Phishing - What it is, red flags to spot, and how to avoid the hook

Gridinsoft Help Center

What it is

Phishing is a scam where someone pretends to be a trusted person or service to trick you into giving up passwords, card numbers, or other sensitive data. It shows up in email, texts, social DMs, and look-alike websites. For a quick overview, see our phishing explainer.

Why it matters

One click on a convincing message can lead to account takeover, drained funds, or identity theft. Phishing is the easiest way for attackers to get in.

How it works - quick tour

- Impersonation: fake invoices, "security alerts," or delivery notices
- Urgency: "your account will be closed today" to push fast action
- Look-alike links: domains that mimic real brands or use URL shorteners
- Data capture: fake login pages or forms steal your credentials

Red flags

- Sender address that’s close but not quite right
- Urgent requests for payment, gift cards, or password resets
- Links that don’t match the displayed domain when you hover
- Attachments asking to enable macros or "unlock" content

Prevent it

- Pause and verify out of band - call the company using a known number
- Check the full sender address and hover to preview links
- Turn on MFA so a stolen password is not enough
- Keep your browser and security tools updated and use DNS/web filtering
- For teams: run phishing awareness training and use email authentication (SPF, DKIM, DMARC)