Address Bar Spoofing explained: signs, quick checks, and fixes

Gridinsoft Help Center

What it is

Address bar spoofing is a visual trick: the page makes your browser’s top bar look like you’re on a trusted site when you’re not. Fake URL, real danger-because you’ll feel safe entering logins or payment details.

Why it works

- Pop-ups or full-screen overlays that mimic the browser chrome
- Malicious mobile pages that hide the real URL
- Unicode look-alikes (paypaI.com with a capital "i")
- Redirect loops that flash a trusted domain, then swap it

Spot the signs

- You can’t edit or select the URL text
- Back/refresh buttons don’t behave normally
- The padlock is shown in the page image, not the browser
- Tiny typos or extra words before/after the domain

Stay safe (quick tips)

- Tap/click the bar and fully reveal the URL; long-press on mobile to copy and inspect.
- Use bookmarks for banks/email; avoid links in messages.
- Prefer app sign-ins or type the address yourself.
- Turn on MFA so a stolen password isn’t enough.

If you clicked already

- Close the tab, clear recent site data for that domain.
- Change the password from a clean device; review sessions.
- Watch statements/alerts; run a malware scan.