Datos para Resguardar su “Bluetooth” y otras Conexiones Inalámbricas

A medida que el uso de las conexiones inalámbricas a Internet aumenta, vertiginosamente, las redes de acceso *Wi-Fi* y las conexiones *Bluetooth* están cada vez más expuestas a actividades ilegales. Pero hay muchas formas de resguardarse, limitando así la probabilidad de convertirse en presa de robos de identidad y de la usurpación de información privada en general.

Codificación

La codificación es la mejor forma de mantener sus datos personales resguardados, para cualquier tipo de acceso a Internet. La codificación mezcla la información contenida en sus mensajes, de manera que sólo el receptor apropiado puede leerlos. Cuando la dirección de un sitio web (conocida como *URL*, en inglés) comienza con las letras “https”, en lugar de “http”, significa que hay codificación.

Las dos formas más comunes de codificación son las de Privacidad Equivalente por Cable (WEP, por sus siglas en inglés) y Acceso Wi-Fi Protegido (WPA, por sus siglas en inglés). La codificación disponible que otorga mayor protección es la WPA2. Úsela en lo posible. Las conexiones Wi-Fi residenciales y en sitios públicos (*hotspots,* en inglés) generalmente le informarán qué tipo de codificación usan.

Wi-Fi de acceso público

Numerosos usuarios de Wi-Fi prefieren usar las redes públicas para acceder de manera remota a Internet, en lugar de usar los planes de carga y descarga de datos de sus equipos móviles. Pero la conveniencia ofrecida por las conexiones Wi-Fi de acceso público no está libre de riesgos. Los piratas cibernéticos (*hackers*, en inglés) pueden acceder a su conexión en cuestión de segundos. Estos invasores tienen la capacidad de poner en peligro la información que usted mantiene en su equipo móvil y en sus cuentas en línea. A continuación, algunas medidas que puede adoptar para minimizar los riesgos:

- Examine la validez de los sitios *hotspot* disponibles. Si más de un *hotspot* parece pertenecer al establecimiento donde usted está, consulte con los dependientes del lugar para evitar conectarse a un *hotspot* impostor.
- Revise para asegurarse de que todos las direcciones electrónicas de los sitios web con los que usted intercambia información comienzan con las letras “https” al comienzo de la dirección de Internet. Si es así, la información que usted transmite será codificada.
- Considere la instalación de una aplicación adicional que obliga a usar codificación a sus navegadores de Internet cuando se conectan con sitios web -- incluso aquellos sitios web comúnmente conocidos y que normalmente no codifican sus comunicaciones.
- Ajuste la configuración de su teléfono inteligente para que no se conecte automáticamente con redes Wi-Fi disponibles. Esto le da más control para elegir dónde y cuándo conectarse.
- Si usted utiliza redes *hotspot* de uso público con regularidad, considere el uso de una red virtual privada (Virtual Private Network, VPN por sus siglas en inglés) que codifique todas las transmisiones entre su equipo móvil e Internet. Numerosas compañías ofrecen redes VPN a sus empleados, para que cumplan con sus tareas laborales. También es posible obtener una subscripción VPN con fines privados.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol

- Cuando necesite transmitir información delicada, estará más resguardado usando su plan de carga y descarga de datos, otorgado por el proveedor de su teléfono celular, que usando conexiones Wi-Fi.

Seguridad para Bluetooth

Las conexiones Bluetooth (un tipo de red inalámbrica de área personal, conocida genéricamente como WPAN por sus siglas en inglés) a sus equipos móviles pueden ser muy útiles. Ofrecen ventajas que va de la conexión a un aparato auricular conectado remotamente a su teléfono móvil, a la transferencia de archivos para permitir llamadas inalámbricas mientras conduce su vehículo. En la mayoría de los casos, los usuarios deben esperar que se concrete la conexión del dispositivo Bluetooth antes de compartir información – es un proceso llamado "acomplamiento" que proporciona resguardo de datos. Sin embargo, al igual que las conexiones Wi-Fi, los Bluetooth podrían exponer sus datos personales si usted no es cauteloso. A continuación algunas medidas de protección cuando utilice su Bluetooth:

- Desactive el Bluetooth cuando no lo esté usando. Si lo mantiene activo, un pirata cibernético podría detectar qué equipos conectó a su Bluetooth, suplantar alguno de sus equipos y obtener acceso a ellos.
- Si usted conecta su teléfono móvil a un automóvil arrendado, gran parte de la información de su teléfono podría ser compartida con el dispositivo del automóvil. Asegúrese de "desacoplar" su teléfono del equipo del automóvil y borre todos sus datos personales, contenidos en el dispositivo del automóvil arrendado, antes de devolverlo. Adopte las mismas medidas cuando venda un auto que lleve Blutooth incorporado.
- Cuando use un Bluetooth, hágalo en modalidad "escondido" más que en modalidad "detectable". Esto evita que otros equipos descubran su conexión Bluetooth.

Resguardo para Wi-Fi residencial

Las redes residenciales Wi-Fi (tecnología inalámbrica que permite la conexión remota a Internet en áreas de extensión limitada) son de uso común, en gran medida porque permiten que computadoras y equipos móviles compartan una misma conexión remota, a Internet de banda ancha, sin necesidad de gastar el tiempo del plan de conexión de sus equipos otorgado por su proveedor de acceso de banda ancha móvil. Además, las conexiones Wi-Fi ofrecen la conveniencia del acceso a Internet prescindiendo de cables para cada uno de los dispositivos. No obstante, al igual que otras conexiones remotas, las redes Wi-Fi residenciales presentan vulnerabilidades que podrían ser explotadas por los piratas cibernéticos con el objeto de acceder a sus datos privados y utilizarlos en actividades criminales. Para proteger su red inalámbrica residencial de usuarios indeseados, considere adoptar las siguientes medidas:

- Active la codificación. A menudo, los enrutadores no tienen activada la codificación cuando han sido recién adquiridos. Asegúrese de activar la codificación inmediatamente después de que su enrutador sea instalado.
- Cambie el nombre que la red trae asignado por la fábrica (identificador de red, *SSID* por sus siglas en inglés). Cuando una computadora con conexión inalámbrica busca y exhibe las redes disponibles, muestra cada red que exhibe el SSID públicamente. Los fabricantes a menudo dan a todos sus enrutadores un SSID que identifica su nombre de fábrica. Es bueno cambiar el SSID de su red. Para proteger su privacidad, no use información personal en la nueva clave, como por ejemplo los nombres de miembros de su familia.
- Cambie la contraseña que la red trae de fábrica. La mayoría de los enrutadores inalámbricos contienen claves de ingreso ya asignadas, para modificar su configuración (esto no es lo mismo que la clave de ingreso usada para conectarse a la red Wi-Fi). Usuarios no autorizados podrían

conocer las claves de acceso de la fábrica, por eso es importante cambiarlas tan pronto instale su enrutador. Las claves de acceso más seguras son las que usan una combinación de varias letras, números y símbolos.

- Considere usar filtrado de direcciones MAC en su enrutador inalámbrico. Todo dispositivo habilitado para conectarse a una red Wi-Fi posee una identificación única llamada "dirección física" o MAC (siglas para *Media Access Control*, en inglés). Los enrutadores inalámbricos pueden determinar las direcciones MAC de todos los dispositivos que se conectan con ellos y los usuarios de redes Wi-Fi pueden disponer la configuración de sus redes inalámbricas para aceptar solo conexiones de equipos con direcciones MAC que el enrutador reconozca. Para crear obstáculos adicionales a intentos de acceso no autorizado, considere activar el filtro de direcciones MAC en su enrutador inalámbrico, incluyendo sólo los dispositivos que usted esté usando.
- Desactive su enrutador inalámbrico cuando no lo esté usando por largos periodos de tiempo.
- Use programas antivirus y anti-*spyware (*anti-espía) en su computadora. Y use aplicaciones similares en todos los equipos que conecte a su red inalámbrica.

Contraseñas (claves de ingreso o de acceso)

Es probable que usted posea contraseñas para numerosas cuentas que usa en línea. Recordarlas es a menudo un problema. Los navegadores de Internet y otros programas podrían ofrecerle recordar sus claves de ingreso, lo que suele ahorrar tiempo al usuario. Sin embargo, esto podría exponerle. Siga los siguientes pasos para proteger su información personal:

- No use la misma contraseña para múltiples cuentas electrónicas, especialmente para las que contienen información más delicada, como cuentas bancarias, tarjetas de crédito, archivos de impuestos o de documentos legales y médicos. De lo contrario, si alguien obtien acceso a su clave común, tendrá acceso inmediato a todas sus cuentas.
- No configure sus navegadores para que recuerden sus claves de ingreso. En especial para cuentas bancarias, legales o médicas. Si una persona no autorizada obtiene acceso a su computadora o teléfono inteligente, podría ingresar a cualquier cuenta a la que su navegador dé acceso automático.
- No use claves que puedan ser adivinadas fácilmente. Como por ejemplo, palabras comunes y cumpleaños de miebros de su familia. En lugar de eso, use una combinación de letras, números y símbolos. Mientras más larga sea su clave de ingreso, mayor será el resguardo que ésta proporcionará a su información privada.

Centro del Consumidor de la FCC

Para obtener más información sobre temas de interés del consumidor, visite la página web del Centro del Consumidor de la Comisión Federal de Comunicaciones (*Federal Communications Commission*, FCC por sus siglas en inglés) en https://consumercomplaints.fcc.gov (en inglés).

Formatos accesibles

Para solicitar este artículo en formato accesible - Braille, letra grande, documento en Word, de texto o de audio – escríbanos o llámenos a la dirección o números telefónicos de más arriba o envíe un correo electrónico a fcc504@fcc.gov**.**

Última edición: 6 de octubre de 2016

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol