VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Enero 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- **Asegurando tu tableta**
- **Manteniéndola segura**

Asegurando tu nueva tableta

Resumen

¡Felicidades por tu nueva tableta! Esta tecnología es una forma poderosa y fácil para comunicarse con otros, comprar en línea, ver películas, jugar y realizar un sin número de actividades. Como probablemente será una parte importante de tu vida, quizás reemplace a tu computadora, aquí tienes algunos pasos clave para mantener segura tu tableta y tu información.

Editor Invitado

Lori Rosenberg tiene una amplia experiencia en el desarrollo de material educativo sobre seguridad de la información y en la capacitación para empleados y clientes; le apasiona la búsqueda de nuevos métodos para la transmisión del conocimiento. Puedes encontrarla en Twitter como **@InfoSecLori**.

Asegurando tu tableta

Te sorprendería saber que el mayor riesgo para tu tableta no son los hackers, podrías ser tú; es mucho más probable que la pierdas, la olvides o te la roben y después la hackeen. Lo primero que debes hacer para protegerla es activar el bloqueo automático de la pantalla, cada vez que desees usarla deberás desbloquearla con una contraseña fuerte, dibujando un patrón o con tu huella dactilar. Esto te asegura que si la pierdes o te la roban nadie podrá acceder a ella, protegiendo tu información personal, tus aplicaciones y todo lo que esté en ella.

Una vez que tienes habilitado el bloqueo automático de tu pantalla, aquí hay otros consejos que te pueden ayudar a proteger tu nueva tableta:

1. Instala o habilita un software que te permita la localización remota del dispositivo a través de Internet. De esta manera, si tu tableta es extraviada o robada, podrás conectarte a ella a través de Internet y ubicarla o, en caso de ser necesario, realizar un borrado remoto de la información contenida en ella.
2. Actualiza tu dispositivo y habilita las actualizaciones automáticas, de esta manera siempre tendrá la última versión del sistema operativo. Los atacantes siempre están buscando alguna vulnerabilidad en el software, y los proveedores están constantemente realizando actualizaciones y parches para repararlas. Si siempre tienes la última versión del sistema operativo y de tus aplicaciones, será más difícil que alguien comprometa tu tableta.

Asegurando tu nueva tableta

3. Pon atención cuando configures tu tableta por primera vez, especialmente en las opciones de privacidad. Uno de los mayores problemas de privacidad es la habilidad de otros para rastrear tu tableta y conocer tu ubicación. Te recomendamos que deshabilites la geolocalización, sólo actívala para las aplicaciones que consideres sea necesaria. Algunas aplicaciones requieren tener habilitada la geolocalización, como las de mapas o las que buscan algún restaurante en la zona, pero la mayoría no necesitan información en tiempo real de tu localización.
4. Muchas tabletas y aplicaciones almacenan tu información en la nube. Por ello, asegúrate de entender dónde están tus datos y cómo los resguardan. Por ejemplo, lo último que quieres es que tus fotos privadas se compartan en Internet, donde el mundo entero puede verlas, con información adicional de geolocalización contenida en ellas. Deshabilita cualquier opción de compartir información en la nube, luego habilítala sólo cuando desees compartir algo específico.
5. Las tabletas sincronizan cada vez más tus aplicaciones con otros dispositivos como tu smartphone o laptop. Esto puede ser maravilloso, pero ten cuidado con cuáles aplicaciones o características permites que se sincronicen. Si tienes habilitada esta opción, no te sorprendas al ver que los sitios que visitas y las pestañas que creaste en el navegador de tu tableta aparecen en el navegador del dispositivo de tu trabajo.

La mejor manera de asegurar tu tableta es habilitar el bloqueo de pantalla, revisar las configuraciones de privacidad y mantenerla actualizada.

Manteniéndola segura

Una vez que has asegurado tu tableta, vas a querer estar seguro que así permanecerá. Aquí tienes algunos pasos clave para mantenerla de ese modo por un largo tiempo.

- Nunca realices jailbreak o hackees tu propia tableta. Esto pasará por alto e inutilizará un gran número de controles de seguridad y harán más vulnerable a tu tableta a los ataques.
- Solamente descarga aplicaciones que necesites y de fuentes confiables. Para las iPad sólo descarga aplicaciones de iTunes, ya que son examinadas por Apple antes de estar disponibles al público; para Google te recomendamos Google Play y para las tabletas de Amazon, la Amazon Appstore. Si bien puedes descargar apps de otros sitios, éstas no han sido investigadas y podrían estar infectadas. Finalmente, sin importar dónde conseguiste una aplicación, cuando no la necesites o dejes de usarla activamente te recomendamos borrarla de tu tableta.

Asegurando tu nueva tableta

- Una vez que instales una nueva aplicación, asegúrate de revisar y configurar las opciones de privacidad, tal como lo hiciste cuando configuraste por primera vez tu nueva tableta. Ten cuidado a qué cosas permites que tenga acceso la aplicación. Por ejemplo, ¿la aplicación que acabas de descargar realmente necesita tener acceso a todos tus amigos e información de contactos? Si te sientes incómodo con los permisos que requiere la aplicación, encuentra una distinta que cumpla con tus necesidades. Adicionalmente, revisa con regularidad los permisos para asegurarte que no han cambiado.

Tu tableta es una herramienta poderosa, una que nosotros queremos disfrutar y usar. Sólo recuerda que estos simples consejos pueden mantenerte a ti y a tu nueva tableta seguros.

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

Básicos de la seguridad en móviles: http://www.seguridad.unam.mx/noticia/?noti=2396

10 consejos para mantener nuestra seguridad en el celular:
http://revista.seguridad.unam.mx/numero-17/10-consejos-para-mantener-nuestra-seguridad-en-el-celular

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

Frases de acceso: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_sp.pdf

El uso seguro de la nube: https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201409_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Célica Martínez y Katia Rodríguez