DNS Hijacking: What it is, red flags to spot, and how to fix it fast

Gridinsoft Help Center

What it is

DNS hijacking is when someone tampers with the internet’s phone book (DNS) so your browser goes to the wrong site-often a fake login page or a malware download-even though you typed the right address. Get the full rundown in our DNS hijacking explainer.

How it works

- Attackers poison DNS answers on your device, router, or a DNS server in the path.
- Your request for a legit site returns a malicious IP instead.
- You land on a look-alike page that steals logins or pushes malware.

What you might notice

- A familiar site looks off (new domain, odd padlock details, typos).
- Browser warnings about certificates, or login pages asking for extra info.
- Your router’s DNS settings changed, or devices all misresolve the same sites.

If you suspect it

- Stop and verify the domain and certificate before logging in.
- Flush DNS cache (device) and reboot the router.
- Set DNS to a trusted resolver (on device and router).
- Scan for malware; change passwords from a clean device.
- Check the router: update firmware, change the admin password, disable remote admin.

Prevent it

- Keep OS, browsers, and router firmware updated.
- Use MFA so a fake page can’t steal your account.
- Lock down the router: strong admin password, no default creds, no exposed management.
- Force all network DNS to a chosen resolver; block outbound DNS to others.
- Prefer HTTPS everywhere and read the address bar before you log in.