VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Febrero 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Revisión previa
- Dispositivos perdidos o robados
- Acceso a Wi-Fi
- Computadoras públicas

Mantener la seguridad en el camino

Resumen

Esperamos que seas capaz de ocupar al máximo la tecnología en todo momento, incluso cuando viajas. En esta entrega abordamos cómo puedes conectarte a Internet y usar tus dispositivos de manera segura en el camino.

Editor Invitado
Mark Williams es el Arquitecto de Seguridad de Información Empresarial en BlueCross Blueshield en Tennessee. También es instructor en el Instituto SANS y presidente del capítulo de ISSA en Chattanooga. Ha viajado ampliamente y comprende los problemas a los que te puedes enfrentar cuando llevas tus dispositivos móviles contigo.

Revisión previa

Mientras que la red en tu hogar o en el trabajo puede ser segura, cuando viajas no puedes confiar en cualquier red a la que te conectes. Nunca sabes quién más está en ella y qué podrían estar haciendo. Aquí se ofrecen algunos pasos simples para protegerte y cuidar de tu información antes de comenzar el viaje.

- La mejor forma de proteger tu información es llevar solo contigo la que sea necesaria. Identifica qué datos no necesitas en los dispositivos que llevas contigo y elimínala. Esto puede reducir significativamente el impacto si tus dispositivos se perdieron, fueron robados o confiscados en alguna aduana o punto de seguridad. Si tu viaje es por trabajo, pregunta a tu supervisor si la organización provee dispositivos específicos para trabajar en un viaje.
- Bloquea tus dispositivos móviles y laptops con una contraseña fuerte o código de acceso. De esta manera si te los roban o se pierden, nadie podrá acceder a tu información. Además, activa o instala algún programa para cifrar por completo la unidad de memoria. En la mayoría de los dispositivos móviles, esto se habilita automáticamente cuando bloqueas la pantalla.
- Instala o habilita software en tus dispositivos para que puedas rastrearlo remotamente y saber dónde está, e incluso para borrar la información a distancia, si lo has extraviado o fue robado.
- Actualiza tus aparatos, aplicaciones y software antivirus antes de irte para que uses las versiones más recientes. Muchos ataques se enfocan en sistemas con software obsoleto.
- Haz un respaldo completo de todos tus dispositivos. De esta manera si algo les sucede cuando viajas, aún tendrás tu información original en un lugar seguro.
- Para viajes internacionales revisa cuál servicio tienes para tu móvil con tu proveedor de servicio. A menudo los

Mantener la seguridad en el camino

proveedores cobran altas tarifas por el uso de datos, probablemente te convenga deshabilitar la transmisión de datos de tu teléfono celular durante tus viajes internacionales o puedes comprar una tarjeta SIM prepagada para usar en el exterior.

Para mantenerte seguro durante tus viajes, protege tus dispositivos antes de salir de casa, mantenlos bloqueados y cifra todas las actividades en línea.

Dispositivos perdidos o robados

Una vez que comienzas tu viaje, asegura que tus dispositivos estén a salvo físicamente. Por ejemplo, nunca los dejes en tu automóvil donde la gente pueda verlos fácilmente, pues los criminales pueden romper la ventana y tomar cualquier objeto de valor que vean. Mientras que el crimen es un riesgo, de acuerdo con un estudio reciente de Verizon la gente es cien veces más proclive a perder sus dispositivos que a ser víctima de robo. Esto significa que siempre debes revisar dos veces si aún llevas tus aparatos contigo, como cuando pasas un punto de seguridad en el aeropuerto, dejas un taxi o un restaurante, al salir de la habitación de un hotel o antes de desembarcar del avión. ¡Recuerda revisar la bolsa trasera del asiento!

Acceso a Wi-Fi

Acceder a Internet mientras viajas a menudo significa que usarás puntos públicos de acceso a Wi-Fi, como los de un hotel, la cafetería local o el aeropuerto. Dos problemas con la conexión a una Wi-Fi pública es que nunca estarás seguro quién la configuró y no sabes quién está conectado a ella; como tal, debes desconfiar. De hecho este tipo de conexiones son la razón por la cual tomas todas las precauciones para asegurar tus aparatos antes de viajar. Incluso, las conexiones Wi-Fi usan ondas de radio, lo que significa que cualquier persona cerca de ti puede potencialmente interceptar y monitorear las comunicaciones. Por estas razones, si usas una Wi-Fi pública, necesitas asegurarte de que toda tu actividad en línea esté cifrada. Por ejemplo, cuando te conectas usando un navegador, asegúrate de que los sitios que visitas estén también cifrados. Puedes confirmar esto al ver escrito “HTTPS://” en tu barra de dirección URL o al ver la imagen de un candado ahí mismo. Además, puedes tener una VPN (Red Privada Virtual, por sus siglas en inglés) que cifra toda la actividad en línea cuando está activada. En el trabajo pueden habilitar para ti una red de este tipo o puedes adquirir una VPN para uso personal. Si te preocupa que no haya una Wi-Fi en la cual confiar, considera usar la red de tu móvil. Advertencia: como mencionamos antes, esto puede ser caro en viajes internacionales, revisa antes con tu proveedor de servicios.

Mantener la seguridad en el camino

Computadoras públicas

No uses computadoras públicas, como las de los hoteles en el lobby o en un cibercafé, para acceder a cualquier cuenta o consultar información sensible. No tienes idea de quién ha usado esa computadora antes que tú y pudo haberla infectado de manera accidental o deliberada. Cuando sea posible, usa solamente dispositivos que controles y en los que confíes. En el mejor de los casos, las computadoras públicas son apropiadas para acceder a información pública, como revisar el estado del tiempo o ponerse al tanto con las noticias. Entrar en una cuenta, como la de Google, puede ser una invitación para los atacantes que puedan estar vigilando.

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

Viaja seguro: http://disc.unam.mx/2016/img/posters/CSC2016_posterfinal.jpg

Mantener seguro el celular en un viaje: http://gph.is/299fAUK?tc=1

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

Privacidad en redes sociales:
http://revista.seguridad.unam.mx/numero-12/redes-sociales-ingenieria-social-riesgos-privacidad

Recomendaciones para mantenerse seguro:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201610_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Raúl Abraham González y Katia Rodríguez

