VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Enero, 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Uso seguro de aplicaciones móviles

Resumen

Los dispositivos móviles como las tabletas y los teléfonos inteligentes se han convertido en una de las principales tecnologías que se utilizan tanto a nivel personal como profesional. Lo que los hace tan versátiles son las millones de aplicaciones que tenemos para elegir. Éstas nos permiten ser más productivos, comunicarnos y compartir con otros al instante, capacitarnos y educarnos o simplemente divertirnos. Debes saber que con el poder de estas aplicaciones móviles vienen ciertos riesgos. Aquí hay algunos pasos que puedes tomar para mantener seguras tus aplicaciones móviles al utilizarlas.

Editor Invitado

Chris Crowley es consultor independiente, instructor certificado del SANS y autor de varios cursos. Puedes encontrarlo en Twitter: **@CCrowMontance** y en Google plus: **+ChrisCrowley**.

Adquirir aplicaciones

El primer paso es descargarlas siempre desde un lugar seguro, una fuente confiable. Recuerda que prácticamente cualquier persona puede crear una aplicación móvil, así que tienes que ser cuidadoso cuando eliges una. Los cibercriminales han mejorado sus habilidades para crear y distribuir aplicaciones móviles infectadas que parecen ser legítimas. Si instalas una de esas aplicaciones infectadas, podrían tomar control de tu dispositivo, es decir, leer tus correos electrónicos, escuchar tus conversaciones o recolectar todos tus contactos. Al descargar aplicaciones solamente desde sitios bien conocidos y confiables, se reducen las posibilidades de instalar una aplicación infectada. Algo que probablemente no has notado es que la marca del dispositivo que utilizas determina las opciones que tienes.

Para los dispositivos Apple como el iPhone o el iPad sólo puedes descargar aplicaciones móviles desde un ambiente controlado, la Apple Store. La ventaja es que así Apple realiza un chequeo de seguridad tanto a las aplicaciones móviles como a sus autores. Aunque Apple no puede rastrear a todos los chicos malos o a todas las aplicaciones móviles infectadas, este entorno controlado te ayuda a reducir de forma importante el riesgo de que instales una aplicación infectada. Además, si Apple encuentra una aplicación en su tienda que podría ser maliciosa, inmediatamente la remueve. Windows Phone utiliza una manera similar de manejar sus aplicaciones.

Los dispositivos móviles Android son diferentes. Android te da más flexibilidad al permitir descargar una aplicación móvil desde cualquier lugar en Internet, pero con tal flexibilidad viene más responsabilidad. Tienes que ser más

Uso seguro de aplicaciones móviles

cuidadoso sobre qué aplicaciones móviles descargas e instalas pues no todas son revisadas. Google realiza mantenimiento y administra la tienda de aplicaciones móviles de forma similar a Apple, la tienda es llamada Google Play. Las aplicaciones que descargas desde ahí cuentan con algunas revisiones básicas. De esta forma te recomendamos que descargues tus aplicaciones móviles para Android sólo desde la tienda Google Play. Evita descargar aplicaciones móviles Android desde otro sitio pues cualquier persona, incluyendo cibercriminales, pueden crear y distribuir de manera muy fácil aplicaciones móviles maliciosas y engañarte para infectar tu dispositivo. Como una protección adicional considera instalar un antivirus en tu dispositivo móvil.

La clave del uso seguro de las aplicaciones móviles es instalarlas sólo desde fuentes confiables, actualizarlas y verificar sus permisos.

Para reducir el riesgo aún más, evita aplicaciones que son nuevas, las que poca gente ha descargado o aquellas que tienen pocos comentarios positivos. Cuanto más ha estado disponible una aplicación o mientras más comentarios positivos tiene, es más probable que la aplicación sea confiable. También te recomendamos instalar únicamente las aplicaciones que necesitas. Pregúntate a ti mismo si realmente necesitas esa app. Cada aplicación trae nuevas vulnerabilidades y también nuevos riesgos a la privacidad. Si dejas de utilizar una aplicación, quítala de tu dispositivo móvil (siempre podrás agregarla nuevamente si crees que la necesitas).

Permisos

Una vez que has instalado una aplicación móvil desde una fuente confiable, el siguiente paso es asegurarse de que está configurada de forma segura y que protege tu privacidad. Instalar o configurar aplicaciones móviles constantemente requiere que tú les concedas ciertos permisos. Piensa, antes de autorizar cualquier acceso, si la aplicación realmente necesita esos permisos para hacer lo que dice que hará. Por ejemplo, algunas aplicaciones usan servicios de geolocalización, si una app sabe siempre tu ubicación podría permitir al creador rastrear todos tus movimientos, incluso podría vender esa información a otros. Si no deseas conceder los permisos a una app que lo requiere, te recomendamos buscar en las tiendas por otra aplicación que realmente alcance tus expectativas. Recuerda, tienes muchas opciones. Los dispositivos Apple permiten cambiar algunos permisos en la sección de configuración o al momento de correr la aplicación, como el acceso a la información de geolocalización. Los dispositivos Windows y Android son diferentes, presentan un formato de todo o nada. Si tú no les concedes todos los permisos que se especificaron, no puedes instalar la aplicación.

Uso seguro de aplicaciones móviles

Actualizaciones

Las aplicaciones móviles, al igual que el sistema operativo de una computadora o de un dispositivo móvil, deben actualizarse con el fin de mantenerse vigente. Los cibercriminales constantemente buscan debilidades en las aplicaciones y desarrollan ataques para explotar esas debilidades. Los desarrolladores que crearon tu aplicación también crean y liberan actualizaciones para corregir esas debilidades y proteger tus dispositivos. Mientras más revises e instales actualizaciones es mejor. Muchas plataformas te permiten configurar tu sistema y actualizar tus aplicaciones móviles de forma automática. Te recomendamos esta característica, pero si no es posible, revisa si hay nuevas actualizaciones al menos cada dos semanas. De cualquier forma, cuando tus aplicaciones están actualizadas asegúrate de verificar si requieren de algún nuevo permiso.

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: http://www.securingthehuman.org

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

Ingeniería social:	http://www.securingthehuman.org/ouch/2014#november2014
Cómo desechar tu dispositivo móvil:	http://www.securingthehuman.org/ouch/2014#june2014
Cómo asegurar tu nueva tableta electrónica:	http://www.securingthehuman.org/ouch/2013#december2013
Consejos de seguridad:	http://www.seguridad.unam.mx/usuario-casero/consejos/
[Curso SANS] SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Jazmín López

