CÓMO PROTEGER SUS DISPOSITIVOS MÓVILES DE LOS HACKERS

IMG

LOS DISPOSITIVOS MÓVILES NECESITAN PROTECCIÓN AL IGUAL QUE LAS COMPUTADORAS

Hay muchas maneras en que los delincuentes pueden robar datos personales valiosos y dinero dirigiéndose a los usuarios móviles. Pueden usar datos personales robados para el robo de identidad y la apropiación de cuentas.

La seguridad de su dispositivo móvil debe estar lista para enfrentar

- Malware móvil
- Aplicaciones sospechosas
- Robo de datos
- Redes inseguras
- Estafas de Phishing

IMG

5

CONSEJOS SOBRE CÓMO PROTEGER SU TELÉFONO Y TABLETA DE LOS HACKERS Y AMENAZAS EN LÍNEA

1. Usa antivirus para dispositivos móviles

Existe malware dirigido específicamente contra dispositivos móviles. Si bien los virus informáticos tradicionales no son una amenaza para los dispositivos móviles, otros tipos de malware sí lo son.

El malware móvil puede:

- Bloquear tu dispositivo y solicita el pago
- Robar datos personales y datos bancarios
- Causar cargos de tarjeta de crédito
- Enviar mensajes SMS a números premium
- Instalar y desinstalar aplicaciones

2. Evita las aplicaciones sospechosas

Si bien las tiendas de aplicaciones oficiales intentan bloquear las aplicaciones maliciosas, ocasionalmente algunas logran pasar. Algunas aplicaciones existen solo para obtener sus datos y ofrecen pocos beneficios. Aceptar sus términos y condiciones les permite obtener sus datos con su permiso. Las aplicaciones de las tiendas de aplicaciones no oficiales no se revisan y pueden ser básicamente cualquier cosa.

Mantenga su ubicación apagada también cuando no la necesite, para que ninguna aplicación pueda rastrearlo sin su conocimiento y consentimiento. De esta manera tu batería también dura más.

IMG

3. No le des permisos innecesarios a las aplicaciones

La autorización de permisos de aplicación innecesarios puede provocar el robo de datos.

Considere siempre qué permisos otorga a las aplicaciones y qué información personal brinda a los servicios.

También puede proteger su teléfono de los hackers **apagando Bluetooth y Wi-Fi cuando no los use.**

Mantenga su ubicación apagada también cuando no la necesite, para que ninguna aplicación pueda rastrearlo sin su conocimiento y consentimiento.

4. Conexiones Wi-Fi seguras con VPN

Nunca se puede saber si una red wifi pública es segura.

Todo lo que haga a través de Wi-Fi no seguro puede ser interceptado por hackers.

Las redes Wi-Fi no seguras también se pueden usar para enviar malware.

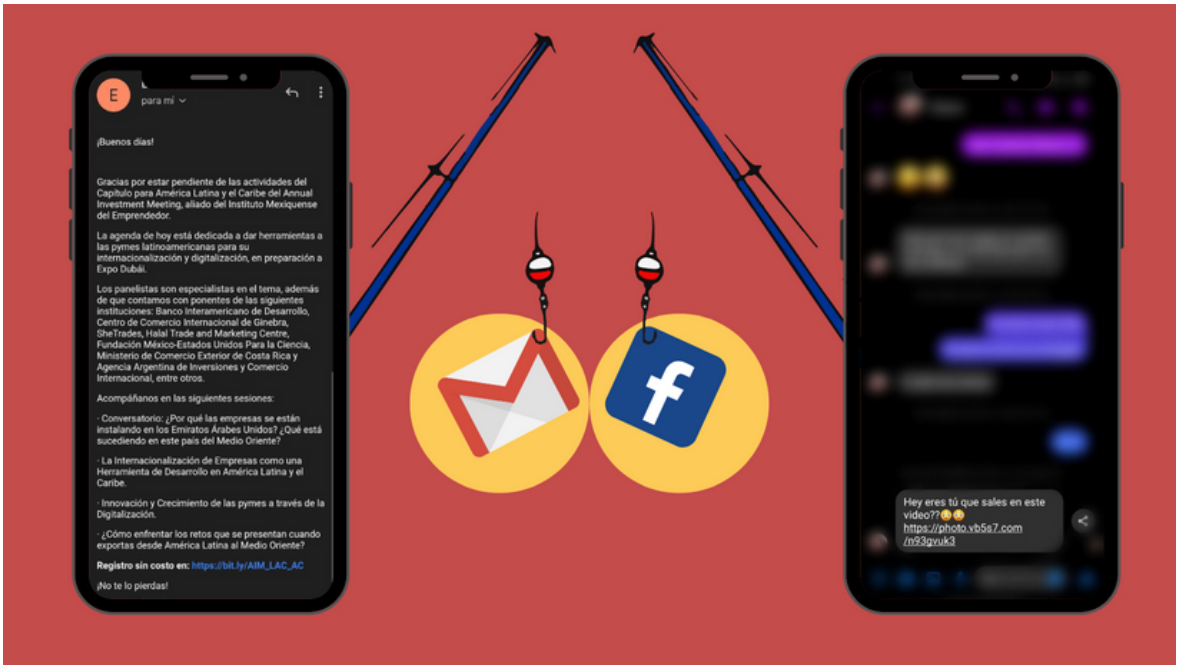
IMG

5. No abras enlaces sospechosos

Las estafas de phishing son más eficaces en los dispositivos móviles. Debido al menor espacio de la pantalla, la mayoría de las aplicaciones de correo electrónico sólo muestran el nombre del remitente, no su dirección.

No abra enlaces sospechosos.

Compruebe la dirección de correo electrónico del remitente. Recuerde, ninguna empresa o autoridad de renombre le pedirá información personal a través de correo electrónico o SMS.



PARA MÁS INFORMACIÓN CONTÁCTANOS EN NUESTRAS REDES SOCIALES

IMAGENTI

info@imagenti.mx

Tel. 55 55 12 73 37