BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°08
FECHA DE PUBLICACIÓN
17 02 17

DISPOSITIVOS MÓVILES, ¿CÓMO MANTENERLOS SEGUROS?

Hoy por hoy los dispositivos móviles –smartphones, tablets, iPads, etc.- se han convertido en una herramienta súper necesaria. La facilidad y comodidad que ofrecen para resolver cuestiones de trabajo, estudio y demás, ha ocasionado que prácticamente todas las personas que se mueven en esos ámbitos o simplemente necesitan estar conectadas la mayor parte del tiempo, dispongan al menos de uno de ellos; razón por la cual sucede que dichos dispositivos se han convertido en uno de los blancos predilectos de los ciberdelincuentes.

Es por eso que, considerando la gran cantidad de información –muchas veces altamente sensible e íntima- que solemos almacenar en ellos, resulta fundamental tomar todas las medidas de seguridad disponibles, a los fines de estar lo más protegidos y resguardados posible.

En virtud de ello, a continuación, te contaremos cuáles son los principales riesgos a los que estás expuesto y cómo estar debidamente protegido.

Debido a la facilidad y comodidad que ofrecen los dispositivos móviles, actualmente múltiples estudios han señalado que constituyen la principal fuente de acceso a Internet en todo el mundo.

Principales riesgos y/o amenazas:

- Infecciones por malware (programa malicioso).
- Problemáticas ocasionadas por spam.
- Phishing.
- Robo o pérdida del dispositivo.

En general, las infecciones por **malware**, **spam** y **phishing** están relacionados, ya que casi el 100% de las veces en las que el sistema operativo de un dispositivo móvil (iOS, Android y Windows Phone) es infectado por un malware, sucede por haber recibido un mensaje de spam o un

A la hora de realizar transacciones online con un dispositivo móvil, es importante estar utilizando una red Wi-fi segura.

Gracias a las múltiples herramientas existentes destinadas a minimizar los riesgos implicado en el uso de estas tecnologías, hoy por hoy podemos aprovechar sus ventajas y utilidades para resolver muchas de las tareas cotidianas.

phishing; ya sea por correo electrónico, por SMS o por alguna otra aplicación de mensajería instantánea como WhatsApp.

Dichas infecciones pueden tener diversos objetivos, de acuerdo a los intereses del ciberatacante que las provoca. Los principales son: controlar remotamente el dispositivo, obtener acceso para conocer la ubicación geográfica de la víctima cada vez que lo desee, instalar diferentes tipos de amenazas en el sistema, o incorporar al dispositivo en cuestión a determinada Botnet (red de dispositivos que se convierten en robots) con el fin de ejecutar nuevos ataques informáticos; un buen ejemplo de ello es el caso del mega-ataque DDoS de 2016.

En cuanto al **spam**, no es en sí mismo un ataque, sino que se trata del envío masivo de mensajes –sea por correo electrónico, SMS, aplicaciones de mensajería, mensajes multimedia o a través de las redes sociales- destinados a promocionar productos o servicios. Asimismo, podríamos considerar también como spam a los mensajes de distintas temáticas, muchas veces con pedidos de ayuda o cuestiones esotéricas -entre otros-, que son reenviados en cadena y cuyo contenido, en la mayoría de los casos resulta ser falso, lo cual constituye un fraude. Por tal motivo es que consideramos que el spam es un potencial riesgo, dado que, más allá de generar molestias y esconder estrategias fraudulentas, pueden contener: malware, enlaces que conduzcan de forma engañosa a sitios inseguros a través de los cuales es posible extraer datos sensibles de las víctimas (práctica que se conoce como Phishing), y la distribución de datos personales, como los correos electrónicos de las personas que reenvían dichos mensajes.

Por último, el hecho de **extraviar o sufrir el robo del dispositivo** puede ocasionar la pérdida de información importante de la cual muchas veces no se tiene backup y la posibilidad de que una gran cantidad de datos privados, íntimos y altamente sensibles queden completamente expuestos y al alcance de cualquiera.

Tips y consejos para asegurar tus dispositivos móviles:

- Instalar y mantener correctamente actualizado algún programa antivirus.
- Descargar e instalar aplicaciones únicamente de las tiendas oficiales; Google Play para dispositivos con sistema Android, AppStore para dispositivos que utilicen iOS y Microsoft Store para Windows Phone.
- Mantener actualizadas todas las aplicaciones, realizándolo también a través de las tiendas antes mencionadas.
- Habilitar el bloqueo automático luego de “x” cantidad de tiempo, de acuerdo con tus preferencias. Se recomienda configurar el desblo-

Recordá implementar siempre claves de acceso en todos tus dispositivos móviles.

queo por contraseña, o pin, ya que otros métodos como la creación de un patrón suelen ser de fácil deducción.

- Activar las opciones de geolocalización y conectividad alternativa como Bluetooth, por ejemplo, sólo en los momentos en los que vayan a ser utilizadas y luego tener la precaución de desactivarlas.
- Evitar, en la medida de lo posible, la utilización de redes Wi-fi públicas y/o desconocidas. En caso de no poder hacerlo, no realizar transacciones bancarias, de compras, ni ninguna otra acción que incluya información confidencial hasta no estar conectado a una red segura.
- Siempre que se pueda, evitar el acceso a sitios y/o aplicaciones a través del escaneo de códigos QR, enlaces provenientes de correos electrónicos o mensajes, popups o banners publicitarios; siempre es conveniente ingresar a los sitios escribiendo manualmente la URL correspondiente.
- Prestar mucha atención a la hora de configurar la privacidad de las redes sociales. Es aconsejable la visibilidad, tanto de contenidos compartidos como de todas las actividades que se realicen dentro de la plataforma, solo para los “Amigos”; así como también, es muy recomendable activar la opción de “revisar antes de aprobar” las etiquetas que otras personas quisieran aplicarte.
- Hacer backups frecuentemente de toda la información importante que tengas en el dispositivo.
- Tener mucha precaución a la hora de transportar tus dispositivos y de los lugares en los que los dejás. ▪