

Redes wifi públicas y el ataque

“Man in the middle”

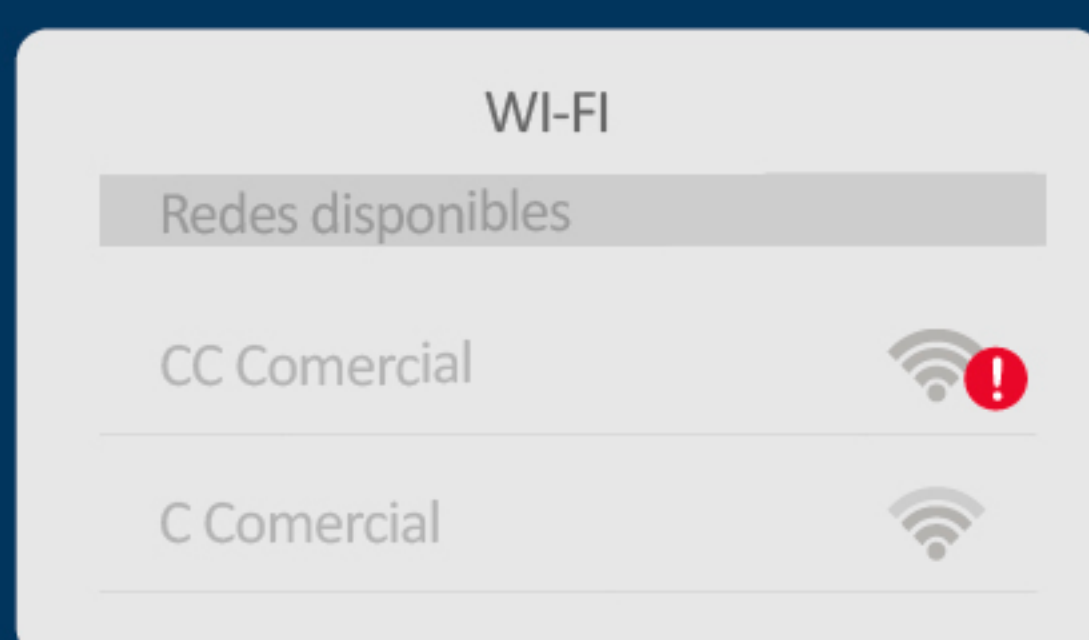
¿Qué debes saber?

Hablamos de un ataque *man in the middle* cuando un **ciberdelincuente se mete en el medio de una comunicación online para espiar a los interlocutores, o hacerse pasar por uno de ellos. Un ejemplo:**

1

1 CREACIÓN DE UNA RED WIFI FALSA

Con el mismo nombre, o uno muy similar al de una red pública cercana. Por ejemplo:



2

2 CONEXIÓN DEL USUARIO

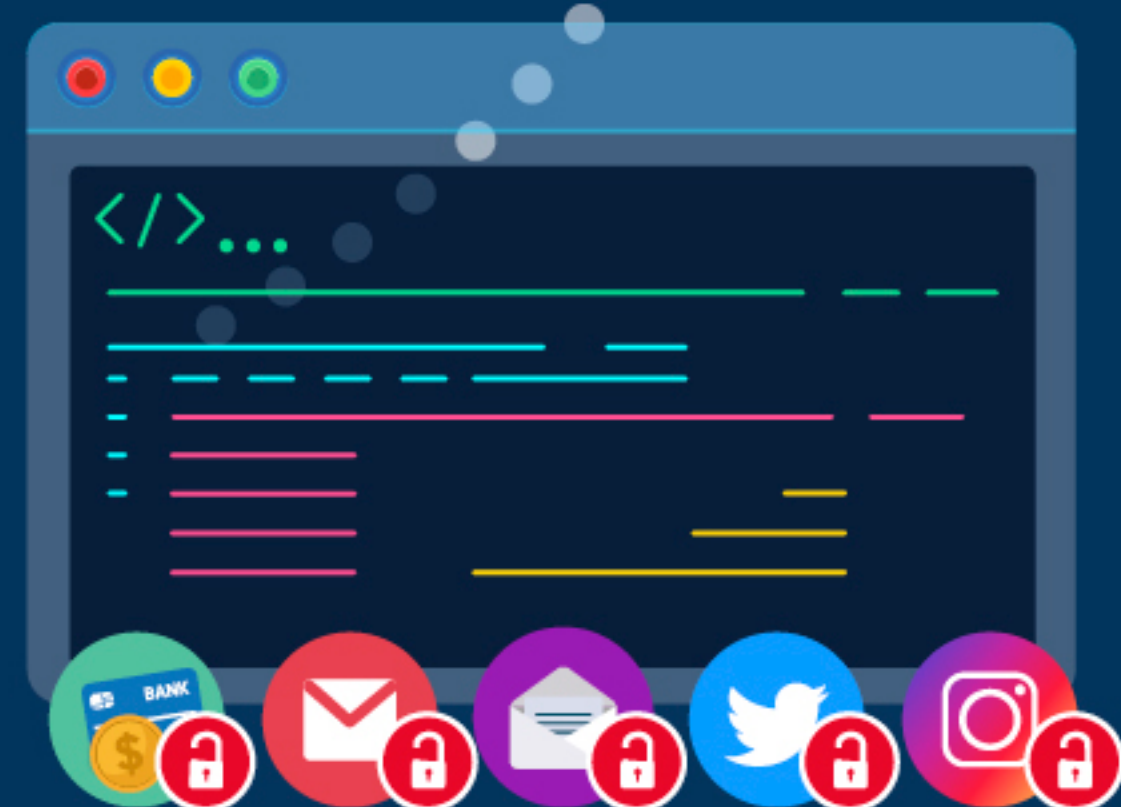
Eligiendo la red falsa, o conectándose automáticamente (si coincide con el nombre de una red a la que ya se hubiera conectado). **No notará ninguna diferencia, y navegará sin sospechar nada.**



3

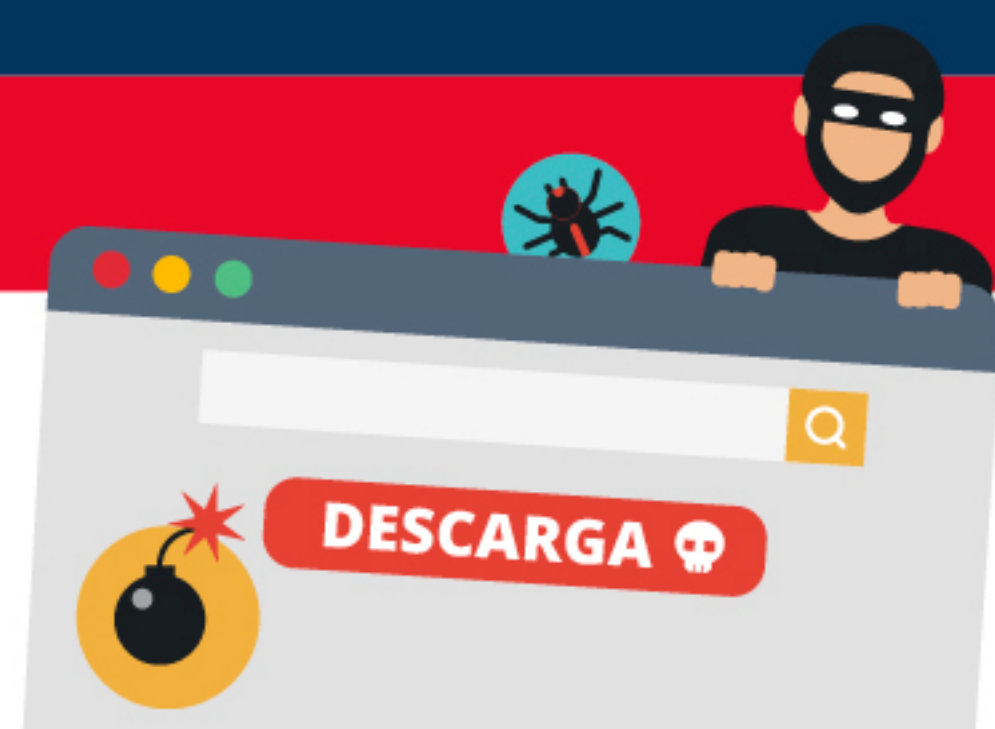
3 MONITORIZACIÓN DE ACTIVIDAD

Desde ese momento, el **atacante podrá recopilar toda su información de navegación**: datos bancarios, cuentas de correo, redes sociales, etc., e incluso suplantar su identidad con fines económicos o para dañar a otras personas.



Man in the browser

Existen otras variantes como el *man in the browser*, donde un **malware en el navegador del usuario registra su actividad online**. La infección suele producirse al descargar software de páginas no oficiales, archivos adjuntos desde un *phishing* o un enlace malicioso.



Medidas de protección

La norma número 1 es **NO conectarnos a redes públicas** (hoteles, centros comerciales, aeropuertos, etc.). Pero existen otras pautas a seguir:

- **Actualizar** los dispositivos, programas y app.
- Emplear **contraseñas robustas** y verificación en dos pasos.
- **Navegar por páginas https** y comprobar su certificado digital.
- Usar **apps con cifrado** extremo a extremo, cifrar documentos y correos.
- Utilizar una **VPN**.



¡La prevención es la mejor forma de proteger nuestros datos!

Si necesitas ayuda con la ciberseguridad, contacta al **teléfono gratuito 017** y te ayudaremos.

www.incibe.es | www.osi.es