Session Hijacking - what it is, common signs, and how to stop it

Gridinsoft Help Center

What it is

Session hijacking is when an attacker steals your "logged-in" state - the cookie or token that proves you're you - and uses it to act as you without knowing your password. They might grab it over a weak or fake Wi-Fi, from a infected device, or by tricking the browser. Once they have that token, they can open your account and do things in your name until the session is killed or expires. Background and examples: https://gridinsoft.com/session-hijack

Why it matters

With a stolen session, attackers can read messages, move money, change settings, or add recovery emails/phones to lock you out - all without triggering a normal login prompt.

How it works - quick tour

- Sniff: capture cookies/tokens on unencrypted or rogue networks.

- Inject/redirect: force the browser to send tokens to the attacker (malicious scripts, evil portals).

- Malware: grab browser data from an infected device.

- Replay/use: load the token in another browser and act as the victim.

Red flags

- You're logged out unexpectedly, then see logins from new places.

- Account changes you didn't make (password, recovery email/phone).

- Security emails about new devices or "session ended due to another login."

- MFA wasn't asked for a "new" login because a valid session was reused.

Do it right

- Use HTTPS everywhere; avoid logging in on public/unknown Wi-Fi without a trusted VPN.

- Turn on MFA and sign out of all sessions after password resets.

- Log out on shared devices and clear cookies when done.

- Keep your browser and extensions clean and updated; remove ones you don't need.

- If you suspect hijacking, change your password from a clean device and revoke active sessions.