GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

S

Smishing: How to Recognize and Respond to Text Scams

Smishing is phishing delivered by text message. Learn the common lures, warning signs, safe verification steps, reporting options, and what to do after interacting.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	5 min

CONTENTS

In this guide

01 How smishing works
02 Common smishing lures
03 Warning signs
04 What to do with a suspicious text
05 If you clicked or responded
06 Reducing smishing risk
07 Frequently asked questions

Quick answer: Smishing is phishing delivered through SMS or another text-messaging service. A scammer impersonates a trusted organization or person and tries to make you click a link, call a number, reply, install an app, reveal a code, or send money. Do not use

contact details in an unexpected message; verify the claim through an app, website, statement, or phone number you already know is genuine.

01 How smishing works

Text messages feel immediate and are often read on small screens where full URLs and sender details are hard to inspect. Attackers create urgency, fear, curiosity, or an attractive offer, then direct the victim to a fake sign-in or payment page. Other campaigns start a conversation and gradually build trust rather than include a link in the first message.

Sender names and numbers are not reliable proof. Messages can come from spoofed identities, disposable numbers, compromised accounts, or legitimate messaging services abused by criminals. A scam may appear in the same conversation as a real organization’s messages in some circumstances.

02 Common smishing lures

- a package cannot be delivered until a small fee or address update is completed;
- an unpaid road toll, tax, fine, or utility balance requires immediate payment;
- a bank or retailer detected fraud and asks you to verify a transaction;
- an account will be suspended unless you sign in through a link;
- a recruiter offers easy remote work and asks you to move money or buy equipment;
- a “wrong number” develops into a friendship, romance, or investment pitch;
- a manager or family member claims to need gift cards, a transfer, or a one-time code.

The FTC’s current guidance on unexpected text scams highlights fake fraud alerts, delivery notices, toll messages, job offers, and wrong-number conversations.

03 Warning signs

- The message is unexpected and pressures you to act before checking.

- It asks for a password, card number, government identifier, MFA code, or remote access.
- The displayed link is shortened, misspelled, unrelated to the organization, or hidden behind a button.
- Payment must use gift cards, cryptocurrency, wire transfer, or a payment app.
- The sender tells you to move money to “protect” it or keep the conversation secret.
- A job requires depositing a check, forwarding funds, or paying for equipment first.

Grammar alone is a poor test: professional messages can be fraudulent, and legitimate alerts can be brief. The strongest check is independent verification.

04 What to do with a suspicious text

1. Do not click, reply, call the included number, or download an attachment.
2. Open the organization’s official app or type its known address yourself. For a bank, use the number printed on the card or statement.
3. Ask the supposed person through a separate channel, especially for money or authentication requests.
4. Use the phone’s “report junk” or spam feature, then block the sender.
5. In the United States, many carriers accept forwarded spam texts at `7726` (SPAM). Reporting options differ by country and carrier.
6. Preserve screenshots, the number, URL, and payment details if money or an organizational account is involved.

Do not respond “STOP” to an obvious scam from an unknown sender; a reply can confirm that the number is active. Use STOP for legitimate subscription programs that you recognize.

05 If you clicked or responded

Clicked but entered nothing: close the page, do not approve downloads or notification prompts, update the device and browser, and monitor accounts. A click alone does not automatically mean the phone is infected, but an exploit is possible on an unpatched device.

Entered a password: use a clean device to change it at the real site, revoke active sessions, check recovery details, and change reused passwords. Protect email first because it can reset other accounts.

Shared an MFA code or approved a prompt: contact the organization immediately, revoke sessions and trusted devices, reset credentials, and review account activity.

Entered card or bank details or sent money: contact the financial institution using a known number now. Ask about blocking the payment or card, then report the fraud to the appropriate national authority.

Installed an app or profile: disconnect the device from sensitive work, document the app and permissions, and contact security support. Remove unknown device-administration, accessibility, VPN, or management access; a managed device may need forensic review or reset.

06 Reducing smishing risk

Use unique passwords and phishing-resistant MFA where supported. Hide message previews on locked screens if codes or sensitive content may appear. Keep the phone updated, restrict app installation to trusted stores, and review accessibility and device-management permissions. Enable carrier and device spam filtering while recognizing it will not catch every message.

Organizations should avoid training customers to click login links in texts. Use consistent message patterns, signed applications, short-lived notifications without sensitive data, and a clearly published verification path. Protect support staff against attackers who follow a smishing attempt with a phone call.

07 Frequently asked questions

Is every unsolicited text smishing?

No. Some are ordinary spam or wrong numbers, but unexpected requests for action, information, or money should be independently verified.

Can opening a text infect my phone?

Usually the attacker needs a click, approval, credential entry, or installation. Rare zero-click vulnerabilities exist, which is why updates and professional review of targeted incidents matter.

Can I trust a message from the same sender name as my bank?

No. Sender identity can be spoofed or abused. Verify through the bank’s official app or a number you obtained independently.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com