Recomendaciones para proteger los celulares de ataques cibernéticos

20/10/2022

Los smartphones se han convertido no solo en instrumentos para realizar **llamadas,** sino también para **tomar fotos**, enviar mensajes, navegar por internet, **jugar**, compartir información, además de tener la capacidad de almacenar datos personales que deben ser resguardados ante posibles **vulneraciones** durante **ataques cibernéticos** o incluso robos.

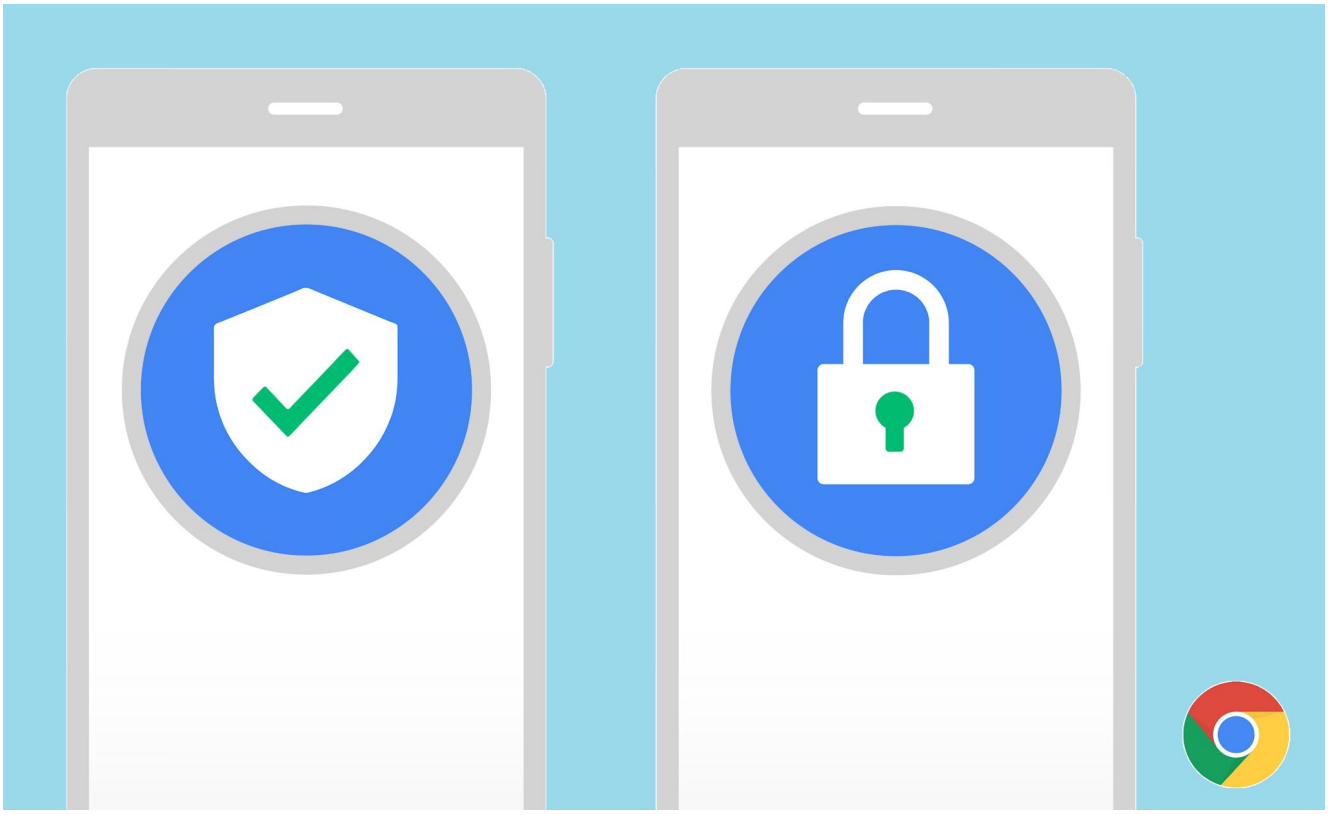
Es debido a este tipo de situaciones que las compañías fabricantes de estos dispositivos no solo invierten sus recursos en desarrollar dispositivos visualmente más atractivos, sino que además, deben tener **elementos de seguridad** que impidan que una tercera persona logre extraer

datos sensibles de ellos, aunque estos deben ser complementados con **actitudes preventivas** por parte de los usuarios.

Protección de la información personal

En caso de robo, el ladrón podría tener acceso a los datos dentro de las aplicaciones de las persona si la pantalla del **dispositivo** no se encuentra bloqueada. Si bien no es posible usar de forma fluida en este estado, lo que se puede hacer para obstaculizar el acceso de los criminales a los **datos sensibles** es configurar el celular con el tiempo mínimo de inactividad antes del **bloqueo**.

Aunque cada **smartphone** es diferente y tiene opciones de acceso propias para esta opción, suele encontrarse dentro de la aplicación de Ajustes, en el apartado de Pantalla.



Los métodos de bloqueo de un smartphone pueden retrasar el acceso de los ladrones a los datos del dispositivo, aunque no

por mucho tiempo. (Google)

Además, mientras más complicado sea el **método de desbloqueo**, la víctima tendrá más tiempo para inhabilitar el dispositivo de manera remota por medio de los servicios disponibles para ello.

Verificar que las aplicaciones provienen de fuentes confiables

Como parte de la prevención ante **infiltraciones** y ataques cibernéticos, una de las más básicas es el evitar o verificar que las aplicaciones que se hayan instalado en el dispositivo provengan de fuentes oficiales o confiables. Las más seguras son la **App Store** y la **Google Play Store**, pues brindan cierta garantía y filtros adicionales para permitir el lanzamiento de aplicaciones maliciosas en sus tiendas virtuales.

Estas plataformas reducen el riesgo de que se infiltre un **virus o malware** al sistema de los dispositivos, sin embargo la mejor forma para evitarlo es no descargar aplicaciones en **sitios web** no seguros o que tengan apariencia sospechosa, aún si estas pueden ser consideradas como útiles.

Es importante recordar que los cibercriminales también son capaces de desarrollar **aplicaciones** que perjudiquen a los usuarios por medio de la infiltración en sus **dispositivos.**

Verificar los permisos para las aplicaciones

Una forma de comprobar que las aplicaciones que se descargan son realmente útiles y no funcionan como intermediarias de **cibercriminales** es verificar los permisos que necesita de parte del usuario para que pueda funcionar correctamente.

Si bien muchas personas ignoran la pregunta de la aplicación

para acceder a ciertas áreas del **dispositivo**, estas dicen mucho de su intención para ver o indagar en áreas con información sensible como los **mensajes** o los **contactos**.

Protegerse durante las compras en línea

Las compras por **internet** son comunes porque facilitan el traslado de las personas a los locales o a las tiendas. Sin embargo también pueden ser ventanas de oportunidad para la infiltración de los **cibercriminales** en los datos de las personas, pues la información bancaria, como el número de cuenta, **clave secreta**, número de tarjeta, entre otros detalles importantes.

Es por eso que se recomienda desvincular la tarjeta de cualquier plataforma de pago recurrente al momento de hacer una compra o **suscripción** y solo activar ese método cuando sea necesario. En todo caso, también se puede usar una cuenta adicional en la que solo se hagan transferencias de dinero dependiendo del fin que se le dará en el plazo más inmediato posible.

Además, es preferible cerra la sesión de los **sitios web** en los que se realizó la transacción una vez que esta haya sido confirmada. Evitar guardar las contraseñas y no aceptar las opciones de autocompletado automático, también son recomendaciones útiles.

Fuente. Infobae