7. CÓMO PROTEGER SU DISPOSITIVO MÓVIL– NIVEL 1 (PRINCIPIOS BÁSICOS)

TERRE DES HOMMES - LAUSANNE

1. Resumen ejecutivo

Después de leer este documento, usted conocerá las mejores prácticas para la seguridad básica de los datos contenidos en su teléfono.

¿Por qué es importante proteger sus dispositivos móviles en todos los contextos?

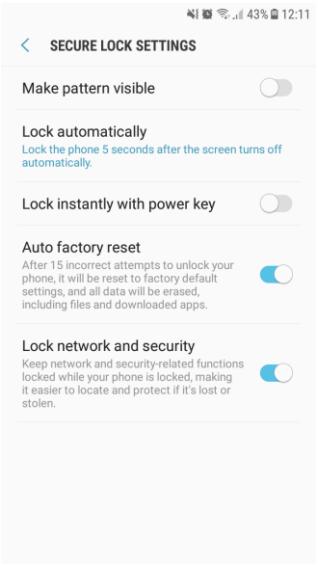
Dependiendo de su contexto operativo, los datos contenidos en sus dispositivos móviles podrían estar en mayor o menor riesgo (debido a grupos armados, intervencionismo gubernamental, etc.). Para contextos muy difíciles es imperativo que usted también consulte el tutorial sobre cómo proteger su dispositivo móvil Nivel 2, pero la mayoría de los principios en este documento se aplican a cualquier tipo de contexto.

2. Mejores prácticas para la seguridad telefónica básica

- Utilice siempre los códigos de bloqueo de seguridad de su teléfono o los ***Números de Identificación Personal (PIN)*** y manténgalos en secreto (desconocidos para los demás). Cambie siempre los ajustes predeterminados de fábrica.

- ***Active el bloqueo de pantalla:*** *después de un período corto de inactividad, su teléfono debería bloquearse automáticamente. Es algo necesario no solo para su dispositivo móvil, sino también para su computadora portátil o tableta. Esta es la forma más fácil de mantener a los intrusos alejados*.

El periodo de inactividad asociado depende del tipo de uso que le dé al teléfono, si usted está llevando a cabo una recolección de datos móvil, este periodo debe ser más prolongado que en el caso de un teléfono a la que la base le da un uso normal por ejemplo, ya que de lo contrario llevaría a una ineficiencia operativa.



- También es esencial que aplique el ***borrado automático de la información contenida en el dispositivo después de 10 intentos fallidos de inicio de sesión***.
- Instale y use un ***anti-virus (Avast, Clam Win, etc.) o anti-malware*** en su dispositivo móvil.
- ***No guarde información sensible en el teléfono.*** Si necesita guardar este tipo de información, considere ponerla en una tarjeta de memoria externa que pueda descartar fácilmente cuando sea necesario, no ponga dichos detalles en la memoria interna del teléfono a menos que los datos estén cifrados.
- ***Cuidado con sus aplicaciones:*** los casos de teléfonos *smartphones* infectados con virus y malware han ido en aumento. Algunos de ellos terminaron con un **adware** molesto, mientras que otros fueron infectados con **ransomware**.
    - Use siempre tiendas de aplicaciones oficiales para descargar e instalar una aplicación. Deshabilite la opción de permitir la instalación de aplicaciones de terceros. Las aplicaciones de terceros usualmente llevan malware que dañará su *smartphone*. ¿Es este un riesgo que vale la pena asumir?
    - Instale solamente aplicaciones que encuentre en la tienda de aplicaciones oficial. Esto significa, nada de aplicaciones de terceros, sin importar si esos terceros son sus amigos en línea, anuncios, blogs o torrents.
    - Si tiene un Android, puede deshabilitar la opción de permitir la instalación de aplicaciones de fuentes diferentes al Play Store (desde Ajustes -> Seguridad).
- ***Instale un bloqueador de anuncios.*** *No, no porque los anuncios sean intrusivos y hayan estado fallando a los clientes potenciales, sino porque pueden ser explotados por*

delincuentes cibernéticos. Es posible introducir publicidad maliciosa directamente a su smartphone a través de servidores de anuncios, ¡y usted ni siquiera necesita hacer clic en nada para infectarse! Como navegador, puede usar Firefox Focus en Android 5+, que integra un bloqueador de anuncios y solo puede utilizarse en navegación privada (todo lo relacionado con la búsqueda se elimina al cerrar el navegador).

- ***Cuidado con la suplantación de identidad (phishing):*** *es mucho más difícil detectar una página de suplantación de identidad (phishing) en su teléfono móvil que en su PC o computadora portátil. Manténgase alerta contra la suplantación de identidad (phishing) en todos sus dispositivos, sin importar si se trata de una computadora de escritorio, computadora portátil, tableta o smartphone*. ***No haga clic en enlaces cortos y sospechosos que no haya solicitado.*** *Y tenga cuidado con los archivos adjuntos que descarga a través del correo electrónico o de los servicios de mensajería instantánea.* ***Ni siquiera el antivirus más potente lo protegerá de la suplantación de identidad (phishing) y el malware****.*
- ***Mantenga su teléfono con usted en todo momento.*** *Nunca lo deje desatendido. Evite mostrar su teléfono en público.*
- ***No*** *debe* ***confiar en los servicios de mensajes de texto*** para transmitir información sensible de forma segura. Los mensajes de texto enviados pueden ser interceptados por el operador del servicio o por terceros con equipos poco costosos.
- ***Marque físicamente (haga un dibujo en) la tarjeta SIM, la tarjeta de memoria adicional, la batería y el teléfono*** con algo único y no inmediatamente perceptible para un extraño (haga una pequeña marca, dibujo, letras o números, o intente usar un marcador ultravioleta, que será invisible a la luz normal) si el teléfono contiene información sensible. Coloque etiquetas de seguridad impresas a prueba de manipulación o cinta adhesiva sobre las juntas del teléfono. Esto le ayudará a identificar fácilmente si alguno de estos elementos ha sido manipulado o reemplazado (por ejemplo, la etiqueta o la cinta se desalineará o dejará un residuo notable).
- ***Proteja su tarjeta SIM y la tarjeta de memoria adicional*** (si su teléfono tiene una), ya que pueden contener información sensible como detalles de contacto y mensajes de texto. Por ejemplo, asegúrese de no dejarlas en el taller de reparaciones cuando le estén dando servicio a su teléfono.
- Considere ***utilizar solo concesionarios y talleres de reparación de teléfonos de confianza***. Esto reduce la vulnerabilidad de su información al adquirir teléfonos de segunda mano o al hacer reparar su teléfono. Considere la posibilidad de comprar su teléfono a un distribuidor telefónico autorizado, pero elegido al azar, de esta manera reducirá la posibilidad de que su teléfono esté especialmente preparado para usted con un software de espionaje preinstalado en él.
- El número **de serie de 15 dígitos o IMEI** (Identidad de Equipo Móvil Internacional) ayuda a identificar su teléfono y puede acceder a este número marcando *#06# en la mayoría de los teléfonos, mirando detrás de la batería del teléfono o buscándolo en los ajustes del teléfono. Tome nota de este número y consérvelo separado de su teléfono, ya que este número podría ayudar a rastrear y probar la propiedad del teléfono rápidamente si es robado.
- **Active el localizador de dispositivos remotos:** En caso su *smartphone* se pierda o sea robado alguna vez, la manera más fácil de localizarlo remotamente es instalando una aplicación dedicada y asegurándose de que la opción de rastrear su ubicación esté

siempre activada. Para iOS existe la solución de rastreo llamada "Find my iPhone", Microsoft tiene "**Find my phone**", y Android tiene "**Android Device Manager**".

- **No conecte su *smartphone* a computadoras desconocidas:** podrían estar infectadas con malware y acabar infectando también su móvil.
- ***Utilice únicamente conexiones inalámbricas seguras*.** Esto significa no usar wifi público o gratuito, especialmente cuando accede a datos sensibles (por ejemplo, el wifi del aeropuerto). A la información enviada a través de redes públicas puede acceder cualquier persona que sepa cómo verla.

    - Utilice sus datos móviles más bien, le costará más, pero sus datos ya no estarán en riesgo.
    - Una VPN, abreviatura de Red Privada Virtual, también puede protegerlo, una red creada para proteger su actividad que cifrará su tráfico y datos de Internet. En los *smartphones* actuales puede configurar fácilmente una VPN.

- ***Mantenga su Bluetooth desactivado*** – no es una forma segura de comunicarse. Habilítelo solo cuando sea necesario. Además, consume su batería.