



Smishing

Responding to Smishing

Smishing is a scam that uses text messages (SMS, MMS, or chat messages) to trick you into clicking a link, downloading content, replying with information, or calling a fake support number. These messages are designed to look urgent, personal, and legitimate. Smishing is commonly used to steal credentials, install malware, or trigger follow-up vishing calls.

Smishing often pretends to be from:

- Delivery services (“package problem”)
- Banks or payment apps
- Government agencies or toll services
- Pphone carriers
- Retailers or subscription services
- Employers or schools

Common Signs of a Smishing Text

Be cautious if a text message:

- Creates urgency or fear (“Account suspended,” “Final notice”)
- Contains a shortened or unfamiliar link
- Asks you to reply YES/NO or confirm information
- Claims a problem with a delivery, payment, or account you weren’t expecting
- Requests codes, PINs, or personal information
- Comes from an unknown number or odd email-style sender
- Pressures you to act quickly or secretly
- If it feels rushed or confusing, treat it as suspicious.

Smishing – Do This First

Do Not Interact Further

If you suspect a scam:

- Do not click links
- Do not download files
- Do not reply, even with “STOP”
- Do not call numbers in the message

Replying confirms your number is active and may increase targeting.





Preserve the Message (optional)

Only preserve evidence if you have interacted further with the message sender. Do not open the message if you have not interacted with the sender yet. Immediately delete and report as junk from your phone. Do not click links or reply. If you can safely report as junk/spam from the message list, do that. If you opened it, do not interact with the content as it will inform the sender your account is active and encourage additional targeting.

- Before deleting:
 - Screenshot the message
- Note:
 - Sender number or address
 - Date and time
 - Link or phone number included
- What the message asked you to do

Verify Through a Separate Channel

If the text claims to be from a real organization:

- Open the organization's official app or website manually
- Contact them using a known, official phone number
- Confirm whether the message is legitimate

If You Clicked a Link or Downloaded Content

Stop and Contain

- Disconnect your phone from Wi-Fi and mobile data
- Do not log into accounts
- Do not continue interacting with the site or message

Secure Accounts Immediately

If you entered information:

- Change passwords for affected accounts from a safe device
- Change passwords for any other accounts using the same or similar password
- Watch for password reset or login alerts you didn't request

Check Your Device

If you downloaded an app or file:

- Remove it immediately if possible
- Run a built-in mobile security scan
- If unsure, seek expert help before continuing to use the device
- Improper removal can hide infections or worsen compromise.





If You Replied or Shared Information

If you shared:

- Verification codes
- Login credentials
- Financial or personal information

Take these steps immediately:

- Contact banks or payment providers
- Monitor accounts for suspicious activity
- Follow guidance from the affected organization
- Expect follow-up scams referencing the interaction

Report the Smishing Attempt

Report to Your Phone Carrier

Report and delete the message immediately. Most phones have an option to flag as spam upon deletion.

If you can't report as spam directly from your phone:

- Forward the message to 7726 (SPAM) (supported by most U.S. carriers)
- This helps carriers block scam campaigns

Additional Reporting

- National Reporting
 - FBI Internet Crime Complaint Center (IC3)
 - <https://www.ic3.gov>
 - (Especially important if accounts, money, or identity data were affected)
 - Federal Trade Commission (FTC) - report consumer fraud and scams at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud).
- Ohio Resources
 - Ohio Attorney General – Consumer Protection & Cybercrime
 - <https://www.ohioattorneygeneral.gov>
 - Hotline: 800-282-0515
- Geauga County
 - Geauga County Sheriff's Office
 - <https://www.geaugasheriff.org>
 - Local police non-emergency line if fraud or identity theft occurred
 - Call 911 if threats or immediate danger are involved

Recovery – After a Smishing Incident

- Monitor phone activity and accounts for several weeks





- Watch for related scam calls or texts
- Review account recovery settings
- Be cautious of “support” messages claiming to fix the issue
- Smishing often leads to multi-step scams.

How to Reduce Smishing Risk

- Treat unexpected texts as suspicious by default
- Slow down, urgency is the scammer’s tool
- Never share codes or passwords by text
- Verify independently before acting
- Ask for help early, second opinions prevent damage

