SANS SECURITY AWARENESS

OUCH!

Boletín mensual de seguridad para todos

Asegura tu dispositivo móvil

Resumen

Tus dispositivos móviles son un medio asombroso y fácil de usar para comunicarte con amigos, comprar o acceder a la banca en línea, ver películas, jugar videojuegos y realizar una gran cantidad de actividades. Dado que tus dispositivos móviles son una parte tan importante de tu vida, aquí hay algunos pasos simples para mantenerte a ti y a tus dispositivos móviles a salvo y seguros.

Cómo asegurarlo

Podría sorprenderte saber que el mayor riesgo de tu dispositivo móvil no son los ciberdelincuentes, sino que muy probablemente lo seas tú. Es mucho más probable que pierdas u olvides un dispositivo y luego alguien lo vulnere. Lo primero que debes hacer para proteger tus dispositivos es habilitar el bloqueo automático de pantalla, también conocido en inglés como screenlock. Esto significa que cada vez que quieras utilizar tu dispositivo, primero deberás desbloquear tu pantalla, como con un código de acceso fuerte o con tu huella dactilar. Esto ayuda a asegurarte de que si pierdes o te roban tu dispositivo nadie pueda tener acceso a él. Además, aquí encontrarás más consejos que te ayudarán a protegerlo:

Actualizaciones

Habilita las actualizaciones automáticas en tus dispositivos, de esta manera siempre ejecutarán la última versión de sistema operativo y las aplicaciones. Los atacantes siempre buscan nuevas debilidades en el software y los fabricantes constantemente liberan nuevas actualizaciones y parches para solucionarlo. Al contar con la última versión del sistema operativo y de las aplicaciones móviles, será más difícil que alguien pueda vulnerarlo.

Rastreo

Instala o habilita el software de rastreo remoto de tu dispositivo móvil a través de Internet. De esta manera, si pierdes o te roban tu dispositivo móvil, te podrás conectar a él a través de Internet y ubicarlo, o en el peor de los casos borrar remotamente toda la información contenida en él.

Aplicaciones confiables

Solo descarga las aplicaciones que necesites y de fuentes confiables. Para Android, descarga aplicaciones de Google Play, y para las tabletas de Amazon, de la tienda de aplicaciones de Amazon. Si bien es posible que puedas descargar aplicaciones de otros sitios, estas no son examinadas y es mucho más probable que estén infectadas. Además, antes de descargar una aplicación asegúrate de que tenga varias valoraciones positivas y que el desarrollador la

actualiza constantemente. Mantente alejado de nuevas aplicaciones, de aquellas con pocas críticas o que raramente son actualizadas. Finalmente, independientemente de dónde hayas descargado la aplicación, una vez que dejes de necesitarla o que no la uses activamente, te recomendamos que la elimines de tu dispositivo.

Opciones de privacidad

Cuando instalas una aplicación nueva, asegúrate de revisar las opciones de privacidad. Por ejemplo, ¿la aplicación que acabas de descargar realmente necesita acceso a la información de todos tus amigos y contactos? También te recomendamos que deshabilites la geolocalización para todo, solo habilítala en las aplicaciones que realmente la necesites. Si no te sientes cómodo con los requisitos de permisos de una aplicación, busca otra que satisfaga tus necesidades. Además, revisa periódicamente los permisos para asegurarte de que no hayan cambiado.

Respaldos

siempre respalda tus datos. En el caso de tus dispositivos móviles, gran parte de su información a menudo se respalda automáticamente, como tus fotos o mensajes. Sin embargo, las copias de seguridad también almacenan tu configuración, aplicaciones y otra información del dispositivo, lo que facilita mucho la recuperación de un dispositivo perdido o la transición a uno nuevo.

Trabajo

Cuando estés en el trabajo, sé extremadamente cuidadoso y nunca tomes fotografías o algún video que pueda contener accidentalmente información sensible, como imágenes de pizarras o pantallas de computadora.

Tus dispositivos móviles son una herramienta poderosa que queremos que disfrutes y utilices. Seguir estos simples pasos podrá ser de gran ayuda para mantenerte a ti y a tus dispositivos seguros.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Resources

Frase de contraseña: https://www.seguridad.unam.mx/experto-en-contrasenas-admite-que-estaba-equivocado

Respaldos:
https://revista.seguridad.unam.mx/numero-10/medidas-preventivas-para-resguardar-la-informacion

Sanitización de información: https://revista.seguridad.unam.mx/numero-28/sanitizacion

Seguridad en móviles: https://www.seguridad.unam.mx/consejos-para-mantener-nuestra-seguridad-en-moviles

Licencia