Qué perfil de víctima tienes tú

México, Julio 2016.-- En nuestros días el mantenerte conectado a Internet es casi como lavarte los dientes: un hábito el cual de no hacerse causa incomodidad. Y es totalmente entendible cuando se ha convertido en la herramienta número uno del trabajo, escuela y comunicación en general. Si no estás conectado a Internet estás desconectado del mundo.

En un estudio hecho a 23 países, incluido México, el mayor porcentaje de adultos se encuentra enterado y preocupado de los peligros de sus datos personales, espionaje a través de sus dispositivos y amenazas financieras en Internet, siendo un 60% de los usuarios de Internet los preocupados por espionaje y únicamente un 38% toma precauciones al usar redes públicas de Wi-Fi, sin tener presente que esta puede ser la principal puerta abierta a los cibercriminales.

Mariel Cuervo, colaboradora de SAINT Tecnologías (empresa mexicana con la misión de proveer seguridad y tranquilidad a las organizaciones, minimizando y controlando las crecientes amenazas en la red) y vocera de la campaña Para Un Internet Seguro, menciona que "así como los más pequeños en casa pueden sufrir los estragos de Internet, los adultos también pueden ser víctimas de otro tipo de violencia, e incluso en esta nueva era en la que los más pequeños prefieren una Tablet de regalo que un coche a control remoto o una muñeca, no sabemos a qué los estamos exponiendo, incluso por la simple configuración de estos dispositivos".

El conectarse a redes públicas, tanto con contraseña como sin ella, representa un peligro latente para nuestros dispositivos, nuestra identidad, nuestros datos y nuestra vida. Tal vez al ir caminando por la calle y encontrar una red "abierta" te haga pensar "¡qué buena onda, Internet gratis!", pero nunca sabrás totalmente la intención que se gesta detrás hasta que seas una víctima. Estos son algunos perfiles para estar expuesto como víctima de una conexión abierta:

El Desnudo: Cuando se establece una conexión en una red "abierta" quedan visibles todos los datos conjuntados en el dispositivo, tanto para el administrador de la red como para cualquiera que esté conectado a la misma. Los cuales pueden ser visibles a quienes los sepan extraer.

El Usurpado: No únicamente permites a los delincuentes de la red espiar tu vida; regalas tus datos, contraseñas, contactos, conversaciones, fotos, documentos y de más, a quienes pueden dar un mal uso, porque no solo lo pueden ver también lo pueden robar.

El Contagiado: Cualquier usuario mal intencionado tiene el acceso y el canal de comunicación a su alcance para realizar todo tipo de amenazas gracias a estas redes, infectando con virus los dispositivos y agrediendo anímicamente al cibernauta.

Con Intermediario: El ciberdelincuente también tendrá a su alcance la opción de configurar su equipo para ser el intermediario en los canales de comunicación entre el usuario y sus contactos; es decir tendrá acceso a cualquier conversación de Whatsapp y modificarla, por mencionar un ejemplo. Incluso puede enviar mensajes, información o archivos con la identidad del usuario.

La Inocente Palomita: Ocasionalmente se puede sentir la curiosidad y desfachatez de "aproveharse" de una red abierta o incluso tratar de hackear una protegida; sin embargo no sabemos la implicaciones y consecuencia legales que esto pueda traer y mucho menos si estén a disposición con el fin de atraer víctimas o delincuentes.

Existen precauciones muy sencillas con la cuales se pueden evitar problemas mayores y mucho más graves, incluso el llegar a ser secuestrado, agredido físicamente, amenazado o robo financiero. Lo principal y más difícil optar es no conectarse a este tipo de redes, sin embargo si estás dispuesto a hacerlo mantente informado sobre los riesgos y soluciones.

El mantener siempre los dispositivos actualizados con lo último en seguridad para el sistema operativo y aplicaciones que utilizamos siempre será la primera opción en protección de datos. Si eliges conectarte a una red abierta evita compartir el siguiente tipo de información: Información bancaria, correo electrónico, acceso a las redes sociales, intercambio de información privada. Entre otras alternativas de seguridad que puede seguir se encuentran:

- Apagar WiFi mientras no sea usado, pues se puede conectar sin percatarnos.
- No olvidar que los dispositivos se encuentran en constante sincronización, por lo que el riesgo es constante; desactivarla en estos casos.
- Borrar lista de puntos de acceso guardados.
- No iniciar sesiones de ninguna cuenta, ni realizar trámites.
- Modificar la configuración de conexión WiFi.

Acerca de "Para un Internet Seguro"

"Para Un Internet Seguro" nace como una iniciativa en Tijuana que busca cambiar la falta de conciencia por educación a través de pláticas y conferencias sobre las situaciones más comunes entre los internautas: redes sociales, grooming, pornografía y cyberbullying.

Contacto de RP
Judith Pérez Fajardo
GPS Imagen y Comunicación México
judith@gpscom.com