Michael Dagan

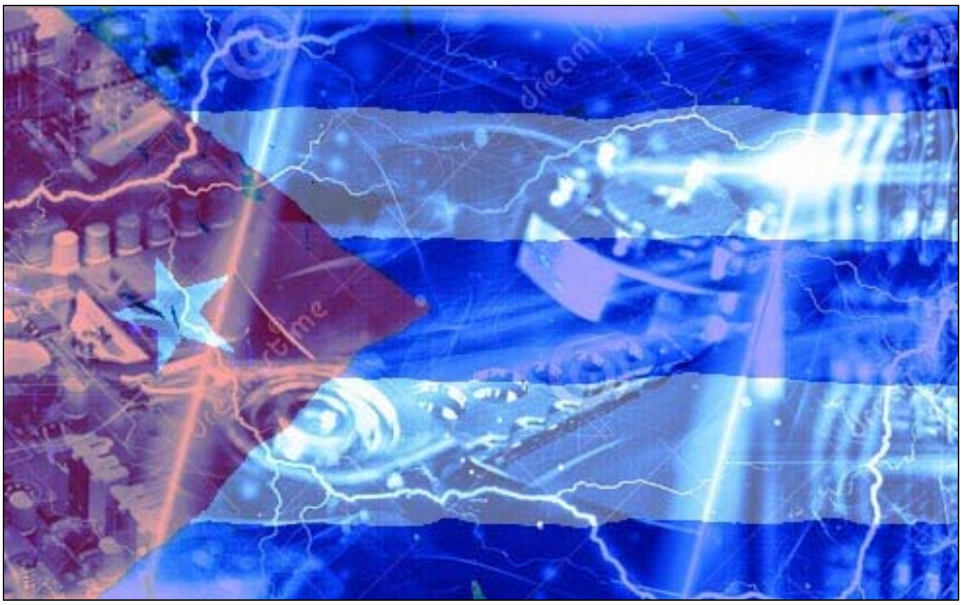
Actualmente, Michael Dagan está en la transición hacia estrategias de contenido y marketing de contenido para pequeñas empresas, después de unos 25 años en puestos de edición senior en el grupo Haaretz, el medio israelí líder. En su último rol, fue editor adjunto de Haaretz, supervisaba y coordinaba todas las operaciones: las ediciones impresas, digitales, en hebreo y en inglés, así como las actividades relacionadas tales como las convenciones.

I. Introducción

Es posible hacer que sea difícil para otra persona tratar de interceptar tus correos electrónicos, los mensajes de texto que envías o tus llamadas telefónicas. Puedes tomar medidas para hacerles la vida más difícil a aquellos que quieren develar tus fuentes y la información que te revelan. Por supuesto, el grado de esfuerzo que estás dispuesto a hacer para proteger tu privacidad, el anonimato de tus fuentes y la seguridad de tus datos, debe ser proporcional a la probabilidad de una amenaza real.

Entonces, ¿qué es lo que se debe hacer para garantizar que las fuentes e información de un periodista estén seguras? A groso modo, los consejos podrían agruparse en las siguientes categorías:

1. **Proteger las aplicaciones y funciones en el dispositivo.** Esto se conoce como reducir la "superficie de ataque", es decir, limitar al máximo las aplicaciones instaladas, usar solo aquellas que sean de fuentes reconocidas, seleccionar aplicaciones que requieran derechos mínimos, mantener el sistema completamente actualizado y con los parches correspondientes, y tener varios controles de seguridad en el dispositivo (según los informes técnicos recientes de mejores prácticas).
2. **Aislar tus dispositivos y/o su entorno**. Por ejemplo, la aislación física de una computadora para revisar archivos, o el uso de dispositivos móviles prepagos.
3. **Actuar con cautela, tanto en el mundo digital como en el real.** Esto tiene mucho que ver con el sentido común y un poco menos con el software. Por ejemplo, nunca escribas el nombre de tu fuente; ciertamente no lo hagas en una aplicación ni en cualquier documento almacenado en tu computadora; y tampoco en nada que esté guardado en la nube.



II. La comunicación con la fuente y el resguardo de los datos confidenciales

Empecemos por enumerar lo que puedes hacer cuando se trata de comunicarte con una fuente y almacenar la información confidencial que obtuviste de ella:

1 - Cuidado con los nombres importantes: Presume que los sistemas de encriptación de las grandes compañías y posiblemente los sistemas operativos más importantes (software patentado) tienen puertas traseras a las que los servicios secretos en sus países de origen pueden acceder. Bruce Schneier, experto en seguridad, lo explica ¨aquí¨

2 - Siempre codificar todo: Los expertos en seguridad utilizan matemática simple para transmitir su mensaje: a medida que aumentas el costo de decodificar tus archivos, automáticamente aumentas el grado de esfuerzo que requiere seguirte. Y si alguien decide seguirte el rastro a pesar de tus esfuerzos, les causará un mayor dolor de cabeza si utilizas codificación fuerte como AES (Advanced Encryption Standard) y herramientas como PGP u OpenVPN, que son los métodos de encriptación más potente disponibles ampliamente. Pero si quieres una seguridad a prueba de balas, necesitarás más que el método de codificación AES.

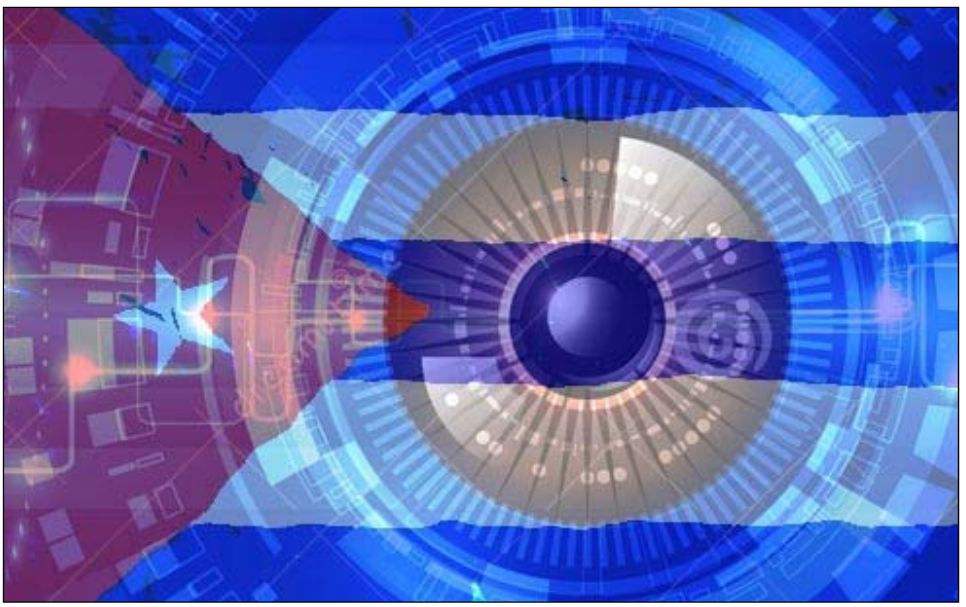
3 - Realizar una codificación del disco entero: Esto se hace por si alguien pone sus manos en tu computadora o teléfono. La codificación del disco entero se puede realizar utilizando FileVault, VeraCrypt, o BitLocker. Poner a “Dormir” una computadora (en lugar de apagarla o ponerla en modo hibernación) puede permitir que un atacante traspase esta defensa. Aquí, Mika Lee te da una guía completa para codificar tu laptop.

4 - No hablar con las fuentes por teléfono: Todas las compañías telefónicas almacenan datos relacionados al número de la persona que llama y de la que recibe la llamada, así como la ubicación de los dispositivos y el horario en que se hicieron las llamadas. En los Estados Unidos y varios otros países, tienen la obligación legal de revelar información sobre las llamadas registradas en su posesión.

¿Qué se puede hacer? Deberías usar un servicio de llamadas seguro, tal como el que posee la aplicación Signal, que fue testeado reiteradamente por seguridad. Aunque esto pueda significar que tanto la fuente como el editor tengan que descargar la aplicación, el proceso toma solo unos minutos. Esta es una guía sobre cómo usarlo.

Solo por diversión, revisa cuántos de tus amigos no periodistas están allí también. Cualquiera sea la manera en que elijas comunicarte con tu fuente, no lleves tu teléfono móvil a reuniones confidenciales. Adquiere un dispositivo descartable y encuentra una manera de transmitirle su número a tu fuente con anticipación. La fuente también debe tener un dispositivo seguro descartable. Las autoridades pueden rastrear tus movimientos a través de las señales de red de celulares y es aconsejable que hagas que sea más difícil para ellos localizarte retroactivamente en el mismo café donde estuvo tu fuente. Si no sigues esta regla,

lo único que deberán hacer las autoridades locales es pedir (cortés y legalmente) el video filmado por la cámara de seguridad de la cafetería en el momento de tu reunión.



5 - Priorizar los mensajeros seguros: Tus llamadas (por celular y líneas hogareñas) pueden ser monitoreadas por agencias del orden público y cada mensaje de texto es como una postal; todo el texto es completamente visible para quienes puedan interceptarlo. Por eso, utiliza mensajeros que permitan una llamada segura de principio a fin: Signal, que ya fue mencionado anteriormente, y Telegram son considerados los más seguros (aunque Telegram así como las aplicaciones web de WhatsApp fueron violentadas una vez y luego reparadas). Según algunos expertos, también puedes considerar el uso de SMSSecure, Threema e incluso WhatsApp.

El Protocolo Signal ha sido implementado en WhatsApp, Facebook Messenger, y Google Allo, para encriptar las conversaciones que se realizan a través de ellos. Sin embargo, a diferencia de Signal y WhatsApp, Google Allo y Facebook Messenger no codifican por defecto, ni notifican a los usuarios que las conversaciones no están encriptadas, pero sí ofrecen codificación de punto a punto de forma opcional.

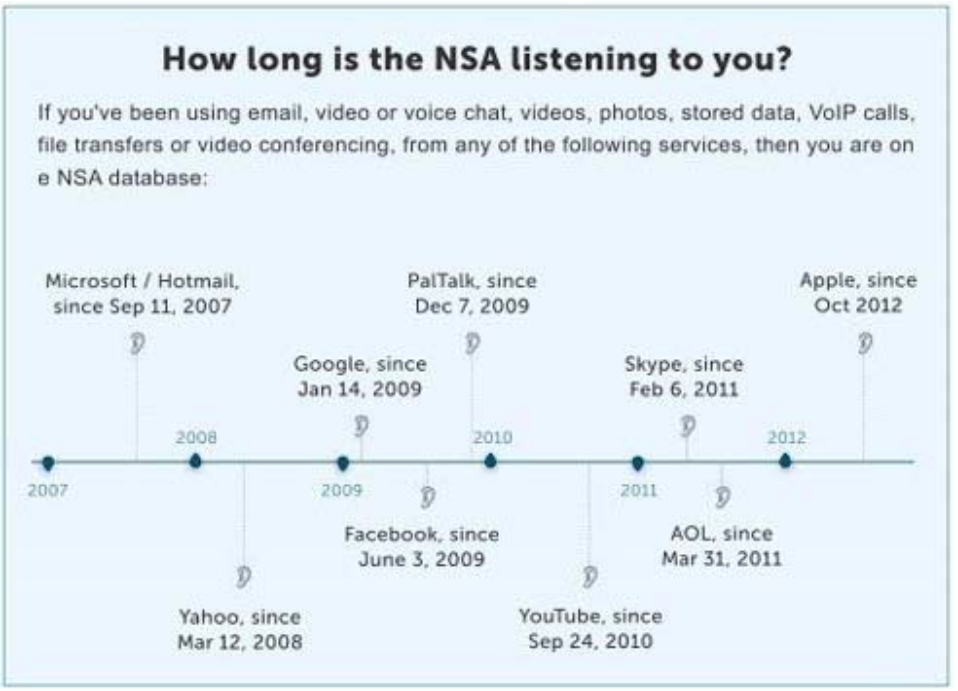
También debes tener en cuenta que tanto Facebook Messenger como WhatsApp son propiedad de Facebook. Adim y Pidgin son los clientes de mensajería instantánea más populares de Mac y Windows que soportan el protocolo de encriptación OTR (Off The Record) y Tor, el navegador web mejor codificado, el cual veremos en detalle más adelante. (Fíjate cómo habilitar Tor en Adium aquí y en Pidgin aquí).

Naturalmente, también podrías usar el mensajero Tor, que probablemente sea el más seguro de todos. Dos avisos finales sobre los mensajes de texto: un experto en seguridad informática con quien hablé de esto dice que debes tener una hipótesis de trabajo que implica que el texto está encriptado, pero el hecho de que estos dos individuos específicos estén hablando, en este momento presente, podría no pasar desapercibido. El segundo aviso es que también debes acordarte de eliminar los mensajes de tu teléfono (aunque esto podría no ser suficiente para pasar una revisión forense), en caso de que tu dispositivo caiga en manos equivocadas, para evitar exponerlos.

6 - No utilizar chats empresariales: Evita utilizar Slac, Campfire, Skype y Google Hangouts para conversaciones privadas. Son fáciles de violentar y están expuestos a solicitudes de divulgación para uso en las cortes de justicia, para resolver problemas en el entorno laboral. Por lo tanto, es mejor evitarlos, no solo cuando se trata de conversaciones con las fuentes, sino también las que mantengas entre colegas, editores, etc., cuando necesites pasar información que recibiste de tu fuente, cuya identidad debe ser resguardada. Muchos servicios de VoIP populares como Jitsi tienen funciones de chat incorporado, y varios de ellos están diseñados para ofrecer la mayoría de las características de Skype, lo cual los convierte en excelentes reemplazos.

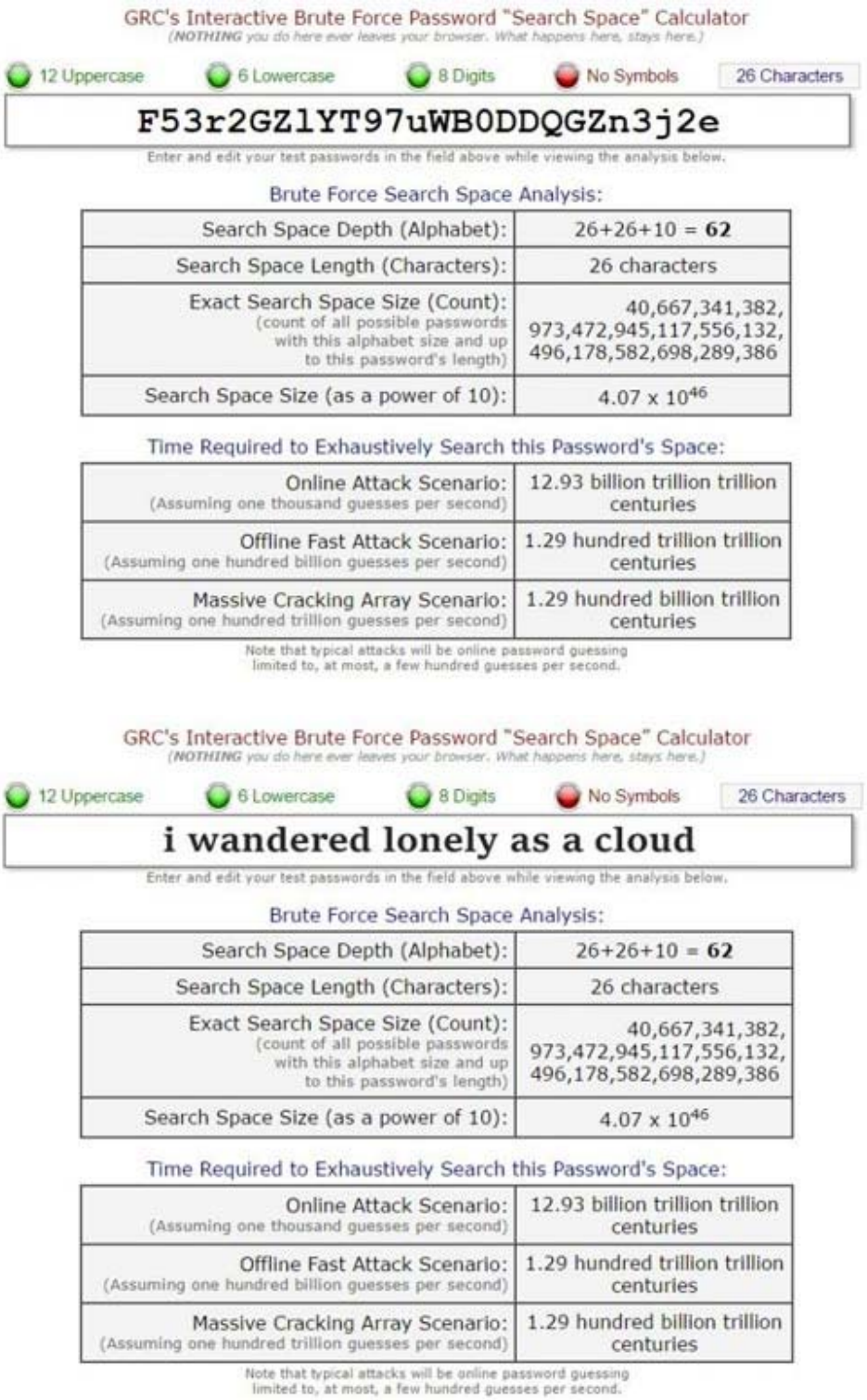
7 - En casos extremos, considera usar un Blackphone: Este teléfono, que se esfuerza

por brindar una protección perfecta para navegar por la web, hacer llamadas, enviar mensajes de texto y correo electrónico, es probablemente el mejor sustituto de un teléfono común si estás a punto de derrocar a tu gobierno o te estás preparando para publicar archivos militares secretos. Un chaleco anti balas también podría serte útil. Por otra parte, intenta lograrlo sin un teléfono celular, o elige un bolso con bloqueo de señal RFID. Siempre existe la opción de que hasta el Blackphone pueda ser rastreado utilizando su IMEI (la identidad del teléfono móvil).



8 - Protege los datos en tu computadora: es muy sencillo decodificar contraseñas normales, pero puede llevar años decodificar frases codificadas, es decir, combinaciones aleatorias de palabras. Te recomendamos que pruebes con herramientas de gestión de contraseñas seguras como: LastPass, 1Password y KeePassX. Solo tendrás que recordar una contraseña, en lugar de muchas. Y aun así, cuando manejes servicios importantes como tu correo electrónico, no dependas de los administradores de contraseñas; asegúrate de recordarla. En una entrevista con Alastair Reid en journalism.co.uk, Arjen Kamphuis, un experto en seguridad de la información recomendó que para los discos duros encriptados, los correos electrónicos seguros y desbloquear laptops, uno debe elegir una contraseña de más de 20 caracteres. Por supuesto, cuando más larga sea la contraseña, más difícil será violentarla, pero también más difícil de recordar.

Por eso él recomienda el uso de una frase. “Puede ser cualquier cosa, como una frase de tu poesía favorita”, dice Kamphuis. “Quizá una frase de algo que escribiste cuando tenías nueve años y que nadie más sabrá”. Reid informa este cálculo provocador, utilizando la calculadora de fortaleza de contraseña de la Gibson Research Corporation: una contraseña como “F53r2GZlYT97uWB0DDQGZn3j2e” de un generador cualquiera de contraseñas, parece muy fuerte, y ciertamente lo es, ya que toma 1,29 cientos de billones de trillones de siglos agotar todas las combinaciones, incluso cuando el programa hace cien billones de cálculos por segundo.



GRC's Interactive Brute Force Password "Search Space" Calculator

(NOTHING you do here ever leaves your browser. What happens here, stays here.)

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

F53r2GZlYT97uWB0DDQGZn3j2e

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

(NOTHING you do here ever leaves your browser. What happens here, stays here.)

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

i wandered lonely as a cloud

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Capturas de pantalla de GRC.com que muestran la diferencia de fortaleza entre una contraseña y una frase de contraseña

La frase: “me paseaba solitario como una nube”, dice, es mucho más fácil de recordar y también mucho más segura, ya que le toma al mismo programa 1.24 cientos de trillones de siglos agotar todas las posibilidades. Bien, entonces usaremos las frases de contraseña.

9 - La doble autenticación también es una buena idea: En una autenticación normal de dos niveles, ingresas con tu contraseña y recibes un segundo código, a menudo a través de mensajes de texto en tu teléfono inteligente. Puedes usar Yubikey, así como identificadores en hardware para proteger aún más los archivos confidenciales en tu computadora. Para

más información, lee las 7 reglas de oro para la seguridad de contraseñas.

10 - Asignar una computadora para inspeccionar archivos o adjuntos sospechosos: La manera más fácil de distribuir software malicioso y espía es a través de la instalación mediante USB o por adjuntos y enlaces en correos electrónicos. Por eso se recomienda que utilices una computadora con espacio de aire (o air-gapped) para examinar estas amenazas en un entorno de cuarentena. Con esta computadora, puedes usar un USB libremente y descargar archivos de internet, pero no los transfieras a tu computadora habitual ni vuelvas a utilizar ese USB.

11- Cómo comprar tu propia computadora protegida: el experto en seguridad, Arjen Kamphuis recomienda adquirir un ThinkPad X60 o X61 de IBM anterior a 2009. Estas son las únicas laptops suficientemente modernas con sistemas de software actuales que permiten reemplazar los programas de nivel bajo. Otro punto a tener en cuenta es que no debes adquirir tu computadora en línea, ya que puede ser interceptada durante el envío. Kamphuis recomienda que la compres de una tienda de segunda mano y en efectivo. También señala que debes eliminar toda la conectividad: quita todas funciones de Ethernet, módem, Wi-Fi o Bluetooth. Personalmente, sé que los expertos en seguridad no confiarían en una computadora como esa.

ThinkPad X60. No la compres en línea.

12 - Concientiza a tus fuentes: Es posible que para cuando te llegue la información original y valiosa, ya sea demasiado tarde. Quizás tu fuente cometió todos los errores posibles, dejando un rastro de evidencia. Pero más allá de la necesidad de proteger la información una vez que está en tus manos, deberías esforzarte por enseñarles a tus fuentes cómo ocultar esos datos: almacénalos en un lugar protegido y comunícate de forma segura a través de dispositivos seguros. La mayoría de las personas no tienen idea de cómo manejar información confidencial, y en general, lo que enfrentan cuando se ponen en contacto contigo.

13 - Utiliza un sistema dedicado seguro para recibir documentos: Reemplaza Dropbox o Google Drive y usa algo menos popular pero más seguro. Por ejemplo, SecureDrop es un sistema designado que te permite recibir archivos de fuentes anónimas y escanearlos y revisarlos de forma segura. Edward Snowden describió a Dropbox como "hostil para la privacidad", y recomendó Spideroak en su lugar. OnionShare es otro servicio gratuito que permite transferir archivos fácilmente y en forma anónima.

How secure is cloud storage?

Most of the big providers of cloud storage - Amazon, Dropbox, Apple, Google, and Microsoft - have collaborated with the NSA at some point in the past. Most reserve the right to investigate all uploaded files, and will hand over the files to authorities when served a court order. There are still several things you can do about that:

1. Try to limit the number of files you upload to the cloud, and always encrypt them using strong encryption. The most secure and simple method is to manually encrypt the files, in which case you can use all Cloud storage services. Don't forget though: Do not upload your encryption keys to the cloud along with your files.

2. Use cloud services that automate encryption before uploading files, and sync everything with local versions. The provider might have the decryption key, but data risk is not as high as is the case with other Cloud providers. SpiderOak, which I've mentioned earlier, has apps for Android and iOS.

3. **Cloudless** Syncing with BitTorrent Sync - this it is not a true Cloud-based service, and cannot be used to store data for long periods of time, but BitTorrent Sync is free, and designed to be a replacement for Dropbox. All you need is to select the files, then you get a password and able to link that folder to another device's folder (if BitTorrent Sync is installed on it).

14 - No hacer anotaciones: Ni en una laptop, ni en calendarios, ni en listas de contactos en tu teléfono celular, ni en la computadora ni en la nube—no guardes registros del nombre de tu fuente, sus iniciales, número de teléfono, correo electrónico o nombre de usuario en los programas de mensajería. Simplemente no lo hagas.

15 - Registro visual: En tu camino hacia una reunión confidencial, evita usar el transporte público y guía a tu fuente para que haga lo mismo. También deberías evitar lugares de reunión como centros comerciales modernos, donde las cámaras de video están por todas partes.

16 - Evadir las redes sociales: Algunas personas prefieren optar por un anonimato radical. Si por alguna razón necesitas desaparecer de la faz de la Tierra sin dejar un perfil totalmente completo en cada red social, debes eliminar tus cuentas en su totalidad. Es diferente a "desactivarlas", un estado en el cual toda tu información está almacenada y puede ser reactivada.

17 - Hazte amigo de los hackers: Esto te ayudará a evitar grandes errores, ahorrarte tiempo y dolores de cabeza, y te mantendrá actualizado respecto a la carrera armamentista tecnológica.

18 - Método de pago: Paga todo en efectivo, considera usar Bitcoins –cómpralos en forma anónima (utiliza esta guía de Business Insider para ese fin)—y, si tienes a alguien que está dispuesto a aceptarlos en el otro extremo de la transacción, utiliza Darkcoin. Una tarjeta de crédito prepaga de una tienda en línea también es una buena opción.

19 - Anota sabiamente: Si escribiste información en un trozo de papel, lo que se llamaba una nota en el mundo precámbrico, destrúyelo. Y no te olvides siquiera de ese papel arrugado en el fondo de tu bolsillo. Sí, el que está junto al chicle.

III. Cómo hacerte anónimo en internet

Además de proteger las comunicaciones con tu fuente, y protegerte de la posible filtración de los datos confidenciales que consigues, debes evitar que te registren mientras navegas. Los hábitos en línea pueden revelar o brindar pistas sobre la historia en la que estás trabajando, o lo que es peor, dar pistas o revelar la identidad de tu fuente. Estas son las reglas de oro para navegar por internet en forma segura y luego, en el próximo capítulo, para proteger tu cuenta de correo electrónico:

1 - Modo de navegación privada: Hay dos maneras básicas de mantener el anonimato mientras navegas por la web. La primera forma, más básica y popular, aunque insuficiente, es navegar por la información en modo privado, una opción que la mayoría de los navegadores ofrece. Tu historial de navegación no se guardará, y las tecnologías básicas de

rastreo que utilizan los anunciantes, como las cookies HTTP, no podrán crear tu perfil detallado. Pero esta es una manera más amable de tener privacidad: básicamente oculta tu historial de navegación de los miembros de tu familia que puedan acceder a tu computadora. Tu dirección IP puede seguir siendo monitoreada y la información respecto a todos los sitios que visitaste sigue expuesta a tu proveedor de internet.

2 - Utiliza navegadores alternativos: Los navegadores como Dooble, Comodo Dragon, o SRWare Iron, que se concentran en la privacidad del usuario, tienen capacidades limitadas. Puedes lograr un nivel similar de privacidad al que ofrecen estos navegadores con solo borrar las cookies, trocitos de código que se han descargado a tu sistema desde los sitios web que visitas y que monitorean tu actividad, y a veces incluso siguen qué contenido consumes. Otra forma de mantenerte anónimo es neutralizando los ajustes de ubicación de tu navegador, e instalando varias funciones que apuntan a lograr el anonimato. Para revisar si desactivaste toda las cookies efectivamente, puedes usar la aplicación CCleaner, que también se encarga de las cookies Flash, pero ninguno de estos navegadores está totalmente codificado. El único navegador estándar que garantiza privacidad total es el Navegador Tor. Tor es feo y lento, pero te protegerá a ti y a tus fuentes. La siguiente sección te dará una descripción más detallada sobre él.

3 - TOR: Este navegador "notorio", que fue desarrollado por la Marina de los Estados Unidos, te permite operar en una red oculta, realizar comunicaciones privadas y establecer sitios web de forma anónima.

El navegador Tor, que se puede descargar en Torproject.org, hace que sea muy difícil monitorear tus actividades en línea, o que el gobierno o tu proveedor de internet conozcan tu ubicación. La única desventaja es que a veces es lento, un poco engorroso; pero es solo porque Tor te guía a través de tres relés encriptados aleatorios en el mundo, antes de llevarte a tu sitio web de destino. También debes tener en cuenta que tus vecinos pueden ser personajes oscuros.

Otra opción relacionada a Tor es descargar Whonix, un sistema operativo seguro que se centra en la privacidad. Funciona como puerta de acceso a Tor, y permite únicamente conexiones con sitios y usuarios de Tor.

Pero el sistema operativo para Tor más popular es Tails (por su nombre en inglés, The Amnesiac Incognito Live System). Tails se puede arrancar desde un dispositivo USB o DVD, y hace toda la información anónima. Edward Snowden es considerado un fanático de este programa. Qubes es otro sistema operativo que soporta Whonix, y es recomendado por Snowden.

4 - Motores de búsqueda alternativos: Google, el motor de búsqueda más usado, guarda tu historial de búsquedas para optimizar los resultados. Para detener esta personalización, debes hacer clic en Herramientas de búsqueda > Todos los resultados > Verbatim. O ingresa a tu cuenta de Google en www.google.com/history, encuentra una lista de tus búsquedas anteriores y selecciona los ítems que quieras eliminar haciendo clic en el botón "eliminar ítems".

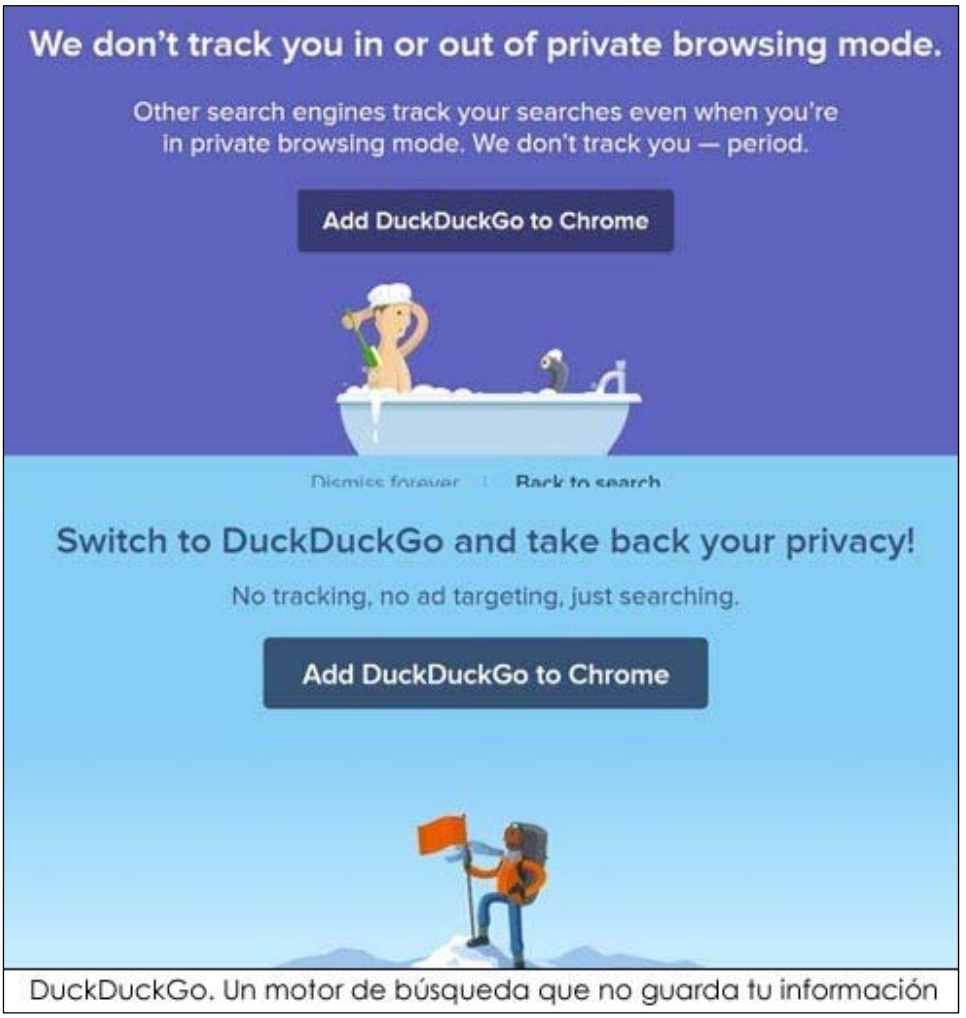
Pero para evitar totalmente que te monitoreen, es preferible usar un motor de búsqueda como DuckDuckGo. Si se te hace difícil abandonar a Google, descarga Searchlinkfix para al menos mantener alejados a los Rastreadores de URL.

5 - Tratamiento directo de la memoria informática de "corto plazo": Otra manera de neutralizar las opciones de monitoreo de tu navegación es eliminar el caché de DNS (sistema de nombre de dominio). La eliminación se realiza utilizando comandos simples en el sistema operativo. Reiniciar el rúter –que a veces tiene una memoria caché de DNS—o la computadora también puede reiniciar los respectivos caché de DNS, si el rúter tiene uno.

6 - Intenta evitar el almacenamiento web HTML: El almacenamiento web está integrado en HTML5, y a diferencia de las cookies, la información guardada no se puede monitorear ni eliminar selectivamente. El almacenamiento web está habilitado de forma predeterminada, así que si estás usando Internet Explorer o Firefox, simplemente puedes apagarlo. También puedes usar el complemento Better Privacy para Firefox para eliminar la información que se guarda automáticamente. La extensión Click and Clean hace el mismo trabajo pero en Google Chrome.

7 - Utiliza una VPN: Como ya mencioné antes, tu proveedor de internet puede monitorear

los sitios que navegas, y cualquiera que desee espiarte puede interceptar tus comunicaciones. Para proteger todas las comunicaciones entrantes y salientes, es importante usar una VPN (para una explicación completa, haz clic aquí). Una VPN encripta todas tus comunicaciones, de forma que ni el proveedor de internet, ni los servicios secretos, ni los hackers que merodean en el Wi-Fi de tu cafetería favorita podrán saber a quién le enviaste un correo electrónico, qué servicios usaste, etc.



El uso de una VPN es muy común entre personas que, por ejemplo, desean ver el catálogo completo de películas de Netflix desde fuera de los Estados Unidos, pero no todas las VPN son aptas para periodistas. Una VPN para periodistas no necesariamente será la más rápida o tendrá el mejor soporte técnico, pero tiene que ser confiable y no guardar registros, es decir, que no pueda determinar quién eres, qué sitios has visitado, y demás. Una VPN segura debe ser provista por una empresa que no esté ubicada en alguno de los países de los "14 ojos", donde redes de inteligencia tienen permitido recolectar y compartir información entre ellos.

Sus cortes no entregan fácilmente órdenes para divulgar información recolectada por empresas locales, ya sea que se relacione con sus ciudadanos o con extranjeros.

Aquí encontrarás una lista de 5 servicios de VPN que se destacan en términos de privacidad y que están ubicados fuera de los países de los "14 ojos". Por cierto, incluso si los gobiernos están a la caza de tráfico que esté oculto en una VPN, puedes utilizar VPN discretas como TorGuard para enfrentar el desafío, ya sea la censura activa del gobierno o si espían lo que tú estás haciendo. Tor y las VPN te dan la protección perfecta en caso de que alguien intente recuperar tu historial de navegación para crear tu perfil.

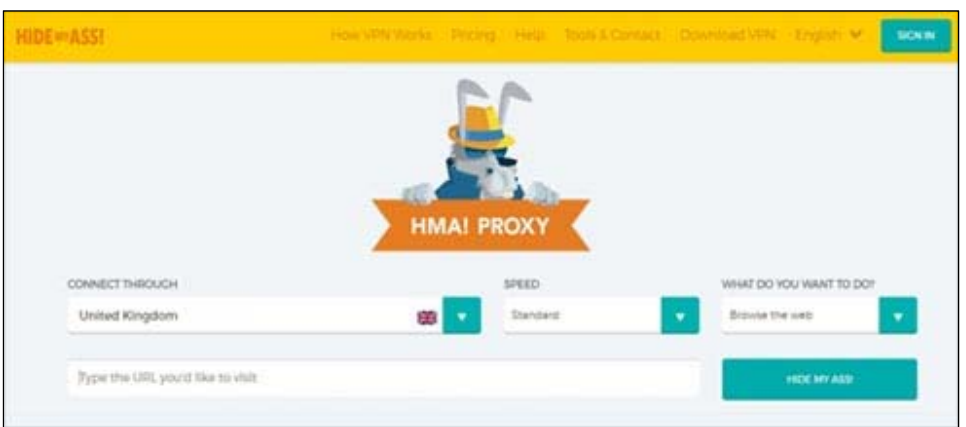
Some tips from Edward Snowden

Adapted from an interview to Micah Lee on the Intercept

1. Encrypt your phone calls and text messages. You can do that with Signal, which is easy to use.
2. Encrypt your hard disk, so that if your computer is stolen, the information isn't retrievable.
3. Use a password manager. One of the main things that gets people's private information exposed are data dumps. Your credentials may be revealed because some service you stopped using in 2007 gets hacked, and the password also works for your Gmail account. A password manager allows you to create unique passwords for every site that are unbreakable, but you don't have the burden of memorizing them.
4. Use two-factor authentication, so if someone does steal your password, it allows the provider to send you a secondary means of authentication.
5. In every step, you have to stop and think, "What would be the impact if my adversary were aware of my actions?" If the answer is making you nervous, change or refrain from that activity, and try to mitigate that through some tools or system to protect the information and reduce the risk, or ultimately, accept the risk of discovery and plan your response. You can't always keep something secret, but you can definitely plan your response.
6. Selective sharing - don't spray your personal info everywhere.
7. Use ad blockers. Service providers are serving ads with active content that can be a vector for attack in your web browser — you should be actively trying to block these.
8. And finally, a quick guide for the whistleblower:
a. Tell no one who doesn't need to know about the wrongdoing you've uncovered.

8 - Reparar filtraciones de DNS: Utilizar una VPN no te protege completamente, porque ese tráfico de DNS puede dar pistas de tu identidad. DNSLeakTest.com te permitirá detectar una filtración. Si el test muestra que el DNS es de tu VPN, puedes relajarte, pero si muestra que es de tu proveedor de internet, no estás en el anonimato. En este caso,mira aquí lo que puedes hacer.

9 - Máquinas virtuales. Este truco ingenioso es en realidad una segunda computadora (virtual), que opera como una aplicación en tu sistema operativo. Puedes descargar archivos o abrir enlaces de forma similar a la computadora aislada que recomendé antes, para que tu computadora esté menos expuesta a software malicioso o espía de cualquier tipo. Los programas de virtualización, como VirtualBox, se deben abrir utilizando un sistema operativo seguro. La descarga de archivos se realiza con la conexión a internet de la máquina virtual deshabilitada; después de usar el archivo, debes eliminarlo; y dependiendo de tu adversario, quizás eliminar también la máquina.



Servidor proxy HideMyAss. Ocultaré el tuyo si ocultas el mío

10 - Servidor proxy: Similar al caso de las máquinas virtuales, aquí la actividad también se muda a otra "área" y te permite mantenerte a salvo de los espías y otros ataques. En realidad, los servidores proxy sustituyen tu dirección IP con las suyas propias, lo cual puede llevar a las personas a pensar que estás en un país diferente, por ejemplo.HideMyAss.com/proxy, Psiphon (de código abierto) y JonDonym brindan un servicio

similar.

Algunos expertos afirman que estos se deben usar junto con una VPN y/o con Tor para tener niveles mayores de seguridad. Pero luego, otros expertos con los que he hablado afirman que si te molestas en usar Tor, estás tan seguro como cualquier puede estarlo.

11 - Tres tipos más de extensiones que aumentan tu nivel de seguridad: Para verificar que el protocolo de internet donde operas es seguro para https, puedes instalar una extensión llamada HTTPS Everywhere, creada por la Electronic Frontier Foundation (EFF), una de las organizaciones que financia el proyecto Tor.

Esta extensión es recomendada por muchos expertos en informática; garantiza que los sitios web que visites utilicen el protocolo seguro, lo cual definitivamente no es una política de seguro contra nada, pero es mejor que el protocolo sin codificación. El segundo tipo de extensión controla los datos que revela javaScript a los sitios web (para mejorar tu experiencia de navegación).

Dos opciones populares son ScriptSafe y NoScript. Otra extensión es el navegador Ghostery. Esta extensión revela quién te rastrea entre 2000 empresas, y te permitirá bloquear las no deseadas. Es genial, pero probablemente no querrás bloquear a la NSA de esta manera.

Privacy badger, un proyecto de la EFF, también funciona de forma similar.

Anti-Malware, Antivirus and Firewall Software

Anti-Malware - There is a massive amount of malicious code, known as Malware, on the internet. Bitdefender comes installed on all versions of Windows newer than Vista. There are also Malwarebytes and Spybot Search and Destroy, that are both free.

Antivirus - After buying a new computer or a clean install of an operating system, this should be the first program you will install. Viruses can not only mess up your computer, but help steal all information processed through it. Most people do have antivirus software installed on their computers, but not on their smartphones. Phones with open-source systems, such as Android phones, are more susceptible than those with closed-source systems, such as iOS (Apple) phones, to mobile viruses.

Firewall - A firewall ensures that no software is accessing your computer. Their drawback is that they have a hard time determining which programs are safe.

IV. Proteger tu correo electrónico

¿Cómo deberías proteger tu correo electrónico? El problema de mantener la confidencialidad de los correos es aún más difícil. Google y Microsoft probablemente le darán tus correos electrónicos a las agencias gubernamentales cuando estas los soliciten. ¿Qué deberías hacer?

1 - Extensiones seguras: La opción más simple, asumiendo que utilizas servicios de correo web comunes como Yahoo y Google, es instalar el complemento Mailvelope en el navegador, y asegurarte de que la persona en el otro extremo del intercambio también lo haga. Esta extensión simplemente codifica (y decodifica) el correo electrónico.

Una extensión similar pero limitada de Gmail llamada SecureGmail realiza una función parecida. Los correos electrónicos que pasan por esta extensión son encriptados, y no pueden ser decodificados por Google.

Otra posibilidad es "Encrypted Communication", y se trata de una extensión de Firefox fácil de usar. Para ello necesitarás una contraseña a la que tendrá acceso el receptor, pero recuerda nunca transmitir la contraseña por correo electrónico.

2 - Proveedores de correo electrónico seguro: Hushmail es un ejemplo de un servicio de correo electrónico que brinda mejor seguridad que las redes más comunes que utilizas, pero puede que los obliguen a entregar los correos al gobierno de los Estados Unidos bajo una orden judicial, y sí guarda las direcciones IP.

Otro servicio de correo electrónico con características y niveles de seguridad similares es Kolab Now, que se enorgullece de almacenar datos exclusivamente en Suiza, entre otras cosas.

3 - Direcciones de Correo Electrónico descartables (DEA, por su sigla en inglés): Se trata de un correo electrónico creado ad hoc para un propósito específico, que es completamente anónimo y se borra inmediatamente después de utilizarlo. Esta solución, comúnmente utilizada cuando uno se inscribe en varios servicios con el fin de evitar el spam, también es una excelente opción para mantener el anonimato. Sin embargo, no les recomendaría a los periodistas comunicarse con sus fuentes a través de ellos, porque la seguridad no es su característica más fuerte.

Hay docenas de este tipo de correos electrónicos temporarios, pero el British Guardian, por ejemplo, recomendó Guerrilla Mail y Mailinator. Usar Guerrilla Mail en el navegador Tor garantiza que ni siquiera ellos puedan conectar tu IP con tu dirección de correo electrónico. De la misma manera, si usas un programa de codificación de correos, como GnuPG, en Tor estás listo y protegido. Ahora, hablemos un poco sobre la codificación del correo electrónico.

4 - Codificar tu correo: Wired obtuvo esta recomendación de Micah Lee, un tecnólogo enfocado en la privacidad que trabajó con EFF y First Look Media (esta es una entrevista que Lee tuvo con Edward Snowden, en inglés): Codificar mensajes con webmail puede ser difícil. A menudo requiere que el usuario copie y pegue mensajes en ventanas de texto y luego utilice PGP para codificar y decodificarlos (PGP – Pretty Good Privacy – es un programa de encriptación que brinda privacidad criptográfica y autenticación para la comunicación de datos).

Por eso Lee sugiere una configuración de correo diferente, utilizando un alojamiento de correo electrónico centrado en la privacidad como Riseup.net, la aplicación de correo electrónico de Mozilla, Thunderbird; el plugin de codificación Enigmail, y otro plugin llamado TorBirdy que dirige los mensajes a través de Tor.

Como señaló Reid en su entrevista con Kamphuis en journalism.co.uk, Greenwald casi pierde la historia de la NSA porque inicialmente ignoró las instrucciones de Snowden sobre encriptación del correo electrónico.

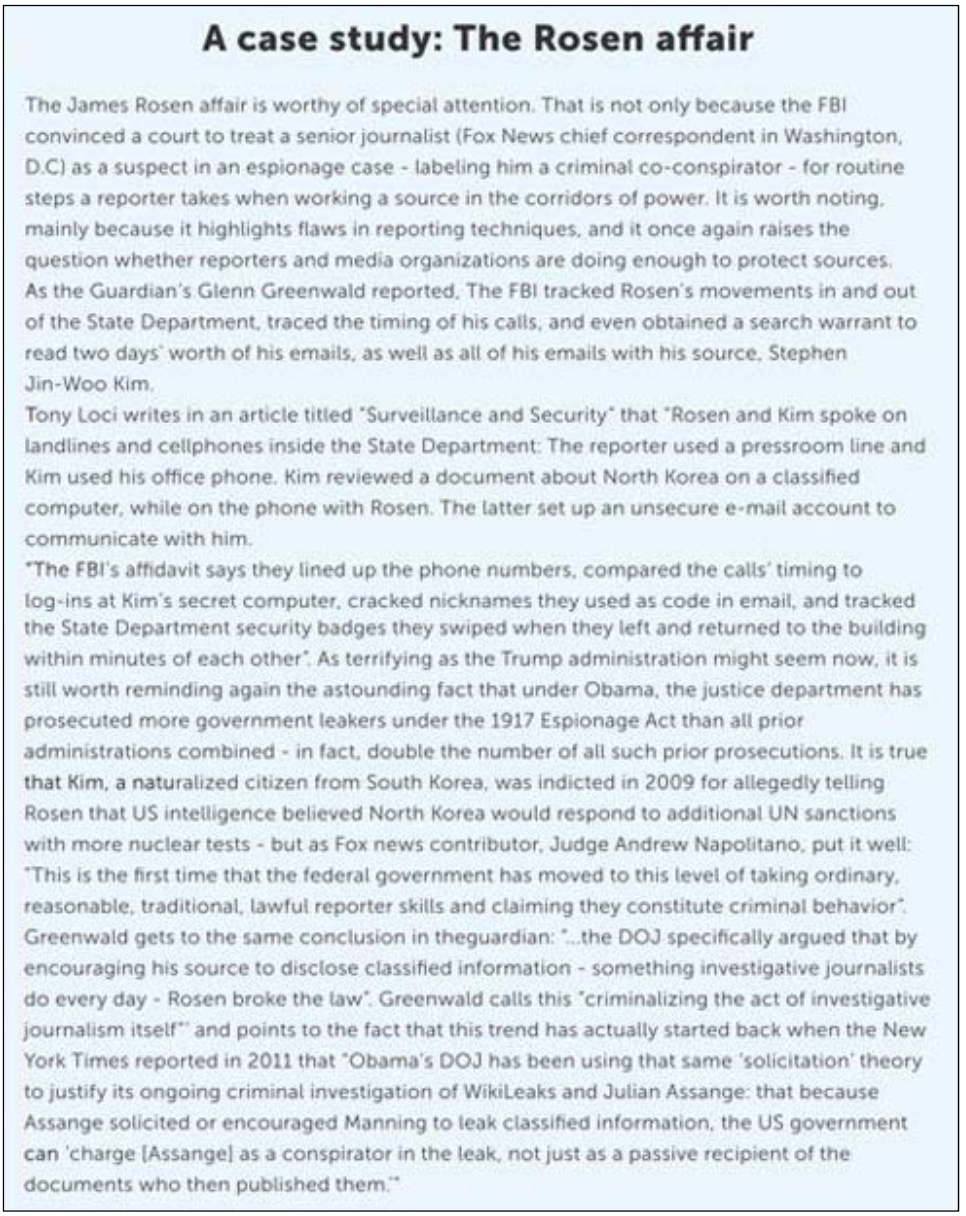
En otras palabras, si quieres que una noticia que haga historia, tiene sentido estar seguro. Kamphuis afirma que se puede confiar en PGP. Como él y Reid explican, con la codificación de PGP, tienes una clave pública, como tu número público de teléfono, y una clave privada. La clave pública puede ir en la biografía de Twitter, en tarjetas personales, en sitios web y donde publiques tu trabajo; pero la clave privada debe ser guardada en forma segura, como cualquier otra información confidencial. Luego, cuando una fuente quiere enviarte información, utilizará tu clave pública para encriptar su correo electrónico, que solo una clave privada puede desbloquear.

Kamphuis recomendó el GNU Privacy Guard, una versión de PGP de código abierto que es simple de configurar y tiene una comunidad de soporte activa. Para codificar archivos, datos y discos rígidos, él sugiere consultar su eBook gratuito, “Seguridad de la Información para Periodistas”, publicado con Silkie Carlo y lanzado a través de CIJ, lo cual explica por completo el proceso.

Si eliges codificar el mensaje en sí mismo sin importar la identidad de tu proveedor de correo electrónico, es una buena idea usar un zip con contraseña, y 7ZIP es una herramienta recomendada para lograrlo.

4 - Volver a las bases: Sí, sé que esto es volver a los conceptos básicos de seguridad del correo electrónico, pero por favor intenta evitar el phising. Mira el campo de “remitente” en tu correo y busca errores de escritura; alguien podría querer hacerse pasar por otra persona que conoces. Y una última palabra sobre la encriptación de correos: uno de los problemas reales a tener en cuenta es que incluso después de codificarlos, no todo está codificado. Las direcciones de correo de quien envía y del receptor, el asunto y la fecha y hora en que fue enviado el correo electrónico, todo eso queda descubierto. Los adjuntos y el mensaje en sí

son los únicos datos encriptados.



A case study: The Rosen affair

The James Rosen affair is worthy of special attention. That is not only because the FBI convinced a court to treat a senior journalist (Fox News chief correspondent in Washington, D.C) as a suspect in an espionage case - labeling him a criminal co-conspirator - for routine steps a reporter takes when working a source in the corridors of power. It is worth noting, mainly because it highlights flaws in reporting techniques, and it once again raises the question whether reporters and media organizations are doing enough to protect sources. As the Guardian's Glenn Greenwald reported, The FBI tracked Rosen's movements in and out of the State Department, traced the timing of his calls, and even obtained a search warrant to read two days' worth of his emails, as well as all of his emails with his source, Stephen Jin-Woo Kim.

Tony Loci writes in an article titled "Surveillance and Security" that "Rosen and Kim spoke on landlines and cellphones inside the State Department: The reporter used a pressroom line and Kim used his office phone. Kim reviewed a document about North Korea on a classified computer, while on the phone with Rosen. The latter set up an unsecure e-mail account to communicate with him.

"The FBI's affidavit says they lined up the phone numbers, compared the calls' timing to log-ins at Kim's secret computer, cracked nicknames they used as code in email, and tracked the State Department security badges they swiped when they left and returned to the building within minutes of each other". As terrifying as the Trump administration might seem now, it is still worth reminding again the astounding fact that under Obama, the justice department has prosecuted more government leakers under the 1917 Espionage Act than all prior administrations combined - in fact, double the number of all such prior prosecutions. It is true that Kim, a naturalized citizen from South Korea, was indicted in 2009 for allegedly telling Rosen that US intelligence believed North Korea would respond to additional UN sanctions with more nuclear tests - but as Fox news contributor, Judge Andrew Napolitano, put it well: "This is the first time that the federal government has moved to this level of taking ordinary, reasonable, traditional, lawful reporter skills and claiming they constitute criminal behavior". Greenwald gets to the same conclusion in theguardian: "...the DOJ specifically argued that by encouraging his source to disclose classified information - something investigative journalists do every day - Rosen broke the law". Greenwald calls this "criminalizing the act of investigative journalism itself"' and points to the fact that this trend has actually started back when the New York Times reported in 2011 that "Obama's DOJ has been using that same 'solicitation' theory to justify its ongoing criminal investigation of WikiLeaks and Julian Assange: that because Assange solicited or encouraged Manning to leak classified information, the US government can 'charge [Assange] as a conspirator in the leak, not just as a passive recipient of the documents who then published them.'"

V. Palabras finales

Estos son quizás los consejos más radicales que encontré cuando preparaba este eBook.

Como dijo Micah Lee cuando lo entrevistaron sobre la privacidad en WIRED: si te hackean la computadora, se terminó el juego. Crear un sandbox virtual para tus comunicaciones en línea es una buena manera de mantener el resto de tu sistema protegido. Tor es genial y puede guardar tu anonimato. Pero si el otro extremo de la comunicación está en peligro, también lo está tu anonimato. Si realmente necesitas permanecer anónimo, también tienes que estar muy protegido".

Y la periodista Tony Loci lo dice con palabras aún más duras en un artículo publicado en un eBook sobre el futuro del periodismo de investigación transfronterizo para la fundación Nieman de Harvard: "Algunos periodistas, científicos informáticos y defensores de la privacidad están tan alarmados que recomiendan que los reporteros hagan las cosas a la vieja escuela… y que se basen en entrevistas cara a cara y correo postal".

Espero haber ayudado a las personas de este ámbito y de otros a reunir información que clarifique qué se puede y qué se debe hacer para garantizar tu seguridad y la de tu fuente en

estos tiempos turbulentos.

VI. List of Sources for This Book

Seguridad para periodistas: Cómo mantener seguros a tus fuentes y tu información

Proteger los datos, las fuentes y a ti mismo

Vigilancia y Seguridad: Los reporteros y las agencias de noticias, ¿están haciendo lo suficiente para proteger a las fuentes?

El periodismo de investigación se hace global: El futuro del periodismo investigativo transfronterizo

La guía más completa para la privacidad en internet

¿Qué es el Caché de DNS?

Cómo convertir en anónimo todo lo que haces en línea

19 formas de mantenerte anónimo y proteger tu privacidad en línea

Edward Snowden explica cómo recuperar tu privacidad

Seguridad de la información para periodistas: mantenerte seguro en internet

NSA apunta a quienes se preocupan por la privacidad

El Departamento de Justicia de Obama acusa formalmente al periodista en caso de filtración de cometer delitos

Tus secretos de WhatsApp ahora están seguros. Pero Gran Hermano sigue observándote…

Obama persigue a quienes filtran información y envía una señal a los informantes

6 errores de encriptación que conducen a la filtración de datos