Web Cache Poisoning - what it is, why it’s risky, and simple ways to stay safe

Gridinsoft Help Center

What it is

Web cache poisoning is when attackers sneak bad content into a website’s cache. The cache is a "shortcut" server use to make pages load faster for everyone. If it’s poisoned, later visitors get the attacker’s fake version instead of the real page - which could show wrong info, a phishing login, or a malware download.

Why it matters

You can land on a trusted site and still see a fake page. That makes phishing more convincing and can spread malware to many people quickly.

How it works

- Find a gap: attacker discovers inputs (headers/URLs) the site doesn’t validate well.
- Plant: crafts a request that makes the cache store a tainted response.
- Serve: other users request the same page and receive the poisoned version.
- Profit: fake logins steal passwords; script injections push malware or scams.

Red flags

- A familiar site suddenly asks you to log in again on an odd-looking page.
- Download prompts or pop-ups appear on pages that normally don’t have them.
- Mixed messages: part of a page looks normal, but buttons/links go somewhere strange.
- Friends report the same weird behavior on the same site around the same time.

Do it right

- If a "trusted" site starts acting weird, stop and reload later or use a different device/network.
- Don’t enter passwords on pages that look off - type the site’s address yourself and compare.
- Use a password manager and MFA; the manager won’t autofill on fakes, and MFA limits damage.
- Keep your browser and security software updated to block known malicious scripts.