

¿Qué tan seguro es su dispositivo móvil?

La mayoría de nosotros tiene un teléfono inteligente, pero ¿cuántos pensamos realmente en las amenazas a la seguridad a las que se enfrentan estos dispositivos móviles? Los dispositivos móviles son vulnerables a muchos tipos diferentes de amenazas. Los estafadores están aumentando los ataques a dispositivos móviles y apuntando a su teléfono mediante aplicaciones maliciosas. Al utilizar estos métodos, pueden robar información personal y comercial sin que usted tenga idea de lo que está pasando.

Incluso si ha descargado una aplicación de seguridad o antivirus, proteger su teléfono inteligente va más allá de estos servicios. Mejorar sus prácticas de seguridad móvil es su mejor defensa contra los problemas de privacidad y seguridad asociados con su dispositivo móvil.

¿Cómo puedo mejorar mis prácticas de seguridad móvil?

Recuerde siempre estas prácticas recomendadas para minimizar el riesgo de ataques a sus dispositivos móviles:

1. **Asegúrese de que el sistema operativo de su teléfono esté siempre actualizado.** Los sistemas operativos suelen actualizarse para corregir fallas de seguridad. Muchas amenazas maliciosas son causadas por fallas de seguridad que no se solucionan debido a un sistema operativo desactualizado.
2. **Tenga cuidado con las aplicaciones maliciosas en su tienda de aplicaciones.** Las tiendas de aplicaciones oficiales eliminan periódicamente aplicaciones que contienen malware, pero, a veces, estas aplicaciones peligrosas pasan desapercibidas, y usuarios desprevenidos pueden descargarlas. Investigue, lea reseñas y preste atención a la cantidad de descargas que tiene. Nunca descargue aplicaciones de fuentes distintas a las tiendas de aplicaciones oficiales.
3. **Asegúrese de que las aplicaciones no soliciten acceso a elementos de su teléfono que sean irrelevantes para su función.** Las aplicaciones suelen solicitar una lista de permisos para archivos, carpetas, otras aplicaciones y datos antes de descargarlas. No apruebe a ciegas estos permisos. Si las solicitudes de permiso parecen innecesarias, busque una aplicación alternativa en su tienda de aplicaciones.
4. **Sin contraseña o protección con contraseña débil.** Mucha gente sigue sin utilizar una contraseña para bloquear su teléfono. Si pierde o le roban el dispositivo, los ladrones tendrán fácil acceso a toda la información almacenada en su teléfono.
5. **Tenga cuidado con la wifi pública.** Los estafadores usan tecnologías que les permiten ver lo que usted está haciendo. Evite iniciar sesión en sus servicios en línea o realizar transacciones delicadas (como operaciones bancarias) a través de wifi pública.



El equipo de seguridad de KnowBe4