URL Hijack - what it is, warning signs, and how to avoid look-alike redirects

Gridinsoft Help Center

What it is

URL hijacking is when scammers get you to visit the wrong website on purpose. They register look-alike addresses for popular sites (like amaz0n.com or gooogle.co) or set up sneaky redirects, so a small typo or a tricky link sends you to a fake page that can steal logins or push malware.

Why it matters

Landing on the wrong site can expose passwords, card details, or install unwanted software. It looks close enough to feel safe - that’s the trap.

How it works

- Look-alike domains: swap letters, add extra characters, or use a different ending (.co vs .com).

- Redirects: ads, pop-ups, or hacked pages bounce you to a malicious site.

- Search tricks: paid ads or poisoned results put the fake above the real site.

- Auto-complete: your browser finishes a mistyped address with the wrong domain.

Red flags

- The address bar is close but not exact (numbers for letters, extra hyphens).

- No padlock (HTTPS) or a certificate issued to a random name.

- Sudden pop-ups to "update your browser," "verify now," or download a "codec."

- Payment pages that look slightly off or ask for unusual info.

Do it right

- Type important addresses yourself or use bookmarks; avoid clicking login links in emails.

- Check the full URL before entering passwords or payment details.

- Use a password manager - it won’t autofill on the wrong site.

- Keep your browser and security software updated; report look-alike domains when you see them.