VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Diciembre 2016

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- **Tu información**
- **Limpiando tu dispositivo**
- **Tarjetas SIM y de almacenamiento externo**

Deshacerse de dispositivos móviles de manera segura

Resumen

Los dispositivos móviles, como los smartphones, relojes inteligentes y tabletas, continúan avanzando e innovándose a un ritmo asombroso. Como resultado, algunas personas reemplazan sus dispositivos móviles casi cada año. Desafortunadamente, muchas personas se deshacen de sus equipos sin pensar cuántos datos personales están almacenados en ellos. En este boletín hablaremos de los tipos de información personal que pueden estar en tus dispositivos móviles y cómo eliminarlos de forma segura antes de devolverlos o deshacerte de ellos. Si tu equipo pertenece a la empresa o tiene alguna información organizacional almacenada, asegúrate de revisar con tu supervisor para realizar un respaldo adecuado de la información y sobre los procedimientos para el desecho de equipos antes de seguir los pasos que presentamos a continuación.

Editor Invitado

Heather Mahalik es la principal científico forense y lidera los esfuerzos forenses en Mantech. Es la coordinadora y coautora del curso avanzado de forense en teléfonos inteligentes (FOR585) e instructora de análisis forense de Windows (FOR408) del Instituto SANS. Ella escribe en **smarterforensics.com**, también puedes encontrarla en Twitter como **@HeatherMahalik** y Google+ como **+HMahalik**.

Tu información

Los dispositivos móviles almacenan más datos sensibles de los que podrías pensar, muchas veces más que en las computadoras. La información que puede incluir es:

- Donde tú vives, trabajas y los lugares que visitas frecuentemente.
- Los detalles de contactos de tu libreta de direcciones y aplicaciones, incluyendo tu familia, amigos y compañeros del trabajo.
- El historial de llamadas entrantes, salientes y perdidas.
- Mensajes de texto (SMS), voz y multimedia.
- Sesiones de chat dentro de las aplicaciones de chat seguro, juegos y redes sociales.
- Historial de ubicaciones basado en las coordenadas GPS o el historial de torres celulares.
- Historial de navegación web, historial de búsqueda, cookies y las páginas en caché.
- Fotografías personales, videos, grabaciones de audio y correos electrónicos.
- Contraseñas almacenadas y el acceso a cuentas personales, como la banca en línea y el correo electrónico.
- Acceso a fotografías, documentos e información almacenados en la nube.
- Cualquier información relacionada con tu salud, como la edad, la frecuencia cardiaca o la dieta.

Deshacerse de dispositivos móviles de manera segura

Limpiando tu dispositivo

Como puedes darte cuenta, hay una gran cantidad de información sensible en tu dispositivo móvil. Independientemente de la forma en que te deshagas de tu equipo, ya sea donándolo, intercambiándolo por uno nuevo, regálaselo a un miembro de la familia, vendiéndolo o incluso tirándolo a la basura, necesitas asegurarte de primero borrar toda la información sensible. Podrías no darte cuenta, pero simplemente eliminar los datos no es suficiente ya que pueden ser recuperados utilizando herramientas gratuitas en Internet. Necesitas borrar de manera segura los datos de tu dispositivo por medio de una limpieza, a través de la cual se sobrescribe la información asegurando que no se pueda recuperar o hace que se vuelva irrecuperable. Recuerda realizar una copia de seguridad antes de limpiar todos los datos, para que puedas reconstruir fácilmente tu nuevo dispositivo.

Cuando reemplaces tu dispositivo móvil, asegúrate de realizar una restauración de fábrica y remover las tarjetas SIM y SD.

La forma más sencilla de realizar la limpieza es utilizar la función “restauración de fábrica”, que devuelve el dispositivo a la condición en la que estaba cuando lo compraste. Hemos encontrado que la restauración de fábrica proporciona el método más seguro y simple para eliminar los datos. La función varía entre los equipos; a continuación enumeramos los pasos para realizarlo en los dos sistemas operativos más populares:

- Dispositivos iOS: Ajustes| General | Restablecer | Borrar contenido y configuración
- Dispositivos Android: Ajustes | Privacidad | Restablecer datos de fábrica

Por desgracia, eliminar los datos personales de los dispositivos Windows Phone no es tan simple como una restauración de fábrica; están realizando investigaciones sobre los métodos para asegurar que los datos personales se limpien desde el dispositivo. Si todavía tienes preguntas sobre cómo realizar una restauración de fábrica, consulta el manual de usuario o el sitio web del fabricante. Recuerda, solo borrar los datos personales no es suficiente, ya que se pueden recuperar fácilmente.

Tarjetas SIM y de almacenamiento externo

Además de los datos almacenados en tu dispositivo, también hay que considerar qué hacer con la tarjeta SIM (Módulo de Identificación del Suscriptor). El dispositivo móvil utiliza una tarjeta SIM para realizar una conexión celular o de datos. Al realizar un restablecimiento de fábrica, la tarjeta conserva la información de la cuenta y la vincula a ti, el usuario. Si deseas mantener tu número de teléfono y utilizar un nuevo dispositivo, habla con tu proveedor de servicios telefónicos para transferir la tarjeta. Si esto no es posible, por ejemplo, si tu nuevo teléfono utiliza un SIM de diferente tamaño, mantén tu antigua tarjeta y tritúrala físicamente o destrúyela para evitar que alguien la vuelva a usar.

Deshacerse de dispositivos móviles de manera segura

Por último, algunos dispositivos móviles utilizan una tarjeta SD (Secure Digital) para almacenamiento adicional. Estas tarjetas a menudo contienen imágenes, aplicaciones para teléfonos inteligentes y otros contenidos sensibles. Recuerda extraer las tarjetas de almacenamiento antes de desechar tu equipo (en algunos dispositivos las tarjetas SD pueden estar ocultas en el compartimiento de la batería, posiblemente debajo de ella). Estas tarjetas pueden ser a menudo reutilizadas en nuevos dispositivos o se pueden usar como almacenamiento genérico en una computadora con un adaptador USB. Si ya no vuelves a utilizarla, al igual que la tarjeta SIM, te recomendamos destruirla físicamente.

Si no estás seguro de los pasos que te sugerimos en este boletín, lleva tu equipo a la tienda donde lo compraste y obtén ayuda de un técnico capacitado. Por último, si vas a tirar a la basura tu dispositivo, te pedimos que consideres donarlo. Hay muchas organizaciones benéficas que aceptan dispositivos móviles usados.

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: securingthehuman.sans.org/ouch/archives

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

Consejos de seguridad para el celular:	http://revista.seguridad.unam.mx/numero-17/10-consejos-seguridad-celular
Información en dispositivos móviles:	https://revista.seguridad.unam.mx/numero-07/informacion-sensible-dispositivos-moviles
Cuida tu teléfono:	https://revista.seguridad.unam.mx/numero-07/cuida-tu-telefono
Cómo proteger otros dispositivos:	https://revista.seguridad.unam.mx/numero-07/y-mis-otros-dispositivos
Dispositivos móviles en redes corporativas:	

http://revista.seguridad.unam.mx/numero-21/dispositivos-moviles-riesgo-seguridad-redes-corporativas

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Katia Rodríguez y Célica Martínez

