SANS SECURITY AWARENESS

OUCH!

Boletín mensual de concientización en seguridad para ti

Desechar tu dispositivo móvil

Resumen

Los dispositivos móviles, como smartphones, relojes inteligentes y tabletas continúan avanzando e innovando de manera asombrosa. Como resultado, algunas personas reemplazan sus dispositivos móviles frecuentemente, por ejemplo cada año. Desafortunadamente, a menudo las personas no se dan cuenta de cuanta información personal se encuentra en ellos. Más adelante te decimos lo que podría estar en tu dispositivo móvil y cómo puedes limpiarlo de forma segura antes de desecharlo. Si tu dispositivo móvil fue proporcionado por tu empresa o tiene datos del trabajo almacenados ahí, asegúrate de verificar primero con tu supervisor sobre el respaldo apropiado y los procedimientos de desecho.

Tu información

Los dispositivos móviles almacenan más información sensible de la podrías imaginar a menudo más que tu computadora.

⚠

- **Dónde vives, trabajas y los lugares que visitas**
- **Los detalles de todos los registros en tu libreta de contactos, incluyendo familia, amigos y compañeros de trabajo**
- **Historial de llamadas incluyendo llamadas entrantes, salientes, mensajes de voz y llamadas perdidas**
- **Mensajes de texto o sesiones de chat dentro de aplicaciones como chats seguros, juegos y redes sociales**
- **Historial de navegación, historial de búsqueda, cookies y páginas en memoria caché**
- **Fotos personales, videos y grabaciones de audio**
- **Contraseñas almacenadas y acceso a tus cuentas, como de tu banco, redes sociales o correo electrónico**
- **Información relativa a la salud, incluyendo tu edad, frecuencia cardiaca, historial de ejercicio o presión sanguínea**

Limpiar tu dispositivo

Independientemente de cómo deseches tu dispositivo móvil, como donarlo, intercambiarlo por uno nuevo, darlo a otro miembro de la familia, venderlo o incluso tirarlo a la basura, primero necesitas asegurarte de que borraste toda la información sensible. Borrar simplemente la información no es suficiente, en su lugar debes asegurarte de borrar de manera segura todos los datos de tu dispositivo. La forma más sencilla de hacerlo es restaurar el dispositivo. La función de restauración varía de un dispositivo a otro, abajo se enlistan los pasos para los dos dispositivos más comunes. Incluso un paso más seguro es asegurarte de que tienes el cifrado (encriptación) habilitado antes de restaurarlo. En la mayoría de los dispositivos recientes la forma más sencilla

de hacerlo es simplemente habilitar el bloqueo de pantalla (el cual con suerte ya tienes habilitado). Finalmente, recomendamos ampliamente respaldar tu dispositivo antes de restaurarlo.

- **Dispositivos Apple iOS: Configuración | General | Restaurar | Borrar todo el contenido y configuraciones.**
- **Dispositivos Android: Configuración | Privacidad | Restaurar la configuración de fábrica.**

SIM y tarjetas externas

Adicional a tu dispositivo, también necesitas considerar qué hacer con tu tarjeta SIM (acrónimo en inglés de Subscriber Identity Module). Esta tarjeta es lo que usa un dispositivo móvil para realizar una conexión celular o de datos. Cuando limpies tu dispositivo, la tarjeta SIM retiene información sobre tu cuenta y está ligada a ti. Si vas a mantener tu número telefónico y estás migrando a un nuevo dispositivo, habla con tu proveedor de servicio sobre transferir tu tarjeta SIM. Si no es posible, conserva tu antigua SIM y destrúyela para prevenir que cualquiera la reutilice para hacerse pasar por ti y obtener acceso a tu información y cuentas. También, algunos dispositivos móviles Android emplean una tarjeta SD (acrónimo en inglés de Secure Digital) removible para almacenamiento adicional. Remueve esas tarjetas de almacenamiento externo de tu dispositivo móvil antes de desecharlo. Esas tarjetas a menudo pueden ser reutilizadas en nuevos dispositivos móviles, o pueden ser empleadas como almacenamiento genérico en tu computadora mediante un adaptador USB. Si reutilizar la tarjeta SD no es posible, entonces como con tu vieja tarjeta SIM, recomendamos que la destruyas.

Si no estás seguro de los pasos cubiertos aquí o si las opciones de restauración de tu dispositivo son diferentes, lleva tu dispositivo móvil a la tienda donde lo compraste y solicita ayuda de un técnico capacitado. Por último, si vas a desechar tu dispositivo, en su lugar considera donarlo. Hay muchas organizaciones que aceptan dispositivos móviles usados y muchos proveedores de servicios móviles tienen contenedores de reciclaje en sus tiendas.

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

Editor Invitado

Christopher Crowley *(@CCrowMontance) es un consultor independiente del área de Washington DC, enfocado en operaciones de seguridad. Publica tuits y entradas de blog ocasionalmente. Mantente atento a la publicación de su próximo libro sobre Seguridad en Centros de Operación. Es consultor senior en el SANS Institute.*

Recursos

Curso de SANS: Pen Testing Mobile Devices:	https://sans.org/sec575
Curso de SANS: Advanced Smartphone Forensics Course:	https://sans.org/for585
¿Qué hacer ante la pérdida de tu smarth phone?:	https://revista.seguridad.unam.mx/sites/default/files/suplemento_30.pdf