

En el mundo digital, hay una frase que cada vez suena más fuerte: **secuestro de cookies de sesión**. Y no, no tiene nada que ver con galletitas dulces, ni «biscochitos de grasa Don Satur», sino con una de las formas más silenciosas que usan los ciberdelincuentes para meterse en tu vida digital... sin que te des cuenta.



□ ¿Qué son las cookies de sesión?

Cada vez que iniciás sesión en la web (como tu correo, redes sociales o banca online), tu navegador guarda un pequeño archivo llamado *cookie*. Ese archivo es como un pase VIP: le dice a la web que **sos vos** quien está ahí. Pero... ¿Qué pasa si alguien roba ese pase? Exacto: **puede hacerse pasar por vos** sin necesidad de tener tu contraseña. Entonces... «estaremos en el horno».

Pero para que eso no te pase, estoy yo que te traigo, en modo simple, esta información.

□ ¿Cómo pueden secuestrar tus cookies?

Hay dos formas muy comunes:

1. Ataques «Hombre en el Medio» (Man in the Middle)

Imaginate que estás en una red Wi-Fi pública. Alguien puede interceptar la conexión entre vos y la web, leer tus datos en tránsito y robar esa cookie que te identifica.

2. Sniffers en redes inseguras

Con programas que «olfatean» el tráfico de red, es posible capturar lo que pasa entre tu navegador y el servidor... incluyendo tus cookies.



□ ¿Y qué pueden hacer con eso?

Con una cookie de sesión robada, pueden:

- Entrar a tu cuenta de redes sociales.
- Leer tus mails.
- Comprar cosas si dejaste datos guardados.
- Cambiar tu contraseña y bloquearte el acceso.

Suena muy mal, ¿no?

□ ¿Cómo protegerte?

Por suerte, **sí se puede evitar**. Y sin volverse paranoico ni un experto en ciberseguridad. Estas son algunas recomendaciones simples:

- **Usá siempre webs que empiecen con «https://»**, no solo en el login. La «s» significa que la conexión es segura.
- **Evitá redes Wi-Fi públicas** para cosas sensibles. Mejor usá tu red móvil o redes de confianza. Si no podés evitarlo, conectate por medio de una conexión con **VPN** (Red Privada Virtual). [Lee + aquí](#)
- **Configurá tu navegador para que elimine las cookies al cerrar la sesión.**

□ Aquí están algunas guías rápidas:

- En **Chrome**, buscá “Configuración > Privacidad > Configuración de sitios > Datos del sitio” y activá el borrado al cerrar.
- En **Firefox**, en “Privacidad y Seguridad”, activá “Eliminar cookies al cerrar Firefox”.
- En **Edge**, activá el borrado automático de cookies en “Privacidad, búsqueda y servicios”.
- En **Safari**, hay que hacerlo manual. Pero también se puede.

□ ¿Y si ya te pasó?

- Cambiá tus contraseñas **YA**.
- Revisá la actividad extraña en tus cuentas.
- Contactá con los servicios afectados.

Cómo ves, esto se pone cada vez más interesante (...) preocupante?, y sí. Pero si queremos seguir haciendo uso de las tecnologías (algo inevitable al día de hoy), educarnos y aprender, es el mejor antídoto al miedo y la falta de confianza que luego nos jugarán en contra. Y recordá: cada vez que no entiendas algo, ¡preguntá!. Nadie nació sabiendo y si necesitas ayuda, me podés contactar.

Por favor, síguenos y danos «me gusta»:

