VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Febrero, 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- **Revisión previa**
- **Dispositivos perdidos o robados**
- **Acceso Wi-Fi**
- **Equipos públicos**

# Seguros en el camino

## Resumen

En este boletín hablaremos de cómo conectarnos de forma segura a Internet y realizar diversas tareas durante un viaje.

## Editor Invitado

Steve Armstrong es Director Técnico de CyberCPR en Logically Secure, es instructor certificado del SANS y anteriormente autor de cursos del SANS. Encuéntralo en Twitter a través de la cuenta **@Nebulator** y en Google Plus como **+SteveArmstrongSecurity**.

## Revisión previa

A pesar de que la red de tu casa o tu trabajo puede ser segura, cuando viajas debes asumir que no todas las redes son dignas de confianza. Nunca se sabe quién más está en la red y qué amenazas puede suponer. Tomar algunas medidas sencillas antes de salir puede ser de gran ayuda para proteger tu información mientras estás de viaje. Una o dos semanas antes de tu viaje:

- Identifica qué información no necesitas en los dispositivos que llevarás contigo y elimínala. Esto puede ayudar de forma significativa a reducir el impacto si alguno de tus dispositivos se perdiera, fuese robado o llegase a ser confiscado en la aduana o por miembros del personal de seguridad fronterizo. Si el viaje está relacionado con tu trabajo, pregunta a tu supervisor si tu organización provee dispositivos alternos que sean utilizados específicamente para trabajar mientras se está de viaje.
- Para viajes internacionales, revisa qué tipo de conectores de energía utiliza el país de destino, quizá sea necesario conseguir un adaptador para cargar la batería de tus dispositivos. Adicionalmente, verifica qué tipo de plan de datos tienes contratado con tu proveedor de servicios móviles. Comúnmente los proveedores móviles cobran cantidades muy altas por el uso de datos en el extranjero, quizá sea necesario deshabilitar las opciones de uso de datos de tu celular o bien, cambiar el tipo de plan para que se adapte al viaje internacional.
- Instala software en tu celular que permita dar seguimiento de su ubicación remotamente, incluso borrar todos los datos en caso de que se pierda o sea robado. Muchos dispositivos móviles cuentan ya con esta característica de forma predeterminada, tú sólo tendrías que habilitarla (recuerda que esto necesita acceso a Internet para operar).

Uno o dos días antes del viaje:

- Actualiza tus dispositivos, aplicaciones y software antivirus para contar con las últimas versiones.
- Habilita todas las configuraciones de seguridad apropiadas en tu dispositivo, por ejemplo firewalls.

# Seguros en el camino

- Bloquea todos los dispositivos móviles con contraseñas seguras o códigos. De esta manera, si pierdes o te roban tu dispositivo, la gente no podrá acceder a la información que contiene.
- Cifra todos tus dispositivos para que en caso de que se pierdan o sean robados, no sea posible acceder a la información. Algunos dispositivos, como el iPhone, hacen esto automáticamente si estableces una contraseña o código en el dispositivo.
- Haz un respaldo completo de todos tus dispositivos. Si algo les llegara a pasar mientras viajas aún tendrás tu información en una ubicación segura.

*La clave para viajar seguro es proteger tus dispositivos antes de salir de casa, mantenerlos físicamente a salvo, saber dónde están todo el tiempo y cifrar todas las actividades en línea.*

## Dispositivos perdidos o robados

Una vez que inicies tu viaje, garantiza la seguridad física de tus dispositivos. Por ejemplo, nunca los dejes en el auto donde puedan verse fácilmente, los criminales podrían, simplemente, romper las ventanas del auto y tomar todos los objetos de valor que estén a la vista. Una idea es llevar un cable de seguridad o una cadena para asegurar físicamente tus dispositivos cuando los dejes en algún sitio, como la laptop. Mientras el crimen es definitivamente un riesgo, ignoramos que es más probable perder algún dispositivo a que sea robado. De acuerdo a un estudio de 10 años por parte de Verizon, las personas están 15 veces más propensas a perder un dispositivo a que éste les sea robado. Esto significa que debes verificar dos veces si aún tienes tu dispositivo mientras viajas, por ejemplo, cuando termina la revisión de seguridad en el aeropuerto, cuando dejas un taxi o restaurante, cuando termina tu estancia en el hotel o antes de bajar del avión.

## Acceso Wi-Fi

Acceder a Internet mientras viajas generalmente significa usar puntos de acceso Wi-Fi públicos, como aquellos que encuentras en hoteles, en un café o en el aeropuerto. El problema con los puntos de acceso Wi-Fi públicos, además de que nunca sabes quién los colocó, es que nunca sabes quién está conectado a ellos. Es por eso que no deben ser considerados de confianza, de hecho, esta es la razón por la que se tomaron todas las medidas para asegurar tus dispositivos antes de salir de viaje. Wi-Fi utiliza ondas de radio para comunicarse desde tu dispositivo hasta el punto de acceso inalámbrico. Esto significa que cualquier persona físicamente cerca de ti, tiene posibilidades de interceptar y monitorear esas comunicaciones.

Por ello, si haces uso de Wi-Fi pública, es necesario asegurarse de que toda tu actividad en línea esté cifrada. Por ejemplo, cuando te conectas en línea usando un navegador, asegúrate de que los sitios web que visitas estén cifrados (tendrán 'https://' al inicio de la dirección URL y una imagen de un candado cerrado). También puedes utilizar

# Seguros en el camino

lo que se conoce como una cuenta de VPN (Virtual Private Network), que cifra toda tu actividad en línea. Es posible conseguirla en el trabajo o puedes comprar las funcionalidades de una VPN para uso personal. Si te preocupa que no haya puntos de acceso Wi-Fi en los que se pueda confiar, considera hacer uso de tu teléfono. (Advertencia: Como hemos mencionado anteriormente, podría ser costoso en viajes internacionales, consulta a tu proveedor de servicios).

## Equipos públicos

No hagas uso de computadora pública alguna, como aquellas que están en los lobbies del hotel, bibliotecas o cibercafés. No tienes idea de quién ha usado esos equipos antes que tú, ellos podrían haber infectado esa computadora pública accidental o deliberadamente. Siempre que sea posible haz uso de dispositivos que estén bajo tu control y en los que confíes para tus actividades en línea. Si es necesario utilizar un equipo público, no hagas uso de servicios que requieran iniciar sesión o escribir una contraseña.

## 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

| | |
|---|---|
| Gestores de contraseñas: | http://www.securingthehuman.org/ouch/2013#may2013 |
| Verificación en dos pasos: | http://www.securingthehuman.org/ouch/2013#august2013 |
| Cifrado: | http://www.securingthehuman.org/ouch/2014#august2014 |
| Asegurdando tu nueva tablet: | http://www.securingthehuman.org/ouch/2013#december2013 |
| Verizon DBIR 2014 [Reporte en inglés]: | http://www.verizonenterprise.com/DBIR/2014/ |



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



 