Alerta de la FTC para Consumidores

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

Entérese Cómo Funciona la Conexión Wi-Fi
Recomendaciones para Usar Redes Inalámbricas Públicas

Wise Up about Wi-Fi: Tips for Using Public Wireless Networks

Las redes inalámbricas públicas – esos *hotspots* o puntos de acceso inalámbricos que están disponibles en cafés, bibliotecas, aeropuertos, hoteles, universidades y otros lugares públicos – permiten el acceso a internet a través de una red compartida. Aunque esto puede resultar muy conveniente, con frecuencia son puntos de acceso inseguros. Usted está compartiendo la red con desconocidos, y algunos de ellos podrían estar interesados en obtener su información personal.

¿Está usando un punto de acceso o *hotspot* Wi-Fi?

Conéctese solamente a sitios Web que estén completamente encriptados.

Los expertos en tecnología de la Comisión Federal de Comercio (*Federal Trade Commission,* FTC), la agencia nacional de protección del consumidor, dicen que la clave para que su información permanezca segura en internet es la encriptación. La encriptación mezcla la información que usted envía a través de internet convirtiéndola en un código inaccesible para los demás. Cuando se usan redes inalámbricas, lo mejor es solamente enviar información encriptada – ya sea por medio de un sitio Web encriptado o de una red segura. Un sitio Web encriptado **sólo** protege la información que usted envía a ese sitio y desde ese sitio. Una red inalámbrica segura encripta **toda** la información que envíe mientras esté conectado a internet.

Cómo Identificar un Sitio Web Encriptado

Si usted envía mensajes de correo electrónico, comparte fotos y videos digitales, usa herramientas disponibles en línea para manejar calendarios y listas de contactos, si utiliza redes sociales, o hace trámites bancarios en línea, usted está enviando información personal a través de internet. La información que usted envía se almacena en un servidor – una computadora de alta potencia que recolecta y distribuye contenidos. Hay varios sitios Web, como los de los bancos, que usan encriptación para proteger la información enviada desde su computadora hasta el servidor.

Para determinar si un sitio Web está encriptado busque las letras **https** al comienzo del domicilio de la página (la letra "s" corresponde a seguro), y un **ícono del candado** en la parte superior o inferior de la ventana de su navegador. La posición exacta del candado dependerá del navegador que use. Algunos sitios Web solamente usan encriptación en la página de ingreso (*sign-in page*), pero si alguna parte de su

¿Es seguro este *hotspot?*

- Si un *hotspot* no requiere una contraseña, no es seguro.
- Si un *hotspot* le pide que ingrese una contraseña en su navegador simplemente para concederle el acceso, o le pide una contraseña WEP, lo mejor es que proceda como si no fuera seguro.
- Usted puede confiar que un *hotspot* es seguro solamente cuando se le pide que ingrese una contraseña WPA. Si no está seguro de que así sea, podría poner en riesgo la información que ingrese. La contraseña de tipo WPA2 es la más segura.

sesión no estuviera encriptada podría afectar la seguridad de toda la cuenta. Fíjese que las letras **https** y el **ícono del candado** permanezcan visibles durante toda su visita al sitio, no sólo cuando ingresa. También puede hacer clic sobre el candado para ver la información sobre el sitio y para verificar que no sea un sitio Web fraudulento.

Redes Inalámbricas Públicas

La mayoría de los *hotspots* inalámbricos **no** encriptan la información que usted envía a través de internet y **no** son seguros. Si usa una red insegura para conectarse a un sitio que no está encriptado – o a un sitio que solamente usa encriptación en la página de ingreso – otros usuarios de la red pueden ver lo mismo que usted ve y los datos que usted envía. Podrían piratear su sesión y conectarse haciéndose pasar por usted. Nuevas herramientas de "pirateo" – que están disponibles en línea gratuitamente – facilitan aún más este tipo de intrusión, incluso a aquellos usuarios que tienen conocimientos técnicos limitados. Su información personal, documentos privados, contactos, fotos familiares e incluso los datos de identificación que utiliza para ingresar en sus cuentas podrían quedar a disposición de cualquiera.

Un impostor podría usar su cuenta para hacerse pasar por usted y estafar a otras personas conocidas o queridas. Además, un atacante podría tratar de acceder a otros sitios Web probando con su nombre de usuario y contraseña – inclusive a sitios que almacenan su información financiera.

Proteja su Información

Pues entonces, ¿Qué puede hacer usted para proteger su información? Aquí van algunas recomendaciones:

- Cuando use un *hotspot* inalámbrico, solamente conéctese o envíe información personal a través de sitios Web que sepa que están completamente encriptados. Y tenga presente que el sitio debería mantenerse encriptado a lo largo de toda su visita – desde el momento en que se conecta hasta que se desconecta. Si cree que está navegando en un sitio encriptado pero de repente se da cuenta que está en una página sin encriptar, salga de la página enseguida.
- No se quede conectado permanentemente a sus cuentas. Cuando termine de usar una cuenta, desconéctese de esa página.
- No use la misma contraseña para distintos sitios Web ya que de esta manera podría estar dándole la llave a quien se apodere de una de sus cuentas para que pueda acceder a varias de sus cuentas.
- Muchos navegadores alertan a los usuarios que tratan de visitar sitios fraudulentos o descargar programas maliciosos. Preste atención a estas advertencias y tómese algunos minutos para actualizar su navegador y software de seguridad con regularidad.
- Si habitualmente accede a sus cuentas en línea a través de *hotspots* inalámbricos, use una red virtual privada (VPN). Estas redes VPN encriptan el tráfico de datos entre su computadora e internet, incluso en las redes inseguras. Puede abrir una cuenta VPN personal recurriendo a un proveedor de servicio VPN. Además, hay algunas organizaciones que crean redes VPN para ofrecerles a sus empleados un acceso remoto y seguro.
- Algunas redes Wi-Fi usan encriptación: Las más comunes son WEP y WPA. La encriptación WPA protege su información contra los programas piratas más comunes. La encriptación WEP tal vez no. Si no está seguro de estar navegando en una red con encriptación WPA, use las mismas precauciones que tomaría en una red insegura.
- También puede resultar útil instalar complementos o componentes a su navegador que agregan capacidades específicas, comúnmente conocidos como *add-ons* y *plug-ins*. Por ejemplo, Force-TLS y HTTPS-Everywhere son complementos o *add-ons* ofrecidos gratuitamente por el navegador Firefox que exigen que el navegador use encriptación en los sitios Web más populares que usualmente no están encriptados. Estos *add-ons* no lo protegerán en todos los sitios Web que visite – para saber si está en un sitio seguro fíjese en el domicilio de la página y busque el ícono del candado.

La FTC trabaja para prevenir las prácticas comerciales fraudulentas, engañosas y desleales en el mercado y proveer información para ayudar a los consumidores a identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite **ftc.gov/consumidor** o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Para más información, vea el video *Cómo Presentar una Queja* disponible en **ftc.gov/videosenespanol**. La FTC ingresa las quejas presentadas por los consumidores a una base de datos segura y herramienta investigativa llamada Red Centinela del Consumidor (*Consumer Sentinel*) que es utilizada por cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y del extranjero.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

Febrero 2011