Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Ciudad de México, a 16 de julio de 2018
INAI/207/18

EMITE INAI RECOMENDACIONES DE SEGURIDAD PARA PREVENIR ROBO DE DATOS PERSONALES EN REDES DE Wi-Fi PÚBLICAS

Actualmente el Wi-Fi gratuito está disponible en una gran variedad de sitios: aeropuertos, hoteles, centros comerciales, cafeterías y librerías, entre otros, incluso el transporte público y algunos parques ofrecen acceso a Internet sin costo aparente; sin embargo, en muchos casos estas redes pueden ser una ventana de acceso a tus datos personales.

Los datos personales que se obtienen en redes Wi-Fi públicas suelen utilizarse, principalmente, para fines publicitarios. Por ejemplo, si dejas activada la conexión Wi-Fi en tu celular mientras recorres un centro comercial, el teléfono busca constantemente redes a las cuales conectarse y cada punto de acceso que recibe una solicitud de tu dispositivo puede registrar algunos de tus datos, como la frecuencia de visitas por mes o el tiempo de permanencia de un usuario en una tienda.

Con esta información, se crean rutas de clientes potenciales, que utilizan los especialistas en marketing para diseñar mapas de consumo.

Más allá del tema de la mercadotecnia, existen otros riesgos, las redes públicas Wi-Fi pueden ser suplantadas por *ciberdelincuentes* para obtener los datos personales de los usuarios; el peligro aumenta cuando las personas realizan transacciones financieras sin las medidas de seguridad adecuadas.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) advierte sobre el eventual riesgo al que se exponen los usuarios de Wi-Fi públicas, ya que podría haber un tratamiento no deseado de datos personales, o bien, en redes abiertas, cualquier persona que se conecte podría acceder a la información personal de los otros usuarios.

En este contexto, el INAI emite las siguientes recomendaciones:

1. Verifica que la red pública a la que te vas a conectar corresponda a la conexión autorizada del establecimiento, comercio, parque, plaza o sitio que ofrece la red Wi-Fi. Esto se hace preguntando por el nombre de la red, el usuario y la contraseña, o bien, revisando que el sitio de ingreso a la red Wi-Fi pida un registro.

2. Cuando se solicite un registro del usuario para utilizar una red pública Wi-Fi, lee detenidamente el aviso de privacidad antes de proporcionar tus datos personales.

3. No confíes nunca en redes abiertas, con nombres como “Wi-Fi Gratis” o que no requieran contraseña. Éstas suelen ser usadas por *ciberdelincuentes* para robar tus datos personales.

4. Desactiva las opciones para compartir archivos en red. Algunas computadoras cuentan con la capacidad de compartir documentos con otros dispositivos que estén conectados a la misma red. Al conectarse a una señal Wi-Fi pública, es recomendable desactivar esta opción.

5. Evita utilizar el mismo nombre de usuario y contraseña para distintas cuentas. Esta medida de seguridad aplica para las redes públicas Wi-Fi, y también disminuye las posibilidades de que quien obtenga esos datos pueda acceder a otras de tus cuentas.

6. Activa la verificación en dos pasos, de tal manera que, si un *ciberdelincuente* obtiene tu contraseña, se necesite un segundo paso de autenticación para acceder a tus cuentas.

7. Es recomendable utilizar herramientas de cifrado en las comunicaciones como son los servicios de VPN (*Virtual Private Network* o Redes Privadas Virtuales).

8. En servicios de mensajería, se recomienda optar por aquellos que incluyan cifrado, de modo que si un tercero intercepta la comunicación a través de una red inalámbrica Wi-Fi pública, no pueda acceder al contenido.

9. Cerciórate de que las direcciones de los sitios que visites inicien con *https* y que cuenten con un candado de seguridad de color verde, en la barra de direcciones.

10. Nunca realices transacciones bancarias en línea desde una red abierta, ya que tu usuario y contraseña podrían ser interceptados.

11. Desactiva la conexión Wi-Fi cuando no lo estés usando. Además de ahorrar batería, evitarás que tus dispositivos se conecten a redes sin que lo sepas.

12. Comprueba que tus dispositivos no tengan activada la opción de conectarse automáticamente a una red Wi-Fi. Si la tienen, desactívala. Esta medida también te protegerá de los métodos de rastreo que usan algunas organizaciones para identificar patrones de consumo.

13. Evita permanecer más de lo necesario conectado a alguna red Wi-Fi pública. Úsala sólo para tareas cortas y desconéctate cuando ya no la necesites.

-o0o-