VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Junio 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- **Tu información**
- **Limpiar tu dispositivo**
- **SIM y tarjetas de almacenamiento externo**

Cómo desechar tu dispositivo móvil

Resumen

Los dispositivos móviles, como teléfonos inteligentes y tabletas, continúan avanzando y evolucionando a un ritmo asombroso. Como resultado, muchos de nosotros cambiamos de dispositivo móvil muy seguido, prácticamente cada 18 meses. Desafortunadamente, mucha gente se deshace de sus equipos viejos sin pensar en toda la información personal que éstos han acumulado. En este boletín hablaremos acerca del tipo de información personal que puede encontrarse en tu dispositivo móvil y cómo puedes borrarla de manera segura antes de devolverlo o deshacerte de él-. Si tu dispositivo pertenece a la empresa para la que trabajas o tiene alguna información organizacional almacenada, asegúrate de revisar con tu supervisor los procedimientos adecuados para el respaldo de información y el desecho de equipos antes de seguir los pasos que aquí presentamos.

Editor Invitado

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) es un consultor residente en Washington, DC. Es el instructor principal del curso de Seguridad en Dispositivos Móviles y Hacking Ético (SEC575) del Instituto SANS y autor del curso Gestión de Equipo de Respuesta a Incidentes (MGT535).

Tu información personal

Los dispositivos móviles almacenan datos mucho más sensibles de lo que te imaginas, muy probablemente más que tu computadora. La información típica almacenada por un dispositivo móvil puede incluir:

- El lugar donde vives, trabajas y lugares que visitas con frecuencia.
- Todos los datos de contactos en tu libreta de direcciones, incluyendo familia, amigos y compañeros de trabajo.
- Historial de llamadas entrantes, salientes y perdidas.
- Mensajes de texto y voz.
- Sesiones de chat dentro de las aplicaciones, como juegos y redes sociales.
- Historial de ubicación basado en coordenadas GPS o historial de torres celulares.
- Historial de navegación web, cookies y páginas en caché.
- Fotos personales, videos, grabaciones de audio y mensajes de correo electrónico.
- Contraseñas almacenadas y acceso a cuentas personales, como tu cliente de banca en línea o correo electrónico.
- Acceso a fotos, archivos o información almacenada en la nube.
- Cualquier información relacionada con la salud, incluida la frecuencia cardíaca, presión arterial o dieta.

Cómo desechar tu dispositivo móvil

Limpiando tu dispositivo

Como podrás darte cuenta, puede haber una gran cantidad de información sensible en tu dispositivo móvil. Independientemente de la forma en que te deshagas de él, ya sea donándolo, dándoselo a otro miembro de la familia, revendiéndolo o incluso tirándolo a la basura, necesitas asegurarte primero de borrar toda tu información sensible. Además, necesitas borrar tus datos si vas a devolver tu dispositivo móvil o a cambiarlo por uno nuevo. Si no lo haces, quien termine con tu dispositivo puede ser capaz de acceder fácilmente a tus datos. No obstante, antes de comenzar a limpiar tus datos, es muy probable que necesites hacer copias de seguridad, incluyendo fotos, videos o cualquier otra información. Una vez que lo limpies, no serás capaz de recuperar ninguno de los datos almacenados en él.

Cuando te deshagas de tu dispositivo móvil, asegúrate de realizar una restauración a los valores de fábrica y remover las tarjetas SIM y SD si tu dispositivo las tiene.

Cuando hayas realizado la copia de seguridad de tus datos, el siguiente paso es borrarlos de forma segura. Simplemente eliminar los archivos, fotos o datos no es suficiente. Los datos eliminados pueden ser recuperados fácilmente utilizando herramientas libres que se encuentran en Internet. En su lugar deseamos borrar de forma segura y definitiva toda la información en el dispositivo, a esto se le conoce como limpieza. Con esto, lo que sucede en realidad es que se sobrescribe la información, así nos aseguramos de que no se pueda recuperar. La forma más sencilla de hacerlo es utilizando la función de restablecimiento de fábrica del dispositivo. Esta acción lo regresará a la condición en que estaba cuando recién fue adquirido. Hemos encontrado que la restauración de fábrica representa el método más seguro y simple para eliminar datos del dispositivo móvil. La función de restablecimiento de fábrica varía en cada dispositivo, por lo que a continuación se enlistan los pasos a seguir para los tres dispositivos más populares.

- Dispositivos Apple iOS: Ajustes | General | Restablecer | Borrar contenidos y ajustes
- Dispositivos Android: Ajustes | Privacidad | Restablecer datos de fábrica
- Windows Phone: Ajustes | Acerca de | Restablecer configuración inicial

Si aún tienes preguntas acerca de cómo llevar a cabo un restablecimiento de fábrica, consulta el manual de propietario o la página web del fabricante. Recuerda, simplemente con borrar tus datos personales no es suficiente ya que se pueden recuperar fácilmente.

Cómo desechar tu dispositivo móvil

SIM y tarjetas de almacenamiento externo

Además de la información almacenada en tu teléfono, también debes considerar qué hacer con la tarjeta SIM (Módulo de Identidad del Suscriptor). La tarjeta SIM es usada por los dispositivos móviles para hacer llamadas o conectarse a Internet a través de la red de un operador. Cuando realizas una restauración a los valores de fábrica en tu dispositivo, la tarjeta SIM retiene información sobre tu cuenta. Si cambias tu dispositivo por uno nuevo y conservas tu número telefónico, solicita al vendedor transferir la tarjeta SIM. Si no es posible, por ejemplo, porque el tamaño de la SIM que usa el equipo nuevo es diferente, conserva la SIM vieja y destrúyela para prevenir que alguien más pueda reutilizarla.

Finalmente, algunos dispositivos móviles utilizan una tarjeta SD (Secure Digital) para almacenamiento adicional. Estas tarjetas usualmente almacenan fotos, aplicaciones y otro tipo de contenido sensible. Recuerda remover cualquier tarjeta de almacenamiento externo de tu dispositivo antes de deshacerte de él (en algunos dispositivos la tarjeta SD está escondida en el compartimiento de la batería o debajo de ella). Estas tarjetas pueden ser reutilizadas en nuevos dispositivos móviles o pueden ser usadas como almacenamiento genérico en una computadora usando un adaptador USB. Si no es posible reutilizar la tarjeta SD, al igual que con la tarjeta SIM vieja, recomendamos destruirla.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

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

Recursos

NIST SP800-88 Rev. 1 [Inglés]:
http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
Guía para borrar datos de un dispositivo móvil:
http://www.welivesecurity.com/la-es/2010/11/19/guia-para-borrar-datos-de-un-dispositivo-movil/
OUCH! Respaldos:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#september2013
Consejos para seguridad móvil:
http://revista.seguridad.unam.mx/numero-17/10-consejos-para-mantener-nuestra-seguridad-en-el-celular

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Demian García y Félix Hernández