4 errores que no debes cometer en la seguridad de tu teléfono

Una de las consultas que más me hacen como perito informático es sobre la seguridad informática en los teléfonos. Efectivamente, la aparición de los teléfonos móviles ha revolucionado las comunicaciones y la dinámica de vida de las personas. Las funciones de estos dispositivos han evolucionado al punto de poder acceder a cuentas bancarias y otros sitios, vulnerables al robo por parte de terceros.

Por ser este tema de vital importancia, he decidido elaborar un artículo sobre este tema. Mi objetivo es guiar las acciones de quienes me consultan constantemente, para que protejan su equipo celular, del acceso no autorizado de terceras personas y programas maliciosos que puedan hackear, extraer información valiosa o apoderarse del control de dispositivo.

¿Sabes qué es el Smishing?

Errores que no debes cometer en la seguridad de tu teléfono

Nunca debemos olvidar que el smartphone es un potente dispositivo informático que tiene acceso a gran parte de tu información empresarial más sensible y a tu información personal más privada. **Los delincuentes profesionales están dispuestos a invertir tiempo, dinero y tecnología, para apropiarse de tus datos.** La seguridad informática inicia con las acciones preventivas que como usuario debes llevar a cabo.

Es importante tomar medidas para proteger el equipo telefónico ante un robo o hurto. Si un ladrón se lleva tu teléfono, puede saber muchas cosas sobre ti, como dónde vives, dónde trabajas, en cuántos bancos tienes cuenta, contraseñas e información de tus tarjetas de crédito, las contraseñas guardadas, entre otros datos que pueden ponerte en una situación peligrosa.

Ante este contexto y debido a la evolución de las técnicas para romper con las barreras de la seguridad informática en todos los dispositivos disponibles en la actualidad, he aquí cuatro medidas esenciales para que protejas tu teléfono de amenazas externas.

Mantener el teléfono sin un patrón o contraseña de bloqueo

El bloqueo de pantalla es fundamental, si no lo tienes, es obligatorio que lo configures ahora mismo. Es la principal línea de defensa básica en seguridad móvil, para evitar que los ladrones o cualquier persona no autorizada, accedan en tu teléfono. En Android, puedes utilizar una contraseña, un PIN o un bloqueo por deslizamiento.

Los PIN y las contraseñas, especialmente las de más de cuatro caracteres, son más difíciles de descifrar, por lo que son un poco más seguros. Algunos teléfonos Android también tienen lectores de huellas dactilares para desbloquear la pantalla, lo que es una opción segura y cómoda. En el caso de los iPhones, puedes utilizar un PIN o Touch ID, que es un bloqueo por huella dactilar sencillo pero eficaz.

Aprende cómo saber si alguien ha entrado en nuestro Gmail

No tener el teléfono protegido con un software antivirus

Los teléfonos Android y, en menor medida, los iPhones, son susceptibles de sufrir la infección de malwares en su sistema operativo. **Sin embargo, existen aplicaciones que escanean tu teléfono para encontrar los programas peligrosos y ayuda a eliminarlos.** Para los iPhones, Apple lanza parches de seguridad cuando encuentra fallos en iOS, como una manera de proteger el sistema operativo del equipo.

Hoy, el malware es un gran negocio. Una vibrante economía sumergida comercia con ciberherramientas, información personal y programadores de alquiler. El Instituto AV-TEST ha advertido que casi 400.000 nuevos elementos de malware surgen cada día. Cada vez con mayor capacidad tecnológica, diseñados y dirigidos para acceder a dispositivos móviles.

Hacer clic en los enlaces dudosos

El phishing es una táctica habitual que utilizan los ciberdelincuentes. El objetivo es lograr que las personas accedan y en cuestiones de minutos infectar el teléfono con programas informáticos capaces de acceder, revelar los datos personales a las personas detrás de los referidos accesos y enlaces o proporcionar el control de tu teléfono a terceros.

Uno de los elementos maliciosos que mayor daño puede causar, es el malware. **Este puede estar incrustado en un sitio web que deja un código para redirigir los enlaces a sitios ilícitos, o se hace pasar por un recurso que no es.** Su objetivo es convencerte de que introduzcas tus credenciales, haciendo posible que los ciberdelincuentes roben tu información.

También, es importante mencionar otras tácticas que pueden quebrar la barrera de la seguridad informática en tu celular, y son los mensajes de texto o WhatsApp al azar con un enlace de alguien que no conoces o que conoces. Lo importante es que no hagas clic en ese enlace, por ningún motivo.

Conectarse a redes de Wifi gratuitas

Las redes Wifi gratuitas no son seguras. **Muchas de las Wifis gratuitas pueden estar diseñadas para robar información del dispositivo que se conecte a ellas.** Son sitios en los que, terceras personas, pueden acceder, sin ningún control al sistema central de tu teléfono, ver en tiempo real que estás haciendo en el mismo y copiar toda la información que le parezca útil.

Las redes Wifi en cafeterías o locales comerciales de reputación o aeropuertos, suelen ser más seguras, sin embargo, no es recomendable disponer de información sensible mientras las utilizas. **Como Perito Informático, siempre sugiero usar en cualquier lugar público, los datos del móvil, para contrarrestar cualquier acción de los ciberdelincuentes en el móvil.**

Descubre qué es y de qué se trata el servicio de Laboratorio Informática Forense

No actualizar el teléfono y las aplicaciones

Una forma sencilla de proteger tu teléfono es mantenerlo actualizado. Descarga las actualizaciones del sistema operativo cuando lleguen a tu teléfono y comprueba que tus aplicaciones también estén al día. A los piratas informáticos les gusta aprovechar los fallos de las aplicaciones y el software obsoletos, pero las empresas los corrigen en las actualizaciones, he ahí la importancia de esta acción.

Descargar aplicaciones y software en sitios sospechosos

Descargar aplicaciones en plataformas poco conocidas, sin reputación o respaldo de empresas consolidadas en el área de las tecnologías telefónicas, es un riesgo. Una consecuencia es la instalación de un adware. Este es cualquier programa que de manera automática ofrece publicidad, pero en segundo plano está instalando programas silenciosos en el teléfono o escaneando datos.

El adware es muy difícil de distinguir del software legítimo. Claramente, pueden robar información o simplemente utilizar la energía del teléfono y la conexión de red para procesar información, ejecutar ataques a otros recursos web y en algunos casos, minar criptomonedas. Es un riesgo acceder a sitios no seguros.

La descarga de aplicaciones desde ubicaciones que no sean Google Play o sitios oficiales puede hacer que tus aplicaciones sean sustituidas por aplicaciones de imitación que en realidad llevan ese software fraudulento para la creación de anuncios. **En estos casos, puedes consultar con un experto**

en seguridad informática para que corrobore las dimensiones de contaminar tu teléfono con un adware.

Conoce 10 Consejos prácticos para mejorar la seguridad informática

Si tu teléfono móvil, cuenta bancaria, redes sociales u otra cuenta de vital importancia, es hackeada, puede implicar consecuencias legales. **En estos casos, debes buscar el apoyo de un Perito Informático para que te ayude a comprobar la acción de control en tu dispositivo.**

Si necesitas de los servicios de un Perito con experiencia en seguridad informática, con capacidad para diseñar protocolos que protejan tu privacidad online, corrija fallos para evitar demandas o accesos no autorizados a tus dispositivos y el de tus familiares, puedes escribirme a: lluis@peritinformatic.com o acceder a mi página web www.peritinformatic.com.