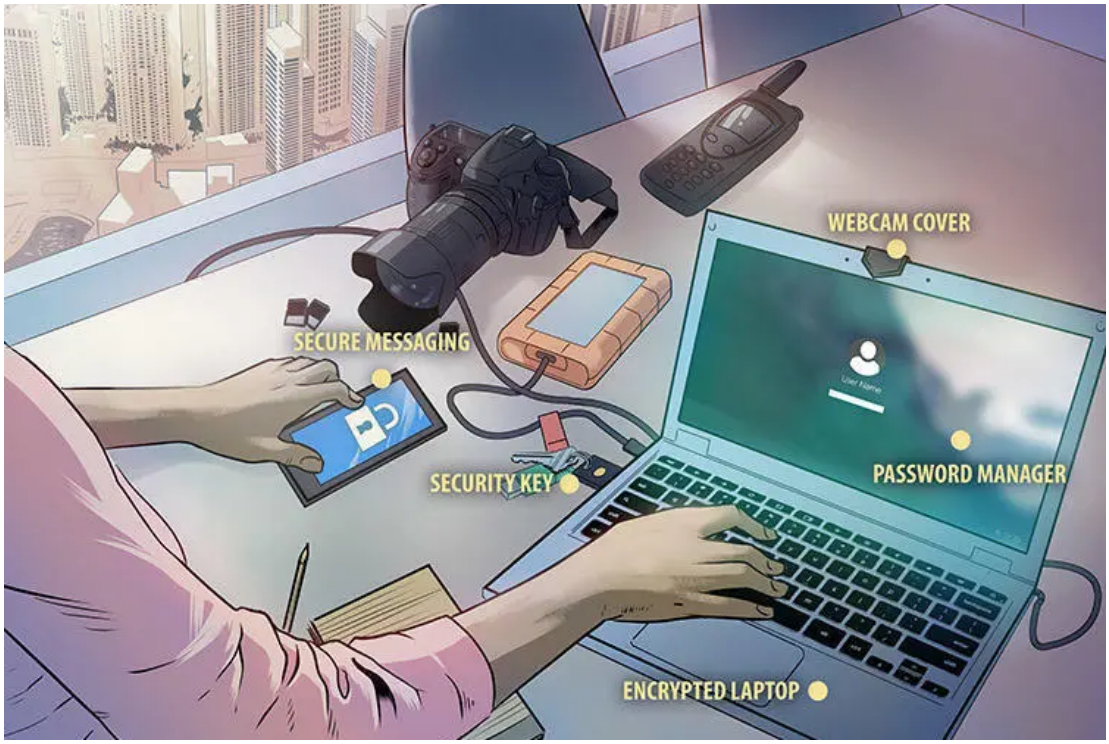

Martial gráfico: Jack Forbes

Seguridad digital

July 30, 2019 11:30 AM EDT

Actualizado al 14 de abril de 2022

Para protegerse a sí mismos y a sus fuentes, los periodistas deben mantenerse al día con las últimas noticias y amenazas en materia de seguridad digital, como por ejemplo el *hacking*, el *phishing* y la vigilancia. Los periodistas deben pensar en la información por la cual son responsables y en lo que sucedería si cayera en las manos equivocadas, y tomar medidas para defender sus cuentas, dispositivos, comunicaciones y actividad en la Internet.

Este kit de seguridad digital se ha concebido para ejercer de punto de partida general para los periodistas que desean aumentar su seguridad digital. Si se quiere obtener recomendaciones de seguridad más detalladas, le rogamos consultar nuestras notas de seguridad. Se recomienda a los periodistas que realicen una evaluación del riesgo antes de comenzar toda cobertura.

Contenido

Proteja sus cuentas

Los periodistas utilizan una variedad de cuentas de Internet que poseen información personal y de trabajo sobre sí mismos, sus compañeros de trabajo, sus familiares y sus fuentes. Segurizar estas cuentas y periódicamente hacer copias de respaldo y borrar información, lo ayudará a proteger sus datos.

Para proteger sus cuentas:

• Piense en qué información está almacenada en cada cuenta, y en cuáles serían las consecuencias para usted, su familia y sus fuentes

si su cuenta es vulnerada.

- Separe el trabajo de la vida privada en la Internet y evite mezclar información profesional y personal en las cuentas. Ello le permitirá limitar el acceso a sus datos si alguien logra ingresar a una cuenta.
- Revise sus ajustes de privacidad y entienda qué información es de carácter público, especialmente en las redes sociales.
- Cree copias de respaldo de toda la información de carácter sensible o que usted no desea que se haga pública, como los mensajes privados y los correos electrónicos, y luego bórrela de su cuenta o dispositivo. Hay herramientas digitales de terceros que lo ayudan a encriptar documentos individuales para luego almacenarlos en un disco duro externo o en la nube. También se recomienda encriptar los discos duros externos. Consulte las leyes vigentes sobre la encriptación en la jurisdicción donde se encuentre.
- Borre toda cuenta que haya dejado de utilizar. Recuerde crear copias de toda la información que usted desee guardar.
- Compruebe si alguna de sus cuentas ha estado implicada en un incidente de vulneración de la seguridad. Para ello, haga una búsqueda en el sitio web have i been pawned. Si verifica que una cuenta suya ha sido vulnerada, entonces debe ingresar a esa cuenta y cambiar la contraseña. Si ya no desea usar esa cuenta, entonces debe borrar todo su contenido antes de borrar la cuenta.
- Active la autenticación de dos factores (2FA) en todas sus cuentas. Lo ideal es que utilice una aplicación autenticadora en lugar de mensajes SMS. Compruebe que un servicio de Internet es compatible con 2FA haciendo una búsqueda en el Directorio 2FA.
- Cree contraseñas largas de más de 16 caracteres y asegúrese de que contengan números, símbolos y letras. No utilice la misma contraseña en más de una cuenta ni incluya en la contraseña información personal que se pueda encontrar fácilmente en la Internet, como la fecha de nacimiento. Valore utilizar un gestor de contraseñas que se encargue de gestionar sus contraseñas. Infórmese sobre las opciones de gestor de contraseñas que están a

su disposición, para ver cuál es la que más le conviene. Cree una contraseña larga y única para su gestor de contraseñas.

- Si corre el riesgo de que lo detengan o le preocupa que alguien acceda sin autorización a sus dispositivos, cierre la sesión de las cuentas cada vez que las use y borre el historial de navegación.
- Con regularidad revise la sección de 'actividad de la cuenta' de cada una de sus cuentas. Por lo general, esta sección se encuentra en los 'ajustes'. Ello revelará si algún dispositivo que usted no reconoce ha iniciado una sesión. Si un dispositivo que usted no reconoce ha iniciado una sesión, entonces debe cerrar la sesión de esa cuenta inmediatamente de ese dispositivo específico. Antes de cerrar la sesión, es aconsejable hacer una captura de pantalla para tener su propia constancia.
- Evite ingresar a sus cuentas desde computadoras compartidas, por ejemplo, en un cibercafé. Si no tiene otra opción, cierre las sesiones inmediatamente después y borre el historial de navegación.

Phishing

Los periodistas a menudo tienen un perfil público y comparten sus datos de contacto para solicitar indicios. Los adversarios que intenten adquirir acceso a los datos y los dispositivos de los periodistas, pueden convertirlos en objetivos –o a sus compañeros de trabajo o familiares– mediante ataques de *phishing* en forma de mensajes personalizados de correo electrónico, SMS, redes sociales o chats diseñados para engañar al receptor y lograr que comparta información sensible o instale *software* malicioso al hacer clic en un enlace o descargar un archivo. Existen muchos tipos de *software* malicioso y *software* de espionaje, los cuales poseen diversos grados de complejidad, pero los más avanzados pueden otorgarles a atacantes remotos acceso al dispositivo y a todo su contenido.

Para defenderse de ataques de *phishing*:

- Investigue las capacidades tecnológicas de sus adversarios para entender la amenaza y la probabilidad de que usted o alguien que conoce pudiera ser un objetivo.
- Sea cauteloso con los mensajes que lo instan a hacer algo rápidamente o que parecen ofrecerle algo que es demasiado bueno para ser verdadero, en particular si implican hacer clic en un enlace o descargar un adjunto.
- Revise cuidadosamente los datos de la cuenta del emisor y el contenido del mensaje para comprobar que es legítimo. Pequeñas variaciones en el deletreo, la gramática, el formato o el tono pudieran indicar que la cuenta ha sido falsificada o hackeada.
- Verifique el mensaje con el emisor utilizando otro método, como llamar por teléfono, si algo sobre el mensaje le resulta sospechoso o inesperado.
- Piense con detenimiento antes de hacer clic en enlaces, inclusive si el mensaje parece venir de algún conocido suyo. Coloque el cursor sobre los enlaces para ver si el URL parece legítimo.
- Previsualice todo adjunto que reciba por correo electrónico; si no descarga el documento, podrá contener todo *software* malicioso. En caso de duda, llame al remitente y pídale que copie el contenido en el mensaje de correo electrónico, o haga usted capturas de pantalla del documento previsualizado en lugar de descargarlo.
- Tenga cuidado con los enlaces o documentos que se envíen mediante un chat de grupo. Los chats con muchos miembros pueden ser infiltrados por las autoridades o por grupos criminales que intenten escoger como objetivo a los participantes.
- Utilice la versión de escritorio de las aplicaciones para revisar mensajes y enlaces, si es posible. Una pantalla de mayor tamaño lo ayuda a verificar lo que ha recibido, y es menos probable que usted haga varias tareas al mismo tiempo.
- Suba los enlaces y documentos sospechosos a Virus Total, un servicio que los escaneará en busca de posible *software* malicioso, aunque sólo aquellos que son conocidos.

- Habilite las actualizaciones automáticas y mantenga al día todo el *software* de sus dispositivos. Ello reparará las vulnerabilidades conocidas de las que depende el *software* malicioso para poner en peligro la seguridad suya.
- Asegúrese de activar la autenticación de dos factores en todas sus cuentas, pues en el caso de que le roben la contraseña, sus adversarios tendrán más dificultad para ingresar a la cuenta.
- Esté particularmente atento a los ataques de *phishing* durante las elecciones y períodos de inestabilidad o si sus compañeros de trabajo u organizaciones locales de la sociedad civil anuncian que son objeto de estos ataques.

Seguridad de los dispositivos

Los periodistas utilizan una amplia gama de dispositivos para producir y guardar contenido, y para entrar en contacto con sus fuentes. Muchos periodistas, en particular los periodistas *freelance*, utilizan los mismos dispositivos en el hogar que en el trabajo, lo cual puede poner en riesgo una gran cantidad de información si se pierden o si alguien los roba o se los lleva. Encripte los discos duros de las computadoras, los teléfonos, las tabletas y los dispositivos de almacenamiento externo, especialmente si viaja, para asegurarse de que otras personas no puedan adquirir acceso a esta información sin una contraseña.

Para segurizar sus dispositivos:

- Bloquee los dispositivos con una contraseña, código o PIN. Mientras más largos sean los números de identificación personal y las contraseñas, más difícil será que otras personas desbloqueen los dispositivos.
- Actualice el sistema operativo, las aplicaciones y los navegadores cuando éstos se lo indiquen. El *software* antiguo posee

vulnerabilidades que se pueden explotar para instalar programas maliciosos en sus dispositivos. Ello es particularmente importante si usted considera que puede ser blanco de *software* de espionaje avanzado.

- Inspeccione la información que está almacenada en sus dispositivos y considere cómo puede ponerlos en riesgo a usted y a otros.
- Haga copias de respaldo del contenido de sus dispositivos con regularidad, por si se destruyen, se pierden o los roban. Almacene las copias de respaldo de manera segura, lejos de su computadora de trabajo habitual.
- Borre la información sensible con regularidad, inclusive los mensajes de los chats. Para evitar que un adversario restablezca los archivos borrados, utilice *software* de borrado seguro para borrar el dispositivo, si está a su disposición; de lo contrario, haga un restablecimiento de fábrica y utilícelo para otras actividades, con el objetivo de reescribir la memoria del dispositivo. (Primero, haga copias de respaldo de todo el contenido que quiera conservar, o perderá todos sus datos).
- No descuide los dispositivos en público, por ejemplo, cuando recarga la batería, pues alguien los puede robar o manipular.
- No utilice memorias USB de las que regalan en eventos. Éstas pudieran contener *software* malicioso que podría infectar su computadora.
- Tenga en cuenta que el dispositivo puede hacer copias de respaldo de sus datos en la cuenta en la nube vinculada con el teléfono. Puede que la información almacenada en la nube no esté encriptada. En las opciones, usted puede desactivar las copias de respaldo automáticas.
- Configure los dispositivos para que le permitan borrar los datos a distancia si alguien los roba. Esta opción debe configurarse por adelantado, y el dispositivo solamente borrará los datos si está conectado a la Internet.

- Siempre repare los dispositivos con una empresa de buena reputación.

Para encriptar su dispositivo:

- Los teléfonos inteligentes más nuevos vienen con la función de encriptación, simplemente asegúrese de que esté activada en los ajustes de configuración.
- Utilice Bitlocker para activar la encriptación de disco completo para Windows, Firevault para Mac, o el *software* gratuito Veracrypt para los discos duros y los dispositivos de almacenamiento externo.
- Crear una contraseña única y larga es clave para utilizar la encriptación; en un teléfono inteligente, marque los ajustes de personalización para añadir una contraseña más larga y compleja.
- Tenga en cuenta que un adversario que conozca la contraseña suya o que tenga el poder de obligarlo a desencriptar el dispositivo, podrá revisar la información.
- Siempre investigue las leyes vigentes para asegurarse de que la encriptación es legal en el país donde vive o al que viaja.

Comunicaciones encriptadas

Los periodistas pueden comunicarse con sus fuentes de manera más segura utilizando aplicaciones de mensajería encriptadas o *software* que encripte el correo electrónico para que únicamente el destinatario deseado lo pueda leer. Algunas herramientas digitales son más fáciles de utilizar que otras. La encriptación protege el contenido de los mensajes, pero las empresas involucradas de todas formas pueden ver los metadatos, los cuales incluyen cuándo usted envió el mensaje, quién lo recibió y otros datos reveladores. Las empresas tienen diversas políticas sobre los datos que recolectan, cómo almacenan estos datos y cómo responden cuando las autoridades los solicitan.

Las aplicaciones de mensajería que se recomiendan ofrecen encriptación de extremo a extremo, lo cual significa que la información está encriptada cuando se envía del emisor al destinatario. Ambas partes deben tener una cuenta con la misma aplicación. Toda persona con acceso a un dispositivo que envíe o reciba el mensaje, o a la contraseña de la cuenta vinculada con la aplicación, de todas maneras puede interceptar el contenido del mensaje. Signal y WhatsApp son ejemplos de aplicaciones de mensajería con encriptación de extremo a extremo activada por defecto. Otras aplicaciones pueden requerir que usted active la encriptación de extremo a extremo.

El correo electrónico encriptado es otra forma segura de intercambiar información con una fuente o contacto. Ambas partes deben descargar e instalar *software* específico para poder enviar y recibir correo electrónico encriptado.

Para utilizar aplicaciones de mensajería encriptadas:

- Investigue quién es la empresa propietaria de la aplicación, qué datos de usuario la empresa retiene y si el Gobierno ha solicitado esos datos mediante orden judicial. Revise cuál es la política de la empresa para responder a las solicitudes de las autoridades para que comparta datos de los usuarios. Las empresas de tecnología deben elaborar un informe de transparencia cada año donde usted pueda revisar las solicitudes que los Gobiernos han efectuado a la empresa para que retire o comparta datos.
- Bloquee la aplicación con un PIN o una contraseña siempre que sea posible, para protegerse mejor contra la posibilidad de que alguien abra la aplicación si tiene acceso material al teléfono de usted.
- Ponga un bloqueo de registro, si el servicio lo ofrece, para requerir que toda persona que instale la aplicación con el número telefónico de usted tenga que ingresar su número PIN.

- Algunas aplicaciones, como Signal y WhatsApp, ofrecen una medida de seguridad adicional para verificar con quién usted chatea y evitar que alguien se haga pasar por uno de sus contactos desde otro dispositivo. Busque la opción de verificar el número de protección o el código de seguridad en los ajustes de la aplicación.
- Entienda en qué carpetas del teléfono queda almacenada la información que se envía a sus aplicaciones de mensajería, como las fotos y los documentos.
- Todo lo que usted descargue, como las fotos, quedará guardado en el dispositivo y podrá copiarse a otros dispositivos y aplicaciones, en particular cuando usted hace copias de respaldo de sus datos.
- Algunos servicios, como WhatsApp, hacen copias de respaldo del contenido de sus mensajes y de su historial de llamadas en la cuenta en la nube vinculada con el número telefónico (iCloud para los usuarios de dispositivos iOS). Esta opción se puede desactivar en los ajustes de la aplicación.
- Los contactos almacenados en su teléfono se sincronizan con las aplicaciones de mensajería y las cuentas en la nube, por lo cual los números que usted intente borrar en un lugar pueden quedar guardados en algún otro lugar.
- Haga copias de respaldo y borre mensajes con regularidad, para almacenar la menor cantidad de contenido posible en un solo dispositivo o cuenta. Cree un proceso para revisar el contenido, que incluya los documentos y los mensajes multimedia, y guarde los archivos descargados o las capturas de pantalla en un dispositivo de almacenamiento externo encriptado.
- La función de desaparición de mensajes de Signal y WhatsApp le permiten borrar automáticamente los mensajes después de cierto tiempo. Active esta función si le preocupa que le quiten el teléfono y accedan a sus mensajes.
- Tanto Signal como WhatsApp ofrecen la posibilidad de configurar las fotos y los videos para borrarse después de verse. Puede ser útil activar esta opción si usted envía imágenes de carácter delicado.

- Las videollamadas de Signal y WhatsApp también ofrecen encriptación de extremo a extremo.

Para utilizar correo electrónico encriptado:

- Busque ayuda con un contacto confiable que sepa de tecnología. El correo electrónico encriptado no siempre es fácil de instalar si es una novedad para usted.
- Escoja *software* de encriptación de correo electrónico con buena reputación que haya sido reseñado por expertos. Siempre actualice el *software* para protegerse de las vulnerabilidades de seguridad.
- Dedique tiempo de antemano a crear una contraseña larga y única para su *software* de correo electrónico encriptado. Si se le olvida esta contraseña, perderá el acceso a los mensajes de correo electrónico encriptados.
- Envíe con regularidad mensajes de correo electrónico encriptados para que no se le olvide cómo utilizar el *software.*
- Ciertos datos del mensaje de correo electrónico, como el título y las direcciones de correo electrónico que envían y reciben el mensaje, no son encriptados.

El uso más seguro de la Internet

Los periodistas dependen de la Internet para hacer sus investigaciones periodísticas. Por tanto, si no toman medidas para protegerse, pueden ponerse en riesgo y poner en riesgo a sus fuentes. Los proveedores de Internet, Gobiernos, empresas y delincuentes recolectan datos sobre los usuarios de Internet, los cuales pueden emplearse para tomar represalias y armar procesos penales contra ellos.

Cómo utilizar con mayor seguridad la Internet:

- Averigüe quién es el propietario de su proveedor de Internet y cuáles son las obligaciones legales de esa empresa respecto a entregar datos sobre usted a Gobiernos, inclusive su propio Gobierno. Verifique qué datos sobre usted almacenan y por cuánto tiempo lo hacen.
- Proteja su historial de navegación de su proveedor de Internet y para ello utilice un servicio VPN. Debe tener en cuenta que el proveedor de Internet registrará que usted se ha conectado a un servicio VPN, y ello pudiera representar un problema para usted si los servicios VPN son ilegales en su país. Asegúrese de escoger un servicio VPN que no siga y ni registre su historial de navegación, pues esta información puede compartirse con Gobiernos y otros actores. Escoja un servicio VPN que se haya creado en un país extranjero y esté ubicado en un país extranjero, pues así será más difícil que su Gobierno obtenga datos sobre usted.
- La mayoría de los sitios web ya están encriptados, lo que significa que, si bien se puede ver que usted está visitando un sitio web o abrió una sesión en un servicio de Internet, no se puede ver el contenido de esa página. Busque 'https' y el símbolo de un candado al inicio de toda URL de un sitio web (por ejemplo, https://cpj.org), lo que indica que el tráfico web entre usted y el sitio web está encriptado. DuckDuckGo Smarter Encryption es una herramienta que garantiza mejor que el sitio que usted está visitando está encriptado.
- Cuando usted visita un sitio web, éste recolecta datos sobre usted, entre ellos su dirección IP, lo cual delata su ubicación aproximada, detalles sobre su dispositivo (inclusive el sistema operativo) y su zona horaria.
- Instale un programa para bloquear anuncios publicitarios con el fin de protegerse del *software* malicioso, que a menudo está oculto en las ventanas de publicidad desplegables. Los programas para bloquear anuncios le permiten escoger los sitios que desea desbloquear, como el de su propio medio de prensa.
- Instale Privacy Badger para impedir que sitios web y anunciantes hagan un seguimiento de los sitios que usted visita en la Internet.

- Valore instalar el paquete gratuito del navegador Tor (Tor Browser Bundle) para utilizar la Internet de manera anónima, o Tails, un sistema operativo gratuito que redirige todo su tráfico de Internet por medio de Tor. Se recomienda especialmente Tor para los periodistas que investigan temas sensibles como la corrupción gubernamental de alto nivel en países con capacidad tecnológica avanzada. Consulte la ley con respecto al uso de Tor en el país donde se encuentra.
- Los Gobiernos, delincuentes y otros actores pueden crear sitios falsos que se pueden emplear para recolectar datos personales, como las contraseñas, y datos de las tarjetas de crédito, entre otros. Compruebe que la dirección del sitio web es auténtica y no una falsificación. La URL debe estar deletreada correctamente e incluir 'https'.
- Si es posible, evite utilizar computadoras públicas, especialmente en cibercafés o salas de prensa. Las computadoras públicas pueden estar infectadas de programas informáticos maliciosos o de espionaje. Si tiene que utilizar una computadora pública, evite ingresar a sus cuentas personales, asegúrese de cerrar todas las sesiones y borre su historial de navegación.

● Jack Forbes

Al cruzar las fronteras

Muchos periodistas cruzan las fronteras llevando consigo información personal y de trabajo en dispositivos electrónicos, y es posible que no quieran que otras personas adquieran acceso a esa información. Si los guardias fronterizos se llevan un dispositivo y éste queda fuera de su vista, ellos tienen la oportunidad de inspeccionarlo, adquirir acceso a alguna cuenta, copiar información o instalar *software* de espionaje. Los periodistas que crucen la frontera para ingresar a Estados Unidos deben consultar la nota de seguridad del CPJ “Nada que declarar”.

Antes de viajar:

• Averigüe qué información está almacenada en sus dispositivos y cómo puede ponerlos en riesgo a usted y a sus contactos. Dé por sentado que sus dispositivos pueden ser sometidos al mismo grado

de escrutinio que los cuadernos y el material impreso que lleva en su equipaje.

- Haga copias de respaldo del contenido de todos sus dispositivos en un disco duro externo o en la nube. Elimine toda la información de sus dispositivos a la cual no desea que los funcionarios de fronteras adquieran acceso.
- Compre dispositivos limpios para utilizarlos solamente durante los viajes si es posible, en particular si está trabajando en historias sumamente sensibles. Si viaja con un dispositivo personal o de trabajo, de manera segura haga copias de respaldo del contenido y luego bórrelo o haga un restablecimiento de fábrica.
- Active la encriptación de disco completo de todos los dispositivos para asegurar que nadie pueda acceder a la información sin una contraseña. Investigue cuáles son las restricciones legales del país que visita con respecto a la encriptación, para asegurarse de no violar ninguna ley. Tenga en cuenta que las fuerzas de seguridad pueden tener la facultad legal de pedirle la contraseña. Asesórese con su empresa o su abogado antes de viajar, si existe la posibilidad de que las autoridades lo paren en la frontera.
- Termine las sesiones de todas las cuentas de sus dispositivos y desinstale las aplicaciones hasta que usted haya cruzado la frontera y alcanzado una conexión de Internet segura.
- Borre el historial de navegación de todos los dispositivos. (El proveedor de servicio de Internet suyo y el navegador de todas maneras tendrán un registro de los sitios web que usted haya visitado).
- Bloquee todos los dispositivos con un PIN o una contraseña en lugar de hacerlo con datos biométricos como su rostro o una huella digital.
- Habilite el borrado a distancia de sus dispositivos y deje instrucciones claras con alguien de confianza para que borre los dispositivos a distancia si usted resulta detenido. Los dispositivos solamente pueden activar el borrado a distancia si están conectados a la Internet.

En la frontera:

- Apague los dispositivos para activar la encriptación de disco.
- Esté atento a sus dispositivos cuando pasen por los controles de seguridad.
- Tenga en cuenta que todo mensaje SMS o llamada telefónica que no tenga encriptación de extremo a extremo serán enviados mediante un proveedor de servicio local que pudiera recolectar el contenido o compartirlo con las autoridades.

Si le confiscan algún dispositivo en la frontera o le insertan algo al dispositivo, dé por sentado que ha sido vulnerado y que toda la información contenida en él ha sido copiada

Nota del editor: *Este kit de seguridad digital se publicó originalmente el 30 de julio de 2019 y su exactitud se revisó en la fecha que aparece al inicio.*