ECIJA
Torre Mural. Av. Insurgentes Sur 1605 piso 10
Col. San José Insurgentes, C.P. 03900,
Ciudad de México, México
Tel: (+52) 5556626840
www.ecija.com

nota informativa

Ciudad de México, 22 de septiembre de 2022

Wi-Fi público: obligaciones de privacidad

Hoy en día, gran parte de las actividades que realizamos cotidianamente, se han traspasado al mundo digital. El denominador común entre ellas es que para llevarlas a cabo se necesita hacer uso del Internet. En ese sentido, el Internet se ha convertido en un bien intangible indispensable para el ser humano. Es por ello que distintos países del mundo, entre ellos México, han reconocido el acceso al Internet como un Derecho Humano.

Derivado de lo anterior, tanto el Estado como establecimientos de toda índole (hospitales, aeropuertos, bibliotecas, restaurantes, hoteles, centros comerciales, etc.), han instalado redes de Wi-Fi públicas para que las personas puedan conectarse a Internet de forma gratuita y rápida. Sin embargo, existe desconocimiento respecto de los riesgos que puede conllevar el conectarse a ellas.

Por una parte, las Wi-Fi públicas pueden no cifrar la información que se transmite a través de ellas, por lo que cualquier otra persona conectada a ellas con ciertos conocimientos, puede intervenir dicha información: correos electrónicos, contraseñas, información de tarjetas bancarias, contenido de redes sociales, entre otros.

Para prevenir el robo de esta información, se han emitido ciertas recomendaciones a seguir en caso de conectarse a una Wi-Fi pública no confiable o desconocida; por ejemplo: no intercambiar información privada o confidencial, no utilizar servicios de banca móvil o por Internet, ni realizar compras en línea que requieren algún dato bancario. Asimismo, actualmente la mayoría de los dispositivos ofrecen la opción de conectarse a dichas redes públicas a través de una VPN (Virtual Private Network, por sus siglas en inglés), cuya finalidad es precisamente cifrar la conexión de los usuarios, evitando así cualquier intercepción de su información.

Estas medidas y recomendaciones pueden brindar cierta protección frente al ataque de terceros, como los delitos de Phishing. Sin embargo, ¿qué sucede con la información recabada por los establecimientos a través de las redes públicas de Wi-Fi? La mayoría de los usuarios no son conscientes de los datos personales que están compartiendo, a quiénes, ni con qué finalidad cuando usan una red pública. La causa primordial de esta problemática se debe a que los establecimientos son omisos en proveer dicha información.

Hablando del sector privado, conforme a lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, tanto los establecimientos como los proveedores del servicio de Internet, tendrían la obligación de informar a los usuarios sobre los datos personales

que recaban de ellos, las finalidades del tratamiento de los mismos, las transferencias de dichos datos personales a terceros, siendo éstos requisitos mínimos.

Sin embargo, la realidad es que un inmenso número de establecimientos incumplen esta obligación al no poner a disposición de los usuarios un aviso de privacidad para darles a conocer el tratamiento al que serán sometidos sus datos personales. De este modo, deberían informar sobre el uso de los datos que los usuarios proporcionan directamente al establecimiento para acceder al servicio de Internet, así como de aquéllos recopilados automáticamente por los establecimientos y de forma simultánea al momento en que los usuarios navegan a través de una Wi-Fi pública.

Lo anterior evidencia la necesidad de continuar fomentando una cultura de protección de datos personales, con la finalidad de que los usuarios conozcan y exijan sus derechos de privacidad y protección de datos. Finalmente, cabe enfatizar el respeto a estos derechos por parte de empresas y entidades públicas y privadas y, sobre todo, que los órganos de control velen por su protección.

Noticia destacada

El pasado **26 de julio**, el **Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional**, emitió un comunicado sobre los puntos más relevantes que los usuarios deben tomar en cuenta, para evitar ser víctima de un ataque de "Phishing" vía correo electrónico, debido al incremento de casos que ha habido de esta actividad delictiva; a saber:

- Nunca entregar datos por correo electrónico, ya que las empresas y bancos jamás solicitarán datos financieros o de tarjetas de crédito por correo.
- Si uno duda sobre la veracidad del correo electrónico, jamás hacer clic en un link incluido en el mismo.
- Si uno sigue dudando sobre su veracidad, llamar o asistir al banco para verificar los hechos.
- Si uno recibe un email de este tipo de "Phishing", ignorarlo y jamás responderlo.
- Comprobar que la página web a la que se accede, sea una dirección segura; deberá empezar con https://. Igualmente, deberá aparecer un candado pequeño y cerrado en la barra de estado del navegador.
- Cerciorarse de siempre escribir correctamente la dirección del sitio web que desea visitar, ya que existen cientos de intentos de engaños de las páginas más populares con solo una o dos letras de diferencia.

Si uno sospecha que fue víctima del Phishing, cambiar inmediatamente sus contraseñas y ponerse en contacto con la empresa o entidad financiera para reportar el incidente.

Área de TMT de ECIJA México
socios.mexico@ecija.com
(+52 55) 56 62 68 40