OUCH! Diciembre 2022

El Boletín Mensual de Concientización en Seguridad para ti

Desechando tus dispositivos móviles

Resumen

Los dispositivos móviles, como celulares, relojes inteligentes y tabletas, continúan avanzando e innovando a un ritmo sorprendente. Como resultado, es posible que estés cambiando de dispositivo cada año. Desafortunadamente, es posible que no te des cuenta de cuánta información personal hay en tus dispositivos (mucha más que en tu computadora). A continuación, cubrimos los diferentes tipos de datos en tus dispositivos móviles y cómo puedes borrar tu dispositivo de forma segura antes de desecharlo o reemplazarlo. Si el dispositivo fue proporcionado por tu trabajo, primero consulta con tu jefe directo sobre los procedimientos de eliminación.

Tu información

Tus dispositivos móviles guardan más información sensible de la que te das cuenta, incluyendo. . .

Donde vives y trabajas, y tus hábitos de traslado diarios.
Los detalles de contacto de todas las personas en tu lista de contactos, incluidos familiares, amigos y compañeros de trabajo.
Historial de llamadas telefónicas, incluidas las llamadas entrantes, salientes, el correo de voz y llamadas perdidas.
Sesiones de chat o mensajes de texto dentro de aplicaciones como chat seguro, juegos y redes sociales.
Fotos personales, videos y grabaciones de audio.
Contraseñas almacenadas y acceso a tus cuentas, como tu banco, redes sociales o correo electrónico.
Información relacionada con tu salud, incluye tu edad, frecuencia cardíaca o historial de ejercicio.
Información financiera que incluye tarjetas de crédito, formas de pago y transacciones.

Borrando la información de tu dispositivo

Independientemente de cómo te deshagas de tu dispositivo móvil, ya sea donarlo, cambiarlo por uno nuevo, dárselo a alguien, revenderlo o incluso reciclarlo, primero borra toda tu información confidencial. No asumas que el próximo dueño "hará lo correcto". El primer paso es hacer una copia de seguridad del dispositivo para que puedas recuperar y transferir todos los datos y configuraciones a tu nuevo equipo. Una vez realizada la copia, deberás restablecer de fábrica el dispositivo, ya que esto borra tus datos y los restablece a los valores predeterminados. Durante el proceso de restablecimiento, se te puede solicitar que ingreses alguna contraseña para eliminar cualquier enlace con ese dispositivo a la nube; asegúrate de hacer esto. A continuación se muestran los pasos para restablecer los dos dispositivos más comunes: Apple y Android.
Dispositivos Apple iOS: Ajustes | General | Transferir o restablecer el iPhone | Borrar contenidos y ajustes.
Dispositivos Android: Configuración | Sistema | Opciones de restablecimiento | Borrar todos los datos (esto puede variar un poco de acuerdo al fabricante).

Tarjeta SIM y externas

Además de restablecer tu dispositivo, también considera qué hacer con tu tarjeta SIM (del inglés, Subscriber Identity Module). Esta es la pequeña tarjeta en tu teléfono proporcionada por el proveedor de telefonía; es lo que identifica tu dispositivo y te permite hacer llamadas o conectarte por datos móviles. Cuando borra los datos del dispositivo, la tarjeta SIM retiene información sobre tu cuenta y está vinculada a ti. Si conservarás tu número de teléfono y cambiarás a un nuevo dispositivo, habla con tu proveedor de telefonía acerca de la transferencia de la tarjeta SIM. Si esto no es posible, retira la tarjeta SIM anterior y destrúyela físicamente. Muchos de los celulares actuales tienen algo llamado eSIM, que es una tarjeta SIM virtual en lugar de una SIM física. La eSIM se borra durante el proceso de restablecimiento.

Finalmente, algunos dispositivos móviles Android utilizan una tarjeta SD (del inglés, Secure Digital) extraíble como almacenamiento adicional. Retira estas tarjetas de almacenamiento externo de tu dispositivo móvil antes de desecharlas. Estas tarjetas generalmente se pueden reutilizar en nuevos dispositivos móviles o se pueden usar como almacenamiento genérico en tu computadora con un adaptador USB. Si no es posible reutilizar la tarjeta SD, al igual que con la antigua tarjeta SIM, te recomendamos que la destruyas físicamente.

Si no estás seguro acerca de alguno de los pasos mencionados anteriormente, o si las opciones de restablecimiento de tu dispositivo son diferentes, lleva tu equipo a la tienda donde lo compraste para obtener ayuda. Finalmente, considera donar en vez de tirar el dispositivo. Hay muchas organizaciones benéficas que aceptan dispositivos móviles usados, y muchos proveedores de telefonía tienen contenedores en sus tiendas para reciclarlos.

Editor invitado

Heather Mahalik (@HeatherMahalik) es Directora senior de Inteligencia Digital en Cellebrite y coordina el plan de estudios de SANS DFIR, autora de FOR585 e instructora del SANS. La carrera de Heather se ha basado en investigación forense y 20 años de trabajo en casos. Su blog es www.smarterforensics.com/blog.

Recursos

Usando aplicaciones móviles de forma segura: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Asegurando tus dispositivos móviles: https://www.sans.org/newsletters/ouch/securing-mobile-devices/
Donando tu teléfono celular: https://www.makeuseof.com/best-places-to-donate-your-old-phone/
Curso del SANS: Curso avanzado de forense en teléfonos inteligentes: https://sans.org/for585

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