BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

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 ("hotspots") para que los clientes lo utilicen para conectarse de forma inalámbrica al internet. Un punto de acceso típicamente tiene una cobertura de alrededor de 65 pies en los interiores y una mayor cobertura en los exteriores.
El acceso al 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 servidor de Wi-Fi (i.e hotel o café) antes de obtener acceso a la red, algún otro usuario del Wi-Fi puede piratear su aparato electrónico, ver su información personal y la información que está enviando. Ellos podrían cambiar sus contraseñas y evitarle el acceso a sus propios archivos. También pueden utilizar su cuenta para personificarle 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 electrónicas, usted está enviando información personal por el 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 de web codificado o a través de una línea inalámbrica segura. Un sitio de red que es codificado **solo** puede proteger 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 esta codificado

Las 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 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 al 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 fuera usted mismo. Hay nuevas utilidades para piratear - disponibles gratis en el 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 autenticación de dos factores si se le ofrece.

El sistema de autenticación de dos factores es un capa adicional de protección que combina algo que usted tiene, tal como un identificador 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 envié información personal a sitios de web que usted sabe 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 de internet) 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 de internet. 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 por sus siglas en inglés) las redes de VPN codifican el tráfico entre su computadora y el 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 más comunes programas piratas, mientras que WEP no las previene. WPA2 es la más potente. Si no está seguro de que está utilizando una red de codificado WPA utilice las mismas precauciones que utilizaría en una red insegura.
- También puede servirle de ayuda el 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 de red más populares que usualmente no están codificados. Estas opciones no le protegen en todos los sitios de 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	OnGuardOnline	Federal Trade Commission
Staysafeonline.org	onguardonline.gov	ftc.gov

Para más información o para presentar una queja, visite nuestra página de internet o contacte al Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

Correo Electronico:
DATCPWisconsinPrivacy@wi.gov

Sitio de Internet: datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058

I:\dtcp\common\FactSheets\ID Theft WiFiTipsSPANISH911 04/17