Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Planea con anticipación**
- **Conexión a redes públicas**
- **Evita el uso de computadoras públicas**

Cuando viajes, revisa tu seguridad en línea

EDITOR INVITADO

Raul Siles es el editor invitado en el boletín OUCH! de abril. Raul es fundador y analista de seguridad senior en Taddong (http://www.taddong.com), autor e instructor del SANS, y apasionado de la seguridad (http://www.raulsiles.com). Puedes seguir a Raul a través de Twitter en @taddong y también en su blog personal blog.taddong.com.

RESUMEN

Estar en línea se ha convertido en una actividad tan cotidiana que esperamos tener acceso a Internet en donde sea y para lo que sea. Sin embargo, cuando estás de viaje o de vacaciones, tener acceso a Internet puede ser todo un reto. Las conexiones pueden no sólo ser lentas, sino implicar un gran riesgo, especialmente cuando te conectas a una red o usas computadoras en sitios públicos. La clave para usar Internet de forma segura mientras viajas es entender los riesgos adicionales, ser precavido y estar preparado.

PLANEA CON ANTICIPACIÓN

Una de las formas más efectivas para protegerte cuando viajas es considerar sencillas acciones preventivas antes de salir.

- Actualiza el sistema operativo y aplicaciones de tu equipo portátil y smartphone a la versión más reciente para reducir las probabilidades de un ataque exitoso.
- Verifica que el firewall en tu equipo portátil esté activo. Esto ayuda a prevenir que otros se conecten a él por la red.
- Verifica que tu antivirus esté actualizado y que funcione adecuadamente.
- Los equipos portátiles y smartphones son fáciles de robar y de perder. Activa el bloqueo de pantalla automático en tus dispositivos móviles usando una contraseña fuerte o al menos un código de bloqueo PIN (Número de Identificación Personal).
- Considera poner una etiqueta con tu nombre y dirección de correo electrónico o número telefónico para que puedan contactarte en caso de perder el dispositivo, por ejemplo, si extravías tu smartphone, el personal de seguridad del aeropuerto podrá localizarte. Ofrecer una recompensa podría ayudarte a recuperar tus pertenencias.
- Si tu equipo portátil o smartphone almacena información personal o confidencial, cifra esta información o todo el disco duro antes de viajar. Verifica con el soporte

Cuando viajes, revisa tu seguridad en línea

técnico de tu empresa las políticas de seguridad, quizás el cifrado sea obligatorio.

- Cuando configures el correo electrónico de tu trabajo con un mensaje de respuesta automática al estar fuera, elije a un colaborador como contacto alterno. Además, no proporciones detalles sobre tu viaje. Si te es posible, limita el envío de este mensaje sólo a los contactos que laboran en la organización o aquellos registrados en tu agenda.
- Verifica con el departamento de Tecnologías de la Información (TI) si cuentan con servicios especiales para viajeros.

Además de planear anticipadamente, hay otros puntos que necesitas considerar durante el viaje.

CONEXIÓN A REDES PÚBLICAS

Una red pública es aquella a la que tiene acceso cualquier persona, como las disponibles en aeropuertos, hoteles, restaurantes y cafés, generalmente con conexiones inalámbricas (Wi-Fi). Cuando te conectas a una red pública, tus actividades pueden ser observadas por otros. Aunado a ello, personas malintencionadas podrían operar redes Wi-Fi falsas diseñadas para engañarte y, al utilizarlas, atacar tu sistema.

Cuando te sea posible, utiliza redes Wi-Fi alojadas por una organización legítima. Identifica el nombre de la red Wi-Fi que se anuncia en la recepción del hotel, terminal aérea o café. Usar alguna de estas redes te brinda mayor

La clave para conectarte con seguridad a Internet mientras viajas es entender los riesgos y anticiparte.

seguridad que elegir una pública al azar. Además, cuando exista la posibilidad, usa redes Wi-Fi cifradas y presta atención al tipo de cifrado. De mayor a menor seguridad, los tipos de cifrado comunes para Wi-Fi son: WPA2, WPA, y WEP.

Incluso con redes Wi-Fi cifradas, tu información podría ser interceptada por otros usuarios de la misma red, por ello considera emplear también una conexión de datos cifrada. Los métodos más comunes de cifrado de datos son HTTPS (SSL/TLS) y VPN (Red Virtual Privada, por sus siglas en inglés). Una sesión HTTPS del navegador, que generalmente se identifica por un icono de candado, cifra la

Cuando viajes, revisa tu seguridad en línea

información que envías a través de la Web. Varios sitios web y servicios en línea, como Google, Gmail, Twitter y Facebook te permiten forzar el uso del cifrado HTTPS en todo momento.

Puedes crear una VPN en tu computadora instalando un programa que cifre tus actividades en línea. Averigua con el departamento de TI si tu organización soporta una VPN. De no ser así, considera adquirir un servicio de VPN para tu uso personal, por ejemplo OpenVPN, consulta (http://tinyurl.com/y998ocf) .

Otra opción es usar tu smartphone como un punto de acceso Wi-Fi. Si tienes un smartphone, contacta a tu proveedor de servicios para habilitar las funcionalidades +3G y configurar una "conexión compartida" (tethered connection) o "un punto de acceso personal Wi-Fi" para tu laptop. Además, si las aplicaciones de correo electrónico y navegador de tu smartphone satisfacen tus necesidades mientras viajas, entonces la seguridad ofrecida por la conexión de banda ancha del smartphone es mejor opción que una conexión Wi-Fi pública.

EVITA EL USO DE COMPUTADORAS PÚBLICAS

Una computadora pública es aquella que puede ser usada por cualquier persona. Las encuentras en bibliotecas, hoteles y cafés; no hay forma de saber quién las utilizó. Por ello, es posible que hayan sido infectadas o comprometidas accidentalmente, o bien afectadas intencionalmente con malware. Cualquier información que ingreses en estos equipos puede ser robada por criminales cibernéticos. Restringe el uso de estas computadoras sólo a consultas simples, como el clima, el estado de un vuelo o las noticias. Si no tienes opción y usas una computadora pública para realizar transacciones o comunicar información sensible, asume que cualquier información como nombre de usuario y contraseña que hayas utilizado, pudo haber sido robada. Recuerda llevar un registro de las cuentas que usaste y una vez que tengas acceso a una computadora o red de confianza cambia inmediatamente las contraseñas.

APRENDE MÁS

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, único 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, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Cecilia Espinosa, Israel Andrade, Galvy Cruz, Mauricio Andrade, Rubén Aquino