VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Marzo 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

Uso seguro de aplicaciones móviles

Resumen

Los dispositivos móviles como tabletas, teléfonos inteligentes y relojes se han convertido en una de las principales tecnologías que utilizamos en nuestra vida personal y profesional. Lo que hace que los dispositivos móviles sean tan versátiles son las millones de aplicaciones que podemos elegir. Estas aplicaciones nos permiten ser más productivos, comunicarnos al instante y compartir con otros, capacitar y educar, o simplemente divertirnos más; sin embargo, vienen con riesgos. Aquí te proporcionamos recomendaciones para hacer más seguro el uso de la mayoría de tus aplicaciones móviles.

Editor Invitado

Joshua Wright es el director técnico en Counter Hack e instructor senior en el Instituto SANS. Él es el autor del curso SEC575: Seguridad en dispositivos móviles y hackeo ético, y del libro Hacking Exposed: Wireless. Puedes encontrar a Josh en Twitter como **@joswr1ght**.

Obtención de aplicaciones móviles

El primer paso es asegurarse de que siempre se descarguen aplicaciones móviles desde una fuente segura y confiable. Los cibercriminales han dominado sus habilidades en la creación y distribución de aplicaciones infectadas que aparentan ser legítimas. Si instalas alguna de estas, los criminales pueden tomar el control completo de tu dispositivo. Al descargar aplicaciones desde fuentes conocidas y de confianza se reduce la posibilidad de instalar una infectada. De lo que posiblemente no te has percatado es que la marca del dispositivo móvil que usas determina tus opciones para descargar aplicaciones.

Para los dispositivos de Apple, como un iPad o iPhone, únicamente se pueden descargar aplicaciones desde App Store. La ventaja de esto es que Apple realiza una revisión de seguridad para todas las aplicaciones antes de que estas estén disponibles. Aunque Apple no puede frenar todas las aplicaciones infectadas, este entorno administrado ayuda a reducir drásticamente el riesgo de instalar una. Además, si Apple encuentra o cree que una aplicación en su tienda está infectada, la elimina rápidamente. Windows Phone utiliza un enfoque similar para administrar sus aplicaciones.

Los dispositivos móviles Android son diferentes. Android brinda una mayor flexibilidad al poder descargar una aplicación móvil desde cualquier lugar de Internet. Sin embargo, esta flexibilidad conlleva una mayor responsabilidad. Tienes que ser más cuidadoso con las aplicaciones móviles que descargas e instalas, ya que no todas son revisadas. Google

Uso seguro de aplicaciones móviles

mantiene una tienda de aplicaciones similar a la de Apple, llamada Google Play. Las aplicaciones que descargas desde ahí han pasado por algunas revisiones básicas de seguridad. Como tal, te recomendamos que descargues tus aplicaciones únicamente desde Google Play. Evita descargar aplicaciones desde otros sitios web, ya que cualquier persona, incluidos los ciberdelincuentes, pueden fácilmente crear y distribuir aplicaciones maliciosas y engañarte para infectar tu dispositivo. Como una protección adicional, cuando sea posible instala un antivirus en tu equipo.

La clave para asegurar tu dispositivo móvil es instalar aplicaciones de fuentes confiables, instalar las actualizaciones cuando estén disponibles y otorgar únicamente los permisos requeridos.

Independientemente del dispositivo que estés utilizando, un paso más que puedes realizar es evitar aplicaciones nuevas que pocas personas han descargado o que tienen muy pocos comentarios positivos. Cuanto más tiempo haya estado disponible una aplicación, más personas la utilizarán y podrá tener más comentarios positivos, por lo tanto, es más probable que sea una aplicación confiable. Además, instala únicamente aplicaciones que necesites y uses. Pregúntate, ¿realmente necesito esta aplicación? Cada aplicación no solo traerá potencialmente nuevas vulnerabilidades sino también nuevos problemas de privacidad. Si dejas de usar una aplicación, desinstálala de tu dispositivo (siempre la puedes volver a instalar después si la necesitas y está disponible). Por último, nunca trates de escalar privilegios realizando un jailbreak o root en tu equipo; este es el proceso de hackear el dispositivo e instalar aplicaciones no aprobadas o cambiar funcionalidades incorporadas. Esto no solo evade o elimina muchos de los controles de seguridad incorporados en tu dispositivo móvil, sino que en la mayoría de los casos también anula garantías y contratos de soporte.

Permisos

Una vez que hayas instalado una aplicación de una fuente de confianza, asegúrate de que está configurada de manera segura y protege tu privacidad. Piensa siempre antes de permitir un acceso a la aplicación: ¿quieres conceder los permisos que solicita? ¿realmente los necesita? Por ejemplo, algunas aplicaciones utilizan servicios de geolocalización. Si permites que conozca siempre tu ubicación, estás autorizando a que el creador de esa aplicación rastree tus movimientos o que incluso venda esa información a otros. Si no deseas otorgar los permisos, niega la solicitud o busca otra aplicación que cumpla con tus requisitos. Recuerda, existen muchas opciones allá afuera.

Uso seguro de aplicaciones móviles

Actualización de aplicaciones

Las aplicaciones, al igual que las computadoras y el sistema operativo de los dispositivos móviles, deben actualizarse para mantenerse al día y seguras. Los criminales constantemente están buscando y encontrando debilidades en las aplicaciones para posteriormente, desarrollar ataques que las exploten. Los autores de la aplicación también crean y publican actualizaciones para corregir estas debilidades y proteger tus dispositivos. Cuanto más a menudo revises e instales actualizaciones, mejor. La mayoría de los dispositivos permiten configurar el sistema para realizar las actualizaciones de forma automática, te recomendamos esta configuración; si no es posible, revisa al menos cada dos semanas si existen. Por último, cuando actualices las aplicaciones, asegúrate siempre de verificar los nuevos permisos que puedan necesitar.

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

Mantener la seguridad en el celular: http://revista.seguridad.unam.mx/numero-17/10-consejos-seguridad-celular

Información sensible en dispositivos móviles:
https://revista.seguridad.unam.mx/numero-07/informacion-sensible-dispositivos-moviles

Riesgos de seguridad en Android: https://revista.seguridad.unam.mx/numero23/riesgos-de-seguridad-en-android

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

Deshacerse de dispositivos móviles de manera segura:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201612_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: José Daniel Campuzano, Víctor Arteaga y Katia Rodríguez