Smishing - what it is, common signs, and how to stay safe over SMS

Gridinsoft Help Center

What it is

Smishing is phishing over SMS. You get a text that looks urgent or official and it tries to make you tap a link or reply with info. The goal is the same as classic phishing: steal passwords, card numbers, or one-time codes. Basics and examples: https://gridinsoft.com/smishing

Why it matters

Texts feel personal and people react fast. One tap can send you to a fake login, install a shady app, or hand over your 2FA code.

How it works

- Hook: "Your package is held," "Bank alert," "Tax refund," "Account locked."
- Bait: a short link to a fake site or a request to text back details.
- Push: pressure to act now - or you'll get fees, fines, or missed deliveries.
- Take: credentials, card data, or a malicious app install.

Red flags

- Unknown numbers or "local-looking" numbers you don't recognize.
- Short links you can't preview, or links that don't match the brand's site.
- Requests for one-time codes, full card numbers, or banking details.
- Threats, countdowns, or prizes you didn't expect.

Do it right

- Don't tap links from unexpected texts. Go to the official app or website yourself.
- Never share one-time codes in a reply - not with anyone.
- Block and report the number; delete the message.
- Turn on MFA and use a password manager so stolen passwords are less useful.
- On Android/iOS, keep the OS and apps updated; remove any app you didn't mean to install.