URL Redirection Attack - what it is, warning signs, and how to avoid malicious jumps

Gridinsoft Help Center

What it is

A URL redirection attack tricks your browser into leaving a real site and loading a fake one. The attacker slips a redirect into a link or page (or abuses a site's "open redirect" bug), so when you click, you're quietly sent to a malicious page that can steal logins or push malware.

Why it matters

You think you're on a trusted site, but the final page is a look-alike built to grab passwords, card details, or install unwanted software.

How it works

- Poisoned link: an email/DM/ad includes a legit-looking link that contains a redirect parameter.

- Open redirect: the real site accepts a ?next= or redirect= value and forwards you anywhere.

- Bounce: your browser follows the chain to a phishing or malware site.

- Take: the fake page asks you to log in, pay, or download something.

Red flags

- Links with long tails like ?redirect= or ?next= pointing to a different domain.

- You see a flash of one site, then land on another.

- The address bar doesn't match the brand you expected.

- Login pages asking for extra info (full card details, recovery codes).

Do it right

- Don't log in through links in emails or texts; open the site from your bookmarks or type it yourself.

- Before clicking, hover to preview the real destination; check the domain after the page loads.

- If a site bounces you somewhere unexpected, close the tab and try again from a clean, known link.

- Use a password manager - it won't autofill on the wrong domain.

- Keep your browser and security software updated to block known bad sites.