Google recomendó evitar el Wi-Fi público: “Consecuencias devastadoras y angustia emocional”

17/11/2025

En un informe recientemente divulgado, **Google alertó a los usuarios de Android acerca de los peligros que supone la conexión al Wi-Fi público**. La compañía estadounidense señaló que los ciberdelincuentes pueden emplear esas redes —por ejemplo, en hoteles, restaurantes, aeropuertos e incluso espacios al aire libre— como un **caballo de Troya para robar información bancaria**.

“Pérdidas devastadoras y angustia emocional” por *culpa* del Wi-Fi

público

De acuerdo al gigante tecnológico, las estafas *online* son cada vez más frecuentes y en ese marco son relevantes las buenas prácticas en ciberseguridad. Una de ellas es **evitar la conexión a redes públicas** porque, según Google, puede derivar en **"pérdidas financieras devastadoras y angustia emocional a las víctimas desprevenidas"**.

¿Por qué es tan riesgos conectarse a esos entornos? "Muchas redes Wi-Fi públicas no están encriptadas y transmiten datos en texto plano, lo que las hace **vulnerables a los ciberdelincuentes** con las herramientas adecuadas», explicó al respecto Oliver Buxton, de la empresa de seguridad Norton, en declaraciones que recoge *New York Post*. "**Los hackers conectados a la misma red pueden interceptar tu actividad en línea**, incluyendo información bancaria, credenciales de inicio de sesión y mensajes personales", agregó.

Conectarse a redes públicas puede derivar en grandes dolores de cabeza. (Foto: Creada con ChatGPT)

Además, Google reveló una de las prácticas maliciosas que, también empleando redes públicas, procuran engañar a los

usuarios. Se trata de los denominados “**puntos de acceso maliciosos**”.

En la práctica, los atacantes realizan **cambios sutiles en el nombre de las conexiones Wi-Fi**, para que los desprevenidos se conecten y queden expuestos. Por ejemplo, modifican una sola letra del nombre de una red legítima. Es una técnica similar a la que se aplica en las URLs o direcciones de correo electrónico alteradas. Buxton las describe como “**redes gemelas malvadas**”.

Esa técnica maliciosa también se inscribe en los ataques homógrafos, una modalidad que repasamos detalladamente en **TN Tecno**.

El Wi-Fi público es un peligro: consejos para evitar dolores de cabeza

- Google recomienda **revisar periódicamente las cuentas bancarias**, para eventualmente detectar indicios de intrusiones o movimientos sospechosos.
- Especialistas aconsejan **desactivar la conexión automática a redes públicas**.
- En caso de que sea imperioso conectarse, es fundamental **chequear que estén cifradas**. Esto se indica con el ícono del candado junto a la conexión.
- Siempre hay que **verificar que la red sea oficial** (en hoteles, bares, terminales, etcétera) para evitar caer en la trampa de las mencionadas “redes gemelas”.
- Otra práctica recomendable en caso de conectarse a un Wi-Fi público es hacerlo a través de una VPN (de un desarrollador confiable, porque las gratuitas también son riesgosas), para esconder información que podría ser útil para los ciberdelincuentes.

Fuente: Canal 26