Domain Spoofing: What it is, red flags to spot, and how to avoid the trap

Gridinsoft Help Center

What it is

Domain spoofing is when attackers pretend to be a trusted website or sender by using a look-alike address - think paypaI.com (with a capital "I"), or emails that seem to come from your bank. The goal is to trick you into entering passwords, downloading malware, or sending money.

How it works

- Look-alike domains: swapped letters, extra words, or different endings (.co vs .com).

- Email impersonation: forged "From" names, copied logos, and real-looking signatures.

- Link masks: buttons say one thing, but the actual URL goes somewhere else.

Red flags

- Urgent messages about payments, deliveries, or account "verification"

- Slight misspellings in the domain or a different domain ending

- Links that don’t match the sender’s real website when you hover

- Attachments you didn’t expect (invoices, resumes, zipped files)

If you suspect spoofing

- Pause - don’t click. Hover over links and read the full address.

- Verify out of band: call the company using a number you trust or visit the site by typing it in.

- Report and delete the message; if you clicked, change passwords from a clean device and turn on MFA.

Prevent it

- Use MFA so a stolen password isn’t enough.

- Bookmark important sites and use those bookmarks to sign in.

- Teach your team/family to hover and check before clicking.

- For businesses: set up DMARC, DKIM, and SPF to block spoofed emails.