Password Sniffer - What it is, red flags, and how to protect your accounts

Gridinsoft Help Center

What it is

A password sniffer is malware or a rogue tool that captures login credentials as they travel over a network. On unsafe Wi-Fi or misconfigured systems, it can read usernames, passwords, cookies, and session tokens to hijack accounts without you noticing.

Why it matters

Once a sniffer steals a password or session, attackers can log in as you, change recovery info, move money, or pivot deeper into company systems.

How it works - quick tour

- Listens to traffic: puts the network card in promiscuous mode to read packets.

- Man-in-the-middle: uses ARP spoofing, rogue APs, or proxies to sit between you and a site.

- Credential grabs: targets plaintext logins, weak protocols, or session cookies on partially encrypted sites.

- Exfiltration: sends captured data to a command server for later use.

What you may notice

- Certificate or padlock warnings on sites that should be secure.

- Forced logouts, unusual login alerts, or new devices on your accounts.

- Unknown root certificates, proxy settings, or VPN profiles added.

- On corporate nets: IDS alerts about ARP spoofing or promiscuous interfaces.

If you suspect it - first moves

- Disconnect from the network and switch to cellular.

- From a clean device, change passwords and enable MFA on email, banking, and cloud.

- Run a full anti-malware scan, reboot, then scan again.

- Remove unknown proxies, certificates, VPNs, and browser extensions.

- Review account activity and sign out of other sessions.

Prevent it

- Prefer HTTPS everywhere and use a VPN on public Wi-Fi.

- Turn on MFA so stolen passwords alone are not enough.

- Keep OS, browsers, and apps updated; disable legacy protocols.

- Avoid auto-connecting to open networks and forget untrusted SSIDs.

- For teams: segment networks, enable HSTS/DoH/DoT, monitor for MITM and ARP spoofing, and restrict SPAN/mirror ports.