Consejos para utilizar Wi-Fi público

Wi-Fi (abreviación de “Wireless Fidelity”) es una tecnología basada en ondas de radio que permite a computadoras, teléfonos inteligentes y otros dispositivos electrónicos conectarse al Internet o comunicarse unos con otros en forma inalámbrica.

Un gran número de cafés, bibliotecas, aeropuertos, hospitales, hoteles, restaurantes de comida rápida y otros negocios utilizan Wi-Fi para proveer puntos de acceso público gratis (o “hotspots”) para que los clientes los utilicen para conectarse de forma inalámbrica a Internet. Un punto de acceso típicamente tiene una cobertura de alrededor de 65 pies en interiores y una mayor cobertura en exteriores.

No se quede conectado permanentemente a sus cuentas.

El acceso a Internet usando un punto de acceso a Wi-Fi público es conveniente y por lo regular gratis para usuarios móviles, pero típicamente estos puntos de acceso no son seguros. Si no se requiere introducir una contraseña proporcionada por el dueño del Wi-Fi (como el hotel o café) antes de obtener acceso a la red, algún otro usuario de Wi-Fi puede piratear su aparato electrónico, ver su información personal y la información que está enviando. Ellos podrían cambiar sus contraseñas y evitar que acceda a sus propios archivos. También pueden utilizar su cuenta para decir que son usted y engañar a sus seres queridos. Entonces, si no está convencido de que una red es segura, trátela como si fuera insegura.

Cómo funciona la codificación

Además de usar redes seguras, lo mejor es enviar información confidencial solamente a sitios de red codificados. Si usted envía correos electrónicos, comparte fotos y videos digitales, usa redes sociales o hace transacciones bancarias en línea, usted está enviando información personal por Internet. La información que usted comparte se almacena en un servidor – una computadora potente que recolecta y envía contenido. Hay muchos sitios web (tales como

bancos) que usan codificación para proteger su información durante el trayecto entre su computadora y los servidores. La codificación es la clave para mantener su información personal segura en línea. La codificación desorganiza la información que usted envía por Internet convirtiéndola en un código que es inaccesible para otros. Cuando se usan redes inalámbricas lo mejor es enviar información personal solamente cuando es codificada –ya sea a través de un sitio web codificado o a través de una línea inalámbrica segura. Un sitio web codificado protege **únicamente** la información que usted envía y recibe **de ese sitio**. Una línea de red inalámbrica segura codifica toda la información que usted envía usando esa red.

Como se puede saber si un sitio web está codificado

Los sitios web codificados tienen las letras “**https**” al inicio de la dirección de internet (la “s” corresponde a seguro). Algunos sitios web solo usan codificación en la página donde se ingresa el nombre del usuario y la contraseña, pero si alguna parte de su sesión no está codificada, la totalidad de su cuenta puede ser vulnerable. Fíjese que aparezcan las letras **https** en cada página que visite y no solo en las cuales ingresa su nombre de usuario y contraseña.

No asuma que un punto de acceso de Wi-Fi es seguro

La mayoría de los puntos de acceso a Internet por Wi-Fi **no** codifican la información que usted envía y **no** son seguros. Si usted utiliza una red insegura para conectarse con un sitio de Internet que solamente usa codificación en la página donde se ingresa el nombre de usuario y contraseña, otros usuarios de la red pueden ver lo que usted ve y lo que envía. Ellos podrían interceptar su sesión de navegación y conectarse como si fueran usted mismo. Hay nuevas utilidades para piratear - disponibles gratis en Internet- que facilitan este tipo de intrusión, incluso para usuarios con conocimientos técnicos limitados. Su información personal, documentos privados, contactos, fotos familiares e incluso su nombre de usuario y contraseña pueden estar en peligro.

Active la autenticación de dos factores si se le ofrece.

El sistema de autenticación de dos factores es una capa adicional de protección que combina algo que usted tiene, tal como un token físico, ya sea una tarjeta o código, con algo que solo usted sabe, tal como algo memorizado, ya sea un número de identificación personal (PIN) o una contraseña.

Protéjase cuando utilice una red de Wi-Fi pública.

- Cuando use un punto de acceso a red con Wi-Fi público solo regístrese o envíe información personal a sitios web que usted sabe que están totalmente codificados. Para proteger su información, la totalidad de su visita a cada sitio de internet debe ser cifrada (busque https en la dirección del sitio web). Si no está seguro de que está en una página cifrada, desconéctese inmediatamente.
- No se quede conectado permanentemente a sus cuentas. Desconéctese cuando termine de usar su cuenta.
- No utilice la misma contraseña para diferentes sitios web. Una persona que logre acceder a una de sus cuentas podría ganar acceso a todas sus cuentas.
- Muchos navegadores de Internet alertan a los usuarios que sin saber tratan de visitar sitios fraudulentos o cuando intentan descargar programas maliciosos. Preste atención a estas advertencias y mantenga actualizados su navegador y su programa de seguridad.
- Si regularmente accede a sus cuentas a través de puntos de acceso a la red por Wi-Fi, utilice una Red Virtual Privada (VPN) las redes de VPN codifican el tráfico entre su computadora e Internet, incluso en redes inseguras. Usted puede obtener una cuenta personal de VPN a través de un proveedor de servicio VPN. También, algunas organizaciones crean redes de VPN para ofrecer acceso remoto y seguro para sus empleados.
- Los sistemas de codificación más comunes para Wi-Fi son WEP y WPA. El sistema de codificación de WPA protege su información contra los programas piratas más comunes, mientras que WEP no las previene. WPA2 es la más potente. Si no está seguro de que está utilizando una red codificada WPA, utilice las mismas precauciones que utilizaría en una red insegura.
- También puede servirle de ayuda instalar programas complementarios para su navegador. Por ejemplo, Force-TLS y HTTPS-Everywhere son dos componentes adicionales gratuitos para Firefox que obligan al navegador a usar codificación en los sitios web más populares que usualmente no están codificados. Estas opciones no le protegen en todos los sitios web, así que recuerde verificar que los sitios comienzan con **https** en la dirección para asegurarse de que son seguros.
- Para más información acerca del uso de puntos de acceso Wi-Fi, visite:

  StaySafe Online
  staysafeonline.org

  OnGuardOnline
  onguardonline.gov

  Federal Trade Commission
  ftc.gov

Términos de Wi-Fi Comunes

Cifrado

El cifrado es la traducción de datos en un código secreto. El cifrado es la forma más efectiva de lograr la seguridad de los datos. Para leer un archivo cifrado, debe tener acceso a una clave o contraseña secreta que le permite descifrarlo. Los datos sin cifrar se llaman texto sin formato; los datos cifrados se refieren texto cifrado.

FTP

Es un protocolo que permite a los usuarios copiar archivos entre su sistema local y cualquier sistema al que puedan acceder en la red.

HTTPS (protocolo seguro de transferencia de hipertexto)

HTTPS es una combinación del protocolo de transferencia de hipertextos con el protocolo SSL/TLS para proporcionar comunicación encriptada e identificación segura de un servidor web de la red. Las conexiones HTTPS a menudo se usan para transacciones de pago en Internet.

"Ataque de intermediario"

Un "ataque de intermediario" es una forma activa de escuchar en la cual el atacante hace conexiones independientes con las víctimas y transmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando de hecho toda la conversación es controlada por el atacante. El atacante debe ser capaz de interceptar todos los mensajes entre las dos víctimas e inyectar nuevos mensajes. Por ejemplo, un atacante dentro del rango de recepción de un punto de acceso Wi-Fi sin cifrar puede integrase como un intermediario. O un atacante puede hacerse pasar por un banco o comerciante en línea, dejando que las víctimas inicien sesión a través de una conexión SSL, y después el atacante puede entrar en el servidor real utilizando la información de la víctima y robar los números de tarjeta de crédito.

SSL - Capa de Puertos Seguros

El protocolo SLL es para proteger las comunicaciones a través de redes informáticas. Establece una sesión segura autenticando electrónicamente cada extremo de una transmisión encriptada. Son utilizados por sitios web cuyos nombres comienzan con https en lugar de http.

VPN - Red Privada Virtual

La Red Privada Virtual (VPN) asegura y privatiza datos a través de una red, generalmente el Internet, mediante la construcción de un "túnel encriptado". Los datos pasan a través de este túnel, protegiéndolo de cualquiera que intente interceptarlo. Incluso aunque los datos se intercepten, sin la clave para descifrar los datos están irremediablemente revueltos e inservibles a cualquiera.

WEP - Privacidad Equivalente a Cableado y WPA/WPA2 – Acceso Protegido a Wi-Fi

WEP y WPA son tipos de conexiones de seguridad que se utilizan para proteger las redes inalámbricas del hogar. WEP es un algoritmo de seguridad que se introdujo en 1997 para proporcionar una confidencialidad comparable a la de una red de cable tradicional. Desde el 2001, varias debilidades graves se han identificado en el protocolo WEP, y hoy una conexión WEP puede ser resquebrajado en minutos. En el 2003 WEP fue reemplazado por el Acceso Protegido a Wi-Fi (WPA). WPA y WPA2 son programas de certificación que prueban el soporte de productos Wi-Fi para protocolos de seguridad estándar IEEE que pueden encriptar datos enviados por el aire, del usuario de Wi-Fi al enrutador de Wi-Fi.

Para obtener más información o para presentar una queja visite nuestro sitio web o contáctese con:

Wisconsin Department of Agriculture, Trade and Consumer Protection

Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio web: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

I:\dtcp\common\FactSheets\ID Theft WiFiTipsSPANISH911 (rev. 04/23)