Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- Información almacenada
- Limpieza de tu dispositivo
- Tarjetas SIM / Tarjetas SD
- Alternativas de desecho

Cómo deshacerse de dispositivos móviles de manera segura

EDITOR INVITADO

El equipo de Ouch! quiere darle la bienvenida y agradecer al Sr. Joshua Wright, nuestro editor invitado. Wright es instructor Senior del SANS y autor del curso Seguridad Wireless SEC617 y el curso Seguridad en Dispositivos Móviles SEC575. Puedes seguir a Wright en Twitter @joswr1ght o en su sitio web www.willhackforsushi.com.

RESUMEN

Los dispositivos móviles, como teléfonos inteligentes y tablets, continúan avanzando e innovando a un ritmo impresionante. Como resultado, muchos de nosotros reemplazamos nuestros dispositivos móviles con una frecuencia de al menos 18 meses. Una pregunta importante es "*¿Qué haces con tus dispositivos anteriores?*" Muchas personas simplemente se deshacen de ellos sin pensar en todos los datos personales que han almacenado. Sin embargo, una cantidad sorprendente de información personal es guardada en estos viejos dispositivos. Si tus dispositivos no son limpiados de manera segura antes de ser desechados, esta información puede ser recuperada fácilmente, exponiéndote a ti o a tu organización a un enorme riesgo.

INFORMACIÓN ALMACENADA

Los dispositivos móviles almacenan datos mucho más sensibles de lo que imaginas, incluso más de los que se encuentran en tu equipo de cómputo. Cuando desechas tus dispositivos podrías estar exponiendo información como:

- Los datos de los contactos en tu agenda, incluyendo familia, amigos y compañeros de trabajo.
- Historial de llamadas; entrantes, salientes y perdidas.
- Mensajes de texto o sesiones de chats.
- Historial de localización basado en coordenadas GPS o del proveedor de telefonía celular.
- Historial del navegador Web, cookies y páginas guardadas en caché.
- Fotos personales, videos, grabaciones de audio y correos electrónicos.
- Contraseñas guardadas y accesos a cuentas personales, como el correo de voz.

LIMPIEZA TU DISPOSITIVO

Antes de iniciar un limpiado seguro de tu dispositivo móvil, considera si quieres o no guardar un respaldo de tus datos, como fotos, videos o cualquier otra información, ya que una vez que hayas seguido los siguientes pasos, no habrá manera de recuperarlos. Además, si el dispositivo es de tu empresa o tiene datos de la organización guardados en él,

Cómo deshacerse de dispositivos móviles de manera segura

asegúrate de revisarlo con tu superior para hacer una copia de seguridad apropiada y conocer los procedimientos a seguir antes de continuar.

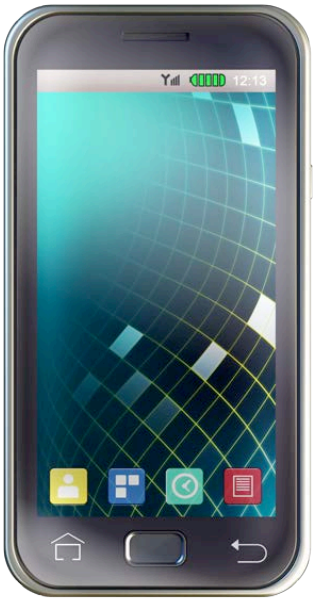
Desafortunadamente, es insuficiente con solo borrar los datos, éstos aun pueden ser recuperados; por lo que te recomendamos usar la función “Restaurar las configuraciones de fábrica” que borrará todos los datos de tu dispositivo y lo regresará a las condiciones que tenía cuando lo adquiriste. Éste es el método más seguro para eliminar los datos de tus dispositivos móviles.
La ubicación de la función de restauración, varía entre dispositivos; a continuación se muestran los pasos a seguir para los más populares.

- Dispositivos Apple iOS: Ajustes | General | Restablecer | Borrar contenidos y ajustes
- Dispositivos Android: Ajustes | Privacidad | Restaurar datos de fábrica
- Windows Phone: Configuración | Acerca de | Restablecer configuración inicial
- BlackBerry: Opciones | Opciones de seguridad | Borrado de seguridad

Si aún tienes dudas acerca de cómo realizar una restauración de fábrica, revisa el manual de usuario o visita el sitio web del fabricante. Otra opción es llevar tu dispositivo móvil a la tienda donde lo adquiriste y solicitar ayuda de un técnico especializado para restaurarlo.
Recuerda que, borrar los datos personales no es suficiente puesto que pueden ser recuperados fácilmente.

TARJETAS SIM

Además de los datos almacenados en tu dispositivo, también debes considerar qué hacer con tu tarjeta SIM (acrónimo en inglés de *Subscriber Identity Module*). Muchos dispositivos móviles usan una tarjeta SIM para identificarse de forma exclusiva ante la red con la clave de



SD Card

SIM

Cuando reemplaces tu dispositivo móvil, asegúrate de eliminar toda la información personal. Por lo menos, asegúrate de realizar una restauración de fábrica y quitar las tarjetas SIM y SD.

servicio de suscriptor cuando haces y recibes llamadas. Al realizar una restauración de fábrica del dispositivo, la tarjeta SIM conserva información sobre tu clave. Si deseas mantener tu número telefónico y usarlo en un nuevo dispositivo, infórmate con tu proveedor sobre cómo transferir tu tarjeta SIM. Si esto no es posible, por ejemplo, si tu nuevo teléfono utiliza un tamaño diferente de tarjeta SIM, conserva tu vieja tarjeta SIM y destrúyela para prevenir que alguien más la reutilice.

TARJETAS EXTERNAS DE ALMACENAMIENTO

Algunos dispositivos móviles usan una tarjeta externa SD (Secure Digital, por sus siglas en inglés) para almacenamiento adicional. Estas tarjetas generalmente

Cómo deshacerse de dispositivos móviles de manera segura

contienen fotos, aplicaciones del teléfono inteligente u otro contenido sensible. Recuerda quitar cualquier tarjeta de almacenamiento externo antes de deshacerte de tu dispositivo (para algunos dispositivos, la tarjeta SD puede estar oculta en el compartimiento de la batería). Estas tarjetas generalmente pueden ser reutilizadas en los nuevos dispositivos móviles, o pueden ser usadas como un almacenamiento genérico en tu computadora con un adaptador USB. Si no es posible reutilizar tu tarjeta SD, entonces procede de la misma manera que con tu antigua tarjeta SIM, destrúyela.

ALTERNATIVAS DE DESECHO

Cuando estés próximo a cambiar tu antiguo dispositivo móvil, en vez de arrojarlo a la basura, considera reciclarlo. Muchas compañías ofrecen descuentos para tu próxima compra cuando reciclas. Otra opción es donar tu dispositivo móvil a la caridad. Te mostramos algunos sitios donde puedes reciclar o donar tus dispositivos móviles.

Programa de reciclaje Apple
http://preview.tinyurl.com/89cd7vm

Programa de reciclaje Verizon
http://preview.tinyurl.com/7obzkly

Programa de reciclaje AT&T
http://preview.tinyurl.com/7crywcb

Programa de reciclaje Nokia
http://preview.tinyurl.com/7fpgvpf

Programa de reciclaje Telefónica
http://preview.tinyurl.com/75bgrco

Reciclaje de móviles
http://preview.tinyurl.com/c6xkd6d

Dona tu móvil
http://preview.tinyurl.com/dajs7q

RECURSOS

Algunos de los enlaces mostrados a continuación, se redujeron para mejorar la legibilidad a través del servicio de TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino solicitando permiso antes de abrirlo.

Términos de Seguridad:
http://preview.tinyurl.com/7m4n6og

Tips diarios de seguridad del SANS:
http://preview.tinyurl.com/6s2wrkp

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Iván Alvarado, Pablo Lorenzana, Israel Andrade, Célica Martínez