VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Febrero 2012

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- Obtén aplicaciones
- Configura y usa las aplicaciones
- Actualiza las aplicaciones
- Realiza compras desde la aplicación

Asegura las aplicaciones de tu dispositivo móvil

EDITOR INVITADO

Kevin Johnson es el editor invitado para esta edición. Kevin es consultor de seguridad sénior en Secure Ideas, está a cargo de MySecurityScanner.com. Además, es instructor sénior en el SANS Institute. Puedes encontrar más información en www.secureideas.net y www.mysecurityscanner.com.

RESUMEN

Los dispositivos móviles se han convertido en una de las principales herramientas que utilizamos tanto en nuestra vida personal como en la profesional. Uno de los aspectos que hacen tan poderosos a estos dispositivos, son las miles de aplicaciones que podemos utilizar. Sin embargo, con el inmenso poder y flexibilidad de las aplicaciones viene una serie riesgos de los que debes ser consciente. En este boletín abordamos los peligros de las aplicaciones para dispositivos móviles, cómo puedes instalarlas, utilizarlas y mantenerlas seguras.

Obtén aplicaciones

El primer paso al usar aplicaciones, es asegurarse de descargarlas siempre de una fuente segura y confiable. Los cibercriminales crean aplicaciones maliciosas que parecen ser auténticas, pero en realidad están infectadas con virus o gusanos. Si instalas de manera inadvertida una de estas aplicaciones, los cibercriminales pueden tomar el control de tu dispositivo móvil. Cuando descargas aplicaciones de fuentes conocidas y de confianza, reduces la posibilidad de instalar una aplicación infectada. Sin embargo, aún en tiendas de aplicaciones en línea reconocidas, se pueden encontrar algunas aplicaciones maliciosas. Esto ocurre específicamente en ciertos dispositivos, como por ejemplo Android, donde las tiendas de aplicaciones no están estrictamente controladas. Para reducir el riesgo, evita descargar aplicaciones que sean muy recientes, que poca gente haya descargado o que tengan muy pocos comentarios. Entre más tiempo esté disponible una aplicación, o más comentarios positivos tenga, es más probable que la aplicación resulte confiable. Finalmente, instala sólo las aplicaciones que necesitas y utilizas. Cada aplicación adicional conlleva el potencial de nuevas vulnerabilidades, así que si dejas de utilizar una aplicación, elimínala de tu dispositivo móvil.

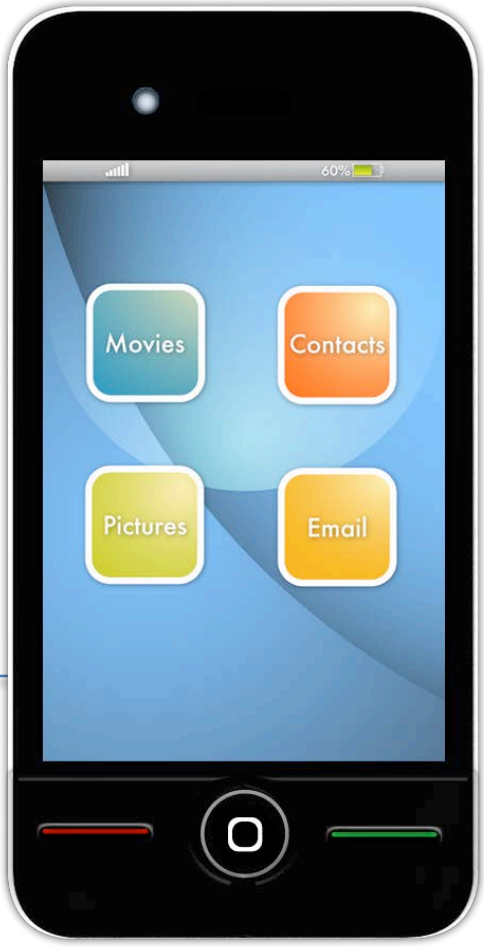
Por otro aparte, puede que estés tentado a realizar un "*jailbreak*" o "*rooteo*" a tu propio dispositivo móvil, el proceso que permite hackear e instalar aplicaciones no aprobadas, o modificar su funcionalidad. Recomendamos no realizar esto, ya que el "*jailbreaking*" no sólo evita o elimina muchos de los controles de seguridad integrados en el dispositivo móvil, sino que a menudo anula cualquier garantía o contrato de soporte.

Asegura las aplicaciones de tu dispositivo móvil

Configura y usa las aplicaciones

Una vez que instalaste la aplicación desde una fuente confiable, el siguiente paso es asegurarse de configurarla de manera segura, y proteger tu privacidad. Instalar y/o configurar ciertas aplicaciones requiere que concedas ciertos privilegios y permisos. Dependiendo del dispositivo, estas aplicaciones pedirán autorización. Piensa siempre antes de autorizar cualquier acceso, ¿tu aplicación realmente necesita estos permisos? Por ejemplo, algunas aplicaciones utilizan servicios de geolocalización. Si permites que una aplicación sepa tu ubicación, podrías permitirle a su autor seguir tus movimientos. Además, cualquier mensaje que publiques podría incluir tu ubicación, permitiendo a cualquiera conocer dónde te encuentras o comprobar dónde has estado. Si no estás de acuerdo con los permisos que te solicita una aplicación, simplemente busca otra que se ajuste mejor a tus expectativas.

Sé cuidadoso al utilizar aplicaciones que soliciten o almacenen información sensible. Incluso si la aplicación es legítima, no hay garantía de que el desarrollador maneje buenas prácticas de programación para proteger tu información mientras la almacena en el dispositivo o la transmite en internet. Las aplicaciones que refuerzan la información sensible pueden ser muy convenientes, pero también son objetivos de los cibercriminales. Lee la descripción detallada de la aplicación y los comentarios de otros usuarios para ver si hay antecedentes de problemas de seguridad.



La clave para mantener seguras las aplicaciones en tus dispositivos móviles, es instalarlas únicamente de fuentes confiables y seguras; así como tenerlas siempre actualizadas.

Actualiza las aplicaciones

Las aplicaciones, al igual que tu computadora y el sistema operativo de tu dispositivo móvil, se deben actualizar para estar al día. Continuamente, los criminales cibernéticos buscan y encuentran debilidades en las aplicaciones; además, desarrollan ataques para aprovechar estas vulnerabilidades. Los desarrolladores que crearon tus aplicaciones, también diseñaron y publicaron actualizaciones para reparar esas vulnerabilidades, y proteger los dispositivos. Verificar e instalar actualizaciones

Asegura las aplicaciones de tu dispositivo móvil

periódicamente es lo más recomendable. Te aconsejamos monitorear tu tienda de aplicaciones, y actualizar las que tengas instaladas al menos una vez al mes. Además, puedes configurar algunas aplicaciones para que se actualicen automáticamente, pero ten en cuenta que esto también podría aprobar permisos si lo solicita la aplicación.

Realiza compras desde la aplicación

Hoy en día, muchas aplicaciones permiten la compra de características adicionales, nuevos contenidos o la eliminación de publicidad. Un error común que algunas personas cometen es almacenar localmente sus credenciales de tienda de aplicaciones en su dispositivo, ya que esto les permite comprar fácilmente futuras aplicaciones. Es muy recomendable que no permitas que tu dispositivo móvil guarde estas credenciales, tampoco información de inicio de sesión o información de pago. Aunque conveniente, esta información podría estar disponible (o ser mal utilizada) para cualquiera que acceda a tu dispositivo móvil, o en caso de que tu dispositivo fuera hackeado de forma remota. Otra opción es utilizar tarjetas de regalo o tarjetas de crédito virtuales que se utilizan una sola vez.

Conclusión

Te recomendamos que sigas cada una de las mejores prácticas discutidas aquí. Los dispositivos móviles y sus aplicaciones, son todavía un campo relativamente nuevo y de rápido crecimiento. Además, uno de los desafíos que enfrentamos es la existencia de pocas opciones disponibles de software de seguridad para ayudar a protegerte a ti y a tus aplicaciones. Recuerda: ¡Tú eres la mejor defensa para tus dispositivos móviles!

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.

Podcast (seguridad en aplicaciones móviles, enfoque Android): http://preview.tinyurl.com/7s4gkt4

5 formas de proteger tus aplicaciones móviles: http://preview.tinyurl.com/8a3n4n5

iPhone Security Overview: http://preview.tinyurl.com/783hg2v

iPhone App Insecurity: http://preview.tinyurl.com/3w5a5cc

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: Mayra Villeda, Francisco Martínez, Galvy Cruz, Mario Martínez, Célica Martínez