Typosquatting - what it is, telltale signs, and how to avoid look-alike sites

Gridinsoft Help Center

What it is

Typosquatting is when scammers make look-alike websites based on common typing mistakes (like gooogle.com or micr0soft.com). If you mistype a URL or tap a tricky link, you land on the fake site that copies the real one to fool you into logging in, paying, or downloading "updates."

Why it matters

These copycat sites can steal your passwords and card details or install malware. One quick typo can hand over your main account.

How it works - quick tour

- Register: scammers buy domains with swapped/extra letters or different endings (.co vs .com).
- Clone: they copy the real site’s logo and layout.
- Lure: links in emails, DMs, ads, or autocomplete mistakes send you there.
- Take: fake logins or "downloads" grab your data or infect your device.

Red flags

- The web address is close but not exact (extra letters, numbers instead of letters).
- No padlock (HTTPS) or a certificate that looks random.
- Pop-ups yelling "update now," "verify," or "download a codec."
- Prices or offers that are way better than the real site.

Do it right

- Type important sites yourself or use bookmarks.
- Check the full address bar before entering a password.
- Use a password manager - it won’t autofill on the wrong site.
- Keep your browser and security app updated and report look-alike domains when you see them.