Por qué conectarse a un Wifi público es peligroso

24/11/2022

Las redes de WiFi público ofrecen muchos aspectos positivos porque permiten ahorrar datos, movilidad y una solución rápida para un momento de consulta o enviar un mensaje. Pero la lista de desventajas es aún más grande.

Un Wifi de una tienda o que pertenezca a las autoridades no es un peligro por si solo, sino que el problema está en el bajo nivel de privacidad y seguridad que le da al usuario.

La red es el canal de acceso a internet donde transitan todos los datos que la persona pone en el dispositivo y llegan a una aplicación, página y demás. Todo esto queda expuesto al usar este tipo de conexiones porque no se sabe quién pueda acceder esa información o tomar el control.

Este tipo de redes representan un riesgo para los usuarios, pero hay formas de cuidarse.

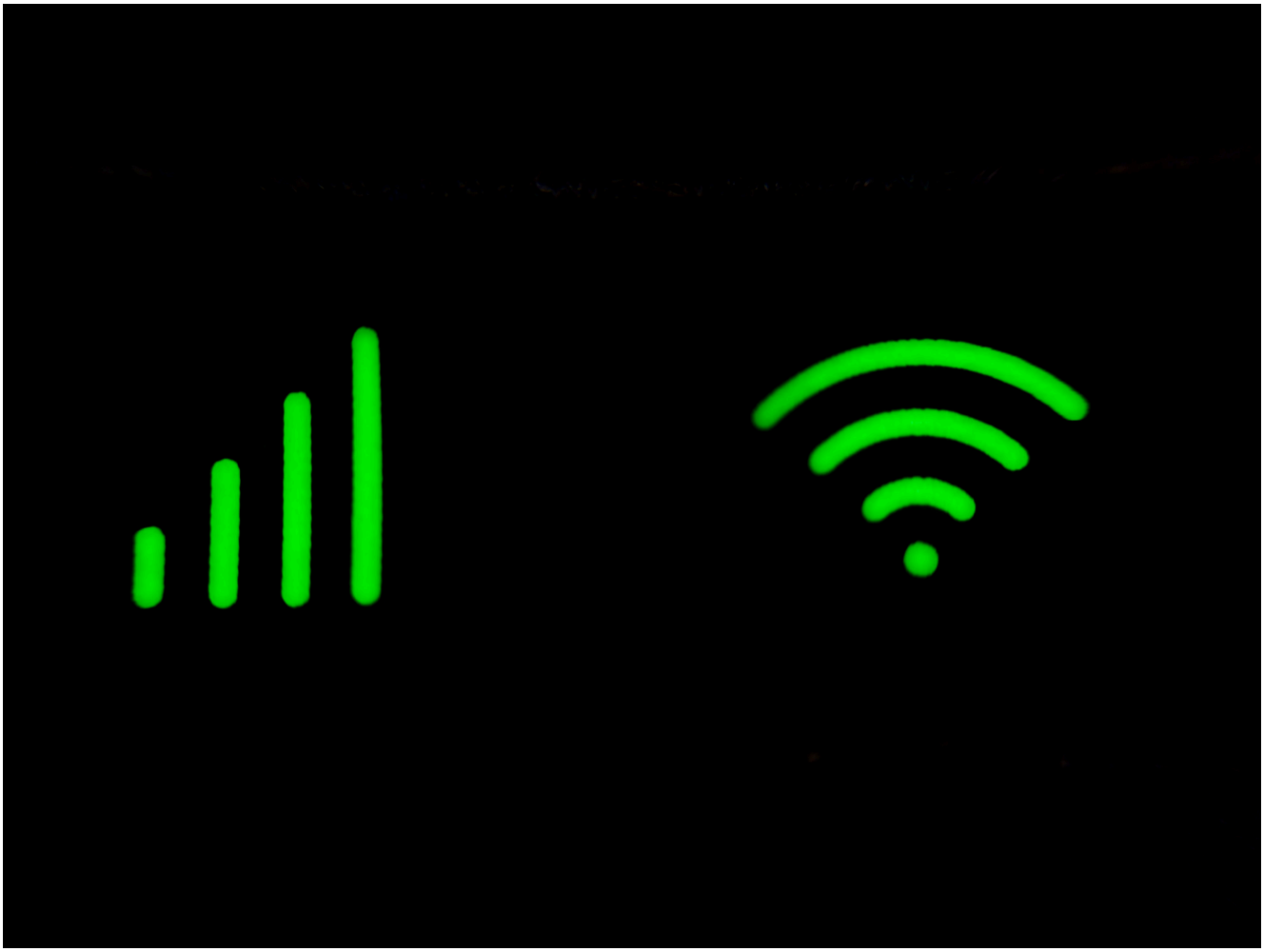
Este tipo de Wifi se suele utilizar para varios tipos de ataques cibernéticos, porque ofrecen muchas herramientas a los delincuentes.

Las maneras de robar información son:

– **MitM:** el delincuente se ubica en medio de la conexión del usuario y la red para tomar, leer y modificar la información que allí transite.

– **Descargar datos:** es similar al anterior, pero la diferencia es que el atacante tiene la posibilidad de analizar y filtrar la información sensible.

– **Descargar malware:** dejando de lado los datos, el delincuente se enfoca en distribuir un virus que les permita controlar el dispositivo a futuro y robar datos.



Este tipo de redes representan un riesgo para los usuarios, pero hay formas de cuidarse.

Cómo evitar estos riesgos

Usar este tipo de redes es algo funcional en varias situaciones, por ejemplo, estar de viaje y que esta sea la única posibilidad de conexión para buscar una ubicación o enviar un mensaje para encontrarse con alguien. Así que es conveniente encontrar soluciones para aprovechar este Wifi sin poner en riesgo los datos y la seguridad del dispositivo.

La primera recomendación es nunca acceder a aplicaciones o páginas que necesiten información personal, como pueden ser bancos, e-commerce o redes sociales en las que no esté abierta la sesión previamente. Al poner una contraseña o número de tarjeta de crédito estos quedarán en evidencia para un potencial atacante. Por lo que tampoco es bueno hacer compras

digitales.

Otra manera de cuidarse es verificando la calidad de la red pública, que está se encuentre encriptada y no sea abierta porque están son insegura. Esto se puede comprobar al conectarse y yendo a las propiedades de Wifi, allí debe salir un apartado que dice ‘Tipo de seguridad’ que debe indicar que es **WPA o WPA2**, lo que garantizará que es una conexión segura.

Otra verificación importante es que la página a la que se va acceder inicie con **‘https’** y que preferiblemente tenga un símbolo de un candado al lado izquierdo. De no tener esto es mejor evitar cualquier conexión porque no será un sitio seguro.

Finalmente, una manera de proteger el teléfono o computador es mantenerlo actualizado para que su sistema de seguridad cuente con todos los parches necesarios para protegerse de potenciales ataques y optar por tener una **VPN** instalada, porque esto permitirá que la conexión se haga de forma privada y proteja los datos.

Fuente: Infobae