Spoofing - what it is, common signs, and how to avoid fakes

Gridinsoft Help Center

What it is

Spoofing is when someone pretends to be a trusted person or service by faking details like email sender, phone number, website address, or even a Wi-Fi name. The goal is to make you drop your guard and click, share a code, or send money. Quick explainer and examples: https://gridinsoft.com/spoofing

Why it matters

If the "from" line or caller ID looks real, people act fast - that’s how logins, 2FA codes, and card details get stolen. Spoofed sites can also install malware or harvest personal data.

How it works

- Email spoofing: forged "from" address looks like your bank or a coworker.
- SMS/voice spoofing: caller ID or text appears local or matches a brand.
- Website spoofing: lookalike domains and pages copy the real site’s design.
- Network spoofing: fake Wi-Fi hotspots or ARP/DNS tricks route you through an attacker.

Red flags

- Urgent messages asking for one-time codes, passwords, or payments.
- Links that look close but not exact (swap letters, extra hyphens, weird endings).
- Caller ID says "bank/police," but they ask for private info or gift-card payment.
- A "free Wi-Fi" with a name almost identical to the real one.

Do it right

- Don’t trust the display name or caller ID - verify using the official app, saved number, or by typing the URL yourself.
- Check the address bar: https and the exact domain before logging in.
- Never share 2FA codes over phone or text.
- Use MFA and a password manager; they help spot fake sites and limit damage.
- Keep your browser/OS updated and avoid logging in on random Wi-Fi.