El Boletín Mensual de Concientización en Seguridad para ti

Asegurando tus dispositivos móviles

Resumen

Los dispositivos móviles son una forma impresionante y sencilla para comunicarse con amigos, comprar o usar la banca en línea, ver películas, jugar videojuegos, y otras actividades. Dado que estos dispositivos son una parte tan importante de tu vida, es esencial mantenerte a ti y a tus dispositivos seguros y protegidos.

Asegurando tus dispositivos

Puede que te sorprenda saber que el mayor riesgo para tu dispositivo móvil probablemente no sean los ciberdelincuentes, sino tú. Es mucho más probable que pierdas u olvides un dispositivo móvil a que alguien lo hackee. Lo primero que debes hacer para proteger tu dispositivo es habilitar el bloqueo automático de pantalla cuando el dispositivo está inactivo. Esto significa que para usar tu dispositivo, debes desbloquear la pantalla con un código de acceso fuerte, tu cara o tu huella digital. Esto ayuda a garantizar que sea mucho más difícil para cualquier persona acceder a tu información si tu dispositivo se pierde o es robado. Como beneficio adicional, para la mayoría de los dispositivos móviles, habilitar el bloqueo de pantalla también habilita el cifrado, lo que ayuda a proteger los datos almacenados en el dispositivo.

Aquí hay varios consejos más para ayudarte a proteger tus dispositivos:

1. **Actualizaciones**: Habilita las actualizaciones automáticas en tus dispositivos, para que siempre estén ejecutando la última versión del sistema operativo y las aplicaciones. Los atacantes siempre están buscando nuevas debilidades en el software y los proveedores constantemente lanzan actualizaciones y parches para corregirlas. Mantener tus dispositivos actualizados hace que sea mucho más difícil hackearlos. Al elegir un nuevo dispositivo Android, verifica el compromiso del proveedor de mantenerlo actualizado. Los dispositivos Apple iOS son actualizados por la propia empresa, mientras que los dispositivos móviles Android son actualizados por el proveedor que te vendió el dispositivo, y no todos los proveedores actualizan activamente sus dispositivos. Si estás utilizando un dispositivo antiguo que ya no es compatible o no se puede actualizar, considera comprar un dispositivo nuevo que sea totalmente compatible.

2. **Rastreo**: Instala o habilita un software confiable para rastrear de forma remota tu dispositivo móvil a través de Internet. De esta manera, puedes conectarte a él a través de Internet y encontrar su ubicación si tu dispositivo se pierde o es robado o borrar de forma remota toda tu información en el peor de los casos.

3. **Aplicaciones móviles confiables**: Solo instala las aplicaciones que necesites y que provengan de fuentes confiables. Para dispositivos Apple iOS como iPads o iPhones, eso significa App Store de Apple. Para dispositivos Android, utiliza Google Play; para tabletas de Amazon, utiliza la tienda de aplicaciones de Amazon. Si bien es posible que puedas instalar aplicaciones de otros sitios, estas no están examinadas y es mucho más probable que estén infectadas o sean completamente maliciosas, cualquiera de las cuales podría comprometer tu privacidad. Además, verifica que la aplicación tenga muchas críticas positivas y que el proveedor la actualice activamente antes de descargarla. Mantente alejado de aplicaciones nuevas, aplicaciones con pocas reseñas o aplicaciones que rara vez se actualizan.

4. **Opciones de privacidad**: Los dispositivos móviles recopilan una gran cantidad de información sobre ti, especialmente porque los llevas a donde quiera que vas. Revisa minuciosamente la configuración de privacidad de tu dispositivo, incluido el seguimiento de la ubicación, y asegúrate de que las notificaciones confidenciales (como los códigos de verificación) no aparezcan en la pantalla cuando el dispositivo esté bloqueado.

5. **Trabajo**: Asegúrate de que cualquier dispositivo móvil que utilices para trabajar esté autorizado para su uso. Cuando estés en el trabajo, ten mucho cuidado y nunca tomes fotografías o videos que puedan incluir accidentalmente información confidencial, como imágenes de pizarrones o pantallas de computadora.

Tus dispositivos móviles son una herramienta poderosa, una que queremos que disfrutes y uses. El solo hecho de seguir estos sencillos pasos puede ser de gran ayuda para que tú y tus dispositivos estén seguros.

Editor invitado

Jeroen Beckers es experto en seguridad móvil en NVISO, coautor de OWASP MASVS y MSTG, instructor del instituto SANS y autor de SEC575: Curso de seguridad en dispositivos móviles y hacking ético. Puedes encontrar a Jeroen en LinkedIn https://www.linkedin.com/in/beckersjeroen/.

Recursos

Actualizaciones: https://www.sans.org/security-awareness-training/resources/power-updating
Usando aplicaciones móviles de forma segura: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Smishing- Ataques a través de mensajería instantánea:https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Creando contraseñas simples: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Vishing- Ataques y estafas a través de llamadas telefónicas: https://www.sans.org/newsletters/ouch/vishing

Traducido para la comunidad por: Célica Martínez Aponte, UNAM-CERT