Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Resumen**
- **Precauciones que puedes tomar desde ahora**
- **¿Qué hacer si tu dispositivo móvil se extravía o es robado?**

Perdiste tu dispositivo móvil

EDITOR INVITADO

La editora invitada para esta publicación es Heather Mahalik, quien es instructora certificada del SANS y técnico forense en dispositivos móviles de tecnologías básicas, cerca de Washington, DC. Puedes seguirla en su cuenta de Twitter @heathermahalik

RESUMEN

Utilizamos dispositivos móviles para comunicarnos, obtener e intercambiar información. Como resultado de esto, los dispositivos a menudo contienen información sensible, incluyendo correos electrónicos, mensajes de texto, correos de voz, calendarios de eventos, localizador, fotos y videos. Si pierdes o te roban tu dispositivo móvil, cualquiera que tenga control físico sobre él puede acceder potencialmente a toda tu información y divulgarla, tus contactos y organización estarían en un serio problema. En este boletín, discutiremos los pasos que puedes tomar para proteger la información de tu dispositivo en caso de que se extravíe o sea robado.

Nota: La mayoría de estos consejos se aplican a tus dispositivos personales. Si tu dispositivo móvil fue comprado o autorizado por tu empresa y contiene datos de ésta, entonces asegúrate de seguir las políticas de la organización sobre aseguramiento de dispositivos móviles y para reportar su pérdida o robo.

PRECAUCIONES QUE PUEDES TOMAR DESDE AHORA

Una de las maneras más eficaces de proteger tu información es asegurar tu dispositivo mientras todavía lo tienes. Una buena forma de comenzar es activando algún tipo de protección de acceso, tal como un NIP, contraseña o patrón de bloqueo. Esto ayuda a asegurar que sólo los usuarios autorizados puedan acceder y utilizar la información en tu dispositivo.

- **NIP:** Un NIP (Número de Identificación Personal) es un número que deberás ingresar para poder acceder a tu dispositivo móvil.
- **Contraseña:** Una contraseña en un dispositivo móvil trabaja del mismo modo que una contraseña en tu computadora o cuentas en línea. Esta es una opción que puedes activar en la mayoría de los teléfonos inteligentes. Una contraseña robusta proporciona mayor seguridad que un NIP.
- **Patrón de bloqueo:** Un patrón de bloqueo es único y lo dibujas en la pantalla del dispositivo.

Considera seriamente habilitar la opción de borrar la información de tu dispositivo tras un determinado número de intentos de acceso fallidos, esto lo protegerá si cae en manos equivocadas. Sin embargo, si activas esta función debes estar alerta de los niños curiosos que quieran jugar con él.

Perdiste tu dispositivo móvil

Independientemente de los mecanismos de autenticación que utilices, asegúrate de no compartir tu NIP, contraseña o patrón de bloqueo con nadie más y que sea difícil de adivinar.

- **Localización remota y borrado de información**: La mayoría de los dispositivos móviles soportan software para localizar y/o borrar remotamente tu información de un dispositivo extraviado. Posiblemente, necesites instalar o configurar algún software especial mientras todavía tienes tu dispositivo. iPhones y iPads vienen con esta característica, llamada "Buscar mi iPhone" y se activa mediante un ID de Apple. Los dispositivos BlackBerry deben estar ligados a un servidor BES o a una aplicación similar para borrar de forma remota la información. Por otro lado, los dispositivos Android deben tener instalado un software especial para localizar y borrar remotamente la información del móvil.
- **Cifrado:** Si alguien tiene acceso físico a tu dispositivo móvil, puede utilizar tecnologías avanzadas e intentar evadir tu contraseña o NIP y acceder a la información almacenada en él. El cifrado protege tu información contra estos o más tipos de ataques. Algunos dispositivos móviles vienen con un cifrado incorporado, mientras que otros requieren que se les habilite la funcionalidad o instale un software de cifrado. iPhones y iPads integran en su sistema el cifrado de hardware que se activa automáticamente. Sin la contraseña, tus datos están protegidos. Android también brinda el cifrado que se puede activar en el menú de seguridad.
- **Copia de seguridad:** Las copias de seguridad ayudan a prevenir que puedas recuperar tu información rápidamente desde un dispositivo extraviado o robado. Los respaldos deben realizarse regularmente y se pueden hacer utilizando los siguientes métodos.

Tomando algunas medidas simples ahora, puedes protegerte después si se extravía alguno de tus dispositivos móviles

  - Hacer la copia de seguridad directamente en tu computadora.
  - iCloud se ofrece como un servicio gratuito para todos los usuarios de iPhone, iPad y iPod. El usuario puede realizar una copia de seguridad de sus contactos, correo electrónico, agenda, fotos, música y otros archivos a su cuenta de iCloud.
  - Google Cloud es un servicio de copia de seguridad gratuito para dispositivos Android. Las características de Google Cloud son similares a las de iCloud.

Perdiste tu dispositivo móvil

¿QUE HACER SI TU DISPOSITIVO MOVIL SE EXTRAVIA O ES ROBADO?

Sigue estos pasos para proteger tu información personal si tu dispositivo se extravía o es robado.

- Si el dispositivo extraviado fue comprado por la empresa en la que trabajas para tu uso o contiene información relacionada con el trabajo, reporta el extravío inmediatamente al centro de atención a usuarios de tu empresa o al equipo de seguridad y sigue sus instrucciones.
- Si instalaste el software de localización en tu dispositivo, lo más probable es que tenga la opción de borrar la información remotamente. Limpiando el dispositivo borrarás toda tu información personal de éste y eliminarás el riesgo de que tus datos sean comprometidos. Si tu dispositivo fue robado, lo recomendable es contactar con las autoridades antes de borrar la información de él y notificarles que tiene activado el software de localización. Si lo roban, no intentes recuperar tu dispositivo tú mismo.
- Contacta con tu compañía telefónica o proveedor de servicio de telecomunicaciones para informarles que tu dispositivo ha sido extraviado o robado. Ellos pueden bloquear tu número telefónico para asegurarse que nadie más use tu dispositivo para realizar llamadas telefónicas hasta que te sea reemplazado.
- Una vez que hayas comprado un reemplazo, puedes utilizar las copias de seguridad para recuperar tu información.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio 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.

3 aplicaciones de seguridad en iPhone
http://preview.tinyurl.com/6qoayu
Google Cloud:
http://preview.tinyurl.com/cy49ntb
iCloud:
https://www.icloud.com/#find
SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp
Consejos de seguridad:
http://preview.tinyurl.com/8fpbhtw
Aplicaciones de seguridad para android:
http://designeed.net/aplicaciones-seguridad-android/
Consejos de seguridad para android:
http://preview.tinyurl.com/92qfqym
Qué hacer en caso de pérdida de smartphones android:
http://preview.tinyurl.com/8rppzuw
¿Qué hago en caso de pérdida de mi smartphone?:
http://preview.tinyurl.com/8m2fwmw

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: Abraham Cueto, Mario Martínez, Célica Martínez, Jazmín López