CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA UNA CONEXIÓN A REDES WIFI PÚBLICAS **MÁS SEGURA**

En vacaciones, solemos estar menos tiempo en nuestra casa y al usar internet, en ocasiones, conectamos nuestros dispositivos a redes wifi abiertas, las que están disponibles en distintos lugares como restaurante, supermercado, hoteles, estaciones de metro, etc., para tener mejor conexión o ahorrar en consumo de datos. Sin embargo, debemos tener cuidado, ya que detrás de esta alternativa hay delincuentes que se aprovechan para cometer algunos delitos.

¿Qué es una red Wifi Pública?

Las redes Wifi permiten conectar nuestro dispositivo tipo laptop, teléfono móvil e incluso tablet a una red de datos de forma inalámbrica.

- La creación de redes inalámbricas falsas es una práctica muy utilizada por ciberdelincuentes con el objetivo de capturar todo el tráfico que pasa por ellas.
- Se les llama también red **Wifi gemela**, porque es un calco exacto de otra legítima y segura. Para crearlas, se utilizan software y hardware para montar la red idéntica, configurada con el mismo nombre y parámetros de conexión, esperando que la víctima caiga se conecte.

Peligros de una red Wifi Pública

Al tener fácil acceso, los ciberdelincuentes se pueden infiltrar y:

- **Robar credenciales, datos e información sensible**
- **Re direccionar el tráfico a páginas fraudulentas**
- **Infectar un dispositivo con malware**

Recomendaciones en caso de conectarse a una red Wifi Pública

- **DESCONECTA** la función **conectarse automáticamente a redes** de tu dispositivo móvil.
- Una Wifi falsa se identifica cuando ves **dos redes con nombres iguales** o muy parecidos. También es muy habitual añadir al nombre de la red Wifi la palabra "gratis".
- **VERIFICA** con el encargado del lugar si disponen de wifi pública y cuáles son los datos de la conexión.
- **NUNCA** realices transacciones bancarias o compres por internet.

Recuerda Siempre

1.- Revisa las URL de los sitios a los que ingresas y asegúrate que sean las páginas oficiales, asegúrate de navegar utilizando el protocolo seguro https.

2.- Mantén actualizado el sistema operativo, navegadores y complementos.

3.- Utiliza un antivirus y actualízalo periódicamente.

4.- Si es posible, evita conectarte a internet en redes abiertas.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl

Síguenos en nuestras redes sociales
Infórmate sobre nuestras actividades y escríbenos directamente