Seguridad en Internet (smartphone)

Contenido:

- Conocer algunos aspectos básicos sobre seguridad relacionados con el uso del teléfono móvil (smartphone).
- **Vídeo** "Cómo proteger nuestros dispositivos móviles".

Nuestros **dispositivos móviles** se han convertido en una de nuestras principales puertas de acceso a Internet. Realmente, este dato no nos resulta extraño y es algo que venimos viendo desde hace tiempo reflejado en estadísticas de uso o en los datos de venta de estos dispositivos (y su comparación con la venta de ordenadores personales).

Cada vez usamos más nuestros dispositivos móviles y, por tanto, intercambiamos información a través de ellos, accedemos a nuestro correo electrónico o a nuestros perfiles en Twitter, Facebook o Instagram. Nuestros smartphones y tablets atesoran información de carácter personal, guardan nuestras fotos, nuestros mensajes o nuestra agenda de contactos; información de valor que debemos proteger adecuadamente (y evitar que caiga en manos de terceros con no muy buenas intenciones).

La **seguridad** debemos verla como una inversión; es un tiempo bien invertido que nos puede sacar de una situación comprometida en el caso que seamos víctima de un robo, nuestro dispositivo móvil sufra una avería o, simplemente, nos lo hayamos dejado olvidado en el tren, en el autobús o en una cafetería.

¿Y por dónde empiezo? Si quieres mejorar la seguridad de tus dispositivos móviles y proteger tus datos pero no sabes por dónde empezar, vamos a intentar ponértelo algo más fácil con algunas pautas y buenas prácticas que te ayudarán a asegurar tus datos.

Evita que alguien acceda a tu dispositivo sin permiso

Partiendo de la base de que en nuestros dispositivos móviles estamos almacenando información personal (conversaciones de WhatsApp, fotografías, correos electrónicos, acceso a redes sociales…), es fundamental **controlar quién accede** a nuestro dispositivo. Lo más normal es que nadie, salvo nosotros mismos, pueda usar nuestro terminal móvil; por tanto, una de las primeras medidas de control que debemos implantar es una **contraseña de acceso**.

Como "no hacer nada" no es una opción que vayamos a considerar como válida, si accedemos a las opciones de seguridad de nuestro *smartphone* encontraremos la **posibilidad de bloquearlo** mediante un PIN o una contraseña.

En el caso de **iOS**, podremos fijar una contraseña numérica o, en el caso del iPhone 5s, podremos recurrir a la biometría y usar el lector de huellas digitales del dispositivo. En el caso de **Android** podremos encontrar algunas opciones adicionales y, dependiendo del dispositivo, podremos usar reconocimiento facial, una contraseña alfanumérica o un patrón visual (dibujar un patrón sobre la pantalla del terminal).

Si alguien intenta usar nuestro teléfono sin autorización, va a encontrar un terminal bloqueado al que no podrá acceder fácilmente (eso sí, no hay que compartir las contraseñas ni tampoco anotarlas en un papel que pueda estar al alcance de cualquiera).

Protégete ante el robo o la pérdida de tu terminal

¿Alguna vez te has planteado qué pasaría si perdieras tu *smartphone* o fueras víctima de un robo? Si nuestro terminal no estuviese protegido por una contraseña, nuestros datos estarían al alcance de cualquiera, algo que podemos evitar con lo que hemos comentado en el apartado anterior.

Aún así, ante un robo o un extravío lo normal es que intentemos recuperar nuestro dispositivo móvil. La localización es algo posible y todas las plataformas nos ofrecen la posibilidad de localizar, de manera remota, nuestros dispositivos móviles para obtener su ubicación e, incluso, emitir una alarma, mostrar un mensaje o eliminar los datos de nuestro terminal de manera remota.

Los usuarios de **iOS** tienen a su disposición los servicios de **iCloud** y, entre ellos, se encuentra un control remoto de dispositivos que ofrece a los usuarios la posibilidad de eliminar datos, hacer sonar una alarma y visualizar en un mapa dónde se encuentra nuestro teléfono móvil. En el caso de **Android** podremos recurrir a los servicios de **Android Device Manager** para localizar nuestros dispositivos, bloquearlos en remoto (por si aún no los teníamos con contraseña) o eliminar todos los datos del terminal.

Para iOS y Android, además de los servicios oficiales que proporcionan Apple y Google respectivamente, podemos encontrar servicios de terceros como **Prey** o **Lookout** que también nos pueden ayudar, evidentemente, si los tenemos configurados en nuestros terminales.

Finalmente, una de las primeras cosas que deberíamos tener en cuenta cuando estrenamos un dispositivo móvil es su **código IMEI** (se obtiene pulsando *#06#). El IMEI (International Mobile Equipment Identity) es un código único que identifica nuestro dispositivo móvil a nivel internacional; un dato que el terminal envía a la red del operador cuando encendemos nuestro dispositivo y que se puede usar para rechazar un dispositivo robado. Si hemos perdido nuestro terminal y no hay manera de recuperarlo, si queremos evitar que se pueda usar, los operadores pueden pasar el IMEI en una lista negra y rechazar su identificación en la red.

Mantén tus datos a salvo, no te olvides del backup (copia de seguridad)

Perder nuestro dispositivo móvil puede ocasionarnos bastantes dolores de cabeza, sobre todo si no tenemos una copia de la información que almacenábamos. En este sentido, las **copias de seguridad** son fundamentales y es una tarea que debemos asumir e implementar para poder recuperarnos ante un desastre como la avería de nuestro dispositivo o su pérdida.

Tanto iOS (a través de iCloud), como Android (en los ajustes de privacidad), nos ofrecen la posibilidad de realizar un respaldo en la nube de nuestros dispositivos. En el caso de iOS, usando iCloud, podremos hacer una copia de seguridad muy completa; en el caso de Android, los datos que se respaldan por defecto son algo más limitados y hay que complementarlo con otras opciones.

Además, servicios como Dropbox y SkyDrive, además de ejercer de sistemas de almacenamiento en la nube, nos ofrecen *apps* que son capaces de respaldar las fotografías que tomamos con nuestros dispositivos móviles.

Controla lo que compartes

Además de almacenar datos en nuestro dispositivo, con el uso del mismo también estamos generando información que es susceptible de pasar a manos de terceros.

Los fabricantes tienden a recopilar datos estadísticos de uso y es algo que nos suelen preguntar la primera vez que arrancamos nuestro dispositivo; si no prestamos atención a estos mensajes, puede que con la emoción estemos compartiendo datos sin darnos cuenta así que no está de más prestar atención a este aspecto.

Ojo con las aplicaciones que instalas

Aunque no muchos usuarios lo hagan, es importante pararse a pensar un poco antes de instalar una aplicación en nuestro dispositivo móvil. Instalar aplicaciones es fácil; de hecho, es tan sencillo que es aprovechado por terceros para implantar *malware* o convertirnos en su "producto" y hacerse con nuestros datos.

Independientemente de la plataforma que usemos, es recomendable revisar los permisos que requiere una aplicación o qué datos utiliza para funcionar. Esta evaluación es importante porque podremos comprobar si realmente la aplicación accede a más datos de los que debiera por la funcionalidad que nos ofrece. También es recomendable revisar qué opinan otros usuarios del servicio o la *app*.

El *malware* en Android es un tema del que se ha hablado mucho; hay aplicaciones que esconden más de lo que declaran y, por ello, es fundamental revisar los permisos que requieren en su instalación. Además, también debemos verificar el origen del *software* que instalamos y no deberíamos instalar aplicaciones de "Orígenes desconocidos", es decir, instalando directamente paquetes Android. Quizás usar un antivirus podría ser la solución pero, el mejor de todos, es el **sentido común**.

Los ecosistemas controlados, como el de iOS, tampoco son ajenos a estos aspectos de seguridad. Si decidimos realizar el *jailbreak* a nuestro terminal, nos estaremos lanzando a los brazos de desarrolladores que no conocemos y que no tienen por qué declarar toda la información relativa a sus *apps*.

Las aplicaciones maliciosas

El malware no es un problema exclusivo de los ordenadores, sino que también afecta a los

smartphones y tabletas. Por tanto, necesitan la misma protección que aplicaríamos a un equipo de sobremesa.

La mayor parte de los virus se "cuelan" en nuestros dispositivos móviles a través de descargas de aplicaciones (apps) de sitios web que no son los canales recomendados. En la medida de lo posible, hay que hacer uso de las tiendas oficiales: App Store (dispositivos iOS) y Play Store (dispositivos Android).

Si descargamos aplicaciones de cualquier otra fuente, corremos el riesgo de instalar aplicaciones maliciosas sin ser consciente de ellos. Para evitar situaciones desagradables:

- **Descarga nuevas aplicaciones solamente a través de los canales oficiales de los fabricantes**. Así te aseguras de que las aplicaciones han sido revisadas tanto por Google o Apple, como por los usuarios.
- **Verifica la reputación de la aplicación**. Revisa la valoración que tiene una app echando un vistazo a los comentarios que los usuarios han hecho sobre ella. Cuando la aplicación se comporta mal o de manera sospechosa, los propios usuarios se encargan de reflejarlo en los comentarios.
- **Mantén el terminal y las aplicaciones actualizadas**. Éstas corrigen errores que ayudan a mantener los dispositivos protegidos.

Estafas en dispositivos móviles

El uso que se hace de los smartphones y tabletas ha contribuido a la aparición de nuevas estafas. Las aplicaciones de mensajería instantánea, por ejemplo, son usadas en muchos casos por personas que no tienen una base tecnológica, en algunos casos no han utilizado nunca un ordenador, convirtiéndolas en un blanco fácil de estafas o fraudes.

Para evitar este tipo de estafas:

- Permanece alerta ante cualquier mensaje sospechoso, y no respondas nunca por SMS a un número de teléfono que no conozcas.
- No devuelvas las llamadas perdidas de números desconocidos. Si alguien quiere localizarte, volverá a llamar.
- Si sospechas que estás siendo víctima de algún tipo de estafa, contacta con tu operador de telefonía.

Precaución con las conexiones

Habitualmente nos conectamos a redes wifi públicas (aeropuertos, cafeterías y otros espacios

públicos), para navegar a más velocidad o para no consumir los datos de nuestra tarifa.

El problema de algunas de estas redes, es que no son seguras, ya que no cifran la información que se transmite a través de ellas, por lo que cualquier usuario conectado a la red con ciertos conocimientos podría hacerse con la información que estemos intercambiando.

En el caso del Bluetooth, si el dispositivo conserva las contraseñas por defecto del fabricante, un atacante podría conectarse al dispositivo y por ejemplo, escuchar todas las conversaciones cuando utilicemos el manos-libres.

Podemos minimizar estos problemas si adoptamos ciertas precauciones:

- **Si te conectas a una red pública, extrema las precauciones**. Evita conectarte a redes inalámbricas abiertas o que tengan un cifrado poco seguro (WEP).
- **Desde una red pública nunca accedas a páginas web bancarias** ni a sitios donde sea necesario introducir un usuario y contraseña.
- **Enciende el Bluetooth solo cuando vayas a hacer uso de él** y configúralo para que no sea visible por otros dispositivos.

Sobre las restricciones del fabricante

Los términos *rooting o jailbreaking* hacen referencia al proceso que permite eliminar las limitaciones que los fabricantes incorporan a los dispositivos móviles. El objetivo es tener acceso absoluto al terminal, tanto al sistema operativo como a su funcionamiento. Muchos usuarios suelen utilizar esta técnica como un método para instalar aplicaciones de manera gratuita.

Sin embargo, debemos tener en cuenta que:

- Estas modificaciones podrían invalidar la garantía del fabricante.
- Si no se realizan correctamente, podemos hacer que nuestro terminal quede inservible, sin posibilidad de reparación.
- Estas protecciones ayudan a que el dispositivo funcione correctamente y limitan la infección por parte de apps maliciosas, por lo que su eliminación no se considera una buena práctica para **usuarios inexpertos**.

Actualizaciones

Además de brindarnos nuevas funcionalidades, las **actualizaciones** también solventan problemas de seguridad detectados tanto en el sistema operativo de nuestro dispositivo como en las aplicaciones instaladas.

Aunque nos pueda llegar a parecer una tarea tediosa, las actualizaciones pueden solventar vulnerabilidades y fallos de seguridad; por tanto, un dispositivo actualizado implica algo menos de riesgo que uno sin actualizar.

La Oficina de Seguridad del Internauta (**OSI)** tiene un curso de seguridad, en Youtube, dedicado a los móviles con Android. Puedes verlo en este enlace:

https://www.youtube.com/playlist?list=PLt0qyS-HSB2Q8CpG7ARckoYAo-OS_7QuI

Si tu móvil es de Apple, también tienes un curso en este otro enlace:

https://www.youtube.com/playlist?list=PLt0qyS-HSB2SUQtWG6pt9dNSv9KfGcueR


OSI
Oficina de Seguridad del Internauta
10 CONSEJOS
para que tu SMARTPHONE
sea SEGURO y feliz
Mantén el sistema operativo y las aplicaciones actualizadas.
Precaución al conectarse a redes WiFi públicas.
Mantén WiFi, bluetooth y NFC desactivados siempre que no los uses.
Descarga e instala aplicaciones sólo de repositorios de confianza.
Instala un antivirus.
Si usas android instala CONAN mobile.
Protege tu Smartphone en caso de robo o pérdida.
Cuidado con las estafas, el número de fraudes en estos dispositivos ha aumentado.
No hagas root o jailBreak a tu dispositivo.
Crea distintos perfiles si utiliza tu smartphone o tablet más de una persona.
www.incibe.es www.osi.es
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD