carta del crédito, si no es ocultado por un token, o placeholder, número, podría revelar al transit potestad quién eres. Reemplazando vuestro número de carta del crédito con un alconocimiento es una opción nueva que Manzana, Androide, y Samsung oferta. Aquella manera el mercader—en este caso el transit la potestad—sólo tiene un token y no vuestro número de carta de crédito real. Utilizando un token cortará abajo en los datos incumple afectar cartas de crédito en un futuro próximo porque el delincuente entonces necesidad dos bases de datos: el token, y el número de carta de crédito real detrás del token.

Pero decirte don't uso un NFC-teléfono habilitado. En cambio tienes un transit carta, como el CharlieCard en Boston, el SmarTrip carta en Washington, D.C., y la carta de Clíper en San Francisco. Estas cartas utilizan tokens para alertar el aparato de recibir—si un turnstile o un boleto-caja de colección—que hay bastante de un saldo para ti para montar el autobús, tren, o transbordador. Aun así, transit los sistemas no utilizan tokens en el fin posterior. La carta él ha sólo un número de cuenta—no vuestra información de carta del crédito—en su tira magnética. Pero si el transit la potestad era para ser incumplido en el fin posterior, entonces vuestra carta de crédito o información

de banco también podrían ser expuestas. Also, algunos transit los sistemas te quieren para registrar para sus cartas on-line de modo que te pueden enviar email, significando vuestras alocuciones de email también podrían ser expuestas en un tajo futuro. Cualquier manera, la capacidad a anónimamente montar un autobús en gran parte ha salido la ventana unless te paga para la carta que utiliza dinero efectivo, no abonar.<sup>12</sup>

Este desarrollo es enormemente útil para aplicación de ley. Porque estos commuter-empresas de carta son en privado poseídas terceras fiestas, no gobiernos, pueden poner cualquier cosa gobierna quieren aproximadamente compartiendo data. Lo pueden compartir no sólo con aplicación de ley pero también con los abogados que persiguen casos civiles—en caso vuestro ex te quiere acosar.

Así que alguien mirando en el transit registros de potestad podrían saber exactamente quién pasó por una canal de metro en tal-y-tal tiempo—pero que la persona no podría saber cuáles entrenan su objetivo entabló,



especialmente si la canal es un hub para varias líneas. Qué si vuestro aparato móvil podría resolver la cuestión del cual te entrena entonces montó y por tanto inferir vuestro destino?

Investigadores de la Universidad de Nanjing, en China, decidieron para contestar aquella cuestión por enfocar su obra encima algo dentro de nuestros teléfonos llamando un acelerómetro. Cada aparato móvil tiene uno. Es un chip minúsculo responsable para determinar la orientación de vuestro aparato—si estás aguantando él en paisaje o vista de retrato. Estos chips son tan sensibles que los investigadores decidieron utilizar datos de acelerómetro sólo en sus cálculos. Y efectivamente, eran capaces a con exactitud pronosticar qué metro entrena un usuario está montando. TSuyo es porque la mayoría de líneas de metro incluyen turnos que afectan el acelerómetro. También importante es el periodo de tiempo entre parones de canal—necesitas sólo para mirar en un mapa para ver por qué. La exactitud de sus predicciones mejoró con cada canal al que pasó. Los investigadores alegan su método tiene una 92 exactitud de porcentaje tasa.

Dejado es decir posees un coche de modelo viejo y te conduces para obrar. Podrías pensar que eres invisible—sólo uno de un millón de coches en la carretera hoy. Y podrías ser derecho. Pero tecnología nueva—incluso si no es separar del automovilístico él—está erosionando vuestro anonimato. Las casualidades son, con esfuerzo, alguien todavía te podría identificar whizzing por en la autopista bastante deprisa.

En la ciudad de San Francisco, la Agencia de Transporte Municipal ha empezado para utilizar el FasTrak sistema de peaje, el cual te deja para cruzar cualquiera de la Ocho Área de Bahía puentes con facilidad, para seguir los movimientos de FasTrak—habilitó coches durante la ciudad. Utilizando la tecnología similar a qué uso de puentes del peaje para

leer el FasTrak (o E-ZPass) aparato en vuestro coche, la ciudad ha empezado buscando aquellos aparatos como círculo de usuarios alrededor buscando aparcamiento. Pero los oficiales no son siempre interesados en *vuestros* movimientos: bastante, están interesados en el aparcamiento espacio—la mayoría de qué está equipado con metros de aparcamiento electrónico. Espacios que es altamente buscado después de que puede cobrar una tasa más alta. La ciudad puede wirelessly ajustar el precio en los metros concretos que—incluyen los metros cercanos un caso popular.

Además, en 2014 oficiales decidieron no para utilizar peaje humano takers en el Puente de Puerta Dorada, así que todo el mundo, incluso turistas, está requerido para pagar electrónicamente o recibir una factura en el correo. Qué

hacer las potestades saben dónde para enviar vuestra factura? Fotografían vuestro plato de licencia cuándo cruzas el peaje plaza. Esta licencia-fotografías de plato son también utilizadas a nab rojos-corredores ligeros en intersecciones problemáticas. Y cada vez más, la policía está utilizando una estrategia similar como conducen por aparcar parcelas y vados residenciales.

Departamentos policiales passively pista vuestro automovilístico's movimientos todos los días con reconocimiento de plato de licencia automatizado (ALPR) tecnología. Pueden fotografiar el plato de licencia de vuestro coche y tienda que dato, a veces para años, según la póliza del departamento policial. ALPR camerComo escáner y leer cada plato pasan, si el coche está registrado a un criminal o no.

Aparentemente ALPR la tecnología está utilizada principalmente para localizar coches robados, quiso delincuentes, y asistir con Alertas de ÁMBAR. La tecnología implica tres cámaras montaron to la copa de un patrullero automovilístico aquello es hooked hasta una pantalla de ordenador dentro del vehículo. El sistema es más allá enlazado a un Departamento de base de datos de Justicia que mantiene pista de los platos de licencia de vehículos y coches robados asociaron con delitos. Como unos paseos de agente, el ALPR la tecnología puede escanear hasta sesenta platos por segundo. Si un plato escaneado empareja un plato en el DOJ base de datos, el agente recibe una alerta tanto visually y audibly.

El *Wall Street Journal* primero informado encima tecnología de reconocimiento de plato de licencia en 2012.<sup>13</sup> En asunto para quienes oppose o cuestionar ALPR la tecnología no es el sistema él sino cuánto tiempo el dato está mantenido y por qué algunas agencias de aplicación de la ley no lo liberarán, incluso al dueño del ser automovilístico siguió. Es una herramienta de perturbar que la policía puede utilizar para imaginar fuera dónde has sido.

“Lectores de plato de licencia automáticos son una manera sofisticada de seguir motor' ubicaciones, y cuándo su dato está agregado con el tiempo ellos puede pintar detalló cuadros de las vidas de las personas,” notas Bennett Stein del ACLU Proyecto encima Habla, Intimidad, y Tecnología.<sup>14</sup>

Una California hombre quién archivó una petición de récords pública estuvo perturbada por el número de fotos (más de cien) que había sido tomado de su plato de licencia. La mayoría era en puente crossings y otras ubicaciones muy públicas. Uno, aun así, le asomó y sus hijas que salen su coche familiar mientras estuvo aparcado en su vado propio. Te importas, esta persona *no fue* bajo sospecha para cometer un delito. Los documentos obtuvieron por el

ACLU espectáculo que incluso la oficina del consejo general del FBI ha cuestionado el uso de ALPR en la ausencia de una póliza de gobierno coherente.<sup>15</sup>

Desafortunadamente, no tienes que archivar una petición de récords pública para ver algunos del ALPR dato. Según el EFF, la imágenes de más de cien ALPR los cámaras son disponibles a cualquiera on-line. Todo necesitas es un navegador. Antes de que fue público con sus hallazgos, el EFF obrados con aplicación de ley para corregir el escape de datos. El EFF dicho este misconfiguration estuvo encontrado en más de justo aquellos cien casos y aplicación de ley instada alrededor del país para apear o limitar qué's posted en el Internet. Pero tan de esta escritura, es todavía posible, si escribes la consulta derecha a una ventana de búsqueda, para obtener acceso a license imágenes de plato en muchas comunidades. Un investigador encontrado más de 64,000 imágenes de plato y su correspondientes locational puntos de dato durante un periodo de una semanas.<sup>16</sup>

Quizás no posees un automovilístico y sólo alquilar uno ocasionalmente. Todavía, eres sin duda ningún invisible, dado todo el personal e información de carta del crédito tienes que suministrar en el tiempo de alquiler. Qué es más, la mayoría de coches de alquiler hoy tienen GPS construido en. Sé. Descubrí la manera dura.

Cuándo estás dado un loaner coche de un dealership porque vuestro coche está siendo serviced, típicamente acuerdas no para tomar él a través de líneas estatales. El dealership quiere mantener el coche en el estado donde estuvo tomado prestado. Esta regla mayoritariamente concierne su seguro, no el vuestro.

Esto pasó a mí. Traje mi coche a una Lexus traficante en Las Vega para servicing, y me dejamos uso un loaner coche. Desde entonces era tiempo de encierro pasado en el dealership, sólo firmé el papeleo sin leerlo, mayoritariamente porque era apresurado por el servicio asocia. Más tarde, conduje el automovilístico a Northern California, al área de Bahía, para una actuación de consultoría. Cuándo el tipo de servicio me llamó para hablar sus recomendaciones, pidió, "¿Dónde eres?" Dije, "San Ramon, California." Dijo, "Yeah, aquello es donde vemos el coche." Él entonces leído me la ley de disturbio aproximadamente tomando el coche fuera de estatal. Aparentemente el loaner acuerdo hube de prisa firmó estipulado que no fui para tomar el coche fuera de Nevada.

Cuándo alquilas o tomar prestado un automovilístico hoy, hay una tentación a par vuestro

aparato inalámbrico a la diversión system, para recrear la experiencia de audio tienes en casa. Naturalmente hay algunas preocupaciones de intimidad inmediata. Esto no es vuestro coche. Tan qué pasa a vuestro infotainment dato una vez regresas el automovilístico a la agencia de alquiler?

Antes de que te pases vuestro aparato con un automovilístico que isn't el vuestro, tomar un cariz en el sistema de diversión. Quizás por tocar el teléfono celular que te pone verá usuarios anteriores' aparatos y/o los nombres listaron en el Bluetooth pantalla. Piensa aproximadamente si quieres unir aquella lista.

En otras palabras,, vuestro dato no sólo desaparece cuándo dejas el coche. Te lo tienes que sacar.

Podrías ser pensamiento , “Qué daño es allí en compartir mis tonadas favoritas con otros?” El problema es que vuestra música isn't la cosa única que coge compartido. Cuando aparatos más móviles conectan a un automóvil infotainment sistema, automáticamente enlazan vuestros contactos al automovilísticos's sistema. La suposición es que podrías querer hacer unas manos-llamada libre mientras conduciendo, así que habiendo vuestros contactos almacenaron en el coche lo hace que mucho más fácil. El problema es, no es vuestro coche.

“Cuándo cojo un coche de alquiler ,” dice David Miller, agente de seguridad del jefe para Covisint, “la última cosa es pasar mi teléfono. Descarga todos mis contactos porque aquello es qué quiere hacer. En la mayoría de coches de alquiler puedes entrar y si—alguien es paired con —ve sus contactos.”

El mismo es cierto cuándo finalmente vendes vuestro coche. Los coches modernos dan acceso a vuestro mundo digital mientras en la carretera. Quiere Twitter de control? Quiere poste a Facebook? Los coches hoy aguantan un increasing parecido a vuestro PC tradicional y vuestro teléfono celular: contienen dato personal que te tendría que sacar antes de la máquina o el aparato está vendido.

Obrando en el negocio de seguridad cogerá tú en el hábito de pensar adelante, incluso sobre transacciones mundanas. “ Paso todo este tiempo que conecta mi vehículo a mi vida entera,” dice Molinero, “y entonces en cinco años lo vendo—cómo yo disconnect él de mi vida entera? I don't querer el tipo quién compra [mi automovilístico] para ser capaz de ver mis amigos de Facebook, así que tienes que de-provisión. Tipos de seguridad son mucho más interesados en las vulnerabilidades de seguridad alrededor de de-provisioning que provisioning.”<sup>17</sup>

Y, tan haces con vuestro aparato móvil, necesitarás a la contraseña protege vuestro coche. Exceptúa en el tiempo de esta escritura, no hay ningún mecanismo

disponible que te dejará a la contraseña cierra vuestro infotainment sistema. Ni es fácil de eliminar todas las cuentas tú've puesto a vuestro coche a lo largo de los años— cómo tú varía por fabricante, marca, y modelo. Quizás que cambiará—alguien podría inventar un botón de una parones que saca un perfil de usuario entero de vuestro coche. Hasta entonces, al menos ir on-line y cambiar todos vuestros medios de comunicación sociales contraseñas después de que vendes vuestro coche.

Quizás el ejemplo mejor de un ordenador en ruedas es una Tesla, un moderno todo-vehículo electrónico. En junio de 2015, la tesla logró un hito significativo: en conjunto, coches de Tesla en todo el mundo habían sido conducidos más de un billón de millas.<sup>18</sup>

I paseo una Tesla. Ellos're coches sumos, pero dados sus salpicaderos sofisticados y comunicación celular constante, crian cuestiones sobre el dato recogen.

Cuándo tomas posesión de una Tesla te unre ofrecido una forma de consentimiento. Tienes la capacidad de controlar si la tesla grabará cualquier información sobre vuestro coche sobre un sistema de comunicación inalámbrico. Puedes habilitar o inutilizar compartiendo vuestro dato personal con Tesla vía una pantalla de tacto en el salpicadero. Muchas personas aceptan la riña que su dato ayudará la tesla hace un coche mejor en el futuro.

Según Tesla's política de privacidad, la empresa puede recoger el número de identificación del vehículo, información de velocidad, lecturas de cuentakilómetros, información de uso de la batería, la batería que cobra historia, información sobre funciones de sistema eléctrico, información de versión del software, infotainment dato de sistema, y seguridad- dato narrado (incluyendo información con respecto al vehículo's SRS sistemas, frenos, seguridad, y e-sistema de freno), entre otras cosas, para asistir en analizar la actuación del vehículo. La tesla declara que pueden recoger tal información en persona (p. ej., durante una cita de servicio) o vía acceso remoto.

Aquello es qué dicen en su póliza imprimida.

En práctica, también pueden determinar vuestro automovilísticos's ubicación y estado en cualquier tiempo. A los medios de comunicación, la tesla ha sido cagey sobre qué dato recoge en tiempo real y cómo utiliza que dato. Como

Uber, la tesla sienta en un Dios-gustar puesto que lo deja para saber todo sobre cada automovilístico y su ubicación en cualquier momento.

Si aquello unnerves te, puedes contactar Tesla y optar fuera de su telematics programa. Aun así, si tú , perderás fuera en actualizaciones de software automático, los cuales incluyen la seguridad fija y características nuevas.

Naturalmente la comunidad de seguridad está interesada en la Tesla, e investigador de seguridad independiente Nitesh Dhanjani ha identificado algunos problemas. Mientras me estoy de acuerdo con que el Modelo de Tesla S es un coche sumo y un producto fantástico de innovación, Dhanjani encontrado que la tesla utiliza un bastante débil autenticación de un factores sistema para acceder los sistemas del coche remotely.<sup>19</sup> El sitio web de Tesla y la aplicación carecen de la capacidad de limitar el número de registro-en intentos en una cuenta de usuario, el cual significa un atacante potencialmente podría utilizar brute fuerza a crack la contraseña de un usuario. Aquello significa una tercera fiesta podría (asumiendo vuestra contraseña está agrietada) registro en y utilizar la Tesla API para comprobar la ubicación de vuestro vehículo. Aquella persona podría también registro en remotely a la aplicación de Tesla y controlar el vehículo's sistemas—su acondicionador de aire, luces, y tan encima, a pesar de que el vehículo tiene que ser stationary.

La mayoría de Dhanjani's las preocupaciones han sido dirigidas por Tesla en el tiempo de esta escritura, pero la situación es un ejemplo de cuántos más fabricantes de coche necesidad de hacer hoy para asegurar sus coches. Sólo ofreciendo una aplicación a remotely inicio y comprobar el estado de vuestro automovilístico isn't bastante bueno. También tiene que ser seguro. La actualización más reciente, una característica llamó Convocar, te dejás para decir el automovilístico de estirar él fuera del garaje o lo aparcar en una algo estanca. En el futuro, Convoca dejará el automovilístico de elegirte arriba de cualquier ubicación a través del país. Kinda Como el Caballero de espectáculo de televisión *viejo Jinete*.

En refuting una crítica negativa en el *New York Times*, la tesla admitió al poder de datos tienen en su lado. *Reportero* de tiempo John Broder dicho que su Modelo de Tesla S había roto abajo y le dejó stranded. En un blog, la tesla contrarrestó, identificando varios puntos de dato dijeron llamados a cuestionar Broder versión de la historia. Por ejemplo, la tesla notó que Broder condujo en las velocidades que varían de sesenta y cinco millas por hora a ochenta y una millas por hora, con un encuadre de temperatura de cabina mediano de setenta y dos grados Fahrenheit.<sup>20</sup> Según *Forbes*, “dato

recorders en el Modelo S supo los encuadres de temperatura en el coche, el nivel de batería durante el viaje, la velocidad del coche de minuto a minuto, y la ruta exacta apeada— al hecho que el automovilístico reviewer condujo círculos en una parcela de aparcamiento cuándo la batería del coche era casi muerto.”<sup>21</sup>

Telematics la capacidad es una lógica al prórroga de las cajas negras obligatorias en todos los coches produjeron para venta en los Estados Unidos después de que 2015. Pero cajas negras en coches aren't nuevos en absoluto. Datan atrás al 1970s, cuándo bolsos de aire eran primero presentó. En colisiones, personas atrás vida sostenida entonces-daños amenazantes de bolsos de aire, y algunos muertos de la fuerza de los bolsos que pegan sus ente. En

algunos casos, tuvo el coche no sido equipado con aquellos bolsos, los ocupantes podrían ser vivos hoy. Para mejoras de marca, los ingenieros necesitaron el dato en el despliegue de los bolsos en los momentos antes de que y después de un accidente, recogido por los bolsos de aire' notando y módulos de diagnóstico (SDMs). Aun así, los dueños de vehículo no fueron dichos hasta que muy recientemente que los sensores en sus coches dato grabado sobre su conducción.

Provocado por cambios repentinos en g-fuerzas, cajas negras en coches, como cajas negras en aviones, record sólo el últimos pocos segundos o tan rodeando un g- caso de fuerza, como aceleración repentina, torque, y duro frenando.

Pero es fácil a envision más clases de los datos que son recogidos en estas cajas negras y transmitidos en tiempo real vía celular conectariones. Imagina, en el futuro, aquel dato recogido sobre un tres-a-periodo de cinco días podría ser almacenado cualquiera en el vehículo o en la nube. En vez de probar para describir que *ping-ping* ruido oyes cuándo vuestros viajes automovilísticos treinta y cinco millas por hora o más, tú'd sólo dar vuestro acceso de mecánico al dato grabado. La cuestión real es, quién más tiene acceso a todo este dato? Even Tesla admite que el dato recoge podría ser utilizado por terceras fiestas.

Qué si la tercera fiesta era vuestro banco ? Si tuvo un acuerdo con vuestro automovilístico's fabricante, podría seguir vuestra capacidad de conducción y juzgar vuestra elegibilidad para préstamos de coche futuro consiguientemente. O vuestro asegurador de salud podría hacer igual. O incluso vuestro asegurador automovilístico. Podría ser necesario para el



gobierno federal para pesar in encima quién posee dato de vuestro automovilístico y lo que derechos tienes que mantener tal dato privado.

hay poco puedes hacer sobre este hoy, pero vale parar atención a en el futuro.

Incluso si no posees una Tesla, vuestro fabricante de coche podría ofrecer una aplicación tel sombrero te dejás para abrir las puertas automovilísticas, inicio el motor, o incluso inspeccionar diagnósticos seguros en vuestro coche. Un investigador ha asomado que estas señales—entre el coche, la nube, y la aplicación—puede ser cortada y utilizada para seguir un vehículo de objetivo, fácilmente unlock lo, gatillo el cuerno y alarma, e incluso controlar su motor. El hacker puede hacer sólo aproximadamente todo exceptúa puesto el coche en tren y conducirlo fuera. Aquello todavía requiere la motor's tono. A pesar de que, yo recientemente imaginado cómo para inutilizar el tono de Tesla fob de modo que la Tesla es completamente grounded. Por utilizar un transmisor pequeño en 315 MHz te lo puede hacer tan el clave fob no puede ser detectado, por ello inutilizando el coche.

Hablando en DEF CON 23, Samy Kamkar, el investigador de seguridad más sabido para en desarrollo el Myspace-specific Samy gusano atrás en 2005, demostró un aparato construyó llamado OwnStar, los cuales pueden impersonate una red de vehículo sabida. Con él podría abrir vuestro OnStar-vehículo de Motores General habilitado, por ejemplo. El truco implica físicamente colocando el aparato en tél parachoques o underside de un coche de objetivo o camión. El aparato spoofs el punto de acceso inalámbrico del automóvil, el cual automáticamente asocia la motor confiada's aparato móvil con el punto de acceso nuevo (asumiendo la motor anteriormente ha asociado con tél punto de acceso original). Siempre que el usuario lanza el OnStar aplicación móvil, en cualquier iOS o Androide, el OwnStar el código explota un defecto en la aplicación para robar la motor OnStar credentials. “Apenas tú're en mi red y tú abren la aplicación, he tomado encima,” Kamkar dijo.<sup>22</sup>

después de obtener el usuario's registro-en credentials para RemoteLink, el software que poderes OnStar, y escuchando para el cerrando o unlocking sonido (*beep- beep*), un atacante puede seguir abajo un coche en una parcela de aparcamiento llenada, lo abre, y steal cualquier cosa interior valioso. El atacante entonces sacaría el aparato del parachoques. Es un ataque muy ordenado , desde entonces no hay ningún signo de una intrusión forzada. El dueño y la empresa de seguro quedan a rompecabezas fuera de qué pasado.

Los investigadores han encontrado tel sombrero conectado-los niveles automovilísticos diseñaron para mejorar flujo de tráfico también puede ser

seguido. El vehículo-a-vehículo (V2V) y vehículo-a- infraestructura (V2I) comunicaciones, juntos sabidos como V2X, pedir coches para retransmitir mensajes diez tiempo un segundo, utilizando un iónportuario del espectro de Wi-Fi en 5.9 gigahertz sabido como 802.11p.<sup>23</sup>

Desafortunadamente este dato es enviado unencrypted— tiene que ser. Cuando los coches están acelerando abajo una carretera, el milisegundo de retrasar necesitado a decrypt la señal podría resultar en un accidente peligroso, así que los diseñadores han optado para abiertos, unencrypted comunicaciones. Sabiendo este, insisten que las comunicaciones contienen ninguna información personal, ni siquiera un número de plato de la licencia. Aun así, para impedir forgeries, los mensajes son digitalmente firmados. El's estas firmas digitales, como el IMEI (número de serial del teléfono celular) el dato enviado de nuestros teléfonos celulares, aquello puede ser localizado atrás al registró dueños del vehículo.

Jonathan Petit, uno de los investigadores detrás del estudio, dijo *Alambrado*, “El vehículo está diciendo que ‘soy Alhielo, esto es mi ubicación , esto es mi velocidad y mi dirección.’ Todo el mundo alrededor puedes escuchar a aquello.... Pueden decir, ‘ hay Alice, alegó era en en casa, pero condujo por la tienda de droga, fue a una clínica de fertilidad,’ esta clase de cosa... Alguien puede inferir información privada

muchísima sobre el pasajero.”<sup>24</sup> Petit ha diseñado un sistema para alrededor \$1,000 aquello puede escuchar para el V2X

comunicaciones, y sugiere que una ciudad pequeña podría ser cubierta con sus sensores para aproximadamente \$1 millones. Más que habiendo una fuerza de policía grande, la ciudad utilizaría los sensores para identificar motor y, más importantes, sus hábitos.

Una propuesta de la Seguridad de Tráfico de Carretera Nacional la administración y las potestades europeas es para tener el 802.11p señal—el seudónimo del “vehículo”—cambia cada cinco minutos. Aquello no, aun así, parón un atacante dedicado—sólo instalará más roadside sensores que identificará el vehículo antes de que y después de que hace el cambio. En corto, allí parecer para ser muy pocas opciones para evitar identificación de vehículo.

“El seudónimo que cambia no para siguiendo. Sólo puede mitigar este ataque,” dice Petit. “Pero él's todavía necesitado para mejorar intimidad... Queremos demostrar que en cualquier despliegue, todavía tienes que tener esta protección, o alguien será capaz de seguirte.”

La conectividad automovilística al Internet es de hecho bien para dueños de vehículo: los fabricantes son capaces de pulsar fuera bug de software fija instantáneamente tener que ellos ser requeridos. En el tiempo de esta escritura, Volkswagen,<sup>25</sup> Tierra Rover,<sup>26</sup> y Chrysler<sup>27</sup> ha experimentado alto-vulnerabilidades de software del perfil. Aun así, sólo unos cuantos automakers, como Mercedes, Tesla, y Ford, envía encima-el-actualizaciones de aire a todos sus coches. El resto de nosotros todavía tienen que ir a la tienda para coger nuestro software de automóvil actualizó.

Si piensas la Tesla de manera y Uber está siguiendo cada paseo tomas es scary, entonces self-conduciendo los coches serán incluso scarier. Como los aparatos de vigilancia personales mantenemos en nuestros bolsillos—nuestros teléfonos celulares—self-conduciendo los coches necesitarán mantener pista de donde queremos ir y quizás incluso saber donde somos en un momento dado para ser siempre en el listo. El escenario propuesto por Google y otros es que las ciudades ya no necesitarán aparcando parcelas o garajes—vuestro coche conducirá alrededor hasta que está necesitado. O quizás las ciudades seguirán el encima-modelo de demanda, en qué propiedad privada es una cosa del pasado y todo el mundo comparte cualquier coche es cercano.

Tan nuestros teléfonos celulares son menos like teléfonos de cable cobrizo que ellos son como tradicionales PCs, self-conduciendo los coches también serán una forma nueva de ordenador. Ellos'll ser self-contuvo computar aparatos, capaces de hacer partidos-segundas decisiones autónomas mientras conduciendo en caso están cortados fuera de sus comunicaciones de red. Utilizando conexiones celulares, serán capaces de acceder una variedad de servicios de nube, dejándoles para recibir información de tráfico de tiempo real, actualizaciones de construcción de la carretera, e informes de tiempo del Servicio de Tiempo Nacional.

Estas actualizaciones son disponibles encima algunos vehículos convencionales ahora mismo. Pero él's pronosticado que por 2025 una mayoría de los coches en la carretera serán conectados —a otros coches, a roadside servicios de asistencia—y él probablemente puede que un sizable el porcentaje de estos será self-conduciendo.<sup>28</sup> Imagina lo que un bug de software en un self-conduciendo el coche parecería.

Entretanto, cada viaje tomas será grabado a algún lugar. Necesitarás una aplicación, mucho como el Uber aplicación, aquello será registrado a ti y a vuestro aparato móvil. Aquella aplicación will récord vuestros viajes y, presumiblemente, los gastos asociaron con vuestro viaje si serían cobrados a

la carta de crédito encima lima, el cual podría ser subpoenaed, si no de Uber entonces de vuestra empresa de carta del crédito. Y dado que una empresa privada más likely tener una mano en diseñar el software que carreras estos self-conduciendo coches, serías en la piedad de aquellas empresas y sus decisiones aproximadamente si para compartir cualquiera o todo de vuestra información personal con agencias de aplicación de la ley.

Bienvenido al futuro.

Espero que por el tiempo leíste esto allí será controles más duros—o al menos la pista de controles más duros en un futuro próximo—con respecto a la fabricación de conectó coches y sus protocolos de comunicaciones. Más que utilizar ampliamente aceptado software y seguridad de hardware practica aquello es estándar hoy, la industria de coche, como la industria de aparato médico y otros, está intentando para reinventar la rueda—como si nosotros puerto't aprendido mucho aproximadamente seguridad de red sobre los últimos cuarenta años. Tenemos, y sería más si estas industrias empezaron seguir existiendo buenas prácticas en vez de insistir que qué están haciendo es radicalmente diferente de qué's sido hecho antes de que. No es.

Desafortunadamente, fallo de asegurar el código en un coche ha mucho consecuencias más sumas que un accidente de software mero, con su pantalla azul de muerte. En un coche, aquel fallo podría hacer daño o matar un ser humano. En el tiempo de esta escritura, al menos una persona ha muerto mientras una Tesla era en beta autopilot modo—si el resultado de faulty frenos o un error en juicio por los restos de software del coche para ser resueltos.<sup>29</sup>

Lectura esto, no puedes querer dejar vuestra casa. En el capítulo próximo, I'll hablar maneras en qué el gadgets en nuestras casas están escuchando y grabando qué detrás cerramos puertas. En este caso no es el gobierno que necesitamos ser temerosos de.

## CAPÍTULO DOCE

### El Internet de Vigilancia

hace Unos cuantos años nadie preocupado sobre el termostato en vuestra casa. Era un termostato operado manualmente sencillo que mantuvo vuestra casa en una

temperatura cómoda. Entonces los termostatos acaecían programables. Y entonces una empresa, Nido, decidió que tendrías que ser capaz de controlar

vuestro termostato programable con un Internet-aplicación basada. Puedes notar donde estoy yendo con este, bien?

En una reseña de producto vengativo del Honeywell Wi-Fi Listo Touchscreen Termostato, alguien quien se llama el General escribió encima Amazona que su ex-la mujer tomó la casa, el perro, y el 401(k), pero él retained la contraseña al Honeywell termostato. Cuando el ex-la mujer y su novio eran fuera de ciudad, el General alegó él jack arriba de la temperatura en la casa y entonces bajarlo atrás abajo antes de que regresaron: “sólo puedo imaginar lo que sus facturas de electricidad podrían ser. Me hago sonrisa.”<sup>1</sup>

Investigadores en EE.UU. de Sombrero Negro 2014, una conferencia para personas en la industria de seguridad de la información, revelado unas cuantas maneras en qué el firmware de un termostato de Nido podría ser compromised.<sup>2</sup> es importante de notar que many de estos compromises requiere acceso físico al aparato, significando que alguien tendría que coger dentro de vuestra casa e instalar un puerto de USB en el termostato. Daniel Buentello, un investigador de seguridad independiente, uno de cuatro presentadores quien habló aproximadamente cortando el aparato, dicho, “Esto es un ordenador que

El usuario no puede poner un antivirus encima. Peor todavía, hay una puerta posterior secreta que una persona mala podría utilizar y estancia allí para siempre. Es una mosca literal en la muro.”<sup>3</sup>

El equipo de investigadores asomó un vídeo en qué cambiaron the interfaz de termostato del Nido (hicieron parece el HAL 9000 fishbowl lente de cámara) y cargó varias otras características nuevas. Curiosamente, no fueron capaces de girar del automáticos informando característica dentro del aparato—así que el equipo produjo su herramienta propia para hacer tan.<sup>4</sup> Esta herramienta cortaría de la corriente de los datos que fluyen atrás a Google, la empresa de padre de Nido.

Comentando en la presentación, Zoz Cuccias del nido más tarde dijo *VentureBeat*, “Todos aparatos de hardware—de los portátiles a smartphones—son susceptibles a jailbreaking; esto no es un problema único. Esto es un físico jailbreak requiriendo acceso físico al Termostato de Aprendizaje del Nido. Si alguien dirigió entrar vuestra casa y tuvo su elección, las casualidad son instalaría sus aparatos propios, o tomar las joyas. Este jailbreak doesn't compromise la seguridad de nuestros servidores o las conexiones a ellos y al mejores de nuestro conocimiento, ningún aparato ha

sido accedido y compromised remotely. Seguridad de cliente es muy importante a nosotros, y nuestra prioridad más alta es en vulnerabilidades remotas. Uno de vuestros defensas mejores es para comprar un Dropcam Pro tan puedes controlar vuestra casa cuándo no eres allí.”<sup>5</sup>

Con el advenimiento del Internet de Cosas, a empresas les gusta Google es ansioso de colonizar partes de él—para poseer las programa then otros productos utilizarán. En otras palabras,, estas empresas quieren los aparatos desarrollaron por otras empresas para conectar a sus servicios y no alguien más's. Google posee ambos Dropcam y Nido, pero quieren otro Internet de aparatos de Cosas, como listos lightbulbs y monitores de criatura, para conectar a vuestra cuenta de Google también. La ventaja de este, al menos a Google, es que cogen para recoger dato más crudo sobre vuestros hábitos personales (y esto aplica a cualquier Manzana de empresa—grande, Samsung, incluso Honeywell).

En hablar sobre el Internet de Cosas, experto de seguridad del ordenador Bruce Schneier concluido en una entrevista, “Esto es mucho como el campo de ordenador en el '90s. Nadie está pagando cualquier atención a seguridad, nadie está haciendo actualizaciones, nadie sabe cualquier cosa— es todo realmente, realmente malo y él's yendo para venir chocando abajo.... Habrá vulnerabilidades, serán explotados por tipos malos, y habrá ninguna manera de parcharles.”<sup>6</sup>

para probar aquel punto, en el verano de 2013 periodista Kashmir Cerro algún investigative informando y algunos DIY el ordenador que corta. Por utilizar una búsqueda de Google encontró una frase sencilla que le dejó para controlar algunos

Insteon hub aparatos para la casa. Un hub es un aparato central que proporciona acceso a una aplicación móvil o al Internet directamente. A través de la aplicación, las personas pueden controlar el encendiendo en sus salones, cerradura las puertas a sus casas, o ajustar la temperatura de sus casas. A través del Internet, el dueño puede ajustar estas cosas mientras, dice, en un viaje empresarial.

Como el cerro asomó, un atacante también podría utilizar el Internet a remotely contacto el hub. Prueba tan más lejana, logró fuera a Thomas Hatley, un desconocido completo, en Oregón, y pedido si podría utilizar su casa como caso de prueba.

De su casa en San Francisco, el cerro era capaz de girar encima y de las luces dentro de Hatley's casa, algunos seiscientas millas arriba de la costa del Pacífico. También podría haber controlado sus cubas calientes, seguidores,



televisiones, bombas de agua, puertas de garaje, y cámaras de vigilancia del vídeo si había tenido aquellos conectaron.

El problema—ahora corrigió—era que Insteon hecho todo Hatley's la información disponible encima Google. Peor, acceso a esta información no fue protegida por una contraseña en el tiempo—cualquiera quién stumbled a este hecho podría controlar cualquier Insteon hub que podría ser encontrado on-line. Hatley's router Tuvo una contraseña, pero aquello podría ser bypassed por buscar el portuario utilizado por Insteon, el cual es qué Cerro hizo.

“Thomas Hatley la casa era una de ocho que era capaz de acceder,” el cerro escribió. “La información sensible era reveló—no sólo lo que electrodomésticos y personas de aparatos tuvieron, pero su huso horario (junto con la ciudad importante más cercana a su casa), alocuciones de IP e incluso el nombre de un niño; aparentemente, los padres quisieron la capacidad de estirar el tapón en su televisión de lejos. En al menos tres casos, había bastante información para enlazar las casas en el Internet a sus ubicaciones en el mundo real. Los nombres para la mayoría de los sistemas era genérico, pero en uno de aquellos casos, incluyó una alocución de calle que era capaz de seguir abajo a una casa en Connecticut.”<sup>7</sup>

Alrededor del mismo tiempo, un problema similar estuvo encontrado por Nitesh Dhanjani, un investigador de seguridad. Dhanjani Era looking en particular en el Philips Hue encendiendo sistema, el cual deja el dueño para ajustar el color y brightness de un lightbulb de un aparato móvil. El bulbo tiene una gama de dieciséis millones de colores.

Dhanjani Encontrado que un guión sencillo insertado a una casa computer en la red de casa era bastante para causar una denegación distribuida-de-ataque de servicio—o DDoS ataque—en el sistema de encender.<sup>8</sup> En otras palabras,, podría hacer cualquier sala con un Hue lightbulb va oscuridad en voluntad. Qué él scripted era un código sencillo de modo que cuando el usuario retomó el bulbo, deprisa saldría otra vez—y mantendría salir mientras el código era presente.

Dhanjani Dicho que esto podría deletrear problema serio para un edificio de oficina o edificio de apartamento. El código render todas las luces inoperantes, y las personas afectaron llamaría la utilidad local sólo para encontrar no había ningún poder outage en su área.

While Internet-casa accesible-aparatos de automatización pueden ser los objetivos directos de DDoS ataques, también pueden ser compromised y unidos a un botnet—un ejército de infectó aparatos debajo un controlador



que puede ser lanzador DDoS ataques contra otros sistemas on el Internet. En octubre 2016, una empresa llamó Dyn, el cual maneja DNS servicios de infraestructura para marcas de Internet importante gustan Twitter, Reddit, y Spotify, estuvo pegado duro por uno de estos ataques. Millones de usuarios en la parte oriental de los Estados Unidos no podrían acceder muchos sitios importantes porque sus navegadores no podrían lograr Dyn DNS servicios.

El culpable era una pieza de malware llamó Mirai, un malicious programa que registra el Internet que busca insecure Internet de aparatos de Cosas, como CCTV cámaras, routers, DVRs, y monitores de criatura, a hijack y apalancamiento en ataques más lejanos. Mirai Intentos de tomar sobre el aparato por la contraseña sencilla que adivina. Si el ataque es exitoso, el aparato está unido a un botnet donde él mentiras en espera para instrucciones. Ahora con un sencillo orden de una líneas, el botnet el operador puede instruir cada centenares—de aparato de miles o millones de ellos —para enviar dato a un sitio de objetivo e inundación él con información, forzándolo para ir off-line.

Mientras no puedes parar hackers de lanzar DDoS entacks en contra otros, puedes acaecer invisible a su botnets. El primer elemento de empresarial cuándo desplegando un Internet de aparato de Cosas es para cambiar la contraseña a algo duro de adivinar. Si ya tienes un aparato desplegó, rebooting lo tendría que sacar cualquier existiendo malicious código.

Guiones de ordenador pueden afectar otros sistemas de casa lista. Si tienes un bebé en vuestra casa, también puedes tener un monitor de criatura.

Este aparato, cualquiera un micrófono o un cámara o una combinación de ambos, deja padres para ser fuera de the vivero pero todavía mantener pista de su criatura. Desafortunadamente, estos aparatos pueden invitar otros para observar el niño también.

Monitores de criatura analógica utilizan frecuencias inalámbricas retiradas en el 43–50 MHz gama. Estas frecuencias eran primero utilizadas para teléfonos inalámbricos en el 1990s, y cualquiera con un escáner radiofónico barato fácilmente podría interceptar llamadas de teléfono inalámbrico sin el objetivo nunca sabiendo qué pasado.

Incluso hoy, un hacker podría utilizar un espectro analyzer para descubrir la frecuencia

que una criatura analógica particular monitor usos, entonces emplear varios esquemas de desmodulación para convertir la señal eléctrica a audio. Un escáner policial de una tienda de electrónica también bastaría. Ha Habido casos legales numerosos en qué vecinos que utilizan la misma marca de

monitor de criatura pone to el mismo canal eavesdropped encima uno otro. En 2009 Wes Denkov de Chicago demandó los fabricantes de la Noche de Día de Niño & de Verano monitor de vídeo de la criatura, alegando que su vecino podría oír las conversaciones privadas aguantaron en su casa.<sup>9</sup>

Como contramedida, podrías querer utilizar un monitor de criatura digital. Estos son todavía vulnerables a eavesdropping, pero tienen seguridad mejor y más opciones de configuración. Por ejemplo, puedes actualizar el monitor's firmware (el software en el chip) inmediatamente después de que compra. También ser seguro para cambiar el default username y contraseña.

Aquí otra vez podrías venir arriba contra una elección de diseño que es fuera de vuestro control. Nitesh Dhanjani Encontrado que el Belkin WeMo monitor de criatura inalámbrica utiliza un token en una aplicación que, una vez instalado en vuestro aparato móvil y utilizado en vuestra red de casa, queda activo—de anywhere en el mundo. Dice apalabras babysit vuestra sobrina de bebé y vuestro hermano te invitas para descargar el Belkin aplicación a vuestro teléfono a través de su red de casa local (con un poco de suerte, está protegido con un WPA2 contraseña). Ahora tienes acceso al monitor de criatura de vuestro hermano de a través del país, de a través del globo.

Dhanjani Notas que este defecto de diseño es presente en muchos Internet interconectado de aparatos de Cosas. Básicamente, estos aparatos asumen que todo en la red local está confiado en. Si, como algunos creen, nosotros'll todos tienen veinte o treinta tales aparatos en nuestras casas antes de largos, el modelo de seguridad tendrá que cambio. Desde entonces todo en la red está confiado en, entonces un defecto en cualquiera aparato—vuestro monitor de criatura, vuestro lightbulb, vuestro termostato—podría dejar un atacante remoto a vuestra red de casa lista y darle una oportunidad de aprender aún más sobre vuestros hábitos personales.

Mucho tiempo antes de aplicaciones móviles, había de mano remotes. La mayoría de nosotros es demasiado joven de recordar las vísperas TVs controles remotos tenidos—los días cuándo las personas tuvieron que físicamente levantarse del couch y girar un dial para cambiar el canal. O para bombear arriba del volumen. Hoy, del consuelo de nuestros sofás, sólo podemos instruir la televisión con nuestras palabras. Aquello puede ser muy conveniente, pero también significa que la televisión está escuchando—si sólo para la orden para girar él encima.

En los días tempranos, controles remotos para TVs línea directa requerida de vista y funcionado

por utilizar ligero—específicamente, infrared tecnología. Una batería-operado remoto emit una secuencia de centellea de ligero apenas visible al ojo humano pero visible (otra vez, dentro de una línea de vista) a un receptor en la televisión. Cómo la televisión sabe si lo quisiste girar encima cuándo era fuera? Sencillo: el sensor infrarrojo localizado dentro de la televisión era siempre encima, en standby, esperando a una secuencia particular de pulsos ligeros infrarrojos del de mano remotos de despertarlo arriba.

Remoto-controlar TVs evolucionado a lo largo de los años para incluir señales inalámbricas, el cual te significaste didn't tiene que estar directamente delante de la televisión; podrías ser fuera a un lado, a veces incluso en otra sala. Otra vez, la televisión era encima en standby modo, esperando a la señal apropiada para despertarlo arriba.

Rápido-adelante a voz-activó TVs. Estos TVs hacer fuera con el remoto aguantas en vuestro entregar—cuál, si tú're me gusto, nunca puedes encontrar cuándo lo quieres en todo caso. En cambio dices algo tonto gusta “televisión encima” u Hola, “televisión,” y la televisión—mágicamente—gira encima.

En el muelle de 2015 investigadores de seguridad Conoce Munro y David Logia quiso ver si voz-activado Samsung TVs escuchaba en en conversaciones en la sala incluso cuándo la televisión no fue en uso. Mientras encontraron que digitales TVs de hecho sienta idle cuándo están girados de qué—está tranquilizando—el TVs récord todo hablado después de que les das una orden sencilla, como “Hola, televisión” (aquello es, graban todo hasta la televisión está mandado para girar fuera otra vez). Cuántos de nosotros recordarán para mantener absolutamente tranquilo mientras la televisión es encima?

Nosotros no, y para hacer asuntos aún más perturbando, qué decimos (y qué está grabado) después del “Hola, orden” de televisión no es encriptada. Si puedo subir vuestra red de casa, puedo eavesdrop en cualquier conversación eres habiendo en vuestra casa mientras la televisión está girada encima. La riña a favor de mantener la televisión en escuchar el modo es que las necesidades de aparato para oír cualesquier órdenes adicionales lo podrías dar, como “Volumen arriba,” “Cambio el canal,” y Mudo “el sonido.” Aquello podría ser vale, excepto las órdenes de voz captadas remontan a un satélite befmena vuelven abajo otra vez. Y porque la serie entera de los datos no es encriptados, puedo llevar fuera de un hombre-en-el-ataque medio en vuestra televisión, insertando mis órdenes propias para cambiar vuestro canal, bomba arriba de vuestro volumen, o sencillamente turno de la televisión siempre que quiero.

Dejado es piensa aproximadamente que para un segundo. Aquello significa si tú're en una sala con una voz-televisión activada, en medio de una conversación con alguien, y decides girar en la televisión, la corriente de conversación que sigue puede ser

grabado por vuestra televisión digital. Moreover, aquello conversación grabada sobre el upcoming cuece la venta en la escuela elemental puede ser streamed atrás a un servidor a algún lugar lejos de vuestro salón. De hecho, Samsung corrientes que datos no sólo a él pero también a otra empresa Matiz llamado, una voz-empresa de software del reconocimiento. Aquello es dos empresas que tiene información vital sobre el upcoming cuece venta.

Y dejado es coge real aquí: la conversación mediana eres habiendo en vuestra sala de televisión probablemente isn't sobre un cocer venta. Quizás estás hablando about algo ilegal, el cual aplicación de ley podría querer saber aproximadamente. Es enteramente probablemente que estas empresas informarían aplicación de ley, pero si aplicación de ley, por ejemplo, era ya interesado en ti, entonces los agentes podrían coger un warrant forzando these empresas para proporcionar completas transcripts. “Triste, pero era vuestra televisión lista que narc'd encima te...”

Samsung Tiene, en su defensa, declaró que tal eavesdropping los escenarios están mencionados en el acuerdo de intimidad que todos los usuarios implícitamente apalabran cuándo giran en la televisión. Pero cuando era la última vez leíste un acuerdo de intimidad antes de girar en un aparato por primera vez? Samsung Dice en un futuro próximo todas sus comunicaciones de televisión serán encriptadas.<sup>10</sup> Pero tan de 2015, más modelos en la lonja no es protegida.

Afortunadamente, hay maneras de inutilizar este HAL 9000—gusta característica en vuestro Samsung y presumiblemente en otros fabricantes' TVs también. En el Samsung PN60F8500 y productos similares, va a la carta de Encuadres, selecciona “Características Listas,” y entonces debajo “Reconocimiento de Voz,” selecciona “Fuera.” Pero si quieres parar vuestra televisión de ser capaz de grabar conversaciones sensibles en vuestra casa, tendrás que sacrificar siendo capaz de andar a una sala y voz- mandar vuestra televisión para girar encima. Puedes todavía, con remoto en hand, seleccionar el botón de micrófono y hablar vuestras órdenes. O te podrías levantar del couch y cambiar los canales tú. Sé. La vida es dura.

Unencrypted Corrientes de dato no son únicas a Samsung. Mientras probando LG listo TVs, un investigador encontrado que el dato está siendo enviado atrás a LG sobre el Internet cada vez el espectador cambia el canal.

La televisión también tiene una opción de encuadres Colección “llamada de mirar info,” habilitado por default. Vuestro “mirando info” incluye los nombres de limas almacenaron en cualquier paseo de USB conectas a vuestro LG la televisión—dice, uno aquello contiene fotos de vuestras vacaciones familiares. Los investigadores llevaron fuera de otro experimento en qué crearon una lima de vídeo simulada y cargado lo a un paseo de USB, entonces plugged él a su televisión. Cuándo analizaron network tráfico, encontraron que el nombre de lima del vídeo estuvo

transmitido unencrypted dentro tráfico de http y enviado a la alocución Gb.smartshare.lgtvsdp.com.

Sensorial, una empresa que marcas embedded habla-soluciones de reconocimiento para productos listos, lo piensa puede hacer aún más. “Pensamos la magia en [listo TVs] es para dejarlo siempre encima y siempre escuchando,” dice Todd Mozer, CEO de Sensorial. “Ahora mismo [escuchando] consume demasiado poder de hacer que. Samsung's Hecho una cosa realmente inteligente y creó un modo de escuchar. Queremos ir allende aquel y hacerlo siempre encima, siempre escuchando ningún asunto donde eres.”<sup>11</sup>

Ahora que sabes lo que vuestra televisión digital es capaz de, podrías ser preguntarte: Puede vuestro teléfono celular eavesdrop cuándo él's girado fuera? Hay tres campamentos. Sí, no, y depende.

Hay aquellos en la intimidad comunitaria quiénes juran tienes que tomar la batería fuera de vuestro girado-fuera smartphone para ser seguro que no está escuchando. Allí no parece para ser evidencia muchísima para apoyar esto; es mayoritariamente anecdotal. Entonces hay las personas quiénes juran que sólo girando de vuestro teléfono es bien bastante; el caso cerró. Pero pienso en realidad hay casos—decir, si malware está añadido a un smartphone—cuándo lo doesn't turno fuera enteramente y podría todavía las conversaciones récord aguantaron cercanas. Así que depende en una variedad de factores.

Hay algunos telefonea aquello despierta arriba cuándo dices una frase mágica, tan voz-activado TVs hacer. Esto implicaría que los teléfonos están escuchando en todo momento, esperando a la frase mágica. Esto también implicaría que qué está dicho de alguna manera está siendo grabado o transmitió. En algún malware-infectado telefonea aquello es cierto: el cámara o el micrófono del teléfono está activado cuándo no hay una llamada en progreso. Estos casos, pienso, es raro.

Pero atrás a la cuestión principal. Hay algunos en la intimidad comunitaria quiénes juran que puedes activar un teléfono cuándo está girado fuera. *hay* malware tel sombrero puede hacer el teléfono parece para ser fuera cuándo no es. Aun así, la posibilidad que alguien podría activar un girado-fuera teléfono (ningún poder de batería) me ataco tan imposible. Básicamente cualquier aparato que tiene poder de batería que deja su software para ser en un running el estado puede ser explotado. No es duro para un firmware puerta posterior para hacer el aparato parece que es fuera cuándo no es. Un aparato sin poder puede't cualquier cosa. O puede él? Algunos todavía discuten que el NSA tiene poner chips en nuestros teléfonos que proporciona poder y dejar siguiendo incluso cuándo el teléfono es físicamente powered fuera (incluso si la batería física está estirada).

Si o no vuestro teléfono es capaz de escuchar, el navegador utilizas encima ciertamente es. Alrededor 2013 Google empezó qué está llamado hotwording, una hazañaure aquello te dejás para dar una orden sencilla que activa el modo de escuchar en Chrome. Otros han hecho lo propio, incluyendo Manzana Siri, Microsoft Cortana, y Amazona's Alexa. Así que vuestro teléfono, vuestro PC tradicional, y que estand-el aparato solo en vuestro café somete todos contienen atrás-fin, en-el-servicios de nube que está diseñado para responder a órdenes de voz como “Siri, qué lejos a la canal gasista más cercana?” Cuál significa escuchan. Y si aquello no te concierne, sabe que las búsquedas dirigieron por estos servicios están grabados y salvó indefinidamente.<sup>12</sup>

*Indefinidamente.*

Tan cuánto estos aparatos oyen? De hecho, él's un poco unclear qué hacen cuando no están contestando cuestiones o girando vuestra televisión encima y fuera. Por ejemplo, utilizando la versión de PC tradicional del Chrome navegador, los investigadores encontraron que alguien—Google?—Parecido para ser escuchando todo el tiempo por habilitante el micrófono. Esta característica vino a Chrome de su equivalente de fuente abierta, un navegador sabido tan Cromo. En 2015, los investigadores descubrieron que alguien—Google?—Parecido para ser escuchando todo el tiempo. A investigación más lejana, descubrieron que esto es porque el navegador gira el micrófono encima por default. A pesar de ser incluido en software de fuente abierta, este código no fue disponible para inspección.

Hay varios problemas con este. Primero, “el código abierto” significa que las personas tendrían que ser capaces de mirar en el código, pero en este caso el código era una caja negra, código que nadie hubo vetted. Segundo, este

código hizo su manera a la versión popular del navegador vía una actualización automática de Google, el cual usuarios weren't dados una casualidad de rechazar. Y tan de 2015 Google no lo ha sacado. Ofrecieron un medio para personas para optar fuera, pero aquello opta-fuera requiere destrezas de codificación tan complicados que los usuarios medianos pueden no él en su propio.<sup>13</sup>

hay otro, más abajo-maneras de tecnología para mitigar este creepy eavesdropping característica en Chrome y otros programas. Para la webcam, sencillamente puesto una pieza de cinta encima lo. Para el micrófono, uno de los defensas mejores es para poner un dummy mic tapón en el casquete de micrófono de vuestro PC tradicional. Para hacer este, coger un conjunto viejo, roto de auriculares o earbuds y sencillamente cortados el cable cercano el micrófono jack. Ahora tapón que colilla de un mic jack al casquete. Vuestro ordenador pensará hay un micrófono allí cuándo allí isn't. Naturalmente si quieres hacer una llamada que utiliza Skype o algunos otro servicio on-line, entonces necesitarás sacar el tapón primero. También—y esto es marca muy—importante seguro los dos cables en el mic la colilla no toca de modo que te don't freír vuestro

puerto de micrófono. Otro aparato conectado que las vidas en la casa es el Eco de Amazona, un

Internet hub aquello deja usuarios para ordenar películas encima demanda y other productos de Amazona sólo por hablar. El Eco es también siempre encima, en standby modo, escuchando a cada palabra, esperando al “despertar palabra.” Porque la amazona Resuena hace más de una televisión lista, requiere primero-usuarios de tiempo para hablar hasta veinticinco specific frases al aparato antes de que lo dan muy órdenes. La amazona te puede decir el tiempo exterior, proporcionar los marcadores de deportes más tardíos, y orden o reorden elementos de su colección si lo pides a. Dado la carácter genérica de algunos de las frases Amazon reconoce—por ejemplo, “llueve mañana?”— Está para razonar que vuestro Eco podría ser escuchar más de vuestra televisión lista es.

Afortunadamente, la amazona proporciona maneras de sacar vuestro dato de voz de Eco.<sup>14</sup> Si quieres eliminar todo (por ejemplo, si planeas vender vuestro Eco a otra fiesta), entonces necesitas ir on-line de hacer que.<sup>15</sup>

Mientras toda esta voz-activó los aparatos requieren una frase concreta para despertar arriba, queda unclear lo que cada aparato está haciendo durante downtime—el tiempo cuándo nadie está mandándolo para hacer cualquier cosa. Cuándo posible, turno de la característica de activación de la voz en los



encuadres de configuración. Siempre lo puedes girar atrás encima otra vez cuándo lo necesitas.

Uniendo el Eco de Amazona en el Internet de Cosas, además de vuestra televisión y termostato, es vuestro refrigerador.

*Refrigerador?*

Samsung Ha anunciado un modelo de refrigerador que conecta con vuestro calendario de Google para mostrar upcoming casos en una pantalla plana embedded en la clase—de puerta del electrodoméstico de como aquel whiteboard te una vez tenido en su sitio. Sólo ahora el refrigerador conecta al Internet a través de vuestra cuenta de Google.

Samsung Hizo varias cosas bien en diseñar esta nevera lista. Incluyeron un SSL/conexión de https tan tráfico entre el refrigerador y el servidor de Calendario del Google es encrypted. Y entregaron su refrigerador futurista para probar en DEF CON 23—un del más intenso hacker convenciones encima tierra.

Pero según investigadores de seguridad Conocen Munro y David Logia, las personaje quién cortó la televisión digital communications, Samsung fallado para comprobar el certificado para comunicar con servidores de Google y obtener Gmail calender información. Un certificado validaría que las comunicaciones

entre el refrigerador y los servidores de Google son seguros. Pero sin él alguien con malicious intent podría venir a lo largo de y crear su certificado propio, dejándole a eavesdrop en la conexión entre vuestro refrigerador y Google.<sup>16</sup>

Así que qué?

Bien, en este caso, por ser en vuestra red de casa, alguien podría no acceso de beneficio único a ynuestro refrigerador y estropear vuestra leche y huevos pero también acceso de beneficio a vuestra información de cuenta del Google por actuar un hombre-en-el- ataque medio en el cliente de calendario de la nevera y robando vuestro registro de Google-en credentials—dejándole o le para leer vuestro Gmail y quizás hacer incluso daño más sumo.

Los refrigeradores listos no son la norma todavía. Pero está para razonar que como conectamos más aparatos al Internet, e incluso a nuestras redes de casa, habrá lapsos en seguridad. Cuál está asustando, especialmente cuándo la cosa que es compromised es algo realmente precioso y privado, como vuestra casa.

El internet de empresas de Cosas está obrando en aplicaciones que girará cualquier aparato a un sistema de seguridad de la casa. Vuestra televisión, para caso, poder someday contener un cámara. En aquel escenario una aplicación en un smartphone o la pastilla te podrían dejar para ver cualquier sala en vuestra casa u oficina de cualquier ubicación remota. Luces, también, puede ser girado encima cuándo hay interior de moción o fuera de la casa.

En un escenario, podrías conducir hasta vuestra casa, und como haces tan la aplicación de sistema de la alarma en vuestro teléfono o en vuestros usos automovilísticos su construidos-en capacidades de geolocalización para notar vuestra llegada. Cuándo tú're cincuenta pies fuera, la aplicación señala el sistema de alarma de la casa a unlock el frente o puerta de garaje (la aplicación en vuestro teléfono ya ha conectado a la casa y autenticado). El sistema de alarma más allá contacta el en-en casa encendiendo sistema, pidiéndolo a illuminate el porche, entryway, y quizás cualquiera el salón o cocina. Además, puedes querer introducir vuestra casa while música de cuarto blando o la Copa más tardía 40 tonada de un servicio como Spotify está tocando en el stereo. Y naturalmente la temperatura de la casa anima o enfría, según la estación y vuestras preferencias, ahora que eres en casa otra vez.

La casa alarma became popular alrededor del turno del veinte-primer siglo. Sistemas de alarma de la casa en aquellos tiempos requirieron un técnico a monte alambró sensores en las puertas y ventanas de la casa. Estos alambraron los sensores estuvieron conectados a un centrales hub aquello utilizó un alambró landline para enviar y recibir mensajes del servicio de control. Pondrías la alarma, y si cualquiera compromised el aseguró puertas y ventanas, el servicio de control te contactaría, normalmente por teléfono. Una batería era a menudo proporcionada en caso el poder salió. Ningúnte que un landline normalmente nunca pierde poder a no ser que el cable a la casa está cortado.

Cuándo las personas muchísimas cogieron libradas de su cobrizos-alambrar landlines y confió sólo a sus servicios de comunicación móviles, la alarma que controla las empresas empezaron ofrecer celulares-basó conexiones. Ultimamente ellos've cambiados a Internet-servicios de aplicación basada.

Los sensores de alarma en las puertas y ventanas ellos es ahora inalámbrico. hay ciertamente menos perforando y stringing de cable feo, pero hay también más riesgo. Investigadores have repetidamente encontrados que las señales de estos sensores inalámbricos no son encriptados. Un -ser la necesidad atacante sólo escucha a las comunicaciones entre aparatos para

compromise les. Por ejemplo, si puedo incumplir vuestra red local, puedo eavesdrop en las comunicaciones entre vuestros servidores de empresa de la alarma y vuestro en-aparato de casa (asumiéndolo's en la misma red local y no encriptado), y por manipular aquellas comunicaciones puedo empezar para controlar vuestra casa lista, spoofing órdenes para controlar el sistema.

Las empresas ahora están proporcionando “-él-tú” en casa controlando servicios. Si cualesquier sensores están perturbados, vuestro teléfono celular alumbrará con un mensaje de texto que informa tú del cambio. O quizás la aplicación proporciona una imagen de webcam de dentro de la casa. Cualquiera way, eres en control y está controlando la casa tú. Aquello es sumo hasta vuestro Internet de casa sale.

Incluso cuándo el Internet está obrando, los tipos malos pueden todavía subvertir o suprimir estos -él-tú sistemas de alarma inalámbrica. Por ejemplo, un attacker puede provocar alarmas falsas (cuál en algunas ciudades el homeowner tiene que pagar para). Aparatos que crean las alarmas falsas podrían ser puestos fuera de la calle delante de vuestra casa o hasta 250 patios fuera. Demasiadas alarmas falsas podrían render el sistema unreliable (y el homeowner fuera de bolsillo para un hefty coste).

O el atacante podría mermar el -él-tú señales de sensor inalámbrico por enviar ruido radiofónico para impedir comunicación atrás al principal hub o panel de control. Suprime la alarma e impide él de sonar, eficazmente neutralizando la protección y dejando al criminal de andar derecho en.

Mucho las personas tienen webcams instaladas en sus casas—si para seguridad, para controlar una persona de limpieza o niñera, o para mantener tabuladores en un homebound seniors o quiso uno con necesidades especiales. Desafortunadamente, muchísimo estos encima-el- webcams de Internet son vulnerables a ataques remotos.

Hay una Web públicamente disponible el motor de búsqueda sabido como Shodan aquello

expone nontraditional los aparatos configuraron para conectar al Internet.<sup>17</sup> Shodan las exposiciones resulta no sólo de vuestro Internet de aparatos de Cosas en casa pero también de redes de utilidades municipales internas y sistemas de control industrial que ha sido misconfigured para conectar sus servidores a la red pública. También muestra corrientes de dato de incontables misconfigured webcams comerciales en todo el mundo. Ha sido estimado que en cualquier día dado allí puede ser tan muchos como cien webcams de millar con pequeños o ninguna seguridad que transmite sobre el Internet.

Entre estos es cámaras de Internet sin default la autenticación de una empresa llamó D-Enlace, los cuales pueden soler espía en personas en su private momentos (según lo que estos cámaras están puestos para captar). Un atacante puede utilizar filtros de Google para buscar “Internet de D Enlaces cámaras.” El atacante entonces puede buscar los modelos que default a ninguna autenticación, entonces ir a un sitio web como Shodan, clic un enlace, y ver las corrientes de vídeo en su ocio.

Para ayudar impedir esto, mantener vuestro Internet-las webcams accesibles giraron fuera cuándo ellos're no en uso. Físicamente disconnect les para ser seguro son fuera. Cuándo son en uso, marca seguro tienen autenticación apropiada y está puesto a una contraseña personalizada fuerte, no el default un.

Si piensas que vuestra casa es una pesadilla de intimidad, espera hasta que ves vuestro workplace. Explicaré en el capítulo próximo.

## CAPÍTULO TRECE

# Cosas Vuestro Jefe no Te Quiere para Saber

Si has leído esto lejos, eres evidentemente preocupado aproximadamente intimidad, pero para la mayoría de nosotros no es un asunto de esconder del gobierno federal. Bastante,

sabemos que cuándo somos en obra, nuestros empresarios pueden ver exactamente qué nosotros're haciendo on-line sobre sus redes (p. ej., compra, tocando juegos, goofing fuera). Muchísimo nos sólo quiere cubrir nuestros asnos!

Y aquello está cogiendo más duro de hacer, gracias en separar a los teléfonos celulares llevamos. Siempre que Jane Rodgers, gerente de finanza de un Chicago landscaping empresa, quiere saber si sus empleados en el campo son donde tendrían que ser, estira arriba de sus ubicaciones exactas en su portátil. Gusta muchas gerente y dueños de empresa, she está girando a seguir software en corporativo-poseído, personalmente habilitado (SOPORTA) smartphones y camiones de servicio con aparatos de GPS a surveil sus empleados. Un día un cliente pidió Jane si uno de su landscapers había sido fuera para actuar un servicio. Después de que unos cuantos keystrokes, Jane verificó que entre 10:00 a.m. y 10:30 a.m. uno de sus empleados había sido al sitio especificado.

El telematics servicio Rodgers los usos proporciona capacidades más allá geolocalización. Por ejemplo, en su nueva empresa-poseyó teléfonos ella can también fotos de vista, mensajes de texto, y los emails enviaron por sus jardineros. También tiene acceso a sus registros de llamada y visitas de sitio web. Pero Rodgers dice sólo utiliza la característica de GPS.<sup>1</sup>

GPS que sigue en la industria de servicio ha sido disponible para un tiempo largo. Él,

Junto con Servicio de Paquete Unido's ORION propio sistema de selección de ruta algorítmica, ha dejado la empresa de entrega del envase para cortar abajo en gastos gasistas por controlar y sugiriendo optimizó rutas para sus motor. La empresa era también capaz de agrietar abajo en motor perezosas. Yon estas maneras, UPS ha aumentado su volumen por 1.4 millones de envases adicionales por día—con mil menos motor.<sup>2</sup>

Todo esto es bien para los empresarios, quiénes discuten que por exprimir fuera de márgenes más altos pueden en el turno proporciona para pagar sueldos mejores. Pero qué hacer los empleados sienten? hay un downside a toda esta vigilancia. En un análisis, *la revista de Harper* constó un perfil de una motor quién era electrónicamente controlado mientras en obra. La motor, quién no dio su nombre, dijo que el software cronometró su deliveries al segundo y le informó siempre que era debajo o sobre optimal tiempo. Al final de un día típico, la motor dijo que podría ser encima por tanto como cuatro horas.

Slacking Fuera? La motor señalada fuera que una parón sola podría incluir envases múltiples—qué el ORION software no siempre cuenta para. La motor describió coworkers en su distribución de Nueva York centra quién batallaba dolor crónico en sus espaldas más bajas y rodillas de probar para llevar demasiado en un viaje solo—a pesar de recordatorios constantes de la empresa con respecto a apropiado manejando de cargas pesadas—para mantener arriba con el software. Tan hay uno amable de coste humano a este control de empleado.

Otro sitio donde vigilancia de obra está utilizada asiduamente es la industria de servicio alimentaria. De cameras en los techos de restaurantes a quioscos en el tabletop, personal de espera puede ser mirado y valorado por varios sistemas de software. Un 2013 estudio por investigadores de Universidad de Washington, Brigham Young Universidad, y MIT encontrado que que controla robo software utilizado en 392 restaurantes produjeron una 22 reducción de porcentaje en servidor-lado robo financiero después de que

estuvo instalado.<sup>3</sup> Como mencioné, activamente controlando las personas cambia su comportamiento.

hay actualmente ningún estatuto federal en los Estados Unidos a prohibir empresas de seguir sus empleados. Delaware único y Connecticut requieren empresarios para decir empleados cuándo están siendo seguidos. En más estados, los empleados no tienen ninguna idea si están siendo mirados en obra.

Qué sobre empleados en la oficina? The Asociación de Gestión americana encontrada que 66 por ciento de empresarios controlan el uso de Internet de sus empleados, 45 por ciento de porcentaje empleado keystrokes en el ordenador (notando idle tiempo como pausas “potenciales”), y 43 por ciento controlan los contenidos de email de empleado.<sup>4</sup> Algunos empleados de monitor de las empresas' entradas de calendario

de la Perspectiva, encabezamientos de email, e instante-messaging registros. El dato es aparentemente utilizado para ayudar las empresas imaginan fuera cómo sus empleados están pasando su tiempo— de cuánto tiempo salespeople es spending con clientes a qué reparto de la empresa están quedándose en tacto por el email a cuántos empleados de tiempo está pasando en reuniones o fuera de sus escritorios.

Naturalmente hay un giro positivo: teniendo tal metrics significa que la empresa puede ser más efficient en planificar reuniones o en fomentar equipos para tener más contacto con cada otro. Pero la línea inferior es que alguien está recogiendo todo este dato corporativo. Y podría someday ser girado encima a aplicación de ley o en el muy menos utilizado against tú en una reseña de actuación.

No eres invisible en obra. Cualquier cosa pasando a través de una red corporativa pertenece a la empresa—no es el vuestro. Incluso si estás comprobando vuestra cuenta de email personal, vuestro último orden con Amazona, o planeando unas vacaciones, probablemente estás utilizando una empresa-teléfono emitido, portátil, o VPN, así que espera tener alguien controlando todo lo que haces.

Aquí's una manera fácil de mantener vuestra gerente e incluso vuestro coworkers de snooping: cuándo dejas vuestro escritorio para ir a una reunión o el baño, cerradura vuestra pantalla de ordenador. Seriamente. No deja vuestro email, o detalles sobre el proyecto tú've pasó semanas encima, abre—sólo sentando allí para alguien a desorden con. Cerradura vuestro ordenador hasta que regresas a vuestra pantalla. Toma unos cuantos segundos extras, pero él'll de sobra te dolor muchísimo. Pone un

temporizador en el sistema operativo para cerrar la pantalla después de un número seguro de segundos. O cariz a uno del Bluetooth aplicaciones que automáticamente cerrará vuestra pantalla si vuestro teléfono celular no es cercano el ordenador. Aquello dijo, hay un ataque nuevo que usas un weaponized aparato de USB. Las oficinas muchísimas sellan los puertos de USB en sus portátiles y desktops, pero si el vuestro no un weaponized palo de USB podría todavía unlock vuestro ordenador sin una contraseña.<sup>5</sup>

Además de secretos corporativos, allí's también una cantidad justa de personal e- correo que pases a través de nuestros ordenadores durante el día de trabajo, y a veces lo imprimimos fuera para nosotros mientras en la oficina. Si estás preocupado aproximadamente intimidad, no *cualquier cosa* personal mientras en obra. Mantener un estricto firewall entre vuestra vida de obra y vuestra vida de casa. O traer un aparato personal como un portátil o un iPad de en casa si sientes la necesidad de hacer material personal mientras encima pausa. Y si vuestro aparato móvil es celular-habilitad, nunca utilizar el Wi-Fi de empresa, y, más allá, turno del SSID emisión si estás utilizando un portátil hotspot (ve [aquí](#)). Uso único dato celular cuándo dirigiendo negocio

personal en obra. Realmente, una vez llegas en vuestra oficina, vuestras necesidades de cara de juego públicas para ser

encima. Tan te wouldn't charla aproximadamente cosas realmente personales con vuestros compañeros de oficina casuales, necesitas mantener vuestro negocio personal de los sistemas de ordenador de la empresa (especialmente cuándo estás buscando salud-narró temas o buscando un trabajo nuevo).

Es más duro que suena. Para una cosa, nosotros're utilizados a la ubicuidad de información y la disponibilidad casi universal del Internet. Pero si estás yendo a maestro el arte de invisibilidad, te tienes que impedir de hacer cosas privadas en público.

Asume que todo escribes a vuestro ordenador de oficina es público. Aquel doesn't malo que vuestro LO el departamento activamente está controlando vuestro aparato particular o nunca ley en el hecho que te imprimido fuera de la ciencia de vuestro niño proyecto justo en la impresora de color cara en el quinto piso—a pesar de que pueden. El punto es, hay un récord que tú estas cosas, y allí tendría que ser sospecha en el futuro, *pueden* acceder los récords de todo hiciste en aquella máquina. Es su máquina, no el vuestro. Y él's su red. Aquello significa están escaneando el contenido que flujos en y fuera de la empresa.



Considerar el caso de Adam, quién descargó su informe de crédito libre en su ordenador de obra. Él logged en a la agencia de crédito's el sitio que utiliza el ordenador de empresa sobre la red de empresa. Dejado es decirte, gusta Adam, también descargar vuestro informe de crédito en obra. Lo quieres imprimir fuera, bien? Así que por qué no enviarlo to la impresora de empresa encima en la esquina? Porque si tú , habrá una copia de la lima de PDF que contiene vuestra historia de crédito que sienta en el paseo duro de la impresora. Te don't Control que impresora. Y después de la impresora está retirada y sacado de la oficina, te don't tiene control encima cómo aquel paseo duro está colocado de. Algunas impresoras ahora están encriptando sus paseos, pero puede te ser seguro que la impresora en vuestra oficina está encriptada? Puedes no.

Aquello no es todo. Cada Palabra o Excel documento que te create utilizando Oficina de Microsoft incluye metadata aquello describe el documento. Típicamente documentar metadata incluye el autor's nombre, la cita creó, el número de revisiones, y la medida de lima así como una opción para añadir más detalles. Esto no es habilitado por default por Microsoft; tienes que pasar por algunos hoops para verlo.<sup>6</sup> Microsoft tiene, aun así, incluido un Inspector de Documento que puede sacar estos detalles antes de que exportas el documento en otro lugar.<sup>7</sup>

Un 2012 estudio patrocinado por Xerox y McAfee encontrado que 54 por ciento de empleados dicen no siempre siguen su empresa's LO pólizas de seguridad,

y 51 por ciento de empleados cuyo workplace tiene una impresora, copier, o multifunction la impresora dice ellos've copiados, escaneados, o imprimidos información personal confidencial en obra. Y no es obra justa: el mismo va para impresoras en la tienda de copia local y la biblioteca local. Ellos todos contienen paseos duros que recuerda todo ellos've imprimidos sobre su lifetimes. Si necesitas algo personal imprimido fuera, quizás lo tendrías que imprimir fuera más tarde en en casa, en una red e impresora encima cuál tienes control.

Espiando, incluso en empleados, ha cogido muy creativo. Algunas empresas enlist nontraditional aparatos de oficina que podemos otherwise tomar para concedido, nunca imaginando podrían soler espía encima nos. Considerar la historia de un joven Columbia el estudiante de posgrado Universitario nombró Ang Cui. Preguntándose si podría cortar a una oficina corporativa y robar dato sensible a través de nontraditional medio, Cui decidido primero para atacar impresoras de láser, una grapa en más oficinas hoy.

Cui Notado que las impresoras eran manera detrás del tiempo. Durante varias pruebas de bolígrafo, he observado esto también. He sido capaz a apalancamiento la impresora para coger acceso más lejano a la red corporativa. Esto es porque los trabajadores raramente cambian el admin contraseña en impresoras que es internamente desplegó.

El software y el firmware utilizado en impresoras—especialmente las impresoras comerciales para la oficina de casa—contienen defectos de seguridad básicos muchísimos. La cosa es, muy pocas personas ven una impresora de oficina como vulnerable. Piensan que están gozando qué es seguridad llamada “a veces por obscuridad”—si nadie nota el defecto, entonces eres seguro.

Pero como he dicho, impresoras y máquinas de copia, según el modelo, tiene uno cosa importante en común—ely ambos pueden contener paseos duros. Y a no ser que aquel paseo duro está encriptado—y muchos son todavía no—es posible de acceder qué ha sido imprimido en una cita más tardía. Todo esto ha sido sabido para años. Qué Cui se preguntó era si podría girar una impresora de empresa contra sus dueños y exfiltrate cualquier cosa estuvo imprimida.

Para hacer cosas más interesantes, Cui quiso atacar la impresora's firmware código, la programación embedded dentro de un chip dentro de la impresora. A diferencia de nuestro tradicional PCs y aparatos móviles, digitales TVs y otra “electrónica” lista no tiene el poder o los recursos de tramitación para correr un lleno- sistema operativo soplado como Androide, Ventanas, e iOS. En cambio estos aparatos utilizan qué está llamado sistemas operativos de tiempo real (RTOS), los cuales están almacenados en chips individuales dentro del aparato (frecuentemente sabido como firmware). Estos chips almacenan sólo las órdenes necesitaron operar el sistema y no

mucho más. Ocasionalmente incluso esta necesidad de órdenes sencilla para ser actualizado por el fabricante o vendedor por centelleo o reemplazando los chips. Dado que esto está hecho tan infrequently, es obvio que muchos fabricantes sencillamente no construyeron en las medidas de seguridad apropiadas. Esto, la carencia de actualización, era el vector que Cui decidido para perseguir para su ataque.

Cui Quiso ver qué pasaría si cortó el formato de lima HP utilizado para su firmware actualizaciones, y descubrió que HP didn't control la validez de cada actualización. Así que creó impresora firmware de su propio—y la impresora lo aceptó. Sólo gustar aquello. no había ninguna autenticación en

la impresora's lado que la actualización provino HP. La impresora sólo se preocupó que el código era en el formato esperado.

Cui Ahora era libre de explorar.

En uno experimento famoso, Cui informado que podría girar en el fuser barra, la parte de la impresora que calorea el papel después de la tinta ha sido aplicado, y dejarlo encima, el cual causaría la impresora para coger fuego. El vendedor—no HP— inmediatamente respondió por discutir que había un thermo fallar-seguro dentro del fuser barra, significando la impresora podría no overheat. Aun así, aquello era Cui punto—él'd dirigido para girar aquello falla-característica segura fuera de modo que la máquina de hecho podría coger fuego.

A raíz de estos experimentos, Cui y su asesor, Salvatore Stolfo, discutió que las impresoras eran enlaces débiles en cualquier organización o casa. Por ejemplo, el HR el departamento de una empresa de Fortune 500 podría recibir un maliciously-coded résumé lima sobre el Internet. En el tiempo toma la gerente de contratar para imprimir aquel documento, la impresora a través de qué viaja podría ser plenamente compromised por instalar un malicious versión del firmware.

Impidiendo alguien de grabbing vuestros documentos de la impresora, imprenta segura, también sabido tan imprenta de atracción, asegura que los documentos son sólo liberados a la autenticación de un usuario en la impresora (usually un passcode tiene que ser introducido antes del documento imprimirá). Esto puede ser hecho por utilizar un ALFILER, carta lista, o biometric fingerprint. La atracción que imprime también elimina unclaimed documentos, impidiendo información sensible de lying alrededor para todo el mundo para ver.<sup>8</sup>

Edificio en sus ataques de impresora, Cui empezó para mirar alrededor de la oficina típica para otros objetos comunes que podría ser vulnerable y resolvió encima Voz encima Protocolo de Internet (VoIP) teléfonos. Como con impresoras, nadie había apreciado el escondido todavía obvio-una vez-tú-pensado-aproximadamente- valora de estos aparatos en recoger información. Y tan con una impresora, una actualización al sistema puede ser

fingida y aceptada por el VoIP teléfono. La mayoría de VoIP los teléfonos tienen unas manos-opción libre que te dejás para poner alguien

en speakerphone en vuestro cubículo u oficina. Cuál significa allí's no sólo un altavoz pero también un micrófono en el exterior del handset. Allí ha también un “del cambio” de gancho, el cual dice el teléfono cuándo alguien

ha elegido arriba del auricular y quiere marcar o escuchar a una llamada así como cuando el auricular ha sido puesto atrás y el speakerphone está habilitado. Cui Dado cuenta que si podría comprometer el “del cambio” de gancho, podría hacer el teléfono escucha a las conversaciones cercanas vía el speakerphone micrófono—incluso cuándo el auricular era en el gancho!

Uno caveat: a diferencia de una impresora, los cuales pueden recibir malicious código vía el Internet, VoIP necesidad de teléfonos para ser “actualizado” individualmente a mano. Esto requiere el código para ser propagado utilizando un paseo de USB. No un problema, Cui decidió. Para un precio, una noche janitor podría instalar el código en cada teléfono con un palo de USB como él o ella limpiaron la oficina.

Cui Ha presentado esta búsqueda en un número de conferencias, cada vez utilizando diferentes VoIP teléfonos. Y cada vez el vendedor estuvo notificado en advance, y cada vez el vendedor produjo un fijar. Pero Cui ha señalado fuera de aquel justo porque un parche existe no significa coge aplicado. Algunos del unpatched los teléfonos todavía podrían ser sentando en oficinas, hoteles, y hospitales ahora mismo.

Tan qué hizo Cui coge the dato del teléfono? Desde entonces redes de ordenador de la oficina están controladas para actividad inusual, necesitó otro significa de extraer el dato. Decidió ir “fuera red” y utilizar olas radiofónicas en cambio.

Anteriormente, investigadores en Stanford Universidad y en Israel encontrado aquello habiendo vuestro teléfono celular colocó luego a vuestro ordenador puede dejar una tercera fiesta remota a eavesdrop en vuestras conversaciones. El truco requiere malware para ser insertado a vuestro aparato móvil. Pero con maliciously coded las aplicaciones disponibles para download de rogue tiendas de aplicación, aquello es bastante fácil, bien?

Con el malware instalado en vuestro teléfono celular, el giroscopio dentro del teléfono es ahora bastante sensible para elegir arriba de vibraciones leves. El malware en este caso, los investigadores dicen, también puede elegir arriba vibraciones de aire del minuto, incluyendo aquellos producidos por habla humana. Google's sistema operativo de Androide deja movimientos de los sensores para ser leídos en 200 Hz, o 200 ciclos por segundo. La mayoría de gama de voces humana de 80 a 250 Hz. Aquello significa el sensor puede elegir arriba de un significant porción de aquellas voces. Los investigadores incluso construyeron una habla hecha de encargo-programa de reconocimiento diseñó para interpretar el 80–250 Hz señales más allá.<sup>9</sup>

Cui encontrado algo similar dentro del VoIP teléfonos e impresoras. Encontró que los alfileres finos que enganchan fuera de of sólo sobre cualquier microchip dentro de cualquier embedded el aparato hoy podría ser hecho para oscilar en secuencias únicas y por tanto exfiltrate dato sobre frecuencia radiofónica (RF). Esto es qué llama un funtenna, y es un patio virtual para -ser atacantes. De ficially, dice investigador de seguridad Michael Ossmann, quien Cui créditos para la idea, “un funtenna es una antena que no fue pretendido por el diseñador del sistema para ser una antena, particularmente cuándo utilizado como una antena por un atacante.”<sup>10</sup>

Aparte de un funtenna, qué es algunos otras personas de maneras pueden espiar en qué haces en obra?

Los investigadores en Israel han encontrado que los teléfonos celulares normales pueden—con malware instalados—ser hechos para recibir dato binario de ordenadores. Y anteriormente, Stanford los investigadores encontraron que sensores de teléfono celular podrían interceptar el sonido de emisiones electrónicas de un teclado inalámbrico.<sup>11</sup> Estas complexiones en la búsqueda similar dirigida por científicos en MIT y Tecnología de Georgia.<sup>12</sup> lo Basta para decir que todo escribes o la vista o el uso en la oficina pueden ser escuchados a en una manera u otro por una tercera fiesta remota.

Para caso, dice utilizas un teclado inalámbrico. La señal radiofónica inalámbrica enviada del teclado al portátil o desktop PC puede ser interceptado. Investigador de seguridad Samy Kamkar desarrollado algo llamó KeySweeper aquello's diseñado para hacer sólo aquello: un USB disfrazado charger que wirelessly y passively busca, decrypts, registros, e informes atrás (sobre GSM) todo keystrokes de cualquier Microsoft teclado inalámbrico en la proximidad.<sup>13</sup>

hemos hablado el peligro de utilizar bogus hotspots en cafeterías y aeropuertos. Igual puede ser cierto en oficinas. Alguien en vuestra oficina puede poner arriba de un inalámbrico hotspot, y vuestro aparato automáticamente podría conectar a él. ÉL departamentos típicamente escáner para tales aparatos, pero a veces ellos no.

Un equivalente moderno de traer vuestro propio hotspot a la oficina está trayendo vuestra conexión celular propia. Femtocells Es los aparatos pequeños disponibles de vuestro transportista móvil. Ellos're diseñados para aumentar conexiones celulares dentro de una casa u oficina donde la señal podría ser débil. No son sin riesgos de intimidad.

Ante todo, porque femtocells es canal de base para comunicaciones celulares, vuestro aparato móvil a menudo conectará a ellos sin informarte. Piensa sobre aquel.

En los Estados Unidos, ley enforcement utiliza algo llamó un StingRay, también sabido como un IMSI catcher, una celda-simulador de sitio. Además hay

TriggerFish, Wolfpack, Gossamer, y caja de ciénaga. Aunque las tecnologías varían, estos aparatos básicamente toda ley como un femtocell sin el celular conexión. Están diseñados para recoger la identidad de suscriptor móvil internacional, o IMSI, de vuestro teléfono celular. Su uso en los Estados Unidos es significativamente detrás que de Europa—por ahora. IMSI catchers Está utilizado en protestas sociales grandes, por ejemplo, para ayudar aplicación de ley identifica quién era en la asamblea.

Presumiblemente los organizadores serán en sus teléfonos, coordinando casos.

Después de un protracted batalla legal, la Unión de Libertades Civil americana de California Del norte obtuvo documentos from el gobierno que detalla cómo va aproximadamente utilizando StingRay. Por ejemplo, agentes de aplicación de la ley están dichos para obtener un registro de bolígrafo o una trampa-y-orden judicial de rastro. Registros de bolígrafo han solido obtiene números de teléfono, un récord de dígitos dialed en un phone. Trampa-y- tecnología de rastro ha solido recoge la información aproximadamente recibió llamadas. Además, aplicación de ley puede, con un warrant, legalmente obtener el registro de voz de una llamada de teléfono o el texto de un email. Según *Alambrado*, los documentos recibend por el ACLU estado que los aparatos “pueden ser capaces de interceptar los contenidos de comunicaciones y, por tanto, tales aparatos tienen que ser configurados para inutilizar la función de interceptación, a no ser que las interceptaciones han sido autorizadas por un Título III orden.”<sup>14</sup> Un Title III orden deja de verdad-interceptación de tiempo de comunicación.

Dejado es dice no eres debajo vigilancia por aplicación de ley. Dejado es dice eres en una oficina que es altamente regulado—por ejemplo, en una utilidad pública. Alguien puede instalar un femtocell para dejar comunicaciones personales fuera de la utilidad's llamada normal-logging sistema. El peligro es que el coworker con el modificó femtocell en su o su escritorio podría actuar un hombre-en-el-ataque medio, y él o ella también podrían escuchar en en vuestras llamadas o interceptar vuestros textos.

En una demostración en EE.UU. de Sombrero Negro 2013, los investigadores eran capaces de captar llamadas de voz, mensajes de texto del SMS, e incluso tráfico de Web de voluntarios en la audiencia en su Verizon femtocells. La vulnerabilidad en Verizon-emitió femtocells ya había sido parchado, pero los investigadores quisieron asomar empresas que tendrían que evitar utilizar les en todo caso.

Algunas versiones de Androide te informarán cuándo cambias redes celulares; iPhones no. “Vuestro teléfono asociará a un femtocell sin vuestro conocimiento,” investigador explicado Doug DePerry. “Esto no es gustar Wi-Fi; no tienes una elección.”<sup>15</sup>

Una empresa, Pwnie Expresa, produce un aparato llamó Pwn Pulso que identifica femtocells e incluso IMSI catchers como StingRay.<sup>16</sup> da companies la capacidad de controlar redes celulares alrededor les. A Herramientas les gustan estos, los cuales detectan el espectro lleno de amenazas celulares potenciales, era una vez comprado en gran parte por el gobierno—pero no anymore.

Como usuario-amistoso como es, Skype no es el más amistoso when viene a intimididad. Según Edward Snowden, cuyo revelations era primero publicado en el *Guardián*, Microsoft obró con el NSA para hacer seguro que Skype las conversaciones podrían ser interceptadas y controló. Uno documenta presume que un NSA el programa saben tan el prisma controla Skype vídeo, entre otros servicios de comunicaciones. “Las porciones de audio de estas sesiones han sido procesadas correctamente todo a lo largo de, pero sin el vídeo acompañante. Ahora, los analistas tendrán el cuadro ‘completo’,” el *Guardián* escribió.<sup>17</sup>

En Marcha de 2013, un ordenador-estudiante de posgrado de ciencia en la Universidad de Nuevo México encontró que TOM-Skype, una versión china de Skype creado a través de una colaboración entre Microsoft y el Grupo de TOM de empresa chino, carga listas de palabra clave a cada Skype la máquina del usuario—porque en China allí es palabras y frases no eres permitted para buscar on-line (incluyendo “Tiananmen Plaza”). TOM-Skype también envía el gobierno chino el titular de cuenta's username, el tiempo y cita de transmisión, e información aproximadamente si el mensaje estuvo enviado o recibido por el usuario.<sup>18</sup>

Investigadores han encontrado que incluso muy alto-acabar videoconferencing sistemas —la clase cara, no Skype—puede ser compromised por hombre-en-el-ataques medios. Aquello significa la señal es



routed through alguien más antes de que llega en vuestro fin. El mismo es cierto con conferencias de audio. A no ser que el moderador tiene una lista de números que ha dialed en, y a no ser que ha pedido para verificar cualesquier números cuestionables—dicen, códigos de área fuera de los Estados Unidos—allí es ninguna manera de probar o determinar si un uninvited la fiesta ha unido. El moderador tendría que llamar fuera de cualesquier llegadas nuevas y, si fallan para los identificar, cuelga y utilizar una segunda conferencia-número de llamada en cambio.

Decir vuestra oficina ha pasado grande bucks y compró un realmente caro videoconferencing sistema. Tú'd pensarlo sería más seguro que un consumidor-sistema de nota. Pero serías incorrecto.

En mirar en estos sistemas de fin alto, investigador H. D. Moore encontró que casi todo de ellos default a coche-unnsver incoming llamadas de vídeo. Aquello hace sentido. Pusiste una reunión para 10:00 a.m., y quieres participantes a dial en. Aun así, también significa que en algunos otro tiempo de día, cualquiera quién sabe que

el número podría dial en y, bien, literalmente tomar un peek en vuestra oficina. “La popularidad de vídeo conferencing sistemas entre el capital de aventura e industrias de finanza dirige a un grupo pequeño de increíblemente alto-objetivos de valor para cualquier atacantes intent en espionaje industrial u obteniendo una ventaja empresarial

injusta,” Moore escribió.<sup>19</sup> Cómo duro es para encontrar estos sistemas? Conferencing Los sistemas utilizan un únicos

H.323 protocolo. Así que Moore miraba en un sliver del Internet e identificó 250,000 sistemas que utilizan que protocolo. Estima de aquel número que menos que cinco mil de estos estuvo configurado a coche-contestar—un porcentaje pequeño de la totalidad, pero todavía un número muy grande por él. Y aquello no está contando el resto del Internet.

Qué puede un atacante aprende de cortar tal sistema? El conferencing cámara de sistema es under el control del usuario, así que un atacante remoto podría tilt lo arriba, abajo, a la izquierda, o derecho. En más casos el cámara no tiene una luz roja para indicar que él's encima, así que a no ser que estás mirando el cámara, no podrías ser consciente que alguien lo ha movido. El cámara puede también zum en. Moore dijo que su equipo de búsqueda era capaz de leer una contraseña de seis dígitos posted en una muro veinte pies del cámara. Podrían email leído también en la pantalla de un usuario a través de la sala.

Tiempo próximo eres en la oficina, considerar qué puede ser visto del videoconferencing cámara. Quizás el departamento's el mapa organizativo es en la muro. Quizás vuestro desktop la pantalla afronta la sala de conferencia. Quizás cuadros de vuestros niños y el cónyuge son visibles también. Aquello es lo que un remoto atacante could ver y posiblemente uso contra vuestra empresa o incluso tú personalmente.

Algunos vendedores de sistema son conscientes de este asunto. Polycom, por ejemplo, proporciona un multipage endurecimiento (que fortalece seguridad) guía, incluso limitando el recolocando del cámara.<sup>20</sup> Aun así, ÉL staffers don't normalmente tener el tiempo para seguir a directrices les gustan estos, y ellos a menudo no incluso considerar seguridad una preocupación. Hay miles de conferencing sistemas en el Internet con default los encuadres habilitaron.

Los investigadores también descubrieron que corporativos firewalls don't saber cómo para manejar el H.323 protocolo. Sugieren dar el aparato una alocución de Internet pública y poniendo una regla para él dentro el corporativo firewall.

El riesgo más grande es que muchos de las consolas de administración para estos conferencing sistemas haber poco o ninguna seguridad construida en. En un ejemplo, Moore y su equipo eran capaces de acceder el sistema de una empresa de ley, el cual contuvo una

alocución-entrada de libro para el boardroom de una inversión bien sabida banco. Los investigadores habían adquirido un utilizados videoconferencing aparato de eBay, y cuándo llegó su paseo duro todavía tuvo dato viejo encima lo—incluyendo el libro de alocución, el cual listó docenas de números privados, muchos del cual estuvo configurado a coche-contestar incoming llamadas del Internet en grande.<sup>21</sup> Como con copia e impresoras viejas máquinas, si tiene un paseo duro, necesitas a securely toallita húmeda el dato de él antes de que lo vendes o darlo (ve [aquí](#)).

A veces en obra somos tasked con colaborar en un proyecto con un colega quiénes pueden ser hasta la mitad a través del planeta. Las limas pueden ser compartidas atrás y adelante sobre email corporativo, pero a veces ellos're tan grandes que sistemas de email sencillamente balk y no aceptarles tan anexos. Cada vez más, las personas han sido utilizando servicios para enviar que comparten lima limas grandes atrás y adelante.

Qué seguro es esta nube-basó servicios? Varía.

Los cuatro jugadores grandes—Manzana iCloud, Paseo de Google, Microsoft OneDrive (anteriormente SkyDrive), y Dropbox—todos proporcionan verificación de dos pasos. Aquello te significará recibir un fuera-de-texto de banda en vuestro aparato móvil que contiene un código de acceso para confirmar vuestra identidad. Y mientras todo cuatro servicios encriptan el dato mientras es en transit te mosto—si te don't querer la empresa o el NSA para leer —encripta el dato antes de que lo envías.<sup>22</sup>

Allí el fin de semejanzas.

Autenticación de dos factores es importante, pero puedo todavía bypass esto por hijacking unused cuentas. Por ejemplo, recientemente hice una prueba de bolígrafo donde el cliente añadió Google's 2FA a su VPN el sitio web que utiliza públicamente herramientas disponibles. La manera era capaz de entrar era por obtener el registro de directorio activo-en credentials para un usuario que no firmó hasta utilizar el VPN portal. Desde entonces era el primer a registro en al VPN servicio, estuve apuntado para poner arriba 2FA utilizando Google Authenticator. Si el empleado nunca accede el servicio él, entonces el atacante habrá continuado acceso.

Para datos en resto, Dropbox usos 256-mordió AES encriptación (cuál es bastante fuerte). Aun así, retiene los tonos, el cual podría dirigir a acceso no autorizado por Dropbox o aplicación de ley. Paseo de Google e iCloud uso un considerablemente más débil 128-mordió encriptación para data en resto. La preocupación aquí es que el dato potencialmente podría ser decrypted por fuerza computacional fuerte. Microsoft OneDrive doesn't molestar con encriptación, el cual dirige uno para sospechar que esto era por diseño, quizás en el instando de algunos gobiernos.

Paseo de Google ha presentado una gestión de derechos de información nueva (IRM)

característica. Además de los documentos, spreadsheets, y las presentaciones crearon dentro Google Docs, Paseo de Google ahora acepta PDF y otros formatos de lima también. Las características útiles incluyen the capacidad de inutilizar la descarga, huella, y capacidades de copia para commenters y espectadores. También puedes impedir cualquiera de añadir personas adicionales a una lima compartida. Naturalmente estas características de gestión son sólo disponibles de archivar dueños. Aquello significa si tanmeone te ha invitado para compartir una lima, aquella persona tiene que poner las restricciones de intimidad, no te.

Microsoft ha también presentó un único por-característica de encriptación de la lima, el cual es qué suena gusta: una característica que encripta cada lima

individual con su tono propio. Si uno clave es compromised, sólo que la lima individual será afectada más que el archivo entero. Pero esto no es el default, tan los usuarios tendrán que entrar el hábito de encriptar cada lima ellos.

Cuál parece como una recomendación buena en general. Los empleados y los usuarios en general tendrían que coger utilizados a encriptar dato antes de que coge enviado a la nube. Aquella manera retienes control de los tonos. Si una agencia de gobierno viene golpear en la puerta de Apple, Google, Dropbox, o Microsoft, aquellas empresas ganadas't ser capaces de ayudar—tendrás los tonos individuales.

También podrías escoger utilizar el proveedor de servicio de la nube que se pone aparte del resto—SpiderOak, el cual ofrece los beneficios llenos de almacenamiento de nube y sync capacidad junto con 100 dato de porcentaje privacy. SpiderOak Protege dato de usuario sensible a través de contraseña de dos factores autenticación y 256-mordió AES encriptación de modo que las limas y las contraseñas se quedan privadas. Los usuarios pueden almacenar y sync información sensible con intimidad completa, porque este servicio de nube has absolutamente cero conocimiento de contraseñas y dato.

Pero más los usuarios continuarán utilizar otros servicios en su riesgo propio. Las personas quieren la facilidad de grabbing dato de la nube, y tan hacer agencias de aplicación de la ley. Una preocupación enorme aproximadamente utilizando la nube es que vuestro dato no tiene las mismas Cuartas protecciones de Enmienda que lo tendría si estuvo almacenado en un cajón de escritorio o incluso en vuestro ordenador de sobremesa.

Agencias de aplicación de la ley están pidiendo nube-dato basado con creciente (y unsettling) frecuencia. Y pueden obtener acceso con facilidad relativa, desde entonces todo cargas on-line—si a una Web-servicio de email basado, Paseo de Google, o Shutterfly— va a un servidor que pertenece al proveedor de servicio de la nube, no a ti. La protección cierta única es para entender que cualquier cosa pusiste allí arriba puede ser accedido por alguien más y para obrar consiguientemente por encriptar todo primero.

## CAPÍTULO CATORCE

### **Obteniendo el anonimato Es Trabajo duro**

hace Unos cuantos años regresaba a los Estados Unidos de un viaje a Bogotá, Colombia, y a llegar en Atlanta, era tranquilamente escoltado por dos

Aduana de EE.UU. agentes a una sala privada. Anteriormente haber sido arrestado, y teniendo servido tiempo en prisión, era quizás un poco menos flustered que la media Joe habría sido. Todavía, era unsettling. No había hecho cualquier cosa incorrecto. Y era en aquella sala para cuatro horas—cinco cortos del máximos que podría ser aguantado sin ser arrestó.

El problema empezado cuándo un agente de Aduana de los EE.UU. golpeó mi pasaporte y entonces stared en la pantalla. “Kevin,” el agente dicho con una sonrisa grande en su cara. “Suposición qué? Hay algunas personas abajo quiénes quieren tener una palabra contigo. Pero no se preocupa. Todo será vale.”

Había sido en Bogotá para dar una habla patrocinada por el diario *El Tiempo*. Era unlso visitando la mujer quién era mi novia en el tiempo. Mientras esperaba en aquella sala abajo, llamé mi novia atrás en Bogotá. Dijo la policía en Colombia había llamado pidiendo su permiso para buscar un envase había puesto en un FedEx caja a los Estados Unidos. “Encontraron rastros de cocaína,” dijo. Conocí hubieron no.

El envase contuvo un 2.5-pulgada paseo duro interno. Aparentemente el colombiano—o quizás las potestades—de EE.UU. quisieron comprobar los contenidos del paseo, el cual estuvo encriptado. La cocaína era una excusa coja para abrir el envase. Nunca cogía mi paseo duro atrás.

Más tarde aprendí que la policía había desgarrado abre la caja, tomado el equipamiento electrónico aparte, entonces destruyó mi paseo duro mientras intentando abrir él por perforar un agujero en él para comprobar para cocaína. Podrían haber utilizado un destornillador especial para abrir el paseo. No encontraron cualesquier drogas.

Entretanto, atrás en Atlanta, los oficiales abrieron mi equipaje y fundar mi MacBook Pro, un Dell XPS M1210 portátil, un Asus 900 portátil, tres o cuatro paseos duros, aparatos de almacenamiento de USB numerosos, algunos Bluetooth dongles, tres iPhones, y cuatro teléfonos celulares de Nokia (cada cual con su propio SIM carta, así que podría evitar vagar cargos mientras hablando en países diferentes). Estos son herramientas estándares en mi profesión.

También en mi equipaje era mi caja que elige cerradura y un aparato de clonación que podría leer y replay cualquier ESCONDIDO proximity carta. El último puede soler recuperar credentials stored encima cartas de acceso por colocar él en cercano proximity a ellos. Puedo, por ejemplo, spoof una persona's carta credentials e introducir cerró puertas sin teniendo que hacer

una carta forjada. Tuve estos porque había dado un keynote presentación aproximadamente seguridad en Bogotá. Naturalmente, los agentes de aduana' los ojos encendieron arriba cuándo les vieron, pensando era hasta algo más—p. ej., skimming cartas de crédito, el cual era imposible con estos aparatos.

Finalmente agentes de Inmigración de EE.UU. y Aplicación de Aduana (HIELO) llegado y pedired por qué era en Atlanta. Era allí para moderar una panel en una conferencia de seguridad patrocinada por la Sociedad americana para Seguridad Industrial (ASIS). Más tarde un agente de FBI en la misma panel era capaz de confirmar la razón para mi viaje.

Las cosas parecían para empeorar cuándo abrí mi portátil y logged en para asomarles el email que confirma mi presencia en la panel.

Mi navegador estuvo puesto a automáticamente aclarar mi historia cuándo empezada, así que cuando lo lancé estuve apuntado para aclarar mi historia. Cuándo confirmé y clicked tél VALE botón para aclarar mi historia, los agentes freaked fuera. Pero entonces sólo pulsé el botón de poder a poder abajo el MacBook, así que mi paseo era inaccesible sin mi PGP passphrase.

A no ser que era debajo arresto, el cual estuve dicho repetidamente que no fui, no tendría que tener tuvo que dar arriba de mi contraseña. Incluso si había sido debajo arresto, no técnicamente tengo tenido que dar arriba de mi contraseña debajo ley de EE.UU., pero si aquel derecho está protegido depende encima cuánto tiempo uno es dispuesto de luchar.<sup>1</sup> Y los países diferentes tienen leyes diferentes en este. En el Reino Unido y Canadá, por ejemplo, las potestades te pueden forzar para revelar vuestra contraseña.

Después de mis cuatro horas, ambos HIELO y los agentes de aduana me dejamos ir. Si una

agencia como el NSA había apuntado me, aun así, ellos haber probablemente succeeded en imaginar fuera de los contenidos de mi paseo duro. Agencias de gobierno pueden compromise el firmware en vuestro ordenador o teléfono celular, impair la red utilizas para conectar al Internet, y explotar una variedad de las vulnerabilidades encontradas en vuestros aparatos.

Puedo viajar a países extranjeros que tiene aún más stringent reglas y nunca tener los problemas tengo en los Estados Unidos debido a mi antecedentes criminal aquí. Tan qué viajas en el extranjero con dato sensible? Y cómo viajas a países “” hostiles como China?

Si no quieres tener cualquier dato sensible disponible en vuestro paseo duro, las elecciones son:

1. Limpio arriba de cualquier dato sensible antes de que viajes y actuar una copia de seguridad llena. 2. Dejar el dato allí pero encriptar él con un tono fuerte (a pesar de que algunos países pueden ser capaces de obligarte para revelar el clave o contraseña). No mantiene el passphrase contigo: quizás dar medio del passphrase a un

amigo fuera de los Estados Unidos quiénes no pueden ser obligados para darlo arriba. 3. Cargar el dato encriptado a un cloud servicio, entonces descarga y cargar

como necesitó. 4. Uso un producto libre como VeraCrypt para crear una carpeta de lima encriptada

escondida en vuestro paseo duro. Otra vez, un gobierno extranjero, si encuentra la carpeta

de lima escondida, puede ser capaz de forzarte para revelar la contraseña. 5. Siempre que introduciendo vuestra contraseña a vuestros aparatos, portada tú y vuestro ordenador, quizás con una chaqueta u otro elemento de ropa, para impedir vigilancia de cámara.

6. 6. Foca vuestro portátil y otros aparatos en un FedEx u otro Tyvek envelope

y firmarlo, entonces puesto él en la habitación de hotel segura. Si el envelope es tampered con, lo tendrías que notar. Nota, también, aquel hotel safes aren't realmente que seguro. Tendrías que considerar comprar un aparato de cámara que te puede poner dentro del seguro de tomar una foto de cualquiera abriéndolo y enviar la foto vía celular en tiempo real.

6. 7. Más de todo, no toma cualquier riesgo. Llevar vuestro aparato contigo en todo momento, y no dejado él fuera de vuestra vista.

Según los documentos obtuvieron por la Unión de Libertades Civil americana a través de la Libertad de Ley de Información, entre octubre de 2008 y junio de 2010, más de 6,500 personas que viajan a y de los Estados Unidos tuvieron sus aparatos electrónicos buscaron en el borde. Esto es una media de más de trescientas búsquedas de borde de aparatos electrónicos por mes. Y casi a medias de aquellos viajeros eran ciudadanos de EE.UU. .

Poco hecho sabido: Cualquiera's los aparatos electrónicos pueden ser buscados sin un warrant o sospecha razonable dentro cien millas de aire del



borde de EE.UU., el cual probablemente incluye San Diego. Sólo porque cruzaste el borde no necesariamente significa eres seguro!

Dos government las agencias son principalmente responsables para inspeccionar los viajeros y los elementos que introducen los Estados Unidos: el Departamento de Seguridad de Patria's Aduana y Protección de Borde (CBP) e Inmigración y Aplicación de Aduana (HIELO). En 2008, el Departamento de Seguridad de Patria anunció que podría buscar cualquier aparato electrónico que introduce los Estados Unidos.<sup>2</sup> Lo también presentó su propietario Automatizó Apuntar Sistema (ATS), el cual crea un instante dossier personal aproximadamente te—un muy detallado uno— siempre que te travel internacionalmente. CBP Los agentes utilizan vuestro ATS lima para decidir si serás subject a un realzado y a veces invasive búsqueda a reentering los Estados Unidos.

El gobierno de EE.UU. puede coger un aparato electrónico, búsqueda a través de todas las limas, y mantener él para escrutinio más lejano sin cualquier sugerencia de wrongdoing cualquier cosa. CBP Los agentes pueden buscar vuestro aparato, copia sus contenidos, y probar a undelete imágenes y vídeo.

Tan aquí es qué hago.

Para proteger mi intimidad y que de mis clientes, encripto el dato confidencial en mis portátiles. Cuándo yo'm en un país extranjero, transmito el encriptó limas sobre el Internet para almacenamiento en servidores seguros anywhere en el mundo. Entonces les seco físicamente del ordenador antes de que regreso en casa, por si acaso gobierno officials decide buscar o coger mi equipamiento.

Secando el dato no es igual tan eliminando dato. Eliminando el dato sólo cambia la bota maestra entrada récord para una lima (el índice utilizó para encontrar partes de la lima en el paseo duro); la lima (o algunos de sus partes) remains en el paseo duro hasta dato nuevo está escrito sobre aquella parte del paseo duro. Esto es qué digital forensics los expertos son capaces de reconstruir dato eliminado.

Secando, por otro lado, securely overwrites el dato en la lima con dato aleatorio. En sólido-state paseos, secando es muy difícil, así que llevo un portátil

que tiene un paseo duro estándar y toallita húmeda él con al menos treinta y cinco pases. Lima- shredding software esto por overwriting centenares de dato aleatorio de tiempo en cada pase sobre una lima eliminada, haciéndolo duro para cualquiera para recuperar aquel dato.

Utilicé para hacer una copia de seguridad de imagen llena de mi aparato a un paseo duro externo y encriptarlo. Entonces enviaría el paseo de copia de seguridad a los Estados Unidos. No secaría el dato en mi fin hasta el paseo era confirmed para ser recibido por un colega en afección legible. Entonces hube securely toallita húmeda todo personal y limas de cliente. Yo no formato el paseo entero, e I'd dejar el sistema operativo intacto. Aquella manera, si estuve buscado, sería más fácil de restaurar mis limas remotely sin teniendo que reinstall el sistema operativo entero.

Desde la experiencia en Atlanta, he cambiado mi protocolo un poco. He empezado para mantener un clon “actual” de todos mis ordenadores de viaje con un colega empresarial. Mi colega puede entonces sólo enviar el clonó sistemas a mí anywhere en los Estados Unidos, si necesitó.

Mi iPhone es otro asunto . Si nunca conectas vuestro iPhone a vuestro portátil para cobrar, y te el clic “Confía en” cuándo te asomas la Confianza “Esta cuestión” de Ordenador, un emparejamiento certificate está almacenado en el ordenador que deja el ordenador para acceder los contenidos enteros del iPhone sin necesitar para saber el passcode. El certificado de emparejamiento será utilizado siempre que el mismo iPhone está conectado a aquel ordenador.

Por ejemplo, si te tapón vuestro iPhone al ordenador de otra persona y confiarlo “en, una relación confiada en está creada entre el ordenador y el iOS aparato, el cual deja el ordenador para acceder fotos, vídeos, mensajes de SMS, registros de llamada, WhatsApp mensajes, y más todo else sin necesitar el passcode. Aún más concerniendo, aquella persona sólo puede hacer una copia de seguridad de iTunes de vuestro teléfono entero a no ser que tú anteriormente puesto una contraseña para copias de seguridad de iTunes encriptado (cuál es una idea buena ). Si te didn't conjunto que contraseña, un atacante podría poner uno para ti y sencillamente atrás arriba de vuestro aparato móvil a su o su ordenador sin vuestro conocimiento.

Aquello significa si aplicación de ley quiere ver qué's en vuestro passcode-iPhone protegido, pueden hacer tan fácilmente por conectarlo a vuestro portátil, desde entonces probablemente tiene un certificado de emparejamiento válido con aquel teléfono. La regla es: nunca “confiar en este ordenador” a no ser que él's vuestro sistema personal. Qué si quieres revocar los certificados de emparejamiento de vuestro aparato de Manzana entero? El bueno noticioso es que puedes reinicialización vuestro certificado de emparejamiento en vuestros aparatos de Manzana.<sup>3</sup> Si necesitas compartir limas, y estás utilizando un producto de Manzana, uso AirDrop. Y si

necesitas cobrar vuestro teléfono, uso el cable de relámpago plugged a vuestro sistema o un eléctrico

outlet, no a alguien más es computarr. O puedes comprar un preservativo de USB de syncstop.com, el cual te dejás a sin incidentes tapón a cualquier USB charger u ordenador.

Qué si sólo tienes vuestro iPhone y no vuestro ordenador cuándo viajando?

He habilitado Tacto ID en mi iPhone de modo que reconoce mi fingerprint. Qué I es reboot mi iPhone antes de acercarse control de inmigración en cualquier país. Y cuándo él poderés arriba, yo intencionadamente no pongo en mi passcode. Incluso aunque he habilitado Tacto ID, aquella característica es por default discapacitado hasta que yo primero pongo en mi passcode. Las cortes de EE.UU. son claras que aplicación de ley no puede reclamar vuestra contraseña. Tradicionalmente, en los Estados Unidos, no puedes ser obligado para dar testimonial evidencia; aun así, puedes ser obligado para girar sobre un tono físico a un seguro. Como tal, una corte te puede obligar para proporcionar vuestro fingerprints a unlock el aparato.<sup>4</sup> solución Sencilla: reboot vuestro teléfono. Aquella manera vuestro fingerprint no será habilitado y no tendrás que dar arriba de vuestro passcode.

En Canadá, aun así, es la ley ; tienes que, si eres un ciudadano canadiense , proporcionar vuestro passcode cuándo él's pidió. Esto pasó a Alain Philippon, de Sainte-Anne-des-Plaines, Quebec. Era en su casa de manera de Puerto Plata, en la República Dominicana, cuándo rechazó proporcionar los agentes de borde en Nova Scotia con su teléfono celular's passcode. Estuvo cobrado debajo sección 153.1(b) de la Ley de Aduana canadiense para obstaculizar o impidiendo agentes de borde de actuar su función. La pena si estás encontrado culpable es \$1,000, con una multa máxima de 25,000 \$y la posibilidad de un año en prisión.<sup>5</sup>

I sabe firsthand sobre la ley de contraseña canadiense. Contraté un servicio automovilístico como Uber para tomarme de Chicago a Toronto en 2015 (I didn't quere mosca en severo thunderstorms), y cuándo cruzamos el borde a Canadá de Michigan, éramos inmediatamente enviados a un sitio de inspección secundario. Quizás era porque un ingenio de tipo Oriental Medioh sólo una carta verde conducía. Apenas llegamos en el punto de inspección secundario, introdujimos una escena directamente fuera de CSI .

Un equipo de agentes de aduana hizo seguro dejamos el vehículo con todo nuestro interior de pertenencias, incluyendo nuestros teléfonos celulares. La motor y yo estuvieron separados. Uno de los agentes fue al lado de la motor

del automovilístico y sacó su teléfono celular de la cuna. El agente reclamó la motor passcode y empezó pasar por su teléfono.

Anteriormente había hecho arriba de mi mente nunca para dar fuera de mi contraseña. Sentía yo

tendría que escoger entre dar arriba de mi contraseña y siendo dejado para viajar a Canadá para mi actuación. Así que decidí utilizar un poco de ingeniería social.

Yo yelled encima al agente de aduana que busca el teléfono de la motor. “Hey—te aren't Yendo para buscar mi maleta, bien? Está cerrado tan puedes no.” Inmediatamente cogía su atención. Dijo que tuvieron cada derecho de buscar mi maleta.

Respondí, “ lo cerré, así que no puede ser buscado.”

Cosa próxima sé, dos agentes anduvieron encima a mí y reclamó el tono. Empecé pedir les por qué necesitaron buscar mi maleta, y explicaron otra vez que tuvieron el derechos de buscar todo. Estiré fuera de mi cartera und entregado el agente el clave a mi maleta.

Aquello era bastante. Completamente olvidaron los teléfonos celulares y concentrados en mi maleta en cambio. La misión cumplida a través de misdirection. Estuve dejado va y, afortunadamente, nunca fue pidió mi celda-contraseña de teléfono.

En la confusión de ser screened, es fácil de acaecer distraído. Don't dejado tú cae víctima a circunstancia. Cuándo pasando por cualquier punto de asistencia de seguridad, marca seguro vuestro portátil y los aparatos electrónicos son el último en la cinta de transportador. Te don't Querer vuestro portátil que sienta en el otro fin mientras alguien al frente de tú está aguantando arriba de la línea. También, si necesitas dar un paso fuera de la línea, marca seguro tienes vuestro portátil y aparato electrónico contigo.

Cualesquier protecciones de intimidad podemos gozar en en casa don't necesariamente aplicar a viajeros en el borde de EE.UU.. Para doctores, abogados, y muchos profesionales empresariales, un invasive búsqueda de borde puede compromise la intimidad de información profesional sensible. Esta información podría incluir secretos de comercio, cliente—de abogado y doctor—comunicaciones pacientes, y búsqueda y estrategias empresariales, algunos del cual un viajero tiene obligaciones legales y contractuales para proteger.

Para el resto de nosotros, búsquedas en nuestros paseos duros y los aparatos móviles podrían revelar email, información de salud, e incluso récords

financieros. Si tú've recientemente viajado a los países seguros consideraron unfriendly a intereses de EE.UU., ser conscientes que esto puede provocar escrutinio adicional de agentes de aduana.

Repressive Los gobiernos presentan otro reto. Pueden insistir encima mirando en vuestros aparatos electrónicos más exhaustivamente—leyendo vuestro email y comprobando vuestra carpeta de Descargas. hay también una posibilidad—especialmente si toman vuestro portátil de ti—que podrían intentar para instalar siguiendo software en vuestro aparato.

Muchos teléfonos de quemador de asunto de empresas y loaner portátiles cuándo los empleados viajan en el extranjero. Estos aparatos son tampoco echados fuera o secados limpios cuándo los regresos de empleado a los Estados Unidos. Pero para la mayoría de nosotros, cargando encriptó limas a la nube o comprando un aparato nuevo y colocando de él al regreso no es opciones prácticas.

En general, don't trae electrónica que tienda información sensible contigo a no ser que absolutamente necesitas a. Si tú , trae sólo el bare mínimo. Y si necesitas traer vuestro teléfono celular , piensa aproximadamente cogiendo un teléfono de quemador para la duración de vuestra visita. Especialmente desde entonces la voz y el dato que vagan las tasas son indignantes. Mejor de traer un unlocked teléfono de quemador y adquirir un SIM carta en el país estás visitando.

Podrías creer que entrar y fuera de la aduana es el más nightmarish parte de cualquier viaje. Pero no podría ser. Vuestra habitación de hotel también puede ser buscada.

Hice varios viajes a Colombia en 2008—no sólo el cuando estuve parado en Atlanta. Encima uno de los viajes hice más tarde taño de sombrero, algo extraño pasado en mi habitación de hotel del Bogotá. Y esto no fue un hotel cuestionable; era uno de los hoteles donde los oficiales colombianos frecuentemente se quedaron.

Quizás aquello era el problema .

Había salido a cena con mi novia, y cuándo volvimos, mi cerradura de puerta mostró amarilla cuándo inserté mi tono de sala. No verde. No rojo. Pero amarillo, el cual típicamente significa la puerta está cerrada del interior.

Bajé delante escritorio y tuvo el empleado me emito una carta clave nueva. Otra vez, la cerradura displayed una luz amarilla. Yo esto otra vez. Resultado mismo. Después del tercer tiempo, persuadí el hotel para enviar alguien arriba conmigo. La puerta abrió.

Interior, nada miraba inmediatamente mal. De hecho en el tiempo, yo chalked la cosa entera hasta la cerradura que es crappy. Lo wasn't Hasta que regresé a los Estados Unidos que me di cuenta qué había pasado.

Antes de dejar los Estados Unidos, había llamado una novia anterior, Darci Madera, quién utilizó para ser el técnico de ventaja en TechTV, y le pidió para venir encima a mi sitio e intercambio fuera del paseo duro en mi MacBook Pro portátil. En el tiempo, MacBook Pro los paseos duros no fueron fáciles de sacar. Ella él, aun así. En su sitio puso una marca-paseo nuevo que tuve que formato e instalar el OSX sistema operativo encima.

Varias semanas más tarde, cuándo regresé de aquel viaje a Colombia, pedí Darci para venir encima a mi sitio en Las Vega a intercambio reculan los paseos.

Inmediatamente notó algo era diferente. Dijo que alguien había

apretado los tornillos de paseo duro mucho más que tuvo. Claro que alguien en Bogotá había sacado el paseo, quizás para hacer una copia de imagen de él cuándo dejé mi sala.

Esto pasó más recientemente a Stefan Esser, un investigador sabido para jailbreaking iOS productos. Él tweeted un cuadro de su paseo duro mal remontado.

Incluso un paseo con dato muy pequeño tiene *algún* dato encima lo.

Afortunadamente, utilicé Symantec's PGP Encriptación de Disco Entero para encriptar los contenidos enteros de mi paseo duro. (También podrías utilizar WinMagic para Ventanas o FileVault 2 para OSX; ve [aquí](#).) Así que el clon de mi paseo duro sería worthless a no ser que el ladrón podría obtener el clave a unlock lo. Es debido a qué I piensa pasado en Bogotá que ahora traigo mi portátil conmigo cuándo viajo, incluso cuándo yo'm saliendo a cena. Si tengo que dejar mi portátil detrás, entonces nunca dejo él en hibernate modo. Bastante, I poder él abajo. Si yo no, un atacante posiblemente podría verter la memoria y obtener mi PGP tonos de encriptación de Disco Enteros.<sup>6</sup> Así que lo giro completamente fuera.

A principios del libro hablé sobre el muchos precautions que Edward Snowden tomó para mantener su comunicación con Laura Poitras privado.

Una vez Snowden secreto cache de los datos estuvo a punto para ser liberados al público, aun así, él y Poitras necesitado un sitio para almacenarlo. Los sistemas operativos más comunes —Ventanas, iOS, Androide, e incluso Linux—contiene vulnerabilidades. Todo software hace. Así que necesitaron un sistema operativo seguro, uno aquello está encriptado de día un y requiere un clave a unlock lo.

Obras de encriptación de disco duro así: cuándo chutas arriba de vuestro ordenador, introduces una contraseña segura o, bastante, un passphrase como “Nosotros don't necesidad ninguna educación” (del famoso Rosa Floyd canción). Entonces las botas de sistema operativo arriba, y puedes acceder vuestras limas y actuar vuestras tareas sin notar cualquier retraso de tiempo, porque una motor actúa las tareas de encriptación limpiamente y en la mosca. Esto , aun así, crear la posibilidad que si te levantas y dejar vuestro aparato, incluso para un momento, alguien podría acceder vuestras limas (desde entonces son unlocked). La cosa importante a remel rescoldo es que mientras vuestro paseo duro encriptado es unlocked, necesitas tomar precauciones para mantenerlo seguras. Apenas cerraste abajo, el tono de encriptación es ya no disponible al sistema operativo: aquello es, sólo saca el tono de memoria así que el datun en el paseo es ya no accesible.<sup>7</sup>

Colas es un sistema operativo que puede ser chutado arriba en cualquier ordenador de día

moderno para evitar dejando cualquier forensically dato recuperable en el paseo duro, preferentemente uno aquello puede ser escribir-protegíó.<sup>8</sup> Colas de Descarga a un DVD o un

palo de USB, entonces puesto vuestro BIOS firmware o EFI (OSX) secuencia de bota inicial para cualquier DVD o USB para chutar la distribución de Colas. Cuándo chutas, empezará arriba del sistema operativo, el cual consta varias herramientas de intimidad, incluyendo el Tor navegador. Las herramientas de intimidad te dejan para encriptar el email que utiliza PGP, encriptar vuestro USB y paseos duros, y asegurar vuestros mensajes con OTR (fuera-el- récord messaging).

Si quieres encriptar limas individuales en vez de vuestro paseo duro entero, hay varias elecciones. Uno opción libre, TrueCrypt, todavía existe pero es ya no mantenido y doesn't oferta encriptación de disco lleno. Porque es ya no vulnerabilidades mantenidas , nuevas no será dirigido. Si continúas utilizar TrueCrypt, ser consciente de los riesgos. Un replacement para TrueCrypt 7.1un es VeraCrypt, el cual es una continuación del TrueCrypt proyecto.

Hay varios programas para venta, también. Uno obvio uno es Ventanas BitLocker, el cual es generalmente no incluido en las ediciones de casa del sistema operativo de Ventanas. Para habilitar BitLocker, si Lima instalada , abierta Explorador, bien-clic en el C paseo, y desplazar hacia abajo al “Turno en BitLocker” opción. BitLocker Aprovecha un chip especial en vuestro motherboard sabido como módulo de programa confiada en, o TPM. Está diseñado a unlock vuestro tono de encriptación sólo después de confirmar



que vuestro bootloader programa hasn't sido modificado. Esto es un defensa perfecto en contra ataques de sirvienta del mal, el cual describiré dentro de poco. Puedes poner BitLocker a unlock cuándo te poder arriba o sólo cuándo allí's un ALFILER o un USB especial que proporcionas. Las elecciones últimas son mucho más seguros. También tienes la opción de salvar el clave a vuestra cuenta de Microsoft. Don't que, porque si tú más o menos has dado Microsoft vuestros tonos (cuál, como verás, ya podría tener).

Hay varios asuntos con BitLocker. Primero, utiliza un pseudorandom generador de número (PRNG) llamó Dual\_EC\_DRBG, corto para dual elliptic curva generador de bit aleatorio determinista, el cual podría contener un NSA puerta posterior.<sup>9</sup> es también en privado poseído, significado que te sólo tiene que tomar la palabra de Microsoft que obra y que no tiene cualesquier puertas posteriores para el NSA—cuáles no pueden ser el caso con software de fuente abierta. Otro problema con BitLocker es que tienes que compartir el tono con Microsoft a no ser que adquieres él para \$250. No haciendo así que puede dejar aplicación de ley para pedir el tono de Microsoft.

A pesar de estas reservas, el EFF de hecho recomienda BitLocker para el consumidor mediano que mira para proteger suyo o sus limas.<sup>10</sup> Aun así, ser consciente hay una manera a bypass BitLocker también.<sup>11</sup>

Otra opción comercial es PGP Encriptación de Disco Entero from Symantec. Las universidades muchísimas utilizan esto, como muchas empresas. Lo he utilizado antiguamente también. PGP Encriptación de Disco entero estuvo creada por Phil Zimmermann, el hombre quién creó PGP para email. Como BitLocker, PGP puede apoyar el TPM chip para proporcionar autenticación adicional cuándo giras en vuestro PC. Una licencia perpetua vende para alrededor \$200.

hay también WinMagic, uno de las pocas opciones que requiere autenticación de dos factores en vez de justo una contraseña. WinMagic También doesn't confiar en una contraseña maestra. Bastante, encriptó las limas están agrupadas, y cada grupo tiene una contraseña. Esto puede hacer recuperación de contraseña más dura, así que no puede ser propio para todo el mundo.

Y para la manzana allí ha FileVault 2. Después de que instalación, puedes habilitar FileVault 2 por Preferencias de Sistema inaugural, clicking en el “icono & de Intimidación” de la Seguridad, y cambiando al FileVault tabulador. Otra vez, no salva vuestro tono de encriptación a vuestra cuenta de Manzana. Esto puede dar acceso de Manzana a él, el cual ellos en turno podrían dar a

aplicación de ley. En cambio escoger “Create un tono de recuperación y no utiliza mi iCloud cuenta,” entonces imprime fuera o escribir abajo el tono de veinticuatro caracteres. Proteger este tono, como cualquiera quién lo encuentra podría unlock vuestro paseo duro.

Si has iOS 8 o una versión más reciente del sistema operativo en your iPhone o iPad, sus contenidos son automáticamente encriptó. Yendo un paso más allá, la manzana ha dicho que los restos claves en el aparato, con el usuario. Aquello significa que el gobierno de EE.UU. no puede pedir Manzana para el tono: él's único a cada cual y cada aparato. Director de FBI James Comey reclamaciones que unbreakable la encriptación finalmente no es una cosa buena. En una habla dijo, “los delincuentes Sofisticados vendrán para contar en este medio de evadir detección. Y mi cuestión es, en qué coste?”<sup>12</sup> El miedo es que las cosas malas serán mantenidas bajo la portada de encriptación.

El mismo miedo retrasó mi caso para meses como yo languished en prisión atrás en el 1990s. Mi equipo de defensa legal acceso querido al descubrimiento que el gobierno planeado para utilizar en contra me en mi prueba. El gobierno refusionado para girar sobre cualquier encriptó limas a no ser que proporcioné el decryption tono. Rechacé.<sup>13</sup> La corte, en turno, rechazado para ordenar el gobierno para proporcionar el descubrimiento porque no les daría el tono.<sup>14</sup>

aparatos de Android, empezando con versión 3.0 (Honeycomb), también puede ser encriptado. La mayoría de nosotros escoge no para hacer tan. Comienzo con Android 5.0 (Piruleta), encriptó los paseos son el default en el Nexus línea de teléfonos de Androide pero opcionales en teléfonos de otros fabricantes, como LG, Samsung, y otros. Yof escoges encriptar vuestro teléfono de Androide, nota que lo podría tomar hasta una hora para hacer tan y que vuestro aparato tendría que ser plugged en durante el proceso. Según se dice, encriptando vuestro aparato móvil no significativamente obstaculiza actuación, pero una vez tú've hecho la decisión para encriptar, no lo puedes deshacer.

En cualquier de estos programas de encriptación de disco entero, allí siempre queda la posibilidad de una puerta posterior. Era una vez contratado por una empresa para probar un producto de USB que dejó usuarios para almacenar limas en un encriptados container. Durante análisis del código, encontramos que el desarrollador había puesto en una puerta posterior secreta—el clave a unlock el envase encriptado estuvo enterrado en una ubicación aleatoria en el

paseo de USB. Aquello significó que cualquiera con conocimiento de la ubicación del tono podría unlock el dato encriptado por el usuario.

Peor, empresas don't siempre saber qué para hacer con esta información. Cuando completé mi análisis de seguridad del aparato de USB encriptado, el CEO me llamó y pedido si tendría que dejar la puerta posterior en o no. Él wtan preocupado que aplicación de ley o el NSA puede necesitar acceder el dato de un usuario. El hecho que necesitó pedir dice mucho.

En su 2014 wiretap informe, el gobierno de EE.UU. informó encontrar encriptó paseos en únicos veinticinco fuera de los 3,554 aparatos that aplicación de ley había buscado evidencia.<sup>15</sup> Y eran todavía capaces a decrypt los paseos encima veintiún del veinticinco. Tan mientras habiendo la encriptación a menudo es bien bastante para mantener un ladrón común de acceder vuestro dato, para un gobierno dedicado, no podría posar mucho de un reto.

Hace años investigador Joanna Rutkowska escribió sobre qué llamó un ataque de sirvienta del mal.<sup>16</sup> Dice alguien deja un powered-abajo portátil cuyo paseo duro está

encriptado con cualquier TrueCrypt o PGP Encriptación de Disco Entero en un hotel sala. (I había utilizado PGP Encriptación de Disco Entero en Bogotá; hube también powered abajo el portátil.) Más tarde, alguien introduce la sala e inserta un palo de USB que contiene un malicious bootloader. El portátil de objetivo entonces tiene que ser chutado del USB para instalar el malicious bootloader aquello roba el usuario passphrase. Ahora la trampa está puesta.

Una sirvienta, alguien quiénes pueden frecuentes una habitación de hotel sin demasiada

sospecha, sería el candidato mejor para hacer este—de ahí el nombre del ataque. Una sirvienta puede reenter casi cualquier hotel room al día siguiente y tipo en una combinación clave secreta que extractos el passphrase aquello era en secreto almacenado en el disco. Ahora el atacante puede introducir el passphrase y obtener acceso a todas vuestras limas.

No sé si alguien esto en mi portátil en Bogota. El paseo duro él había sido sacado y entonces reemplazado con los tornillos giraron demasiado estrechamente. Cualquier manera, afortunadamente, el paseo contuvo no información real.

Qué aproximadamente poniendo vuestra electrónica en un hotel seguro? Es mejor que dejándoles fuera o manteniéndoles en maletas? Sí, pero no mucho

mejor. Cuando atendiendo un Sombrero Negro reciente, me quedé en las Cuatro Estaciones en Las Vega. Coloqué \$4,000 dinero efectivo en el seguro con varias cartas de crédito y controles. Unos cuantos días más tarde, fui y probado para abrir el seguro but el código falló. Llamé la seguridad y ellos lo abrieron arriba. Inmediatamente noté que la pila de 100 \$facturas era mucho menos grueso. había \$2,000 dejó. Así que dónde hizo el otros \$2,000 van? Seguridad de hotel No tuvo ninguna idea. Un amigo del mío quién especializa en physical testaje de bolígrafo probó cortar el seguro pero no lo podría explotar. Hoy, es todavía un misterio. Irónicamente, el seguro se apellidó un Sitio Seguro.

Un alemán antivirus empresa, DATO de G, encontrado que en habitaciones de hotel donde su personal de búsqueda se quedó, “más a menudo que no” el seguro tuvo el default contraseña (0000) en sitio. En a casos les gusta que, ningún asunto lo que contraseña privada seleccionas, cualquiera sabiendo el default la contraseña podría también acceso de beneficio a vuestro valubles interior. DATO de G dijo que esta información no fue discovered sistemáticamente pero anecdotally sobre varios años.<sup>17</sup>

Si un atacante doesn't saber el default contraseña para un hotel dado-la sala segura, otra opción para él es a literalmente brute-forzar la cerradura. A pesar de que la gerente de hotel está confiada con una emergencia aparato electrónico que taponas al puerto de USB y unlocks el seguro, un savvy el ladrón sencillamente puede desenroscar el plato en el frente del seguro y utilizar un aparato digital para abrir la cerradura debajo. O puede corto-circuito el seguro e iniciar una reinicialización, entonces enter un código nuevo.

Si aquello no te molesta, considera esto. DATO de G también encontrado que los lectores de carta del crédito encima sala safes—a menudo el medio por qué pagas para su uso— puede ser leído por una tercera fiesta quién podría skim el dato de carta del crédito y entonces uso o vender aquella información en el Internet.

Hoy los hoteles utilizan NFC o incluso cartas de golpe de tira magnética para cerrar y unlock vuestra sala. La ventaja es que el hotel puede cambiar estos códigos de acceso deprisa y fácilmente del escritorio de frente. Si pierdes vuestra carta, puedes pedir un

nuevo un. Un código sencillo está enviado a la cerradura, y por el tiempo coges a vuestra sala, las obras de carta claves nuevas. Samy Kamkar's MagSpoof La herramienta puede soler spoof las secuencias correctas y abrir una cerradura de habitación del hotel que usos cartas de tira magnética. Esta

herramienta estuvo utilizada en un episodio del Robot de Señor *de espectáculo de televisión*.

La presencia de una tira magnética o un NFC el chip ha dado aumento a la idea que la información personal podría ser almacenada en el hotel carta clave. No es. Pero la leyenda urbana continúa. Allí ha incluso una historia famosa que originado en Condado de San Diego. Presuntamente el diputado de un sheriff allí emitió un advirtiéndolo que un huésped de hotel's nombre, domicilio particular, e información de carta del crédito había sido encontrada en un hotel carta clave. Quizás has visto el email. Mira algo así:

aplicación de ley de California Del sur los profesionales asignaron para detectar amenazas nuevas a asuntos de seguridad personal recientemente descubrieron qué tipo de información es embedded en el hotel de tipo—de carta de crédito tonos de habitación utilizaron durante la industria.

A pesar de que la sala claves diferir de hotel a hotel, un clave obtenido del DoubleTree cadena que era utilizado para una presentación de robo de identidad regional estuvo encontrada para contener la información siguiente:  
el cliente de nombre del cliente habitación de Hotel de domicilio particular  
parcial Control de número-en cita y checkout el número de carta del crédito  
de Cliente de cita y cita de expiración!

Cuándo les giras en delante escritorio, vuestra información personal es allí para cualquier empleado para acceder por sencillamente escaneando la carta en el escáner de hotel. Un empleado puede tomar un handful de casa de cartas y, utilizando un aparato de barrido, acceso la información a un ordenador de portátil e ir de compras en vuestro gasto.

Sencillamente puesto, los hoteles no borran estas cartas hasta una empleada emite la carta al huésped de hotel próximo. Es normalmente mantenido en un cajón delante escritorio con VUESTRA INFORMACIÓN ENCIMA LO!!!!

La línea inferior es, mantener las cartas o destruirles! NUNCA dejarles detrás y NUNCA girarles en delante escritorio cuándo compruebas fuera de una sala. No cobrarán tú para la carta.<sup>18</sup>

El truthfulness de este email ha sido ampliamente discutido.<sup>19</sup> Francamente, suena como bullshit a mí.

La información listó ciertamente podría ser almacenado en una carta clave, pero aquello parece extremo, incluso a mí. Los hoteles utilizan qué puede ser considerado un token, un placeholder número, para cada huésped. Sólo con

acceder al atrás-ordenadores de fin que hacer el enunciando puede el token ser conectado con información personal.

No pienso necesitas recoger y destruir vuestras cartas claves viejas, pero hey— te podría querer hacer tan todo igual.

Otra cuestión común que viaje de preocupaciones y vuestro dato: Qué es en el código de barras en el fondo de vuestra entrada de plano? Qué, si cualquier cosa, poder revela? En verdad, relativamente poca información personal, a no ser que tienes un número de aviador frecuente.

Empezando en 2005, la Asociación de Transporte de Aire Internacional (IATA) decidió utilizar barra-coded entablado passes para la razón sencilla que pases de abordaje magnético eran mucho más caros de mantener. Los ahorros han sido estimados en \$1.5 mil millones. Además, utilizando códigos de barras encima entradas de aerolínea deja pasajeros para descargar sus entradas del Internet e imprimirles en en casa, o pueden utilizar un teléfono celular en la puerta en cambio.

Needless Para decir, este cambio en procedimiento requirió alguna clase de estándar. Según investigador Shaun Ewing, el abordaje típico-código de barras de pase contiene información que es mayoritariamente harmless— nombre de pasajero, nombre de aerolínea, número de escaño, aeropuerto de salida, aeropuerto de llegada, y número de vuelo.<sup>20</sup> Aun así, la mayoría de parte sensible del código de barras es vuestro número de aviador frecuente.<sup>21</sup> Todos sitios web de aerolínea ahora protegen sus cuentas de cliente con contraseñas personales. Dando fuera de vuestro número de aviador frecuente no es gustar dando fuera de vuestro número de Seguridad Social, pero todavía es una preocupación de intimidad.

Una preocupación de intimidad más grande es las cartas de lealtad ofreció en supermercados, farmacias, canal gasistas, y otro businesses. Entradas de aerolínea diferente, los cuales tienen que ser en vuestro nombre legal, cartas de lealtad pueden ser registradas bajo un nombre de falsificación, alocución, y número de teléfono (una falsificación te numeras puede recordar), así que vuestros hábitos de adquirir no pueden ser enlazados atrás a ti.

Cuándo compruebas a vuestro hotel y bota arriba de vuestro ordenador, podrías ver una lista de redes de Wi-Fi disponible, como “Huésped de Hotel,” “tmobile123,”

“iPhone de Kimberley,” “attwifi,” “el androide de Steve,” y Echar “es Hotspot.” Cuál tiene que conectas a? Espero que sabes la respuesta por ahora!



La mayoría de Wi-Fi de hotel no utiliza encriptación pero requiere el huésped's último nombre y número de sala como autenticación. Hay trucos para coger alrededor de paywalls, naturalmente.

Uno burla para coger el internet libre en cualquier hotel es para llamar cualquiera otra sala— quizás el a través de la sala que—posa tan servicio de sala. Si la visita de usos del hotel ID, sólo utilizar el teléfono de casa en el lobby. Decir la fiesta que contesta el teléfono que su dos burgers es en el camino. Cuando el huésped dice no colocó un orden, tú politely pedir su apellido para fijar el error. Ahora tienes ambos el número de sala ( llamaste él) y el apellido, el cual es todo aquello está necesitado para autenticarte (un nonpaying huésped) como huésped legítimo en aquel hotel.

Dejado es dice estás quedándote en un cinco-protagonizar hotel con acceso de Internet, libre u otherwise. Como te registro encima, quizás ves un mensaje que te informa que Adobe (o algunos otro fabricante de software) tiene una actualización disponible. Siendo un ciudadano bueno del Internet, podrías ser tentado para descargar la actualización y move encima. Excepto la red de hotel todavía tendría que ser considerada hostil—incluso si tiene una contraseña. No es vuestra red de casa—así que la actualización no podría ser real, y si vas adelante y descargarlo puedes inadvertently instala malicious código en vuestro PC.

Si te unres en la carretera mucho, como soy, si para actualizar o no es una llamada dura. hay poco puedes hacer exceptúa verifica que hay una actualización disponible. El problema es, si utilizas el hotel's Internet para descargar aquella actualización, podrías ser dirigido a un spoofed el sitio web que proporciona el malicious “actualización.” Si puedes, uso vuestro aparato móvil para confirmar la existencia de la actualización del sitio del vendedor y, si él's no crítico, espera hasta que eres atrás en un entorno seguro, como una oficina corporativa o casa posterior, para descargarlo.<sup>22</sup>

Investigadores en Kaspersky Laboratorio, una empresa de seguridad del software, descubrió un grupo de criminal hackers llaman DarkHotel (también sabidos como Tapaoux) quiénes utilizan esta técnica. Operan por identificar ejecutivos empresariales quién podría ser quedarse en un hotel de lujo particular, entonces anticipar su llegada por colocar malware en el servidor de hotel. Cuando el control de ejecutivos en y conectar al Wi-Fi de hotel, el malware está descargado y ejecutado en sus aparatos. Después de la infección es completa, el malwares está sacado del servidor de hotel.

Aparentemente esto ha sido yendo en para casi una década, los investigadores notaron.



A pesar de que principalmente afecta ejecutivos quedando prpers en hoteles de lujo en Asia,

podría ser común en otro lugar. El DarkHotel el grupo en general utiliza una lanza de nivel bajo-phishing ataque para objetivos de masa y reserva los ataques de hotel para altos- perfil, objetivos singulares—como ejecutivos en la energía nuclear e industrias de defensa.

Uno el análisis temprano sugirió que DarkHotel era Corea del Sur—basó. Un keylogger—malware utilizado para grabar el keystrokes de compromised los sistemas —utilizaron en los ataques contiene caracteres coreanos dentro del código. Y las vulnerabilidades de cero—días en software que es desconocido al vendedor—era defectos muy adelantados que era anteriormente desconocido. Además, un nombre coreano Del sur identificado dentro del keylogger ha sido localizado a otro sofisticado keyloggers utilizado por coreanos antiguamente.

Tendría que ser notado, aun así, que esto no es bastante para confirmar atribución. El software puede ser cortado y pasted de una variedad de fuentes. También, el software puede ser hecho para mirar como si está creado en un país cuándo es de hecho creado en otro.

Para coger el malware en los portátiles, DarkHotel los usos forjaron certificados que parecer como si están emitidos from el gobierno malasio y Deutsche Telekom. Certificados, si recuerdas de capítulo 5, suele verificar el origen del software o el servidor de Web. A más allá esconder su obra, el hackers lo arregló de modo que el malware estancias dormant para arriba de to seis meses antes de acaecer activo. Esto es para echar fuera EL departamentos que podría enlazar una visita con una infección.

Kaspersky Sólo aprendido de este ataque cuándo un grupo de sus clientes acaeció infectado después de quedarse en hoteles de lujo seguro en Asia. El researchers girado a un tercer-Wi-Fi de fiesta anfitrión común a ambos, y el Wi-Fi anfitrión partnered con el antivirus empresa para descubrir qué pasaba en sus redes. A pesar de que las limas utilizaron para infectar los huéspedes eran mucho tiempo idos, lima deletion los records eran left detrás de aquel correspondidos a las citas de los huéspedes' estancias.

La manera más fácil de proteger tú contra esta clase de ataque es para conectar a un VPN servicio apenas conectas al Internet en el hotel. El I uso es barato—único seis dólares por mes. Aun así, aquello's no una elección buena si quieres ser invisible, desde entonces no dejará anónimo setup.

Si quieres ser invisible, don't confianza el VPN proveedor con vuestra información real. Esto requiere poner arriba de una alocución de email de la

falsificación por adelantado (ve [aquí](#)) y utilizando una red inalámbrica abierta. Una vez tienes que alocución de email de la falsificación, uso Tor para poner arriba de un Bitcoin cartera, encontrar un Bitcoin ATM para financiar la cartera, y entonces utilizar un tumbler a esencialmente lavar el Bitcoin así que no puede ser

Localizado atrás a ti encima el blockchain. Esto lavando el proceso requiere poner arriba dos Bitcoin las carteras que utilizan diferentes Tor circuitos. La primera cartera suele send el Bitcoin al servicio de lavar, y el segundo está puesto hasta recibir el lavado Bitcoin.

Una vez te ha conseguido anonimato cierto por utilizar Wi-Fi abierto fuera de vista de cámara más Tor, encontrar un VPN servicio que acepta Bitcoin para pago. Paga con el laundered Bitcoin. Algunos VPN proveedores, incluyendo WiTopia, bloque Tor, así que necesitas encontrar uno aquello no—preferentemente con un VPN proveedor que no conexiones de registro.

En este caso, no estamos “confiando en” el VPN proveedor con nuestra alocución de IP real o nombre. Aun así, cuándo utilizando el nuevamente puesto-arriba de VPN, tienes que ser prudente no para utilizar cualquiera de los servicios conectó a vuestro nombre real y no para conectar al VPN de una alocución de IP que puede ser ligado atrás a ti. Podrías considerar tethering a un quemador anónimamente adquirido teléfono, ve [aquí](#).

Es más para adquirir un portátil hotspot—adquirido de tal manera que lo sería muy difícil de identificarte. Por ejemplo, puedes contratar alguien para adquirir él para ti tan vuestra cara no parece en un cámara de vigilancia en una tienda. Cuándo tú're utilizando el anónimo hotspot, tendrías que girar de cualquier de vuestros aparatos personales que uso señales celulares para impedir el patrón de vuestros aparatos personales que registran en el mismo sitio como el aparato anónimo.

A summarize, aquí es qué necesitas hacer para utilizar el Internet en privado mientras viajando:

1. Compra prepaid cartas de regalo anónimamente (ve [aquí](#)). En la UE, puedes adquirir prepaid cartas de crédito anónimamente en viabuy.com.
2. Uso Wi-Fi abierto después de cambiar vuestro MAC alocución (ve [aquí](#)).
3. Encontrar un proveedor de email que te dejas para firmar arriba sin validación de SMS. O puedes firmar arriba para un Skype-en numera utilizar Tor y un prepaid carta de regalo. Con Skype-en, puedes recibir voz calls para verificar vuestra identidad. Marca seguro eres fuera de vista de cámara

(i.e., no en un Starbucks o anywhere más con vigilancia de cámara). Uso Tor para enmascarar

vuestra ubicación cuándo firmas arriba para este servicio de email. 4.

Utilizando vuestra alocución de email anónima nueva, signo arriba en un sitio como paxful.com, otra vez utilizando Tor, para firmar arriba para un Bitcoin cartera y comprar un

suministro de Bitcoin. Paga para ellos utilizando el prepaid cartas de regalo.

5. Puesto arriba de un segundo email anónimo alocución y nuevo secundario Bitcoin cartera después de cerrar y establishing un nuevo Tor circuito para impedir cualquier asociación con la primera cuenta de email y cartera.

6. 6. Uso un Bitcoin lavando servicio como bitlaunder.com para hacerlo duro de localizar el origen de la moneda. Tiene el lavado Bitcoin enviado al segundo Bitcoin alocución.<sup>23</sup>

7. 7. Signo arriba para un VPN el servicio que utiliza el lavado Bitcoin aquello no tráfico de registro o conexiones de IP. Normalmente puedes descubrir qué es logged por revisar el VPN la política de privacidad del proveedor (p. ej., TorGuard).

8. Tiene un cutout obtener un quemador portátil hotspot aparato en vuestro behalf. Dar el cutout dinero efectivo para adquirirlo.

9. Para acceder el Internet, uso el quemador hotspot aparato fuera de en casa, obra, y vuestros otros aparatos celulares.

10. Una vez powered arriba, conecta a VPN a través del quemador hotspot aparato. 11. Uso Tor para explorar el Internet.

## CAPÍTULO QUINCE

### El FBI Siempre Coge Su Hombre

En la sección de ficción de la ciencia de la rama de Parque del Glen del San Francisco Biblioteca Pública, no lejos de su apartamento, Ross William Ulbricht

estuvo comprometido en un cliente on-line-chat de apoyo para la empresa poseyó. En el octubre—de tiempo de 2013—la persona en el otro fin del chat de Internet pensó hablaba al sitio admin, quién pasó de largo el nombre de Internet de Temer Roberts Pirata, un nombre tomado de la película *La Novia de Princesa*. Roberts, también sabido como DPR, era de hecho Ross Ulbricht—no sólo el admin pero también el dueño de Carretera de Seda, una

droga on-line emporium, y como tal era el tema de un federal manhunt.<sup>1</sup> Ulbricht frecuentemente ubicaciones de Wi-Fi públicas utilizadas como el library para su obra, quizás bajo la impresión equivocada que el FBI, tener que nunca le identifica tan DPR, nunca dirigiría una redada en un sitio público. En aquel día, aun así, la persona con quien Ulbricht charlaba pasado para ser un undercover agente de FBI.

Corriendo una droga on-line emporium, en qué clientes podrían ordenar cocaína y heroin y una gama ancha de drogas de diseñador anónimamente, requirió un seguro moxie. El sitio era hosted en la Web Oscura (ve [aquí](#)) y era sólo accesible a través de Tor. El sitio sólo tomó Bitcoin tan pago. Y el creador de Carretera de Seda había sido prudente, pero no bastante prudente.

Unos cuantos meses antes de Ulbricht sentados en el San Francisco Biblioteca Pública con el FBI circling le, un héroe improbable conectado con el federal manhunt vino adelante con la evidencia que liga Ulbricht a DPR. El héroe, un IRS agente

Gary nombrado Alford, había sido leyendo arriba encima Carretera de Seda y sus orígenes, y en las tardes había sido running búsquedas de Google adelantado para ver qué podría encontrar. Uno del más temprano menciona de Carretera de Seda encontró era de 2011. Alguien quién pasó de largo el nombre “altoid” había sido hablándolo arriba en un grupo de chat. Desde entonces Carretera de Seda no había lanzado todavía, Alford imaginado que altoid más interior tenido probablemente conocimiento de la operación. Naturalmente Alford empezado un buscar otras remisiones.

Atacó oro.

Aparentemente altoid hubo posted una cuestión a otro grupo de chat—pero había eliminado el mensaje original. Alford Estirado arriba de una respuesta a la consulta ahora eliminada que contuvo el mensaje original. En aquel mensaje, altoid dicho que si cualquiera podría contestar su cuestión, aquella persona le podría contactar en rossulbricht@gmail.com.<sup>2</sup>

no fue la última vez que slipup sería hecho. Elre era otro posted cuestiones, uno a un sitio llamó Stack Desbordamiento: la cuestión original había sido enviada de rossulbricht@gmail.com, pero entonces, extraordinariamente, el sender el nombre había sido cambiado a DPR.

Número de regla 1 aproximadamente siendo invisible: puedes no nunca enlazar vuestro anónimo on-line persona con vuestro real-mundial persona. Sólo puedes't.

Había otras conexiones estableció después de que aquello. Ulbricht, como DPR, espoused Ron Paul—lonja libre—filosofías libertarias. Y en uno señala Ulbricht hubo incluso ordenó un conjunto de falso IDs—las licencias de la motor en nombres diferentes de varios declara—cuál dibujó potestades federales a su doorstep en San Francisco en julio de 2013, pero en aquel tiempo las potestades no tuvieron ninguna idea hablaban con DPR.

Despacio la evidencia creció tan obligando que una mañana en octubre de 2013, apenas DPR's cliente-chat de apoyo empezó, los agentes federales empezaron tranquilamente introduciendo la biblioteca de Parque del Glen. Entonces, en una huelga quirúrgica, cogieron Ulbricht antes de que podría cerrar abajo su portátil. Tuvo cerró él wn, la evidencia clave segura habría sido destruida. Como era, eran capaces de fotografiar las pantallas de administración del sistema para un sitio momentos de Carretera de Seda llamados después del arresto y así establecer un enlace concreto entre Ulbricht, Pirata de Pavor Roberts, y Carretera de Seda, por ello acabando cualquier esperanza futura de anonimato.

En aquella mañana de octubre en Glen Parque, Ulbricht era logged en a Carretera de Seda como un administrador. Y el FBI supo que porque habían sido observando su máquina logging encima al Internet. Pero qué si podría haber fingido su ubicación? Qué si él wasn't en la biblioteca en absoluto pero utilizando un proxy servidor

en cambio?

En el verano de 2015, investigador Ben Caudill de Seguridad de Rinoceronte anunció aquello no sólo estar hablando en DEF CON 23 sobre su nuevo device, ProxyHam, también sería vendiendo él en costado—alrededor \$200—en el DEF CON vendedores' sala. Entonces, aproximadamente una semana más tarde, Caudill anunciado que su charla estuvo anulada y que todo existiendo ProxyHam las unidades serían destruidas. Ofreció no explicación más lejana.<sup>3</sup>

Charlas en conferencias de seguridad importante cogen estiradas para varias razones. Cualquiera las empresas cuyos productos están siendo discutidos o el gobierno federal pone presión en investigadores a no ir público. En este caso, Caudill no señalaba fuera de un particular defecto; había construido algo nuevo.

Cosa graciosa sobre el Internet: una vez una idea es allí, tiende para quedar allí. Tan incluso si el feds o alguien más convenció Caudill que su charla no fue en los intereses de seguridad nacional, parecía probablemente que alguien más crearía un aparato nuevo. Y aquello es exactamente qué pasó.

ProxyHam Es un acceso muy remoto punto. Utilizando es mucho gusta poner un Wi-Fi transmisor en vuestra casa u oficina. Exceptúa que la persona que utiliza y controlando ProxyHam podría ser hasta una milla fuera. El transmisor de Wi-Fi utiliza un 900 MHz radio para conectar a una antena dongle en un ordenador según lo que 2.5 millas fuera. Tan en el caso de Ross Ulbricht, el FBI podría haber estado amasando fuera de la biblioteca de Parque del Glen mientras era en alguien es sótano haciendo ropa sucia muchos bloquea fuera.

La necesidad para tales aparatos es clara si vives en un oppressed country. Contactando el mundo exterior a través de Tor es un riesgo muchos toman. Esta clase de aparato añadiría otra capa de seguridad por enmascarar la geolocalización del requester.

Exceptúa alguien no quiso Caudill para hablar aproximadamente él en DEF CON.

En entrevistas Caudill negados que la Comisión de Comunicaciones Federal había desalentado le. *Alambró* speculated que en secreto plantando un ProxyHam encima alguien más la red podría ser interpretada como acceso no autorizado debajo América draconian y Fraude de Ordenador impreciso y Ley de Abuso. Caudill Residuos para comentar en cualquier de la especulación.

Como dije, una vez una idea es allí, cualquiera puede correr con él. Tan investigador de seguridad Samy Kamkar creó ProxyGambit, un aparato que esencialmente reemplaza ProxyHam.<sup>4</sup> Exceptúa utiliza inverso celular traffic, significando que en vez de vuestro ser sólo unas cuantas millas del aparato cuándo lo utilizas,

podrías ser hasta la mitad a través del mundo. Fresco! ProxyGambit Y a aparatos les lo gusta naturalmente creará dolores de cabeza para aplicación de ley cuándo los delincuentes deciden utilizarles.

Ulbricht Carretera de Seda era una droga on-line emporium. No fue algo podrías buscar encima Google; no fue en qué's llamado la Web de Superficie, los cuales fácilmente pueden ser indexed y buscó. La Web de Superficie, conteniendo a sitios familiares les gusta la amazona y Entubas, representa sólo 5 por ciento del Internet entero. Todos los sitios web la mayoría de ti ha sido a o saber aproximadamente la marca arriba de un número trivial comparó al número real de sitios allí. La mayoría vasta de sitios de Internet es de hecho escondido de más semotores de arco.

Después de la Web de Superficie, el próximo más grande chunk del Internet es qué's llamado la Web Profunda. Esto es la parte de la Web que está escondido detrás acceso de contraseña —por ejemplo, los contenidos de la carta catalogan para la rama de Parque del Glen del San Francisco Biblioteca Pública. La Web Profunda también incluye la mayoría de suscripción- sitios únicos y sitios de intranet corporativa. Netflix. Pandora. Coges la idea .

Finalmente, hay una mucha pieza más pequeña del Internet sabido como la Web Oscura. Esta parte del Internet no es accesible a través de un navegador normal, ni es searchable en sitios como Google, Bing, y Yahoo.

La Web Oscura es donde Carretera de Seda vivió, junto a sitios donde te puede contratar un assassin y adquirir pornografía de niño. Sitios como estos mantenerse a base de la Web Oscura porque es virtualmente anónimo. Digo “virtualmente” porque nada verdaderamente nunca es.

El acceso a la Web Oscura puede ser obtenido sólo a través de un Tor navegador. De hecho sitios de Web Oscura, con complicados alfanuméricos URLs, todos acaban con .Cebolla. Como mencioné earlier, la cebolla router estuvo creado por los EE.UU. Laboratorio de Búsqueda Naval para dar oppressed personas una manera de contactar cada cual otro así como el mundo exterior. Yo've también explicó que Tor no conecta vuestro navegador directamente a un sitio; bastante, establece un enlace a otro servidor, el cual entonces adosa a otro servidor a finalmente lograr el sitio de destino. El múltiple hops lo hace más duro de localizar. Y los sitios como Carretera de Seda son los productos de servicios escondidos dentro del Tor red. Su URLs está generado de un algoritmo, y las listas de sitios de Web Oscura cambian frecuentemente. Tor Puede acceder ambos la Web de Superficie y el Dark Web. Otro navegador de Web Oscuro, I2P, también puede acceder la Web de Superficie y Web Oscura.

Incluso antes del takedown de Carretera de Seda, personas speculated que el NSA u otros tuvieron una manera de identificar usuarios en la Web Oscura. Una manera para el NSA para hacer

que sería a plhormiga y controlar qué se apellida nodos de salida, los puntos en qué una petición de Internet está pasado a uno de estos servicios escondidos, aun así que todavía no dejaría identificación del inicial requester.

Para hacer que el observador de gobierno tendría que ver tsombrero una petición estuvo hecha para acceder sitio X y que unos cuantos segundos más tempranos, alguien en Nuevo Hampshire disparó arriba del Tor navegador. El observador podría sospechar que los dos casos estuvieron narrados. Con el



tiempo, acceso al sitio y acceso repetido a Tor alrededor del mismo tiempo podría establecer un patrón. Una manera para evitar creando que el patrón es para mantener vuestro Tor el navegador conectó en todo momento.

En Ulbricht caso— cogía sloppy. Ulbricht Apparently didn't tener un plan temprano encima. En sus discusiones iniciales de Carretera de Seda, alternó entre utilizar su alocución de email real y un pseudonymous un.

Como puedes ver, es muy duro de operar en el mundial hoy sin dejar rastros de vuestra identidad cierta a algún lugar en el Internet. Pero como dije en el principio, con un poco de care, tú, también, puede maestro el arte de invisibilidad. En las páginas siguientes, te asomaré qué.

## CAPÍTULO DIECISÉIS

### Mastering el Arte de Invisibilidad

después de leer este lejano, podrías ser pensar sobre vuestro nivel de experiencia y qué fácil (o duro) será para ti para desaparecer on-line. O te podrías ser pedir qué lejos tendrías que ir o si cualquiera de este es para ti. Después de todo, no puedes tener secretos estatales para compartir! Puedes, aun así, estar luchando vuestro ex en una disputa legal. O podrías ser en un disagreement con vuestro jefe. Podrías ser contactar un amigo quién sigue en tacto con un miembro familiar abusivo. O podrías querer mantener algunas actividades privados y unobservable por un abogado. Hay una variedad de razones legítimas por qué podrías necesitar comunicar con otros on-line o para utilizar la Web y otra tecnología anónimamente. Así que...

Qué pasos realmente necesitas tomar para ir todo-en? Cuánto tiempo toma? Y cuánto costó?

Si no es abundantemente aclarar por ahora, para ser invisible on-line you más o menos necesitar crear una identidad separada, uno aquello es completamente no relacionado a ti. Aquello es el significado de ser anónimo. Cuando tú're no siendo anónimo, tienes que también rigurosamente defender la separación de vuestra vida de aquella identidad anónima. Qué I malo por aquel es que necesitas adquirir unos cuantos aparatos separados que es sólo utilizado cuando eres anónimo. Y esto podría coger costoso.

Podrías, por ejemplo, uso vuestro portátil actual y crear qué está llamado una máquina virtual (VM) en vuestro desktop. Una máquina virtual es un ordenador de software . Está contenido dentro de una aplicación de máquina virtual, tal VMware

Fusión. Puedes cargar una copia autorizada de Ventanas 10 dentro de un VM y decirlo cuánta RAM quieres, cuánto espacio de disco necesitas, y tan encima. A alguien observándote por otro lado del Internet, parecería que estás utilizando un Windows 10 máquina incluso si de hecho estás utilizando un Mac.

Investigadores de seguridad profesional utilizan VMs todo el tiempo que—crea y destruyéndoles fácilmente. Pero incluso entre los profesionales allí existe la posibilidad de escape. Por ejemplo, podrías ser en vuestra VM versión de Ventanas 10 y, para alguna razón, registro en a vuestra cuenta de email personal. Ahora que VM puede ser asociado contigo.

Así que el primer paso de ser anónimo está adquiriendo un estand-portátil solo que te sólo uso para vuestras actividades on-line anónimas. Como hemos visto, el nanosecond que te lapso y, dice, control vuestra cuenta de email personal en aquella máquina, el juego de anonimato es encima. Así que recomiendo un bajo-tasó portátil de Ventanas (Linux es mejor, si sabes cómo para utilizar él). La razón no estoy recomendando un MacBook Pro es que es mucho más caro que un portátil de Ventanas.

Anteriormente recomendé que compras un segundo portátil, específicamente, un Chromebook, para utilizar sólo para on-line amontonando. Otra opción para banca on-line sería para utilizar un iPad. Tienes que firmar arriba para una Manzana ID utilizando vuestra alocución de email y una carta de crédito, o por adquirir una carta de regalo del iTunes. Pero desde este aparato es sólo utilizado para vuestra banca personal segura, la invisibilidad no es el gol.

Pero si vuestro objetivo aquí es invisibilidad, un Chromebook no es la solución mejor porque no tienes el mismo flexibility como utilizando un portátil con Ventanas o un Linux-sistema operativo basado como Ubuntu. Windows 10 es vale mientras tú skip la opción que te pides para firmar arriba para una cuenta de Microsoft. No quieres crear cualesquier enlaces de vuestro ordenador a Microsoft whatsoever.

Tendrías que adquirir el portátil nuevo con cobrar en persona, no on-line—que manera la compra puede no fácilmente ser localizado a ti. Recuerda, vuestro portátil nuevo tiene una carta de red inalámbrica con un único MAC alocución. No quieres cualquiera posiblemente localizando el equipamiento a ti—en el caso vuestro real MAC la alocución es de alguna manera filtró. Por ejemplo, si eres en un Starbucks y poder arriba del portátil, el sistema sonda para cualquier anteriormente “conectado a redes” inalámbricas. Si allí está

controlando equipamiento en el área que registros la petición de sonda, podría posiblemente resultado en revelar vuestro real MAC alocución. Uno concierne es que el gobierno puede tener una manera de localizar la compra de vuestro portátil si cualquier enlace existe entre el MAC alocución de vuestra carta de red y el serial number de vuestro ordenador. Si tan, el feds sólo necesitaría encontrar quién adquirió el ordenador concreto para identificarte, el cual probablemente no es tan difícil.

Tendrás que instalar ambas Colas (ve [aquí](#)) y Tor (ve [aquí](#)) y utilizar aquellos en vez del nativos operatinsistema de g y navegador.

No registro en a cualesquier sitios o aplicaciones bajo vuestra identidad real. Ya aprendiste los riesgos basaron encima qué fáciles es para seguir personas y ordenadores en el Internet. Como hemos hablado, utilizando sitios o cuentas bajo vuestro reales identify es una idea muy mala—bancos y otros sitios routinely aparato de uso fingerprinting para minimizar fraude, y esto deja una huella enorme que puede identificar vuestro ordenador si nunca accedes los mismos sitios anónimamente.

De hecho, es más para girar vuestro wireless router fuera antes de que chutas vuestro portátil anónimo en casa. Vuestro proveedor de servicio podría obtener vuestro portátil anónimo MAC alocución si conectas a vuestra casa router (asumiendo el proveedor posee y dirige el router en vuestra casa). Él's siempre más a purchase vuestra casa propia router que tienes control lleno encima, así que el proveedor de servicio no puede obtener el MAC las alocuciones asignaron a vuestros ordenadores en vuestra red local. Como tal, el proveedor de servicio sólo verá el MAC alocución de vuestro router, el cual es no risk a ti.

Qué quieres es verosímil deniability. Quieres proxy vuestras conexiones a través de capas múltiples de modo que él muy, muy duro para un detective a nunca ligarles atrás a una persona sola, dejado sólo te. Me equivoqué mientras todavía un fugitive. Yo repetidamente dialed hasta módems en Netcom—un fantasma de proveedores de servicio del Internet pasados—utilizando un módem de teléfono celular para enmascarar mi ubicación física. Desde entonces era en una ubicación fija era niño's juego para utilizar dirección radiofónica-encontrando técnicas para encontrarme—una vez supieron qué torre celular mi teléfono celular utilizaba para conexiones de datos. Esto dejó mi adversary (Tsutomu Shimomura) para encontrar la ubicación general y pase él a lo largo de a el FBI.<sup>1</sup>

Qué esto significa es que puedes no nunca utilizar vuestro portátil anónimo en casa u obra. Ever. Así que coge un portátil y cometer a nunca utilizándolo para comprobar vuestro email personal, Facebook, o incluso el tiempo local.<sup>2</sup>

Otra manera puedes ser localizado on-line es a través del probado-y-método cierto de siguiente el dinero. Necesitarás pagar fo unas cuantas cosas, tan con anterioridad a tomar

vuestro portátil anónimo fuera y encontrando una red inalámbrica abierta, el primer paso es a anónimamente adquirir algunas cartas de regalo. Desde cada tienda que vende cartas de regalo más probablemente tiene cámaras de vigilancia en el quiosco o counter, tienes que ejercitar precaución extrema. No tendrías que adquirir estos tú. Tendrías que contratar una persona aleatoriamente escogida de la calle para adquirir las cartas de regalo mientras esperas una distancia segura fuera.

Pero cómo tú que? Te podrías acercar, como yo , alguien en una parcela de aparcamiento y decir que vuestras obras ex en aquella tienda allí y te don't querer una confrontación—u ofrecer algunos otra excusa que los sonidos verosímiles. Quizás añades que tiene un restraining orden en contra te. Para \$100 en efectivo, haciendo una compra para ti podría sonar muy razonable a alguien.

Ahora que nosotros've conjunto arriba de nuestro cutout para ir dentro de la tienda y adquirir un handful de prepaid cartas, el cual las cartas tienen que él o ella adquieren? Recomendando adquirir unos cuantos prepaid, preset \$100 cartas. No purchase cualquiera del refillable cartas de crédito, como tienes que proporcionar vuestra identidad real bajo la Ley de Patriota cuándo les activas. Estas compras requieren vuestro nombre real, alocución, cita de nacimiento, y un número de Seguridad Social que emparejará la información about te encima lima con las agencias de crédito. Proporcionando un hecho-arriba nombre o alguien más número de Seguridad Social es contra la ley y es probablemente no valor el riesgo.

Estamos intentando ser invisibles on-line, no romper la ley.

Recomiendo habiendo el cutout Visado de Vainilla de la compra o Vainilla MasterCard \$100 cartas de regalo de una farmacia de cadena, 7-Once, Walmart, o tienda de caja grande. Estos son a menudo dados fuera tan regalos y puede ser utilizado crédito tan regular las cartas serían. Para estos no tienes que proporcionar cualquier identificando información. Y les puedes adquirir anónimamente, con dinero efectivo. Si vives en la UE, anónimamente tendrías que ordenar una carta de crédito física que utiliza viabuy.com. En Europa pueden embarcar las cartas a la oficina de poste, el

cual requiere ningún ID para elegir arriba. Mi understanding es que te enviáis un código de ALFILER, y puedes abrir arriba de la caja de gota con el ALFILER a anónimamente elegir arriba de las cartas (asumiendo no hay ningún cámara).

Así que dónde puede utilizas vuestro portátil nuevo y anónimamente adquirido prepaid automovilístico ds?

Con el advenimiento de inexpensive aparatos de almacenamiento óptico, los negocios que proporcionan el acceso inalámbrico libre puede almacenar imágenes de cámara de la vigilancia para años. Para un detective es relativamente fácil de coger aquellas imágenes y buscar

sospechosos potenciales. Durante el tiempo de vuestra visita, el detective puede analizar los registros que—buscan MAC las alocuciones autenticaron en la red inalámbrica que partido vuestro MAC alocución. Es por eso que es importante de cambiar vuestro MAC alocución cada vez conectas a una red inalámbrica libre. Así que necesitas encontrar una ubicación cercana o adyacente a uno aquello ofrece Wi-Fi libre. Por ejemplo, puede haber un restaurante chino puerta próxima a un Starbucks u otro establecimiento que ofertas acceso inalámbrico libre. Sienta en una mesa cercana la muro contigua el proveedor de servicio. Puedes experience ligeramente velocidades de conexión más lenta, pero tendrás anonimato relativo (al menos hasta el detective empieza mirar en absoluto las imágenes de vigilancia del área circundante).

Vuestro MAC la alocución probablemente será logged y almacenó una vez autenticas en la red inalámbrica libre. Recuerda David General Petraeus's mistress? Recuerda que el tiempo y las citas de sus inscripciones de hotel emparejaron el tiempo y citas de su MAC el aspecto de la alocución en la red del hotel? No quieres equivocaciones sencillas como these a compromise vuestro anonimato. Así que recuerda para cambiar vuestro MAC alocución cada vez accedes Wi-Fi público (ve [aquí](#)).

Tan lejos esto parece bastante sincero. Quieres comprar un portátil separado de qué te hará vuestra actividad anónima. Quieres anónimamente adquirir algunas cartas de regalo. Quieres encontrar una red de Wi-Fi que te puede acceder de un sitio cercano o adyacente para evitar siendo visto encima cámara. Y quieres cambiar vuestro MAC alocución cada vez conectas a una red inalámbrica libre.

Naturalmente allí ha más. Mucho más. Sólo estamos empezando.

También podrías querer contratar un segundo cutout, este tiempo para hacer una compra más importante: un personal hotspot. Como mencioné antes, el

FBI me cogí porque era dialing hasta sistemas alrededor del mundiales utilizando mi teléfono celular y módem, y con el tiempo mi ubicación fija era compromised porque mi teléfono celular estuvo conectado a la misma torre celular. En aquel punto era fácil de utilizar radiofónico-la dirección que encuentra para localizar el transceptor (mi teléfono celular). Tú can evita que por contratar alguien para ir a un Verizon tienda (o AT&T o T-Móvil) y adquirir un personal hotspot aquello te dejás para conectar al Internet que utiliza dato celular. Aquello significa tienes vuestro acceso local propio al Internet, así que te don't tiene que pasar por una red de Wi-Fi pública. La mayoría de importante, nunca tendrías que utilizar un personal hotspot en una ubicación fija para demasiado mucho tiempo cuándo necesitas mantener vuestro anonimato.

Idealmente la persona contratas no verá vuestro plato de licencia o tener cualquier manera de identificarte. Dar el dinero efectivo de persona: \$200 para el hotspot y otro \$100

cuándo los regresos de persona con el hotspot. El operador móvil venderá el cutout un personal hotspot aquello no lleva ninguna información de identificar. Y mientras eres en él, por qué no adquirir unas cuantas cartas de recambio para añadir más dato? Hopefully El cutout ganado't abscond con vuestro dinero, pero es un riesgo interesante para anonimato. Más tarde puedes recambio el aparato de quemador que utiliza Bitcoin.<sup>3</sup>

Una vez te ha anónimamente adquirió un portátil hotspot, es muy importante que, como con el portátil, tú nunca, nunca, *nunca* girar el aparato encima en casa. Cada vez el hotspot está girado encima, registra con la torre celular más cercana. No quieres vuestra casa u oficina o anyplace te frecuente de aparecer en las limas de registro del operador móvil.

Y nunca turno en vuestro teléfono personal o portátil personal en la misma ubicación donde giras en vuestro portátil anónimo o teléfono de quemador o anónimo hotspot. La separación es realmente importante. Cualquier récord aquello te enlazas a vuestro anónimo self en una cita más tardía y cronometrar negates la operación entera.

Ahora, armado con prepaid cartas de regalo y un personales hotspot con un prepaid plan de dato—tanto adquirió anónimamente por dos personas muy diferentes quién no tendría cualquier información aproximadamente te para identificarte a la policía—somos casi puestos. Casi.

De este punto encima, el Tor el navegador siempre tendría que soler crear y acceder todas las cuentas on-line porque constantemente cambia vuestra alocución de IP.

Uno de los primeros pasos es para poner arriba de un par de cuentas de email anónimo usando Tor. Esto era algo que Ross Ulbricht desatendió para hacer. Como vimos en el capítulo anterior, utilizó su cuenta de email personal más de una vez mientras dirigiendo su negocio de Carretera de la Seda en la Web Oscura. Estos involuntarios crossovers de Temer Pirate Roberts a Ross Ulbricht y atrás otra vez ayudó los detectives confirman que los dos nombres estuvieron asociados con una persona.

Para impedir abuso, la mayoría de proveedores de email—como Gmail, Hotmail, Perspectiva, y Yahoo—requiere verificación de teléfono celular. Aquello significa tienes que proporcionar vuestro número móvil y, inmediatamente durante el signo-arriba proceso, un mensaje de texto está enviado a aquel aparato para confirmar vuestra identidad.

Todavía puedes utilizar un servicio comercial like los mencionaron encima si utilizas un teléfono de quemador. Aun así, aquel teléfono de quemador y cualesquier cartas de recambio tienen que ser obtenidos securely—i.e., adquirió en efectivo por una tercera fiesta quiénes no pueden ser localizados atrás a ti. También, una vez tienes un teléfono de quemador, no lo puedes utilizar cuándo eres cercano a cualesquier otros aparatos celulares posees. Otra vez, dejar vuestro teléfono

personal en casa. Para adquirir Bitcoin on-line, vas a necesitar al menos dos email anónimamente creado alocuciones y Bitcoin carteras. Tan qué creas anonymous alocuciones de email como aquellos creados por Edward Snowden y Laura Poitras?

En mi búsqueda, encontré era capaz de crear una cuenta de email en protonmail.com y uno en tutanota.com utilizando Tor, ambos sin cualesquier peticiones para verificar mi identidad. Tampoco de estos dos proveedores de email me pedimos para verificación a setup. Puedes dirigir vuestra búsqueda propia por buscar proveedores de email y comprobando para ver si requieren vuestro número de teléfono celular durante el signo-arriba proceso. También puedes ver cuánto información necesitan crear las cuentas nuevas. Otra opción de email es fastmail.com, el cual no es casi tan la característica rica como Gmail, pero porque es un servicio pagado, hay no minero de dato de usuario o mostrando de anuncios.

Tan ahora tenemos un portátil, con Tor y las colas cargadas, un teléfono de quemador, un handful de anónimo prepaid cartas de regalo, y un anónimos hotspot con un dato anónimamente adquirido plan. Nosotros're todavía no a punto. Para mantener este anonimato, necesitamos convertir nuestro anónimamente adquiridos prepaid cartas de regalo a Bitcoin.



En [capítulo 6](#) I hablé sobre Bitcoin, moneda virtual. Por él Bitcoin no es anónimo. Pueden ser localizados a través de qué's llamados un blockchain atrás a la fuente de la compra; de modo parecido, todas las compras subsiguientes pueden ser localizadas también. Tan Bitcoin por él no va a esconder vuestra identidad. Tendremos que correr los fondos a través de un mecanismo de anonimato: convirtiendo prepaid cartas de regalo a Bitcoin, entonces running el Bitcoin a través de un servicio de lavar. Este proceso resultará en anonymized Bitcoin para ser utilizado para pagos futuros. Necesitaremos el lavado Bitcoin, por ejemplo, para pagar para nuestro VPN servicio y cualesquier compras futuras de uso de datos en nuestro portátil hotspot o teléfono de quemador.

Utilizando Tor, puedes poner arriba de un inicial Bitcoin cartera en [paxful.com](#) u otros Bitcoin sitios de cartera. Algunos sitios broker tratos en qué te puede comprar Bitcoin con prepaid cartas de regalo, como aquellos preset Visado de Vainilla y Vainilla MasterCard cartas de regalo mencioné más temprano. El downside es que pagarás una prima enorme para este servicio, al menos 50 por ciento.

[Paxful.com](#) Es más como un eBay sitio de subasta donde encuentras Bitcoin vendedores —el sitio sólo conecta tú con compradores y vendedores.

Aparentemente el anonimato tiene un coste alto. La menos información de identidad tú

Proporciona en una transacción, el más pagarás. Aquello hace sentido: las personas que venden el Bitcoin está tomando un riesgo enorme por no verificando vuestra identidad. Era capaz de adquirir Bitcoin en cambio para mi Vainilla anónimamente adquirida cartas de regalo del Visado a razón de 1.70 \$por dólar, el cual es indignante pero necesario de asegurar unonymity.

Mencioné que Bitcoin por él no es anónimo. Por ejemplo, hay un récord que intercambié seguro prepaid cartas de regalo para Bitcoin. Un detective podría localizar mi Bitcoin atrás a las cartas de regalo.

Pero hay maneras de lavar Bitcoin, ocultando cualquier enlace atrás a mí.

El dinero que lava es algo aquellos delincuentes todo el tiempo. Es más a menudo utilizado en narcotráfico, pero también toca una función en blanco-cuello delito financiero. Lavando significa que disfrazas la propiedad original de the fondos, a menudo por enviar el dinero fuera del país, a bancos múltiples en países que tiene leyes de intimidad estricta. Te resulta puede hacer algo similar con moneda virtual.

Hay servicios llamados tumblers que tomarán Bitcoin de una variedad de fuentes y mezcla—o tumble—los juntos de modo que el resultante Bitcoin retiene su valor pero lleva rastros de muchos dueños. Esto lo hace duro para alguien para decir más tarde qué dueño hizo una compra segura. Pero tienes que ser extremadamente prudente, porque hay toneladas de estafas allí.

Tomé una casualidad. Encontré un servicio de lavar on-line y tomaron un coste extra fuera de la transacción. De hecho cogía el Bitcoin valor que quise. Pero pensar sobre este: aquello lavando el servicio ahora tiene uno de mis alocuciones de email anónimas y ambos Bitcoin alocuciones que estuvo utilizado en la transacción. Así que a cosas de mezcla más lejana arriba, tuve el Bitcoin entregado a un segundo Bitcoin cartera que estuvo puesto arriba por inaugurar un nuevo Tor circuito, el cual estableció nuevo hops entre mí y el sitio I quiso visitar. Ahora la transacción es exhaustivamente obfuscated, haciéndolo muy duro para alguien para venir a lo largo de más tardío y cifra fuera que el dos Bitcoin las alocuciones están poseídas por la misma persona. Naturalmente, el Bitcoin lavando el servicio podría cooperar con terceras fiestas por proporcionar ambos Bitcoin alocuciones. Es por eso que es tan importante a securely compra el prepaid cartas de regalo.

Después de utilizar las cartas de regalo para adquirir Bitcoin, recuerda a securely colocar de las cartas plásticas (no en vuestra basura en casa). Recomiendo utilizar una cruz-trituradora cortada aquello's valorado para cartas plásticas, entonces colocando del shreds en un aleatorio dumpster fuera de vuestra casa u oficina. Una vez el lavado Bitcoin ha sido recibido, puedes firmar arriba para un VPN servicio que marcas vuestro

privacy una prioridad. La póliza mejor cuándo estás intentando ser anónimo es sencillamente no para confiar en cualquier VPN proveedor, especialmente los que alegan no para retener cualesquier registros. Las casualidad son'll tos quieta arriba de vuestros detalles si contactados por aplicación de ley o el NSA.

Por ejemplo, no puedo imaginar cualquier VPN proveedor no siendo capaz a troubleshoot asuntos dentro de su red propia. Y troubleshooting requiere mantener algunos registros—p. ej., registros de conexión que podría soler clientes de partido a su IP de originar alocuciones.

Tan becauso incluso el mejor de estos proveedores no pueden ser confiados en, adquiriremos un VPN el servicio que utiliza lavó Bitcoin a través del Tor navegador. Sugiero revisar un VPN proveedor's plazos de servicio y políticas de privacidad y encontrar el aquello parece el mejor del ramo. Tú're no yendo para encontrar un partido perfecto, sólo un bueno uno. Recuerda que

no puedes confiar en cualquier proveedor para mantener vuestro anonimato. Tienes que él tú con el entendiendo que un error solo puede revelar vuestra identidad cierta.

Ahora, con un estand-portátil solo, corriendo cualquier Tor o Colas, utilizando un VPN el proveedor adquirido con lavó Bitcoin, sobre un anónimamente adquirió hotspot, y con un suministro de aún más lavó Bitcoin, has completado la parte fácil: el setup. Esto te costará un couple de centenar bucks, quizás cincocientos, pero todas las piezas han sido randomized de modo que pueden no fácilmente ser conectados atrás a ti. Ahora viene la parte dura que— mantiene que anonimato.

Todo el setup y procesos acabamos de pasar por puede ser perdido in un segundo si utilizas el anónimo hotspot en en casa, o si te poder en vuestro teléfono celular personal, pastilla, o cualquiera otro aparato celular enlazó a vuestra identidad real en la ubicación física donde estás utilizando vuestra identidad anónima. Sólo toma uno slip por tú para un detective forense para ser capaz a correlate vuestra presencia a una ubicación por analizar el proveedor celular's registros. Si hay un patrón de acceso anónimo al propio tiempo vuestro aparato celular está registrado en el mismo sitio de celda, podría dirigir a desenmascarar vuestra identidad cierta.

Ya he dado un número de ejemplos de este.

Ahora, tener que vuestro anonimato ser compromised y tener que decides comprometer en otra actividad anónima, podrías necesitar pasar por este proceso una vez más—secando unnd reinstalling el sistema operativo en vuestro portátil anónimo y creando otro conjunto de cuentas de email anónimo con Bitcoin carteras y adquiriendo otro anónimos hotspot. Recuerda que

Edward Snowden y Laura Poitras, ambos de quien ya hubo anonymous e-cuentas de correo, puestos arriba de cuentas de email anónimas adicionales tan podrían comunicar específicamente con cada otro. Esto es sólo necesario si sospechas que el anonimato original tú've establecido es compromised. Otherwise te Podría utilizar el Tor navegador (después de establecer un nuevo Tor circuito) a través del anónimo hotspot y VPN para acceder el Internet que utiliza un diferente persona.

Naturalmente, cuánto o qué poco escoges seguir estas recomendaciones depende de ti.

Incluso si sigues mis recomendaciones, es todavía posible para alguien en el otro fin para reconocerte. Qué? Por cierto escribes.

Hay un ente considerable de investigar aquello ha enfocado en las personas de elecciones de palabra concretas hacen cuándo escribiendo emails y comentando en sociales media postes. Por mirar en aquellas palabras, los investigadores a menudo pueden identificar sexo y etnicidad. Pero más allá que no pueden ser más concretos.

O puede ellos?

En Segunda Guerra mundial el gobierno británico puesto arriba de un número de escuchar canal alrededor del país para interceptar señales del ejército alemán. Los avances que dirigidos a los Aliados decrypting estos mensajes vinieron un poco más tarde—en Bletchley Parque, el sitio del Código de Gobierno y Cypher Escuela, donde el alemán Enigma el código estuvo roto. Temprano encima, las personas en Bletchley el parque que intercepta los mensajes de telégrafo alemanes podrían identificar características únicas seguras de un sender basados en los intervalos entre el puntos y el dashes. Por ejemplo, podrían reconocer cuándo un operador de telégrafo nuevo vino encima, e incluso empezaron dar los nombres de operadores.

Cómo podría puntos meros y dashes revelar las personas detrás les?

Bien, el intervalo de tiempo entre el sender está tocando de un clave y el tocando del clave otra vez puede ser medido. Este método de la diferenciación más tarde acaeció sabida como el Puño del Sender. Varios código de Morse los operadores claves podrían ser identificados por sus puños “únicos.” Lo wasn't Lo que el telégrafo estuvo diseñado para hacer (quién se preocupa quién envió el mensaje; qué *era* el mensaje?), pero en este caso el único tocando era un subproducto interesante.

Hoy, con avances en tecnología digital, los aparatos electrónicos pueden medir el nanosecond diferencias en la manera cada persona pulsa tonos encima teclados de ordenador—no sólo la periodo de cronometrar un tono dado está aguantado pero también qué deprisa el tono próximo sigue. Puede decir la diferencia entre alguien quién escribe normalmente y alguien quién caza y pecks en el teclado. Aquello,

coupled con las palabras escogidas, puede revelar mucho sobre una comunicación anónima.

Esto es un problema si has pasado por el problema de anonymizing vuestra alocución de IP. El sitio por otro lado todavía te puede reconocer—no debido a algo técnico pero debido a algo singularmente humano. Esto es también sabido como análisis conductista.

Dejado's decir un Tor-anonymized el sitio web decide seguir vuestro keystroke perfil. Quizás las personas detrás es malicious y sólo quiere saber más aproximadamente te. O quizás obran con aplicación de ley.

Muchos las instituciones financieras ya utilizan keystroke análisis a más allá autenticar titulares de cuenta. Aquella manera si alguien tiene vuestro username y contraseña, él o ella pueden no realmente fingir la cadencia de vuestro escribiendo. Aquello's tranquilizando cuándo quieres ser autenticado on-line. Pero qué si tú no?

Porque keystroke el análisis es tan disturbingly fácil de desplegar, investigadores Por Thorsheim y Paul Moore creó un Chrome tapón de navegador-en Intimidación de Teclado llamado. El tapón-en caches vuestro individual keystrokes y entonces les toca fuera en intervalos diferentes. La idea es para presentar randomness en vuestro normal keystroke cadencia como medios de conseguir el anonimato on-line. El tapón-en más allá podría enmascarar vuestras actividades de Internet anónimas.<sup>4</sup>

Como hemos visto, manteniendo la separación entre vuestra vida real y vuestra vida anónima on-line es posible, pero requiere constante vigilante. En el capítulo anterior hablé aproximadamente algunos fallos espectaculares en ser invisibles. Estos eran magníficos pero intentos de plazo corto en invisibilidad.

En el caso de Ross Ulbricht, él didn't realmente planear suyo alterar ego muy cuidadosamente, ocasionalmente utilizando su alocución de email real en vez de un unonymous un, particularmente en el comienzo. A través del uso de una búsqueda avanzada de Google, un detective era capaz a la pieza junta bastante información para revelar el dueño misterioso de Carretera de Seda.

Así que qué aproximadamente Edward Snowden y a otros les le gustar quién es concerned sobre su vigilancia por uno o más agencias de gobierno?

Snowden, por ejemplo, tiene una cuenta de Twitter. Tan hacer bastante unos cuantos otra intimidación folks—qué más poder les comprometo en una ronda de feisty la conversación on-line? Hay un par de posibilidades para explicar cómo estas personas quedan “invisibles.”

**No son bajo vigilancia activa.** Quizás un gobierno o agencia de gobierno sabe exactamente dónde sus objetivos son pero no se preocupa. En aquel caso, si los objetivos no están rompiendo cualesquier leyes, quién's para decir han no dejar su

guardia abajo en algún punto? Podrían alegar a uso único Tor para sus emails anónimos, pero entonces otra vez podrían ser utilizar que cuenta para su Netflix compras también.

**Son debajo vigilancia, pero no pueden ser arrestados.** Creo que poder muy bien describir Snowden. Es posible ha resbalado con respecto a su anonimato en algún punto y que ahora está siendo activamente siguió wherever va—exceptúa está viviendo en Rusia. Rusia tiene no razón real para arrestarle y regresarle a los Estados Unidos.

Notarás dije “resbalado”: a no ser que tienes atención asombrosa para detallar, es realmente duro de vivir dos vidas. Sé. Yo've hecho lo. Dejé mi guardia abajo por utilizar una ubicación fija cuándo accediendo ordenadores a través de una red de teléfono celular.

Allí's un truism en el negocio de seguridad que un atacante persistente tendrá éxito dado bastante tiempo y recursos. Tengo éxito todo el tiempo cuándo probando los controles de seguridad de mi cliente. Todo eres realmente haciendo por probar para te hacer anónimo es putting arriba tantos obstáculos que un atacante dará arriba y movimiento encima a otro objetivo.

La mayoría de nosotros sólo tienen que escondrijo para un poco mientras. Para evitar aquel jefe quién es fuera para cogerte disparó. Para evitar que ex cuyos abogados están buscando algo, cualquier cosa, to control en contra te. Para evadir que creepy acosador quién vio vuestro cuadro encima Facebook y está determinado para acosarte. Cualquier cosa vuestra razón para ser invisible, los pasos he perfilado obrará mucho tiempo bastante para cogerte fuera de bajo una situación mala.

Siendo anónimo en hoy el mundo digital requiere obra muchísima y constante vigilance. Cada persona's los requisitos para anonimato difieren—necesitas proteger vuestras contraseñas y mantener documentos privados fuera de vuestro coworkers? Necesitas esconder de un abanicar quién es stalking te? Necesitas evadir aplicación de ley porque tú're un whistleblower?

Vuestros requisitos individuales dictarán los pasos necesarios necesitas tomar para mantener vuestro nivel deseado de anonimato—de poner contraseñas fuertes y dándose cuenta que vuestra impresora de oficina es fuera para cogerte completamente a pasar por los pasos detallaron aquí para hacerlo extremadamente difícil para un detective forense para descubrir vuestra identidad cierta.

En general, aun así, podemos todos aprenden algo aproximadamente cómo para minimizar nuestro fingerprints en el mundo digital. Podemos pensar antes de posting que foto con un domicilio particular visible en el fondo. O antes de proporcionar una cita de nacimiento real y otra información personal en nuestros perfiles de medios de comunicación sociales. O antes de explorar

el ingenio de Internethout utilizando el HTTPS En todas partes prórroga. O antes de hacer llamadas confidenciales o enviando textos sin utilizar un fin-a-herramienta de encriptación del fin como Señal. O antes de que messaging un doctor a través de AOL, MSN Mensajero, o Charla de Google sin OTR. O antes enviaring un email confidencial sin utilizar PGP o GPG.

Podemos pensar proactively sobre nuestra información y darse cuenta que incluso si qué estamos haciendo con *siente* benigno—compartiendo una fotografía, olvidando para cambiar default registro-ins y contraseñas, utilizando un teléfono de obra para un mensaje personal, o poniendo arriba de una cuenta de Facebook para nuestros niños—nosotros're de hecho haciendo decisiones que lleva un lifetime de ramificaciones. Así que necesitamos obrar.

Este libro es todo aproximadamente quedándose on-line mientras reteniendo nuestra intimidad preciosa. Todo el mundo—del most tecnológicamente desafiado a expertos de seguridad profesional—tendrían que hacer una práctica comprometida de mastering este arte, el cual acaece más esencial con cada día que pasa: el arte de invisibilidad.

## Acknowledgments

Este libro está dedicado a mi madre amorosa, Shelly Jaffe, y mi abuela Reba Vartanian, quién ambos sacrificaron un trato sumo para mí toda mi

vida. Ningún asunto qué situación me cogía a, mi mamá y el gramo eran siempre allí para mí, especialmente en mi tiempo de necesidad. Este libro no habría sido possible sin mi familia maravillosa, quién me ha dado tanto apoyo y amor incondicionales durante mi vida.

Encima abril 15, 2013, mi madre pasó fuera después de una lucha larga con cáncer de pulmón. Vino después de años de trance y luchando para tratar the efectos de quimioterapia. Había pocos los días buenos después de los tratamientos terribles utilizaron en medicina moderna para luchar de estos tipos de cánceres. Normalmente los pacientes tienen un tiempo muy corto—típicamente es meses únicos antes de que ellos succumb a la enfermedad. Siento very afortunado para el tiempo era capaz de pasar con su mientras luchaba esta batalla horrible. Soy tan agradecido a ha sido criado por tal madre amorosa y dedicada, quien también considero mi amigo mejor. Mi mamá es tal una persona asombrosa y yo miss le increíblemente tan.

Encima Marcha 7, 2012, mi abuela pasó fuera inesperadamente mientras siendo tratado en Sunrise Hospital en Las Vega. Nuestro familiar estuvo a la



espera su para regresar casa, pero nunca pasó. Para el pasado varios años que dirigen hasta mi abuela que pasa fuera, su corazón era en tristeza constante debido a mi madre's batalla con cáncer. Está perdida terriblemente y deseo era aquí para gozar este accomplishment.

Espero que este libro traerá mucha felicidad a mi madre es y los corazones de la abuela y hacerles orgulloso que yo'm ayudando para proteger personas' derechos a intimidad.

Deseo mi papá, Alan Mitnick, y mi hermano, Adam Mitnick, era aquí a 75

Celebrar la publicación de este libro importante encima acaeciendo invisible cuándo espionando y la vigilancia es ahora la norma.

He tenido la fortuna buena de ser teamed arriba con seguridad y experto de intimidad Robert Vamasi para escribir este libro. Rob's conocimiento notable en la seguridad y las destrezas como escritora incluyen su capacidad de encontrar que obliga historias, búsqueda estos temas, y tomar la información proporcionada por mí y escribirlo arriba en tal moda y manera que cualquier nontechnical la persona lo podría entender. Tengo que verter mi sombrero para Atracar, quién una cantidad enorme de trabajo duro en este proyecto. Truthfully, no podría haber hecho él sin él.

Soy ansioso de dar las gracias a aquellas personas quiénes representan mi carrera profesional y está dedicado en manera extraordinarias. Mi agente literario, David Fugate de LaunchBooks, negoció el contrato de libro y obrado como enlace con el editor, Poco, Brown. El concepto del *Arte de Invisibilidad* estuvo creado por John Rafuse de 121 Mentas, quién es mi agente para hablar engagements y aprobaciones, y también actúa desarrollo empresarial estratégico para mi empresa. Enteramente a su iniciativa propia, John me di una propuesta de libro intrigante, junto con un simulado-arriba de la portada. Fuertemente me fomenté para escribir este libro para ayudar educate la población del mundo encima cómo para proteger sus derechos de intimidad personales del overstepping de Hermano Grande y Dato Grande. John es awesome.

Soy agradecido de tener tenido la oportunidad de obrar con Pequeño, Brown encima desarrollando este proyecto apasionante. Deseo dar las gracias a mi editor, John Perejil, para todo su trabajo duro y consejo sumo en este proyecto. Gracias, John.

Deseo dar las gracias a mi amigo Mikko Hypponen, agente de búsqueda del jefe de F- Seguro, para pasar su tiempo valioso penning el prólogo para este

libro. Mikko es una seguridad altamente respetada y la intimidad experta quién ha enfocado en malware búsqueda para encima veinticinco años.

también me gustaría dar las gracias a Tomi Tuominen de F-Seguro para tomar tiempo fuera de su horario ocupado para hacer una reseña técnica del manuscrito y algo de ayuda cualesquier errores y coger cualquier cosa aquello estuvo pasado por alto.

## Sobre el Autor

KEVIN MITNICK ha sido el tema de los perfiles incontables publicados y retransmitidos durante el mundo. Mitnick's Penetración principal-probando el equipo es altamente respetado y buscó después para sus servicios de seguridad por el mundiales's gobiernos y empresas superiores. La empresa fundó, Mitnick Consultoría de Seguridad LLC, tiene clientes que incluye docenas del Fortune 500 y muchas naciones a través del globo. Mitnick Es el bestselling autor de *Fantasma en los Cables*, *El Arte de Intrusión*, y *El Arte de Engaño*. Vive en Las Vega y viaja el mundo como el superior keynote altavoz en cybersecurity.

[mitnicksecurity.com](http://mitnicksecurity.com) [twitter.com/kevinmitnick](https://twitter.com/kevinmitnick)

## Libros por Kevin Mitnick

*El Arte de Invisibilidad* (con Robert Vamosi)

*Fantasma en los Cables* (con William L. Simon)

*El Arte de Intrusión* (con William L. Simon) *El Arte de Engaño* (con William L. Simon)

## Nota

*Toda fuente URLs citado abajo era cuidadoso como de la escritura original de este libro, julio 2016.*

### Introducción: Tiempo para Desaparecer

1. [https://www.youtube.com/watch?t=33&v=xevlyp4\\_11m](https://www.youtube.com/watch?t=33&v=xevlyp4_11m).
2. Snowden Primero fue a Hong Kong antes de recibir permission para vivir en Rusia. Desde entonces ha aplicado para vivir en Brasil y otras naciones y no ha

gobernado fuera de un regreso a los Estados Unidos si era para recibir una prueba justa.

1. 3.

<http://www.reuters.com/article/2011/02/24/idsn2427826420110224>.

2. 4. <https://www.law.cornell.edu/supct/html/98-93.ZD.html>.

3. 5. <https://www.law.cornell.edu/uscode/text/16/3372>.

4. 6. [http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-](http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-Manera-a-pensar-aproximadamente-vigilancia/)

[Manera-a-pensar-aproximadamente-vigilancia/](#).

## **Capítulo Un: Vuestra Contraseña Puede Ser Agrietada!**

1. 2.

3. 4.

5.

6. 7.

8. 9.

10. 11. 12.

13. 14. 15.

16.

17. 18.

<https://www.apple.com/pr/library/2014/09/02apple-media-advisory.html>.

<http://anon-ib.com/>. Complacer notar este sitio no es seguro para obra y también puede contener perturbando imágenes también.

<http://www.wired.com/2014/09/eppb-icloud/>. <https://www.justice.gov/usao-mdpa/pr/lancaster-county-man-sentenced-18-Meses-federales-prisión-hacking-manzana-y-google-email>.

<http://arstechnica.com/security/2015/09/new-stats-show-ashley-madison-Contraseñas-es-justo-tan-débil-tan-todo-el-resto/>.

<http://www.openwall.com/john/>.

“MaryHadALittleLamb123\$” Como rendered por

<http://www.danstools.com/md5-hash-generator/>.

<http://news.bbc.co.uk/2/hi/technology/3639679.stm>.

<http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-Ascendió-a-3-1-millones-último-índice/de-año.htm>.

[http://www.mercurynews.com/california/ci\\_26793089/warrant-chp-Agente-](http://www.mercurynews.com/california/ci_26793089/warrant-chp-Agente-)

dice-robo-desnudo-photos-de. <http://arstechnica.com/security/2015/08/new-data-uncovers-the-surprising-predictability-De-androide-cerradura-patrones/>. <http://www.knoxnews.com/news/local/official-explains-placing-david-kernell-En-ky-facilidad-ep-406501153-358133611.html>. <Http://www.wired.com/2008/09/palin-e-mail-ha/>. <http://fusion.net/story/62076/mothers-maiden-name-security-question/>. [http://web.archive.org/web/20110514200839/http://latimesblogs.latimes.com/webscout/A\\_medias-hac.html](http://web.archive.org/web/20110514200839/http://latimesblogs.latimes.com/webscout/A_medias-hac.html). <http://www.commercialappeal.com/news/david-kernell-ut-Estudiantil-en-palin-email-caso-es-liberado-de-supervisi3n-ep-361319081-326647571.html>; <http://edition.cnn.com/2010/crime/11/12/tennessee.palin.hacking.case/>. <http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-Que-entrega-usuarios-encima-email-cuenta-acceso>. <https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-Cuenta-era-cort3/>.

## Capítulo Dos: Quién Más está Leyendo Vuestro Email?

1. 1. En caso est3s pregunt3ndote, imágenes de niño el abuso sexual está identificado y tagged por el Centro Nacional para Desaparecido y Explotó Niños, el cual es qué Google y otras empresas de motor de búsqueda' sistema de barrido automatizado distingue aquellas imágenes del nonpornographic imágenes en sus redes. Ve <http://www.dailymail.co.uk/news/article-2715396/Google-s-email-esc3ner-ayudas-coger-sexo-infractor-puntas-policiales-indecenes-im3genes-ni3os-Gmail-cuenta.html>.
2. 2. <http://www.braingle.com/brainteasers/codes/caesar.php>.
3. <https://theintercept.com/2014/10/28/smuggling-snowden-secrets/>. 4. Por ejemplo, ver la lista aquí: [https://en.wikipedia.org/wiki/category:Cryptographic\\_algoritmos](https://en.wikipedia.org/wiki/category:Cryptographic_algoritmos).
5. Mailvelope Obras con Perspectiva, Gmail, Yahoo Correo, y muchos otra Web-servicios de email basado. Ve <https://www.mailvelope.com/>.
6. 6. Para ver el metadata en vuestro Gmail cuenta, escoger un mensaje, lo abre, entonces clic el abajo flecha en la esquina derecha superior del mensaje. Entre las elecciones (“Respuesta,” “Respuesta Todo,” “Adelante,” y tan encima) es “Original de Espect3culo.” En Correo de Manzana, seleccionar el mensaje, entonces escoger Mensaje>de

Vista>Todos los Encabezamientos. En Yahoo, clic “Más,” entonces “Ver Encabezamiento Lleno.” Las opciones similares parecen en otros programas de correo.

6. 7. <http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-Intimidad>.

8. <https://immersion.media.mit.edu/>. 9.

[http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-](http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-Para-gobierno-peticiones)

[rubberstamp-Para-gobierno-peticiones](http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-Para-gobierno-peticiones). 10. Puedes escribir “Alocución de IP” a la ventana de búsqueda del Google para ver vuestra alocución

de IP propia en el tiempo de la petición. 11.

<https://play.google.com/store/apps/details?id=org.torproject.android>. 12.

<http://www.wired.com/threatlevel/2014/01/tormail/>. 13.

<https://www.theguardian.com/technology/2014/oct/28/tor-users-advised-Control-ordenadores-malware>. 14.

[http://arstechnica.com/security/2014/07/activo-ataque-encima-tor-red-probado-](http://arstechnica.com/security/2014/07/activo-ataque-encima-tor-red-probado-a-decloak-usuarios-para-cinco-meses/)

[a-decloak-usuarios-para-cinco-meses/](http://arstechnica.com/security/2014/07/activo-ataque-encima-tor-red-probado-a-decloak-usuarios-para-cinco-meses/). 15. Para el Tor caja en una Frambuesa Pi, puedes utilizar a algo le gusta el portal:

<https://github.com/grugq/portaloypi>.

16. <https://www.skype.com/en/features/online-number/>. 17.

<http://www.newyorker.com/magazine/2007/02/19/the-kona-files>. 18. Otra vez, él's probablemente más no para utilizar Google o proveedores de email grande, pero

por el bien de ilustración estoy utilizándolo aquí.

## Capítulo Tres: Wiretapping 101

1. 1. Puedes optar fuera de compartir vuestro personal dato con commuting servicios en el Androide. Va a los encuadres>Buscan & Ahora>intimidad & de Cuentas>Commute compartiendo. Apple no proporciona un servicio similar, pero versiones futuras de iOS te puede ayudar viajes de plan basaron encima dónde vuestro teléfono es en un momento dado.

2. 2. <http://www.abc.net.au/news/2015-07-06/nick-mckenzie-speaks-out-about-Su-pincel-con-el-mafia/6596098>.

3. De hecho adquirirías una carta de recambio que te utilizaría con el teléfono él. Más para utilizar Bitcoin para hacerlo.

4. <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/german-Investigadores-descubrir-un-defecto-aquello-podría-dejado-cualquiera-escuchar-a-vuestro-celda-llamadas-y-leídos-vuestro-textos/>.
5. <http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-Necesitado-a-eavesdrop-encima-gsm-llamada/>.
6. <http://www.latimes.com/local/la-me-pellicano5mar05-Historia.html#navtype=storygallery>.
7. <http://www.nytimes.com/2008/03/24/business/media/24pellicano.html?pagewanted=Todo>.
8. <https://www.hollywoodreporter.com/thr-esq/anthony-pellicanos-prison-Frase-vacated-817558>.
9. <http://www.cryptophone.de/en/products/landline/>. 10. <https://www.kickstarter.com/projects/620001568/jackpair-safeguard-your-Teléfono-postes/de-conversación/1654032>. 11. <http://spectrum.ieee.org/telecom/security/the-athens-affair>. 12. <http://bits.blogs.nytimes.com/2007/07/10/engineers-as-counterspys-how-El-greek-cellphone-sistema-era-bugged/>. 13. <https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone>.

## **Capítulo Cuatro: Si no Encriptas, eres Unequipped**

1. 2. 3.
- 4.
5. 6.
7. 8.
9. 10.
11. 12. 13. 14. 15. 16.
17. 18.
- <http://caselaw.findlaw.com/wa-supreme-court/1658742.html>.
- <http://courts.mrsc.org/mc/courts/zsupreme/179wn2d/179wn2d0862.htm>.
- <http://www.komonews.com/news/local/justices-people-have-right-to-Intimidación-en-texto-mensajes-247583351.html>.

[http://www.democracynow.org/2016/10/26/headlines/project\\_hemisphere\\_at\\_ts\\_secret\\_](http://www.democracynow.org/2016/10/26/headlines/project_hemisphere_at_ts_secret_) <http://www.wired.com/2015/08/know-nsa-atts-spying-pact/>.

[Http://espn.go.com/nfl/story/\\_/id/13570716/tom-brady-new-england-patriotas-gana-apelación-nfl-deflategate](Http://espn.go.com/nfl/story/_/id/13570716/tom-brady-new-england-patriotas-gana-apelación-nfl-deflategate).

[https://www.bostonglobe.com/sports/2015/07/28/tom-brady-destroyed-his-cellphone-Y-textos-a lo largo de-con/ZuIYu0he05XxEeOmHzwTSK/historia.html](https://www.bostonglobe.com/sports/2015/07/28/tom-brady-destroyed-his-cellphone-Y-textos-a-lo-largo-de-con/ZuIYu0he05XxEeOmHzwTSK/historia.html). DES Estuvo agrietado partly porque sólo encriptó el dato una vez. AES Usos tres capas de encriptación y es por tanto mucho más fuerte, incluso independiente del número de bits.

Diskreet Es ya no disponible.

<https://twitter.com/kevinmitnick/status/346065664592711680>. Este enlace provides una explicación más técnica del treinta y dos-mordió DES utilizó: [https://www.cs.auckland.ac.nz/~pgut001/pubs/ningun\\_r\\_a\\_n.txt](https://www.cs.auckland.ac.nz/~pgut001/pubs/ningun_r_a_n.txt).

[http://www.theatlantic.com/technology/archive/2014/06/facebook-texting-Adolescentes-instagram-snapchat-la mayoría de-populares-sociales-red/373043/](http://www.theatlantic.com/technology/archive/2014/06/facebook-texting-Adolescentes-instagram-snapchat-la-mayoría-de-populares-sociales-red/373043/). <http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015>.

<http://www.forbes.com/sites/andygreenberg/2014/02/21/whatsapp-comes-Debajo-nuevo-escrutinio-para-intimidación-póliza-encriptación-gaffs/>.

<https://www.wired.com/2016/10/facebook-completely-Encriptado-mensajero-actualización-ahora/>. <https://community.skype.com/t5/security-privacy-trust-and/skype-to-Skype-Que-graba-llamada/td-p/2064587>.

<https://www.eff.org/deeplinks/2011/12/effs-raises-concerns-about-new-aol-Instante-mensajero-0>.

[http://www.wired.com/2007/05/siempre\\_dos\\_ther/](http://www.wired.com/2007/05/siempre_dos_ther/).

<http://venturebeat.com/2016/08/02/hackers-break-into-telegram-revealing-15-millones-usuarios-teléfono-números/>.

p

19. <http://www.csmonitor.com/world/passcode/2015/0224/private-chat-app-Telegrama-poder-no-ser-tan-secreto-tan-anunció>.

20. <https://otr.cypherpunks.ca/>. 21. <https://chatsecure.org/>. 22.

<https://guardianproject.info/apps/chatsecure/>. 23. <https://crypto.cat/>. 24.

<https://getconfide.com/>.

## Capítulo Cinco: Ahora Me Veo, Ahora Tú no

1. 1.

<https://www.techdirt.com/articles/20150606/16191831259/accor>



ding-to- Que aclara gobierno-vuestro-navegador-historia-es-felony.shtml.

2. 2. <http://www.cbc.ca/news/trending/clearing-your-browser-history-can-be-Considerado-obstrucción-de-justicia-en-el-u-s-1.3105222>.
3. 3. <http://ftpcontent2.worldnow.com/whdh/pdf/Matanov-Khairullozhon-Acusación.Pdf>.
4. 4. <https://www.eff.org/https-everywhere%20>.
5. 5. <http://www.tekrevue.com/safari-sync-browser-history/>.
6. 6. <http://www.theguardian.com/commentisfree/2013/aug/01/government-Siguiendo-google-búsquedas>.
1. 7. <https://myaccount.google.com/intro/privacy>.
2. 8. <http://www.fastcompany.com/3026698/inside-duckduckgo-googles-tiniest-fiercest-Competidor>.

## **Capítulo Seis: Cada Clic de Ratón Haces, Seré Mirar Te**

1. 2.
- 3.
4. 5.
6. 7.
8. 9.
10. 11.
12. 13. 14.
15. 16.
17. 18. 19. 20.

[https://timlibert.me/pdf/libert-2015-health\\_privacy\\_on\\_web.pdf](https://timlibert.me/pdf/libert-2015-health_privacy_on_web.pdf). Una prueba informal dirigida mientras escribiendo este libro asomó que el

Ghostery tapón-en en Chrome bloqueado hasta veintiuna peticiones de socios del Mayo Clínica y doce peticiones de partners de WebMD cuándo regresando resultados para “atletas pie.” Para un cariz más detallado en qué información vuestras filtraciones de navegador, control fuera de <http://browserspy.dk/>.

<https://noscript.net/>.

<https://chrome.google.com/webstore/detail/scriptblock/hcdjknjpbnhdoabbngpmfekaecn?hl=en>. <https://www.ghostery.com/en/download?src=external-ghostery.com>. Por “gota de correo” I buzón comercial malo outfits como el UPS Tienda,

a pesar de que muchos requieren una foto ID antes de que puedes obtener uno. <http://www.wired.com/2014/10/verizons-perma-cookie/>.

<http://www.pcworld.com/article/2848026/att-kills-the-permacookie-stops-Siguiendo-clientes-internet-uso-para-ahora.html>.

<http://www.verizonwireless.com/support/unique-identifier-header-faqs/>.

<http://www.reputation.com/blog/privacy/how-disable-and-Eliminar-centellear-galletas>; <http://www.brighthub.com/computing/smb-prendas-de-seguridad/59530.aspx>.

[http://en.wikipedia.org/wiki/samy\\_kamkar](http://en.wikipedia.org/wiki/samy_kamkar).

<https://github.com/samyk/evercookie>.

<http://venturebeat.com/2015/07/14/consumers-want-privacy-yet-demand-personalization/>. <http://www.businessinsider.com/facebook-will-not-honor-do-not-track-2014-6>.

<https://chrome.google.com/webstore/detail/facebook-disconnect/ejpepfjfmamnambagiibghpglaidiec?hl=en>.

<https://facebook.adblockplus.me/>. <https://zephoria.com/top-15-valuable-facebook-statistics/>. <http://www.latimes.com/business/la-fi-lazarus-20150417-column.html>. <https://www.propublica.org/article/meet-the-online-tracking-device-that-is->

p

Virtualmente-imposible-a-bloque#. 21. <https://addons.mozilla.org/en-us/firefox/addon/canvasblocker/>. 22.

<https://chrome.google.com/webstore/detail/canvasfingerprintblock/ipmjngkmngdcnpm>

hl=en-EE.UU..

23.23. <https://trac.torproject.org/projects/tor/ticket/6253>.

24.24. <https://www.technologyreview.com/s/538731/how-ads-follow-you-from->

[Teléfono-a-desktop-a-pastilla/](#).

23.25. <https://theintercept.com/2014/10/28/smuggling-snowden-secrets/>.

## Capítulo

### de g Siete: Paga Arriba o Más!

1. 1. <http://www.computerworld.com/article/2511814/security0/man-used-Vecino-s-wi-fi-a-acechar-vicepresidente-biden.html>.
2. 2. <http://www.computerworld.com/article/2476444/mobile-security-comcast-xfinity-wifi-Justo-decir-no.html>.
3. <http://customer.xfinity.com/help-and-support/internet/disable-xfinity-wifi-En-casa-hotspot/>.
4. BitTorrent Es un streaming servicio de vídeo para películas, algunos de los cuales están proporcionados por fuentes otro que los titulares de copyright.
5. <http://blog.privatewifi.com/why-six-strikes-could-be-a-nightmare-for-Vuestro-internet-intimidad/>.
6. 6. hay también el conjunto de servicio básico (BSS), el cual proporciona el bloque de edificio básico de un 802.11 inalámbrico LAN (red de área local). Cada BSS o ESS (conjunto de servicio extendido) está identificado por un identificador de conjunto del servicio (SSID).
7. 7. <http://www.techspot.com/guides/287-default-router-ip-Alocuciones/>.
8. <http://www.routeripaddress.com/>. 9. É'l's fácil de imaginar fuera del MAC alocución de autorizó aparatos por utilizar una penetración-herramienta de prueba sabida como Wireshark. 10. <https://www.pwnieexpress.com/blog/wps-cracking-with-reaver>. 11. <http://www.wired.com/2010/10/webcam-spy-settlement/>. 12. <http://www.telegraph.co.uk/technology/internet-security/11153381/how-hackers-Tomó-encima-mi-ordenador.html>. 13. <https://www.blackhat.com/docs/us-16/materials/us-16-seymour-tully-Weaponizing-Datos-Ciencia-Para-Social-Ingeniería-Automatizado-E2E-Lanza-Phishing-Encima-Twitter.Pdf>. 14. <http://www.wired.com/2010/01/operation-aurora/>. 15. <http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-Cortó.html>.

16.16. <http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see->

[Vuestro-datos-otra vez-paga-nos-300-en-bitcoins/](http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-Vuestro-datos-otra-vez-paga-nos-300-en-bitcoins/).

16.17. <https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay->

[El-rescate/](https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-El-rescate/).

## **Capítulo Ocho: Cree Todo, Confía en Nada**

1.

2. 3. 4.

5.

6.

7.

8.

9.

10.

11. 12.

Él's importante de notar que Wi-Fi público no es abrir en todas las partes del mundo. Por ejemplo, en Singapur, para utilizar Wi-Fi público fuera de vuestro hotel o un McDonald's restaurante, necesitarás registrar. Los lugareños tienen que tener una celda de Singapur-número de teléfono, y a uristsel mosto presenta sus pasaportes a una potestad local antes de coger aprobación. <https://business.f-secure.com/the-dangers-of-public-wifi-and-crazy-things-Personas--a-uso-lo/>. <http://dnlongen.blogspot.com/2015/05/is-your-home-router-spying-on-te.html>.

Hay muchas consideraciones un usuario tendría que saber aproximadamente cuándo escogiendo un VPN proveedor. Ve

<https://torrentfreak.com/anonymous-vpn-service-proveedor-reseña-2015-150228/3/>. Uno comercial VPN la elección es TunnelBear, un canadiense VPN empresa. Declaran: “TunnelBear NO almacena los usuarios que originan alocuciones de IP cuándo conectadas a nuestro servicio y así no puede identificar usuarios cuándo alocuciones de IP proporcionada de nuestros servidores. Además, no podemos revelar información sobre las aplicaciones, servicios o sitios web nuestro usuarios consumir mientras conectado a nuestros Servicios; como TunnelBear NO almacena esta información.” <https://www.tunnelbear.com/privacy-policy/>.

<http://www.howtogeek.com/215730/how-to-connect-to-a-vpn-from-your-iphone-or-ipad/>. <http://www.howtogeek.com/135036/how-to-Conectar-a-un-vpn-encima-androide/?PageSpeed=noscript>.

<http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-Viajeros-edward-snowden-documentos-1.2517881>.

<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/9673429/david-Petraeus-Ordenado-amante-Paula-Broadwell-a-parón-emailing-Jill-Kelley.html>. <http://www.nytimes.com/2012/11/12/us/us-officials-say-petraeuss-affair-Sabido-en-verano.html>.

<https://www.wired.com/2012/11/gmail-location-data-petraeus/>.

<http://www.howtogeek.com/192173/how-Y-por-qué-a-cambio-vuestro-mac-alocución-encima-ventanas-linux-y-mac/?PageSpeed=noscript>.

## **Capítulo Nueve: no Tienes Ninguna Intimidad? Coge Encima Lo!**

1. <http://www.wired.com/2012/12/ff-john-mcafees-last-stand/>.

2. <http://defensetech.org/2015/06/03/us-air-force-targets-and-destroys-isis-hq-Que-utiliza-edificio-social-medios-de-comunicación/>.

3. <http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-Intimidad>. 4. <http://www.dailymail.co.uk/news/article-3222298/is-el-chapo-hiding-Costa-Rica-Neto-cierra-mundial-s-querido-droga-señor-desventurado-hijo-olvida-cambio-ubicación-datos-Twitter-cuadro.html>.

5. <https://threatpost.com/how-facebook-and-facial-recognition-are-creating-Minoría-informe-moda-intimidad-fusión-de-un-reactor-nuclear-080511/75514>.

6. <http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-Reconocimiento-lata-ser-utilizado-a-coger-vuestro-social-seguridad-número/2/>.

7. <http://searchengineland.com/with-mobile-face-recognition-google-Cruces-el-creepy-línea-70978>.

8. Robert Vamosi, *Cuándo Gadgets Traicionarnos: El Lado Oscuro de Nuestro Enamoramiento*

- con Tecnologías Nuevas* (Nueva York: Libros Básicos, 2011). 9.  
<http://www.forbes.com/sites/kashmirhill/2011/08/01/how-face-Reconocimiento-lata-ser-utilizado-a-coger-vuestro-social-seguridad-numero/>. 10. <https://techcrunch.com/2015/07/13/yes-google-photos-can-still-sync-your-Fotos-después-de-que-tú-eliminar-el-aplicación/>. 11.  
<https://www.facebook.com/legal/terms>. 12.  
<http://www.consumerreports.org/cro/news/2014/03/how-to-beat-facebooks-Más-grande-intimidación-índice/de-riesgo.htm>. 13.  
<http://www.forbes.com/sites/amitchowdhry/2015/05/28/facebook-security-Chequeo/>. 14.  
<http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-Índice-de-intimidación.htm>. 15. <http://www.cnet.com/news/facebook-will-the-real-kevin-mitnick-please-Estand-arriba/>.  
16.16. [http://www.eff.org/files/filenode/social\\_network/training\\_course.pdf](http://www.eff.org/files/filenode/social_network/training_course.pdf).  
17.17. <http://bits.blogs.nytimes.com/2015/03/17/pearson-under-fire-for-Control-estudiantes-twitter-postes/>.  
18. <http://www.washingtonpost.com/blogs/answer-Capa/wp/2015/03/14/pearson-control-social-medios-de-comunicación-para-seguridad-incumple-durante-parcc-probando/>. 19.  
<http://www.csmonitor.com/world/passcode/passcode-Voces/2015/0513/Es-estudiantil-intimidación-borrado-tan-aulas-turno-digital>.  
20. <https://motherboard.vice.com/blog/so-were-sharing-our-social-security-Números-encima-sociales-medios-de-comunicación-ahora>.  
21.21. <http://pix11.com/2013/03/14/snapchat-sexting-scandal-at-nj-high-school-Podría-resultado-en-niño-porno-cargos/>.  
21.22. <http://www.bbc.co.uk/news/uk-34136388>.

23. <https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-Cargos-que-desaparecen-promesas-mensajes-era>. 24. <http://www.informationweek.com/software/social/5-ways-snapchat-Violado-vuestro-intimidad-seguridad/d/d-id/1251175>. 25. <http://fusion.net/story/192877/teens-face-criminal-charges-for-taking-Manteniendo-en-cueros-fotos-de-ellos/>.

26.26. <http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-Intimidad>.

26.27. [http://fusion.net/story/141446/a-little-known-yelp-setting-tells-businesses-Vuestro-género-edad-y-ciudad-natal/?utm\\_Fuente=rss&utm\\_el\\_medio=alimenta&utm\\_autor=/de-campaña/kashmir-el-cerro/alimenta/](http://fusion.net/story/141446/a-little-known-yelp-setting-tells-businesses-Vuestro-género-edad-y-ciudad-natal/?utm_Fuente=rss&utm_el_medio=alimenta&utm_autor=/de-campaña/kashmir-el-cerro/alimenta/).

28. En el iPhone o iPad, va a Servicios>de Ubicación>de Intimidad de Encuadres, donde encuentras una lista de todo de vuestra ubicación-aplicaciones conscientes. Por ejemplo, es posible de inutilizar la geolocalización para la aplicación de Mensajero del Facebook por él. Rollo a Mensajero “de Facebook” y asegurar que sus servicios de ubicación están puestos a Nunca. “” Encima aparatos de Androide, Abre la aplicación de Mensajero del Facebook, clic el “ícono” de Encuadres (shaped como una tren) en la esquina derecha superior, el rollo a mensajes “Nuevos incluye vuestra ubicación por default,” y uncheck lo. Encima aparatos de Androide en general tendrás que individualmente inutilizar geolocalización (si está ofrecido como elección); hay nadie-medida-acceso-todo poniendo.

29. <https://blog.lookout.com/blog/2016/08/25/trident-pegasus/>.

## **Capítulo Diez: Puedes Correr pero No Esconder**

1. 1. Puedes girar fuera GPS en más tardío verions de iOS como describió aquí: <http://smallbusiness.chron.com/disable-gps-tracking-iphone-30007.html>.
2. 2. <https://gigaom.com/2013/07/08/your-metadata-can-show-snoops-a-whole-Parcela-justo-cariz-en-mina/>.
3. <http://www.zeit.de/datenschutz/malte-spitz-data-retention>. 4. <https://www.washingtonpost.com/local/public-safety/federal-appeals-court-Aquello-incluye-va-md-deja-warrantless-siguiendo-de-histórico-celda-sitio->



récords/2016/05/31/353950d2-2755-11e6-a3c4-0724e8e24f3f\_historia.html.

5. [http://fusion.net/story/177721/phone-Que sigue ubicación-google-feds/?](http://fusion.net/story/177721/phone-Que sigue ubicación-google-feds/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)

[utm\\_Fuente=rss&utm\\_el medio=alimenta&utm\\_autor=/de](http://fusion.net/story/177721/phone-Que sigue ubicación-google-feds/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)  
[campaña/kashmir-](http://fusion.net/story/177721/phone-Que sigue ubicación-google-feds/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)

[el cerro/alimenta/](http://fusion.net/story/177721/phone-Que sigue ubicación-google-feds/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/).

6. [http://www.forbes.com/sites/andyrobertson/2015/05/19/strava-flyby/?](http://www.forbes.com/sites/andyrobertson/2015/05/19/strava-flyby/?ss=Futuro-tecnología)

[ss=Futuro-tecnología.](http://www.forbes.com/sites/andyrobertson/2015/05/19/strava-flyby/?ss=Futuro-tecnología)

6. [http://fusion.net/story/119745/in-the-future-your-insurance-company-will-](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)

[Saber-cuando-youre-teniendo-sexo/? utm\\_Fuente=rss&utm\\_el](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)  
[medio=alimenta&utm\\_autor=/de campaña/kashmir- el cerro/alimenta/](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/).

8. [http://thenextweb.com/insider/2011/07/04/details-of-fitbit-users-sex-lives-](http://thenextweb.com/insider/2011/07/04/details-of-fitbit-users-sex-lives-Sacado-de-búsqueda-motor-resultados/)  
[Sacado-de-búsqueda-motor-resultados/](http://thenextweb.com/insider/2011/07/04/details-of-fitbit-users-sex-lives-Sacado-de-búsqueda-motor-resultados/).

9. [http://fusion.net/story/119745/in-the-future-your-insurance-company-will-](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)  
[Saber-cuando-youre-teniendo-sexo/? utm\\_Fuente=rss&utm\\_el](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/)  
[medio=alimenta&utm\\_autor=/de campaña/kashmir- el cerro/alimenta/](http://fusion.net/story/119745/in-the-future-your-insurance-company-will-Saber-cuando-youre-teniendo-sexo/?utm_Fuente=rss&utm_el medio=alimenta&utm_autor=/de campaña/kashmir-el cerro/alimenta/).

10. <http://www.engadget.com/2015/06/28/fitbit-data-used-by-police/>. 11.

[http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-](http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-Violación-informe/)

[Violación-informe/](http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-Violación-informe/). 12.

[http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-](http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-Salud-rastreador)

[fitbit-Salud-rastreador](http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-fitbit-Salud-rastreador). 13.

[http://www.smithsonianmag.com/innovation/invention-snapshot-changed-](http://www.smithsonianmag.com/innovation/invention-snapshot-changed-Manera-nosotros-vistos-mundiales-180952435/?Todo&ningún-ist)

[Manera-nosotros-vistos-mundiales-180952435/?Todo&ningún-ist](http://www.smithsonianmag.com/innovation/invention-snapshot-changed-Manera-nosotros-vistos-mundiales-180952435/?Todo&ningún-ist). 14.

[https://books.google.com/books?](https://books.google.com/books?id=SI MEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22El+kodak+ha+añadido+un+neS3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22El%20koda&f=falso)

[id=SI MEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22El+kodak+ha+añ](https://books.google.com/books?id=SI MEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22El+kodak+ha+añadido+un+neS3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22El%20koda&f=falso)  
[adido+un+ne](https://books.google.com/books?id=SI MEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22El+kodak+ha+añadido+un+neS3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22El%20koda&f=falso)

[S3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22El%20koda&f=falso](https://books.google.com/books?id=SI MEAAAAMBAJ&pg=PA158&lpg=PA158&dq=%22El+kodak+ha+añadido+un+neS3Cg&ved=0CCAQ6AEwAA#v=onepage&q=%22El%20koda&f=falso). 15.

[http://www.smithsonianmag.com/innovation/invention-snapshot-changed-](http://www.smithsonianmag.com/innovation/invention-snapshot-changed-Manera-nosotros-vistos-mundiales-180952435/?No-ist=&página=2)

[w](http://www.smithsonianmag.com/innovation/invention-snapshot-changed-Manera-nosotros-vistos-mundiales-180952435/?No-ist=&página=2)

[Manera-nosotros-vistos-mundiales-180952435/?No-ist=&página=2](http://www.smithsonianmag.com/innovation/invention-snapshot-changed-Manera-nosotros-vistos-mundiales-180952435/?No-ist=&página=2).

16. [https://www.faa.gov/uas/media/part\\_107\\_summary.pdf](https://www.faa.gov/uas/media/part_107_summary.pdf).

17. [https://www.faa.gov/uas/where\\_to\\_fly/b4ufly/](https://www.faa.gov/uas/where_to_fly/b4ufly/).

18.

[http://www.slate.com/articles/technology/future\\_tense/2015/06/facial\\_recognition\\_priv](http://www.slate.com/articles/technology/future_tense/2015/06/facial_recognition_priv)

19.19. <http://www.extremetech.com/mobile/208815-how-facial-recognition-will->

Cambio-compra-en-tiendas.

19.20. <http://www.retail-week.com/innovation/seven-in-ten-uk-shoppers-find->

Facial-reconocimiento-tecnología-creepy/5077039.Prenda.

19.21.

<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?actid=3004&chapterid=57>.

20.22. <http://arstechnica.com/business/2015/06/retailers-want-to-be-able-to-scan->

Vuestro-cara-sin-vuestro-permiso/.

19.23. <http://fusion.net/story/154199/facial-recognition-no-rules/?>

utm\_Fuente=rss&utm\_el\_medio=alimenta&utm\_autor=/de  
campana/kashmir-

el\_cerro/alimenta/.

19.24. <https://www.youtube.com/watch?v=nesmw7jpodc>.

20.25. <http://motherboard.vice.com/read/glasses-that-confuse-facial-recognition->

Sistemas-es-venidero-a-japan.

Un

## **Capítulo Once: Hey, KITT, no Comparte Mi Ubicación**

1. 2.

3. 4.

5. 6.

7. 8. 9.

10. 11.

12.

13.

14. 15. 16.

17.

<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>. Esto es tonto. Sólo porque algo está prohibido doesn't lo significa ganado't pasa. Y esto crea un escenario peligroso en qué cortó los coches todavía pueden afectar el público de conducción. Cero-días para automóviles, cualquiera?  
<http://keenlab.tencent.com/en/2016/06/19/keen-security-lab-of-tencent-Que-Corta-automovilistico-Búsqueda-Remoto-Ataque-a-Tesla-Coches/>.  
<http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-Ejecutivo-para-intimidad>.  
[http://www.theregister.co.uk/2015/06/22/epic\\_uber\\_ftc/](http://www.theregister.co.uk/2015/06/22/epic_uber_ftc/).  
<http://nypost.com/2014/11/20/uber-reportedly-tracking-riders-without-Permiso/>.

<https://www.uber.com/legal/usa/privacy>. <http://fortune.com/2015/06/23/uber-privacy-epic-ftc/>.

<http://www.bbc.com/future/story/20150206-biggest-myth-about-phone-Intimidad>. <http://tech.vijay.ca/of-taxis-and-rainbows-f6bc289679a1>.  
<http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-Revelar-nyc-taxi-motor-detallados-paradero/>.

Puedes andar a un transit oficina de potestad y petición para pagar en metálico para un NFC carta, pero esto requiere tiempo extra y indudablemente resultado en una conferencia aproximadamente ligando vuestro banco o carta de crédito a la carta en cambio.

<http://www.wsj.com/articles/sB10000872396390443995604578004723603576296>. <https://www.aclu.org/blog/free-future/internal-documents-show-fbi-was-wrestling-Licencia-plato-escáner-intimidad-asuntos>.  
[http://www.wired.com/2015/05/incluso-fbi-intimidad-preocupaciones-licencia-plato-](http://www.wired.com/2015/05/incluso-fbi-intimidad-preocupaciones-licencia-plato-lectores/)

[lectores/](#). Cinco de las fuentes eran el St. Tammany La oficina del sheriff parroquial, el

Jefferson la oficina del sheriff Parroquial, y el Kenner Departamento de Policía, en Luisiana; el Hialeah Departamento de Policía, en Florida; y la Universidad de Departamento de California Del sur de Seguridad Pública.  
<http://www.forbes.com/sites/robertvamosi/2015/05/04/dont-sell-that-Conectado-automovilistico-o-en-casa-justo-todavía/>.

18. <https://www.washingtonpost.com/blogs/the-switch/wp/2015/06/24/tesla-Dice-su-motor-tener-viajado-un-mil-millones-millas-y-tesla-sabe-qué-muchos-millas-youve-conducidos/>.

19. <http://www.dhanjani.com/blog/2014/03/curosry-evaluation-of-the-tesla-Modelo-s-nosotros-cant-proteger-nuestro-estilo-coches-nosotros-proteger-nuestro-workstations.html>.

20. <http://www.teslamotors.com/blog/most-peculiar-test-drive>.

21.21. <http://www.forbes.com/sites/kashmirhill/2013/02/19/the-big-privacy-takeaway-De-tesla-vs-el-nuevo-york-tiempo/>.

21.22. <http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/>.

23. <http://spectrum.ieee.org/cars-that-think/transportation/advanced->

Investigadores/de coches-probar-conectado-coches-lata-ser-siguió. 24.

<http://www.wired.com/2015/10/cars-that-talk-to-each-other-are-much->

Más fácil-a-espía-encima/. 25.

<https://grahamcluley.com/2013/07/volkswagen-security-flaws/>.

26.26. <https://grahamcluley.com/2015/07/land-rover-cars-bug/>.

27.27. <http://www.wired.com/2015/07/hackers-remotely-kill-jee-highway/>.

28. <http://www.forbes.com/sites/robertvamosi/2015/03/24/securing->

Conectado-coches-un-chip-en-un-tiempo/. 29.

<http://www.nytimes.com/2016/07/30/business/tesla-faults-teslas-brakes->

Pero-no-autopilot-en-fatal-accidente.html.

## **Capítulo Doce: El Internet de Vigilancia**

1. 1. <http://www.amazon.com/review/r3imeyjfo6ywhd>.

2. 2. <https://www.blackhat.com/docs/us-14/materials/us-14-jin-smart-nest->

[Termostato-Un-Listo-Espía-En-Vuestro-Casa.Pdf](#).

3. <Http://venturebeat.com/2014/08/10/hola-dave-i-control-vuestro-termostato->

[googles-nido-coge-cortó/](#). 4.

<http://www.forbes.com/sites/kashmirhill/2014/07/16/nest-hack-privacy->

Herramienta/. 5. <http://venturebeat.com/2014/08/10/hello-dave-i-control-your-thermostat->

[googles-Nido-coge-cortó/](#).

6. 6.

[http://www.networkworld.com/article/2909212/security0/schneider-on-](http://www.networkworld.com/article/2909212/security0/schneider-on-Realmente-malo-iot-seguridad-él-s-yendo-a-venir-chocando-abajo.html)

[Realmente-malo-iot-seguridad-él-s-yendo-a-venir-chocando-abajo.html](http://www.networkworld.com/article/2909212/security0/schneider-on-Realmente-malo-iot-seguridad-él-s-yendo-a-venir-chocando-abajo.html).

6. 7. <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/>.

8. <http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html>. 9. <http://www.wired.com/2009/11/baby-monitor/>.

10. <http://www.bbc.com/news/technology-31523497>. 11.

<http://mashable.com/2012/05/29/sensory-galaxy-s-iii/>. 12.

[http://www.forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-](http://www.forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-Él-es-para-google-chrome-a-eavesdrop-encima-vuestro-pc-micrófono/)

[Él-es-para-google-chrome-a-eavesdrop-encima-vuestro-pc-micrófono/](http://www.forbes.com/sites/marcwebertobias/2014/01/26/heres-how-easy-Él-es-para-google-chrome-a-eavesdrop-encima-vuestro-pc-micrófono/). 13.

[http://www.theguardian.com/technology/2015/jun/23/google-](http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-Herramienta-instalado-ordenadores-sin-permiso)

[eavesdropping-Herramienta-instalado-ordenadores-sin-permiso](http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-Herramienta-instalado-ordenadores-sin-permiso). 14. Quizás la manera más fácil es para abrir la aplicación de Eco de la Amazona. Va a vuestros

encuadres, entonces ir a Grifo>de Historia el registro Individual>Elimina.

15. Registro en a vuestra cuenta encima Amazona, entonces de Encuadres “de Cuenta,” el clic en

Vuestro Eco>de Amazona de los Aparatos>Elimina.

16.16.

[http://www.theregister.co.uk/2015/08/24/smart\\_fridge\\_security\\_fubar/](http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/).

17.17. [www.shodan.io](http://www.shodan.io).

## **Capítulo Trece: Cosas Vuestro Jefe no Te Quiere para Saber**

1.

2. 3. 4. 5. 6.

7.

8.

9. 10. 11.

12. 13. 14.

15. 16. 17.

<http://www.wsj.com/articles/sB10001424052702303672404579151440488919138>. <http://theweek.com/articles/564263/rise-workplace-spying>.  
[https://olin.wustl.edu/docs/faculty/pierce\\_cleaning\\_house.pdf](https://olin.wustl.edu/docs/faculty/pierce_cleaning_house.pdf).  
<http://harpers.org/archive/2015/03/the-spy-who-fired-me/>.  
<https://room362.com/post/2016/snagging-creds-from-locked-machines/>.

Normalmente documentar metadata está escondido de vista. Puedes ver el metadata incluido con vuestro documento por clicking Lima>Info, entonces viendo las haciendas en el lado derecho de la ventana. Si utilizas Inspector de Documento, primero hacer una copia de vuestro documento, porque los cambios hicieron no puede ser deshecho. En la copia de vuestro documento original, clic el “tabulador” de Lima, entonces clic “Info.” Debajo “Preparar para Compartir,” Control “de clic para Asuntos,” entonces el clic “Inspecciona Documento.” En la caja de diálogo de Inspector de Documento, seleccionar las cajas de control para el contenido que te quiere ser inspeccionado. El clic “Inspecciona.” Reseña los resultados de la inspección en la caja de diálogo de Inspector de Documento. El clic “Saca Todo” próximo a la inspección results para los tipos de contenido escondido que te quiere sacar de vuestro documento. <http://www.infosecurity-magazine.com/news/printer-related-security-Incumple-afectar-63-de/>.  
<http://www.wired.com/2014/08/gyroscope-listening-hack/>.  
<http://ossmann.blogspot.com/2013/01/funtenna.html>.  
<http://cs229.stanford.edu/proj2013/chavez-reconstructingnon-IntrusivelyCollectedKeystrokeDataUsingCellphoneSensors.Pdf>.  
<http://www.cc.gatech.edu/~traynor/Papeles/traynor-ccs11.Pdf>.  
<http://samy.pl/keysweeper/>. <http://www.wired.com/2015/10/stingray-gobierno-espía-herramientas-lata-récord-llamadas-nuevos-documentos-confirmar/>. <http://phys.org/news/2013-07-femtocell-hackers-isec-smartphone-Contenido.html>. <http://arstechnica.com/information-technology/2015/04/this-machine-Coge-stingrays-pwnie-expresar-demos-celular-amenaza-detector/>.  
<http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-Usuario-datos>. 18. <http://www.computerworld.com/article/2474090/data-privacy/new-snowden-revelation-Espectáculos-skype-poder-ser-intimidad-s-más-grande-enemigo.html>.

19.

20.

21.

conferencing-Y-self-seleccionando-objetivos. 22. Por ejemplo,

<https://www.boxcryptor.com/en>.

<https://community.rapid7.com/community/metasploit/blog/2012/01/23/video>

-

conferencing-Y-self-seleccionando-objetivos.

[http://www.polycom.com/global/documents/solutions/industry\\_solutions/government/](http://www.polycom.com/global/documents/solutions/industry_solutions/government/)

Despliegue-para-máximo-seguridad.Pdf.

<https://community.rapid7.com/community/metasploit/blog/2012/01/23/video>

-

m

## **Capítulo Catorce: Obteniendo el anonimato Es Trabajo duro**

### **1.**

Aquello esto es una búsqueda de borde y el arresto no es realmente pertinente. Cortes de EE.UU. no han resuelto si una persona de interés tiene que dar arriba de sus contraseñas —tan lejos no. Aun así, una corte ha gobernado que una persona de interés puede ser forzada a autenticar suyo o su iPhone por utilizar Tacto ID (huellade dedo). Para eliminar el riesgo, siempre que pasas a través de aduana en cualquier país, reboot vuestro iPhone o cualquiera otro aparato de Manzana con Tacto ID y no puesto en vuestro passcode. Mientras te don't introducir vuestro passcode, Tacto ID fallará. [Http://www.computerweekly.com/articles/2008/03/13/229840/us-Departamento-de-patria-seguridad-controles-más-grandes-nunca-cybersecurity.htm](http://www.computerweekly.com/articles/2008/03/13/229840/us-Departamento-de-patria-seguridad-controles-más-grandes-nunca-cybersecurity.htm). En iOS 8 o versiones más recientes del sistema operativo, puedes reinicialización todas relaciones de emparejamiento por ir a Encuadres>Reinicialización>de Reinicialización>General Location & Intimidad o Red de Reinicialización Encuadres. Investigador Jonathan Zdziarski ha publicado un número de postes de blog en el tema. Las instrucciones son allende el alcance de este libro, pero si eres serio aproximadamente sacando estos, ofrece una manera. Ve

<http://www.zdziarski.com/blog/?p=2589>.

<http://www.engadget.com/2014/10/31/court-rules-touch-id-is-not-Protégido-por-el-quinto-enmienda-bu/>. <http://www.cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-A-pelea-cargo-para-que-da-no-arriba-teléfono-contraseña-en-airport-1.2982236>.

<http://www.ghacks.net/2013/02/07/forensic-tool-to-decrypt-truecrypt-bitlocker-Y-pgp-contiene-y-discos-liberó/>.



[https://www.symantec.com/content/en/us/enterprise/white\\_papers/b-pgp\\_how\\_wholedisk\\_encryption\\_works\\_wp\\_21158817.en-nos.Pdf](https://www.symantec.com/content/en/us/enterprise/white_papers/b-pgp_how_wholedisk_encryption_works_wp_21158817.en-nos.Pdf).  
<http://www.kanguru.com/storage-accessories/kanguru-ss3.shtml>.  
[https://www.schneier.com/blog/archives/2007/11/the\\_strange\\_sto.html](https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html).  
<https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/>.  
<http://www.securityweek.com/researcher-demonstrates-simple-bitlocker-bypass>. <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-Y-público-seguridad-encima-un-colisión-curso>.  
<http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html>.

2. 3.

4. 5.

6. 7.

8.

9. 10. 11.

12.

13. 14.

<https://partners.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html>.

15. <https://www.wired.com/2015/10/cops-dont-need-encryption-backdoor-to-Tajo-iphones/>.

16.16. <http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html>.

16.17. <https://blog.gdatasoftware.com/blog/article/hotel-safes-are-they-really-Seguro.html>.

18. <http://www.snopes.com/crime/warnings/hotelkey.asp>. 19.

<http://www.themarysue.com/hotel-key-myth/>. 20.

<https://shaun.net/posts/whats-contained-in-a-boarding-pass-barcode>.

21.21. Aparentemente Unido es uno de las pocas aerolíneas que sólo da una milla de aviador frecuente parcial número. La mayoría otras aerolíneas ponen el número lleno en el código de barras.

21.22. <http://www.wired.com/2014/11/darkhotel-malware/>.

23. <https://bitlaunder.com/laundry-bitcoin>.

## Capítulo Quince: El FBI Siempre Coge Su Hombre

1. 1. <https://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-> Vida-prisión/.
2. 2. [http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-Agente-quién-puesto-un-cara-encima-el-seda-carretera.html?\\_r=0](http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-Agente-quién-puesto-un-cara-encima-el-seda-carretera.html?_r=0).
3. 3. <http://www.wired.com/2015/07/online-anonymity-box-puts-mile-away-ip-> Alocución/.
4. 4. <https://samy.pl/proxygambit/>.

## Capítulo Dieciséis: Mastering el Arte de Invisibilidad

1. 1. Allí ha más. Incluso aunque el FBI identificó mi complejo de apartamento, no supieron donde era. Aquello cambiado cuándo di un paso exterior una noche. Esta historia puede ser encontrada en mi *Fantasma de libro en los Cables*.
2. 2. A Sitios les gusta Subterráneo de Tiempo puesto la longitud y latitud del visitante en el URL.
3. 3. For Ejemplo, <https://www.bitrefill.com>.
4. 4. <https://nakedsecurity.sophos.com/2015/07/30/websites-can-track-us-by-El-manera-nosotros-tipo-heres-qué-a-parón-lo/>.

## Gracias Para comprar este ebook, publicado por Hachette Digital.

Para recibir ofertas especiales, contenido de bonificación, y noticioso sobre nuestro más tardío ebooks y aplicaciones, signo arriba para nuestro newsletters.

O visitarnos en [hachettebookgroup.com/newsletters](http://hachettebookgroup.com/newsletters)