Los riesgos de usar redes WiFi 'abiertas'

Conectarse a una red WiFi desconocida siempre entraña riesgos, más o menos graves. Un gesto tan cotidiano como acceder a internet en una cafetería, en el aeropuerto o en un establecimiento público expone nuestra vida digital a la vista de cualquier usuario avezado y, peor aún, a la vista de los numerosos ciberdelicuentes que pueblan las redes.

MARIÁN LEZAUN
marianlezaun@gmail.com

EL PRINCIPAL MOTIVO de conectarse a una red abierta es que, en la mayoría de los casos, desconocemos quién es el administrador y, sobre todo, qué medidas de seguridad utiliza para blindarse ante posibles ataques cibernéticos. De hecho, conectarse sin contraseña significa que cualquier interesado puede acceder a nuestros datos sin demasiados problemas. No es necesario ser un experto informático para descifrar determinadas claves de entrada y, además, en internet, existen numerosos tutoriales e información disponible para entrar en dispositivos ajenos y robar toda serie de datos con facilidad.

Por eso, para evitar esta debilidad generalizada entre la mayoría de los usuarios ante el uso de las tecnologías, los expertos recomiendan una buena educación digital que nos permita navegar de manera segura y adquirir una mayor consciencia de los peligros a los que nos exponemos. Esa educación debe comenzar desde la infancia, ya que los menores comienzan, cada vez antes, el manejo de las nuevas tecnologías y también son víctimas de estos peligros. No hay más que ver el aumento de casos de *cyberbullying*, por ejemplo. Según las conclusiones publicadas tras el último Mobile World Congress, el 65 por ciento de los usuarios de internet no sa-

ben distinguir si están conectados a través de una red segura o una desprotegida y muchos de ellos transmiten información sensible, como datos bancarios y correos personales, sin cifrar y sin medir las consecuencias ni el rastro que dejan en la Red.

Así, cuando uno está fuera de casa y quiere conectarse busca, en primer lugar, una red abierta que evite el consumo de datos del dispositivo (*smarthphone, tablet*, ordenador portátil, etc…) y que le permita estar conectado en todo momento. El 57% de estas personas da por hecho que todas las redes inalámbricas disponibles en lugares públicos (como aeropuertos, restaurantes u hoteles) cuentan con sistemas de seguridad integrados, según las conclusiones del último Mobile World Congress celebrado en Barcelona, pero la realidad dista mucho de esta situación. Caso aparte son las aplicaciones para Android, ya que tampoco tienen la seguridad garantizada: el 23 por ciento de las aplicaciones para móviles y tabletas transmiten información sensible sin cifrar. Y lo mismo ocurre con determinados buscadores o empresas de servicios en internet. La mayoría de los usuarios las utilizamos sin conocer exactamente cuáles son sus normas de seguridad ni cómo funcionan realmente.

No es necesario ser un experto informático para descifrar determinadas claves de entrada

¿Son interesantes nuestros datos? Pensar que tus datos no interesan a nadie o que tú no eres susceptible de un *ciberataque* es un error de partida. Por eso, los expertos recomiendan en cualquier caso utilizar, en la medida de lo posible, una red con seguridad WPA (WiFi Protected Access) o WPA_2. Este tipo de redes son mucho más difíciles de descifrar y son una buena garantía para proteger las redes inalámbricas.

Muchos usuarios transmiten información sensible, como datos bancarios y correos personales, sin cifrar y sin medir las consecuencias

¿Qué precauciones hay que tomar si se utiliza una WiFi pública? Si se va usar una red pública, hay que evitar las conexiones automáticas y eliminar los accesos a las redes WiFi una vez que se haya terminado la navegación: un simple gesto que acaba con muchos problemas y que se debe interiorizar como un hábito. También es aconsejable ponerse fuera del alcance de la vista de otros usuarios que haya en el local y mantener en todo momento actualizados los dispositivos que utilizamos. Por otro lado, cuando se usa una WiFi abierta, hay que navegar por páginas con certificados de seguridad. Es decir, páginas cuya URL comienza por HTTPS, en lugar de HTTP.

Los expertos recomiendan también comprobar que la red disponible es la oficial del lugar en el que se está y que realmente pertenece a ese establecimiento. Sólo es necesario preguntar al encargado del local en ese momento. Incluso cuando se utilice una red protegida, los expertos recomiendan utilizar un antivirus con licencia e instalar un *firewall* (sistema para bloquear accesos no autorizados). Si eres de los que no puedes vivir sin conexión, es conveniente que utilices un red privada virtual (VNP), ya que con este método consigues cifrar todo lo que envías. En realidad se trata de estar siempre alerta y poner en práctica ciertas medidas de seguridad básicas.

¿Se pueden realizar compras *online* desde una red abierta? La realización de compras *online* o de cualquier operación que requiera el intercambio de información sensible están totalmente desaconsejada cuando no existe una red segura. La misma norma aplicaremos a la hora de conectarse a las cuentas bancarias o cuentas de correo personales.

¿A qué tipo de delitos nos exponemos? Cuando nos conectamos a una red abierta, los paquetes de información que manejamos viajan por ella sin ninguna protección y cualquiera con el dispositivo adecuado puede capturarlos. De esta manera, los *hackers* pueden lograr direcciones de correo electrónico, contraseñas, claves de entrada y leer mensajes cifrados o no. Los delitos más habituales son aquellos relacionados con el robo de datos personales, especialmente los datos bancarios. Los ataques se relacionan también con la suplantación de la personalidad en redes sociales, secuestro de cuentas y direcciones de correo, amenazas y coacciones a través de estas mismas redes y los daños y modificaciones en los

Para saber más

● La Oficina de Seguridad del Internauta del Ministerio de Industria, Energía y Turismo presenta un decálogo para una navegación segura y mucha información para evitar cualquier problema.
http://cort.as/eJ6b

● En la web de la Policía Nacional explican qué precauciones se deben tener para conectarse a internet y qué precauciones tomar ante los ciberdelincuentes
http://cort.as/1ZBM

● También la Guardia Civil cuenta con una unidad especial dedicada a los delitos informáticos y pone a disposición de los usuarios información de interés para usar las redes y las tecnologías de la manera más segura.
http://cort.as/1lel

El 65 por ciento de los usuarios de internet no saben distinguir si están conectados a través de una red segura o una desprotegida

El principal riesgo de conectarse a una red abierta es que desconocemos quién es el administrador y, sobre todo, qué medidas de seguridad utiliza para blindarse

dispositivos (ordenadores, tabletas y teléfonos). Incluso si el propietario de la red tiene algún tipo de virus en su sistema informático, estas infecciones pueden llegar a tu dispositivo.

Además, cualquiera puede conocer cuáles son nuestros gustos, aficiones, comportamientos de compra, etcétera; una información realmente valiosa para las empresas dedicadas a la gestión y distribución de datos personales.

¿Dónde hay que acudir si eres víctima de un ataque informático? Tanto la Policía Nacional como la Guardia Civil disponen de un servicio especializado en este tipo de delitos. Si crees que puedes estar sufriendo algún tipo de ataque, lo mejor es que lo comuniques a las autoridades. Ellos se encargan de indicarte la manera de proceder. Si crees que el ataque puede deberse al mal funcionamiento de los servidores, de los dispositivos o de las páginas que visitas, también puedes ponerte en contacto con las asociaciones de consumidores. ●

JEAN-BERNARD AUDUREAU,
director de Comunicaciones de Asgeco

asgeco@asgeco.rog
ASGECO
@ASGECO

Derechos y deberes inalámbricos...

Los consumidores viven en un mundo conectado que les ofrece una infinidad de productos o servicios que facilitan su vida. Pueden informarse, divertirse, comparar, realizar trámites administrativos, consultar horarios de autobuses o el estado de sus cuentas bancarias, comunicarse por texto, voz o vídeo, ubicarse en una ciudad desconocida, interactuar en las redes sociales, comprometerse con la economía colaborativa, estrenarse como #CoopSumidores (ver **www.coopsumidores.net**), etc..

Aunque virtual, este mundo digital que posibilita internet es muy real e indispensable para muchos consumidores, y su uso cada vez está más presente en la vida cotidiana. Sin embargo, la brecha digital continúa existiendo en nuestro país, ya sea por edad, situación económica, educación o ubicación. Más del 20% de los hogares no están equipados y millones de consumidores no acceden a los servicios en línea. Este porcentaje no desciende tan rápidamente como sería deseable y se necesitan políticas más activas para facilitar el acceso, por ejemplo mediante redes wifi públicas.

Por ello, la Asociación General de Consumidores, Asgeco Confederación, considera que, aunque internet pueda sumarse a la oferta física de productos y servicios, todavía no puede sustituirla por completo, especialmente en lo que concierne a productos y servicios básicos o de interés general. La accesibilidad del mundo digital sigue estando condicionada por aspectos financieros, técnicos o culturales que aun excluyen a una importante parte de la población, sobre todo a los colectivos más vulnerables.

Los millones de españoles que se conectan cotidianamente a la Red, que se benefician de las oportunidades de lo digital, y no se imaginan vivir sin internet, lo hacen en casa o fuera de ella, utilizando, cada vez más habitualmente, la conexión inalámbrica wifi, a partir de un ordenador, una tableta, un teléfono móvil o cualquier otro dispositivo. Es fácil, cómodo, también, a menudo, gratuito, cuando las conexiones 3G o 4G pueden tener costes relativamente altos, especialmente en el extranjero. Por eso, está tan extendida la costumbre de buscar una conexión wifi cuando estamos fuera de casa, con el fin de poder utilizar internet sin gastar dinero.

Sin embargo, todas estas modalidades de acceso wifi nos hacen vulnerables ante los riesgos que conlleva conectarse a una red no segura, abriendo la puerta al posible robo de datos, contraseñas o imágenes, instalación de *software* malicioso, etc. De la misma manera, como propietarios de una red wifi, si no la protegemos debidamente podemos ser víctimas de intrusiones por atacantes que querrán interceptar los datos que circulan en ella o realizar acciones delictivas, resultando como aparente responsable el dueño legítimo de la red. Aunque este no tenga por qué ser consciente de esta intrusión, puede ver su responsabilidad implicada si no ha implantado medidas de seguridad razonables en su red wifi.

En 2011, el Instituto Nacional de Tecnologías de la Comunicación (Inteco) resaltaba que si bien un 37,8% de los consultados evitaba en la medida de lo posible el uso de redes de terceros y sólo se conectaba para realizar ciertas operaciones concretas, los usuarios que afirmaban conectarse siempre y en cualquier lugar llegaban a la preocupante cifra del 42,9%.

Desde Asgeco alertamos regularmente a los consumidores sobre la necesidad de actuar con cautela a la hora de conectarse a internet, y sobre todo de las precauciones necesarias para proteger nuestros datos personales (ver nuestra web **www.asgeco.org** y la de nuestra campaña **www.noclamesreclama.org**). La primera es desconfiar de las redes wifi desconocidas y desactivar las conexiones automáticas en nuestros terminales, porque el usuario debe ser consciente en cada momento de la red que usa (wifi libre, wifi protegido o 3G/4G propio). No debe usar redes desconocidas para comprar o consultar sus cuentas bancarias o emails, por el riesgo de robo de sus contraseñas. Y aunque nos limitemos a navegar en la red o a buscar nuestro camino en una aplicación GPS, recordemos que así también dejamos rastros que se pueden desviar.

«El usuario no debe usar redes desconocidas para comprar o consultar sus cuentas bancarias o *emails*, por el riesgo de robo de sus contraseñas»

También queremos incidir en que las empresas que ofrecen este servicio (hoteles, bares, wifi públicos, etc.), tienen que asumir la responsabilidad que eso conlleva, exigiéndoles la adopción de medidas sólidas de seguridad. La conexión gratis a internet constituye un servicio diferenciador que muchos consumidores toman en cuenta a la hora de elegir un producto o servicio. Por eso no pueden ver sus datos peligrar por un servicio deficiente que sin embargo ha orientado su decisión de compra.

Asimismo, es necesario que las administraciones públicas desarrollen una normativa específica que no solo faculte extender las posibilidades de conexión a internet, sino que también permita proteger la seguridad de los usuarios, el incremento de redes wifi municipales, las subvenciones a la conexión de familias desfavorecidas, la formación ofrecida a colectivos vulnerables, etc. Sobran las iniciativas, pero deben coordinarse para incluir a todos en esta llamada revolución digital.

Las polémicas sobre el wifi son un síntoma del cambio de paradigma que está experimentando nuestra sociedad, afectando directamente a la economía, pero también a la seguridad y la propiedad de nuestros datos personales. Se puede reivindicar el derecho de poder conectarse a internet en cualquier momento y cualquier lugar. ¿Podríamos extender un derecho universal de acceso a internet a las conexiones inalámbricas? Hemos visto muchos matices que lo complican, limitan o imposibilitan. Las modalidades de conexión no deberían constituir un freno o un riesgo. Mientras sea el caso, los consumidores, los nuevos #CoopSumidores, así como la sociedad en su conjunto, no podrán beneficiarse verdaderamente de la revolución digital.