Packet Sniffing - What it is, risks, and how to protect your traffic

Gridinsoft Help Center

What it is

Packet sniffing is the inspection of network traffic as it flows across a wire or Wi-Fi. Admins use it to troubleshoot and secure networks, while attackers use it to steal logins, spy on activity, or stage malware. For a short primer and tools, see our packet sniffer explainer.

Why it matters

Most apps still pass valuable clues in their traffic. On unsafe networks or misconfigured systems, sniffing can reveal credentials, session tokens, visited sites, and device details.

How it works - quick tour

- Capture: a sniffer listens on a network interface or mirror port
- Decode: protocols like DNS, HTTP, TLS handshakes are parsed
- Filter: analysts search by host, user, app, or indicator
- Act: findings power fixes, detections, or - in attacks - credential theft

Red flags

- Unexpected certificate warnings or captive portals that never finish
- New root certificates or proxy settings you did not add
- Open or weak Wi-Fi where logins are requested
- Strange tools running with promiscuous mode on endpoints

Prevent it

- Prefer HTTPS and TLS 1.2+ everywhere; enable HSTS on sites you manage
- Use VPN on public Wi-Fi and disable auto-join to unknown networks
- Turn on MFA so stolen passwords are not enough
- Segment networks, lock down mirror/SPAN ports, and monitor for sniffing tools
- For admins: capture only with authorization, mask sensitive fields, and secure pcap storage