breve guía de *seguridad digital*

Purna

Introducción

Esta guía pretende funcionar como una primera aproximación a la seguridad digital, principalmente dirigida al uso de smartphones, pero también de ordenadores. En la actualidad vivimos constantemente conectados: el ordenador, y especialmente el teléfono móvil, se han convertido en extensiones de nuestro propio cuerpo. Con ellos generamos constantemente información que nos resulta de gran utilidad, pero que también nos hace vulnerables y, en las manos equivocadas, puede llegar a dañarnos. ¿Cómo evitarlo? La respuesta depende de nuestro contexto: cuál es nuestra situación concreta, qué tipo de información es susceptible de ser robada, de qué modo y por quién —cuáles son los adversarios de los que buscamos protegernos—.

Esta breve guía está escrita desde una óptica militante. Las organizaciones que nos autodefinimos como revolucionarias, a pesar de nuestra reducida capacidad de acción e influencia, corremos el riesgo de ser investigadas por la policía. No se trata de ser paranoicos/as, sino de ser conscientes del contexto en el que nos movemos y tomar las precauciones necesarias. Por ello, en las siguientes páginas se esbozarán algunas medidas de seguridad mínimas si se quiere estar protegido ante diversas situaciones, como el acudir a una movilización o a un lugar en el que no quieres que se te localice, poder llevar a cabo conversaciones que no puedan ser interceptadas, o mantener tu información segura en caso de que la policía acceda a tu teléfono tras una detención o realice un registro en tu casa y requise tu ordenador.

¿Significa esto que todo militante de una organización o persona implicada en los movimientos sociales debe tomar estas medidas de seguridad? No. Cada uno/a ha de valorar su propia situación y actuar en consecuencia, sopesando especialmente el tipo de información que posee y la sensibilidad de la misma. Pero si decides tomar precauciones y tratar de fortalecer la seguridad de tus dispositivos, puedes empezar por aquí.

1. Introducción a la red telefónica

El uso de cualquier teléfono móvil conlleva necesariamente el uso de la red de telefonía móvil. La utilización de las funciones de telefonía de nuestro teléfono (llamadas, SMS y "datos") implica que el teléfono móvil, y por ende la persona que va con él, esté permanentemente localizada por el proveedor de telefonía (Vodafone, Movistar, etc.). Además de tenerte constantemente geolocalizado/a, tu compañía telefónica tiene acceso al contenido y metadatos de tus SMS y llamadas, así como a algunas partes de tu navegación web, como qué sitios visitas, cuándo y desde dónde. Todo esto ha de tenerse en cuenta a la hora de hacer uso del teléfono móvil, ateniendo siempre al contexto y las necesidades de cada momento. Si deseas acudir a un lugar comprometedor, o verte con alguien que no quieres que se relacione contigo, deja el móvil en casa. En vez de SMS, utiliza aplicaciones seguras de mensajería instantánea y, en vez de llamadas convencionales, puedes hacer llamadas encriptadas a través de Signal.

2. Desbloqueo de pantalla

El desbloqueo de pantalla es la medida más básica que podemos tomar de protección frente al acceso físico al teléfono. Sin ella, el acceso a la información de nuestro dispositivo se hace extremadamente fácil. ¿Qué método de desbloqueo es más seguro? El patrón de desbloqueo es la opción más vulnerable: el abanico de combinaciones es reducido, es fácil de ver y memorizar por terceras personas y la grasa presente en nuestros dedos puede dejar trazas en la pantalla que permiten reconstruir la combinación. El desbloqueo biométrico, con la huella dactilar o el rostro, puede ser robusto, pero también vulnerable si el adversario puede reproducir nuestra biometría o forzarnos a utilizarla. Las opciones más recomendadas son el pin numérico (siempre que sea suficientemente largo), y la contraseña, que al poseer un alfabeto más amplio ofrece un abanico mucho más grande de combinaciones. Sin embargo, como en todo, has de encontrar un equilibrio entre usabilidad (una contraseña alfabética es más costosa de introducir) y seguridad.

3. Cifrado

El desbloqueo de pantalla, aunque mínimo necesario, resulta también insuficiente, pues la memoria del teléfono puede ser copiada y accederse a ella mediante equipo especializado. Para evitar esto, es imprescindible proteger criptográficamente la memoria de nuestros dispositivos, garantizando que la información contenida en ellos no pueda ser accedida si no se dispone de la clave de cifrado. ¡Ojo!, es altamente recomendable realizar un respaldo de seguridad de nuestros datos antes de habilitar el cifrado de memoria, para evitar perderlos en caso de que hubiera algún problema durante el proceso. Utiliza siempre una contraseña compleja y que no uses en otros dispositivos o cuentas, y recuérdala bien: si la olvidas, perderás el acceso a tus datos definitivamente. ¿Cómo cifrar mi dispositivo?

1.Teléfonos móviles

a. iPhone Los dispositivos iPhone a partir del modelo 5S incorporan cifrado de memoria por defecto. Pero importante, repetimos: no sirve de mucho el cifrado el cifrado si utilizas una contraseña numérica débil, especialmente si es del estilo "1234" o "0000".

b. Android En los dispositivos Android, normalmente el cifrado de memoria ha de ser activado manualmente, aunque algunos dispositivos de gama alta pueden incorporarlo por defecto, y en los terminales más viejos puede no estar disponible. En el momento de activarlo, es necesario tener la batería cargada al 100% y tener el teléfono conectado a un cargador. Normalmente encontraremos la opción para cifrar nuestro teléfono Android en la aplicación de Ajustes, bajo la opción Seguridad o Privacidad. Una vez en este menú, sencillamente pulsaremos Cifrar teléfono y seguiremos los pasos indicados.

2. Ordenadores
También es posible cifrar discos duros de ordenadores, carpetas y documentos. En Windows 10 Pro es posible hacerlo con una aplicación que viene instalada por defecto, Microsoft BitLocker. Sin embargo, es las versiones que normalmente utilizamos esta opción no está disponible, y es necesario descargar otros programas para hacerlo. Uno de los más recomendables es VeraCrypt, disponible para Windows, Linux y Mac. Puedes descargarlo en su página web: https://www.veracrypt.fr/en/Home.html, donde también encontrarás guías de uso en inglés. En castellano hay una guía muy completa, aunque desactualizada, en https://securityinabox.org/es/guide/veracrypt/windows/. Si eres usuario de Mac, puedes utilizar su propia aplicación de encriptación, FileVault.

4. Actualizaciones

Una de las cosas más importantes a la hora garantizar la seguridad del teléfono móvil es mantenerlo actualizado. Cada semana se publican nuevas fallas y vulnerabilidades que amenazan la seguridad del terminal: actualizar regularmente tanto las aplicaciones como el sistema operativo es la única forma de solucionar estos problemas de seguridad que se van descubriendo. Esto no siempre resulta fácil, pues las marcas suelen dejar de publicar actualizaciones para los modelos que van quedando viejos. En Android normalmente dispondremos de actualizaciones durante entre uno y tres años desde la salida del dispositivo al mercado, mientras que Apple ofrece entre cuatro y cinco años de soporte para los iPhone.

5. Aplicaciones seguras

Instala únicamente aplicaciones de proveedores y canales de comunicación fiables, a ser posible de código abierto, y mantenlas siempre actualizadas para minimizar los posibles agujeros de seguridad. Nunca instales aplicaciones de fuentes desconocidas. A continuación, mencionamos cuatro aplicaciones especialmente relevantes desde el punto de vista de la seguridad:

1. Signal / Aplicación de mensajería instantánea. Cifrado de extremo a extremo, código abierto, posibilidad de llamadas cifradas, opción de autoborrado de mensajes en chats privados y grupales. Es la opción más sólida cuando se trata de seguridad. La posibilidad de autoborrado de mensajes es especialmente útil: asegurarte de que la información que se genera desaparece regularmente de todos los dispositivos es la mejor forma de protegerla.

Al contrario de lo que se suele decir, Telegram no es una aplicación segura, ni siquiera en comparación con Whatsapp. No utiliza cifrado de extremo a extremo excepto en los chats privados, siendo el contenido de las conversaciones predefinidas y de los grupos legible para la compañía. Posee opción de autoborrado de mensajes, pero, de nuevo, sólo disponible en los chats secretos.

2. Firefox / Navegador web. Desarrollado por Mozilla, fundación sin ánimo de lucro y comprometida con la privacidad. Además, permite habilitar complementos que aumentan la privacidad al navegar por internet.

3. FairEmail / Gestor de correo para Android. Este cliente de correo electrónico posee código abierto y, usado junto a un proveedor de correo electrónico seguro (como Tutanota, Inventati o Protonmail) supone una mejora considerable de la privacidad. En el ordenador (sea Windows, Mac o Linux) puedes utilizar Thunderbird.

4. ObscuraCam / Aplicación de fotografías para Android. Realiza o edita fotografías protegiendo la información contenida en ellas. Permite pixelar rostros y borrar los metadatos de las imágenes.

6. Navegación

Es posible alcanzar distintos niveles de privacidad y anonimato navegando en internet. Como con el resto de aspectos que estamos abordando, un mayor nivel de seguridad implica una reducción en la usabilidad del medio, por lo que es necesario alcanzar un equilibrio en base a las necesidades y el contexto concreto en el que nos movemos.

1. En un primer nivel, para aumentar nuestra privacidad y dar los menos datos posibles a Google, Facebook, y otras empresas que hacen negocio con nuestra información, es recomendable utilizar un navegador respetuoso con la privacidad como Firefox, y añadirle complementos para dificultar la monitorización como uBlock Origin, Privacy Badger, Cookie AutoDelete, HTTPS Everywhere, DuckDuckGo Privacy Essentials y Facebook Container. Estos complementos pueden descargarse e instalarse desde https://addons.mozilla.org. Además, es posible utilizar otro buscador distinto de Google, como DuckDuckGo o StartPage que no colectan tu información personal. Sin embargo, este tipo de buscadores muchas veces no son tan precisos como lo es Google.

2. Si queremos una capa extra de privacidad, es posible anonimizar nuestra IP de origen utilizando una VPN o Tor, a costa de perder velocidad de navegación. En las ocasiones en las que queramos tener una navegación lo más anónima posible podemos usar estos servicios, que evitan que tanto las páginas web que visitamos como nuestro proveedor de internet pueda obtener información sobre nosotros.

7. Seguridad operacional

La seguridad operacional (OPSEC) es la rama de la seguridad que no se ocupa de desarrollar o aconsejar herramientas, sino pautas de uso y comportamiento estratégico. No es el qué utilizar, sino el cómo utilizar la tecnología y la técnica de la que disponemos para aumentar nuestra privacidad y maximizar las posibilidades de resistir un ataque.

Como conclusión a esta pequeña guía, queremos cerrar con una serie de pautas y consejos para aumentar nuestros conocimientos de seguridad operacional:

1.

Haz un inventario general de todas las cosas que llevas en tu mochila de datos (mensajes, fotografías, correos, registros de actividad, etc.). Valora cuáles de ellas te merecen la etiqueta de «sensible» (informaciones que de veras no quisieras ver comprometidas) para establecer, en relación al contexto, mecanismos de protección adecuados.

2.

No existe información mejor protegida que la que no se llega a generar. Evita producir más información de la necesaria. Si estás manejando información sensible, quizás no haga falta hablar de ella a través del teléfono móvil.

3.

No seas un bocazas. No hables de aquello que no haya que hablar, especialmente en grupos grandes donde la información es más vulnerable. En grupos y colectivos, y en los distintos niveles en los que sea necesario, **asegúrate de que existe un compromiso colectivo por mantener a salvo la información calificada como privada**.

4.

Calendariza borrados de memoria de tu terminal. Con el tiempo, acumulamos mucha información que ya no resulta útil y, sin embargo, puede ser comprometedora en manos equivocadas. **Todo aquello que no necesitamos puede ser borrado o trasladado a dispositivos más seguros, como un disco duro cifrado**.

5.

No incrementes injustificadamente el umbral de seguridad, **no caigas en la paranoia**, **analiza tu contexto y tus necesidades y despliega una defensa eficaz** a la hora de anular las capacidades de adversarios reales. Pretender estar a salvo de la NSA es incompatible con llevar una vida «corriente», usando a diario dispositivos conectados a internet.

Bibliografía

Esta guía se ha elaborado a partir del manual de Críptica *Resistencia digital. Manual de seguridad operacional e instrumental para smartphones*. Críptica es una asociación sin ánimo de lucro centrada en la defensa de la privacidad y la seguridad. Como indican en su página web (www.criptica.org), consideran que la privacidad es una cuestión tanto técnica como política, que buscan hacer llegar a la comunidad creando un espacio de confluencia entre ambas disciplinas. Para ampliar esta información, recomendamos descargar su manual completo, disponible gratis en su página web. Otros recursos de interés son:

1. Autoprotección digital contra la vigilancia: consejos, guías y herramientas para tener comunicaciones más seguras, aunque algunos artículos pueden haber quedado un poco desactualizados:
https://ssd.eff.org/es

2. PrivacyTools, sitio web con análisis y recomendaciones de las distintas opciones de seguridad que están disponibles: ¿Qué motor de búsqueda usar? ¿Qué VPN es más fiable? ¿Qué servidor de correo? Aquí encontraras las respuestas:
https://victorhck.gitlab.io/privacytools-es/

3. Security in a Box, herramientas y tácticas de seguridad digital:
https://securityinabox.org/es/

4. ONG internacional dedicada a difundir un uso seguro y anónimo de las tecnologías digitales:
https://tacticaltech.org/#/

*Aviso de obsolescencia: este manual se terminó de editar a finales de 2020. Es posible que parte de la información dada, especialmente la relativa a aplicaciones, cambie con el tiempo.