

# ¿Es seguro su dispositivo móvil?

La mayoría de las personas tienen teléfonos inteligentes, pero ¿cuántas piensan de verdad en las amenazas de seguridad a las que se enfrentan estos dispositivos móviles? Los dispositivos móviles son vulnerables ante muchos tipos de amenazas distintos. Los estafadores están aumentando el número de ataques a dispositivos móviles y atacan a su teléfono a través de aplicaciones maliciosas. Mediante estos métodos, pueden robar su información personal y empresarial sin que se dé cuenta de lo que está ocurriendo.

Incluso aunque haya descargado una aplicación de seguridad o antivirus en su teléfono inteligente, deberá ir un paso más allá para proteger su dispositivo. Mejorar las medidas de seguridad de su dispositivo móvil constituye la mejor defensa ante los problemas de seguridad y privacidad asociados a este.

## ¿Cómo puedo mejorar las medidas de seguridad de mi dispositivo móvil?

Recuerde siempre estas prácticas recomendadas para minimizar el riesgo de vulnerabilidades en sus dispositivos móviles:

1. **Asegúrese de que el sistema operativo de su teléfono esté siempre actualizado.** A menudo, los sistemas operativos se actualizan para arreglar fallos de seguridad. La causa de muchas amenazas maliciosas se encuentra en fallos de seguridad que no se corrigen porque el sistema operativo está desactualizado.
2. **Tenga cuidado con las aplicaciones maliciosas en la tienda de aplicaciones.** Las tiendas de aplicaciones oficiales suelen eliminar las aplicaciones con malware, pero, en ocasiones, estas peligrosas aplicaciones se les escapan y los usuarios, ajenos a esto, pueden descargarlas. Investigue, lea reseñas y preste atención al número de descargas que tenga la aplicación. Nunca descargue aplicaciones de fuentes que no sean las tiendas de aplicaciones oficiales.
3. **Asegúrese de que las aplicaciones no le pidan acceso a elementos de su teléfono que no sean pertinentes para su funcionamiento.** A menudo, las aplicaciones solicitan acceso a una lista de permisos de archivos, carpetas, otras aplicaciones y datos antes de su descarga. No autorice estos permisos sin pensarlo antes. Si la solicitud de permiso no le parece necesaria, busque una alternativa a la aplicación en la tienda de aplicaciones.
4. **Utilice siempre una contraseña y asegúrese de que no sea débil.** Hay muchas personas que aún no usan contraseñas para bloquear sus teléfonos. Si pierde el dispositivo o se lo roban, cualquiera podrá acceder fácilmente a toda la información almacenada.
5. **Tenga cuidado con las redes wifi públicas.** Los estafadores usan tecnología que les permite ver lo que hace. Cuando use redes wifi públicas, evite iniciar sesión en sus servicios en línea o efectuar transacciones confidenciales, como transacciones bancarias.



El equipo de seguridad de KnowBe4