MITM (Man in the Middle) - What it is, red flags, and how to prevent it

Gridinsoft Help Center

What it is

A Man in the Middle (MITM) attack is eavesdropping with extra steps: an attacker quietly positions between you and a website or app, reading or altering traffic as it passes. For a short primer and examples, see our MITM explainer.

Why it matters

MITM can steal logins, reroute payments, inject malware, or swap downloads, all while the page still looks normal.

How it works - quick tour

- Rogue Wi-Fi/evil twin: a fake hotspot captures your traffic.
- SSL stripping/DNS hijack: traffic is downgraded or sent to a copycat site.
- ARP spoofing on LAN: the attacker impersonates your router.
- Proxy injection: malware installs a local proxy or root certificate.

Red flags

- Certificate warnings or padlock missing on sites that should be secure.
- Login pages at odd domains or with spelling look-alikes.
- Public Wi-Fi that forces installs, proxies, or captive portals that never end.
- Sudden logouts, re-prompts for passwords, or mixed-content alerts.

Prevent it

- Use HTTPS everywhere; verify the padlock and certificate details.
- Prefer cellular or trusted Wi-Fi; avoid unknown hotspots.
- Turn on VPN on public networks; disable auto-connect to Wi-Fi.
- Enable MFA so stolen passwords alone are not enough.
- Keep OS, browsers, and apps updated; remove shady root certificates.
- For teams: use HSTS, DNSSEC, DoH/DoT, and monitor for TLS downgrade events.