**Evil Twin: ¿Qué es un ataque de Gemelo Malvado?**

**Ciberseguridad 12vos**



Estás un día tranquilamente desayunando en una cafetería, te conectas al [WIFI](https://es.wikipedia.org/wiki/Wifi) público, ¡Y ZÁS! Tu móvil o portátil dejan de responder sin que entiendas bien lo que ha sucedido. Pues bien, hoy queremos prevenir que esto te ocurra, por lo que te contaremos qué es un ataque de Evil Twin, o Gemelo Malvado.

1. **No es una película de terror, pero se le parece.**
2. **Cómo evitar un ataque Evil Twin.**

1. ¡Desactiva la conexión automática!

2. Evita conectarte a redes desprotegidas.

3. No inicies sesión en cuentas personales.

4. Quédate con los sitios web HTTPS.

5. Usa autenticación de dos factores.

[6. ¡No te olvides de la VPN!](https://www.interbel.es/evil-twin/#elementor-toc__heading-anchor-7)

7. Consejo final: ¡Usa un antivirus!

No es una película de terror, pero se le parece.

**Evil Twin o Ataque del Gemelo Malvado**:

¿Qué es esto?

Un ataque Evil Twin es una clase de ataque cibernético al que los usuarios de Internet son vulnerables cuando se conectan al WIFI público. Los piratas informáticos instalan puntos de acceso maliciosos en lugares donde los consumidores esperan encontrar WIFI de acceso libre. Es por eso que tiene este nombre: esperamos encontrarnos con una red abierta inofensiva, pero nos encontramos en su lugar con su gemelo malvado, dispuesto a atacar nuestros dispositivos.

Si te conectas a un punto de acceso Evil Twin, los piratas informáticos pueden monitorear tus visitas a la web y, potencialmente, robar tu información personal para phishing, fraude y robo de identidad. Un ataque Evil Twin podría incluso infectar tu dispositivo con malware, dando a los piratas informáticos acceso remoto para descargar cosas como spyware, keyloggers o un troyano capaz de apoderarse completamente del dispositivo.

Esto hace que sea muy importante saber qué es un ataque Evil Twin y qué puedes hacer para protegerte contra ellos. ¡Empecemos pues!

**Cómo evitar un ataque Evil Twin.**

La forma más fácil de evitar ser víctima de un ataque Evil Twin es evitar los puntos de acceso wifi públicos por completo. En la práctica, sin embargo, la mayoría de las personas confían en Internet gratis para ahorrar en sus planes de datos móviles. Como resultado, la abstinencia total del WIFI público no será posible realmente en la práctica. La buena noticia es que hay varias cosas que puedes hacer para protegerte. Vamos por pasos.

1. **¡Desactiva la conexión automática!**

Entrar en la configuración de tu dispositivo y desactivar la conexión automática es una manera fácil de evitar que se conecte automáticamente a todos los puntos de acceso WIFI a los que te acerques.

El problema con los puntos de acceso de Evil Twin es que a menudo no tienen protección con contraseña. Esto significa que todo lo que necesitas hacer es hacer clic en el punto de acceso, conectarte y comenzar a usar el Internet gratuito proporcionado por el hacker. Por supuesto, si tu dispositivo móvil está configurado para conectarse automáticamente a cualquier red disponible, puedes conectarte accidentalmente a un punto de acceso **Evil Twin** sin siquiera darse cuenta. ¡Mucho cuidado!

2. **Evita conectarte a redes desprotegidas**.

Cuando te muevas por tu ciudad, te vayas de vacaciones o necesites viajar por trabajo, tendrás la oportunidad de conectarte a muchos puntos de acceso WIFI públicos. Algunos de estos serán puntos de acceso legítimos que han sido asegurados por el establecimiento que proporciona Internet gratis.

Una red WIFI protegida es fácil de distinguir de una red desprotegida. Esto se debe a que, por lo general, deberás solicitar la contraseña al proveedor del punto de acceso WIFI para poder conectarse. En caso de duda, pregunta al establecimiento que estás visitando el nombre (SSID) de su punto de acceso WIFI.

3. **No inicies sesión en cuentas personales.**

Cuando usas WIFI público, puedes reducir enormemente los peligros involucrados al evitar iniciar sesión en cuentas privadas. El WIFI público puede ser útil para jugar juegos móviles, verificar el clima, obtener direcciones, realizar búsquedas en la web y otras tareas inofensivas.

En general, sin embargo, es mejor no iniciar sesión en tus cuentas personales, y es extremadamente importante no ingresar detalles de pago ni acceder a servicios financieros como la banca por Internet. Recuerda que, en un ataque de este tipo, toda la información que ingreses está comprometida.

4. **Quédate con los sitios web HTTPS.**

Los sitios web [HTTPS](https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto) están protegidos con el sólido protocolo Transport Layer Security (TLS). Los sitios web HTTPS y los servicios en línea brindan un sólido cifrado de extremo a extremo para tus datos. Esto garantiza que están protegidos contra intrusos y significa que los datos transmitidos desde tu dispositivo al sitio web están seguros.  
  
Lo importante a recordar es que la “S” en HTTPS significa “seguro“. Esto hace que esos sitios HTTPS sean mucho más seguros que los sitios web que tienen el prefijo HTTP. Por esta razón, es importante ceñirse a los sitios web HTTPS, especialmente si estás utilizando WIFI público.

5. **Usa autenticación de dos factores**.

Un ataque de Evil Twin puede sorprenderte donde menos lo esperas.

Al configurar la autenticación de dos factores para tus cuentas en línea, te aseguras de que sea imposible iniciar sesión en tus cuentas sin una contraseña y el código de autenticación que se envía a tu dispositivo físico. Esto te quita presión al aumentar su seguridad y hacer que sea menos preocupante si una contraseña se ve comprometida.

6. **¡No te olvides de la VPN!**

Una [VPN](https://es.wikipedia.org/wiki/Red_privada_virtual) es un servicio en línea diseñado para brindarte privacidad y seguridad en línea. Funciona protegiendo tus datos dentro de un túnel encriptado. El cifrado de la VPN codifica por completo tus datos a medida que viajan desde tu dispositivo y por Internet hasta la ubicación del servidor VPN remoto.

La seguridad que brinda una VPN confiable hace que sea imposible que los administradores de redes locales, los proveedores de servicios de Internet, los piratas informáticos u otros espías vean lo que estás haciendo en línea. El beneficio de una VPN es que se vuelve imposible para los atacantes leer los datos cuando pasan por WIFI.

7. **Consejo final: ¡Usa un antivirus!**

Cada vez que te conectas a Internet, te expones potencialmente a la amenaza de ciberataques y piratería. Ya sea que uses WIFI público o te conectes a Internet en casa, te recomendamos encarecidamente que siempre habilites un firewall confiable que monitoree activamente todos los paquetes de datos entrantes para garantizar que estén seguros. Los mejores cortafuegos también supervisan el tráfico saliente para evitar que infecciones graves de malware, como los troyanos, puedan comunicarse con los servidores de comando y control.

 