Robocall - what it is, scam red flags, and how to block and avoid them

Gridinsoft Help Center

What it is

A robocall is an automated phone call that plays a recorded message when you pick up. Legit uses exist (school alerts, appointment reminders, public notices), but criminals abuse robocalls to push scams, fake tech support, and phishy "urgent" requests.

Why it matters

Scam robocalls trick people into sharing card numbers, 2FA codes, or remote-access permissions. They waste time, invade privacy, and can lead to identity theft or drained accounts.

How it works - quick tour

- Auto-dialers place thousands of calls per minute using cheap VoIP.
- Caller ID can be spoofed to look local or mimic trusted brands.
- A menu or live agent takeover steers you to pay, install software, or give data.
- Some campaigns "validate" active numbers to target you again.

Red flags

- "Act now" pressure: police, bank, or tax threats with a countdown.
- Requests for payment by gift cards, crypto, or wire.
- Calls asking for your one-time code or full card details.
- Numbers that look like yours (neighbor spoofing) calling repeatedly.

Prevent it

- Let unknown numbers go to voicemail; call back using the official number on the website or card.
- Enable carrier call-filtering and add your number to do-not-call lists (won’t stop criminals, but reduces legit spam).
- Never read out 2FA codes or install software at a caller’s request.
- Block and report scam numbers; use phone settings or your carrier’s app.