CS-036 · Email Security

Smishing

Phishing delivered through text messages to steal information or push malicious links.

Executive Summary

Smishing is phishing carried out through text messages, most commonly SMS, that trick recipients into tapping a malicious link, revealing personal or financial information, or installing harmful software. It exploits the trust and immediacy people give to texts, along with the difficulty of inspecting links on a small screen. Smishing has grown rapidly as more services and organizations legitimately communicate by text.

What It Is

Smishing is a channel-specific form of phishing that uses text messaging instead of email. A typical smishing message impersonates a bank, a delivery service, a government agency, or an internal system, and prompts the recipient to act urgently by tapping a link or replying with information. The link often leads to a counterfeit login or payment page, or attempts to install a malicious app. Because texts are short, informal, and read quickly on mobile devices, recipients have fewer cues to judge legitimacy and less ability to preview where a link really goes. Smishing is part of the broader phishing family and is frequently combined with voice calls (vishing) to add pressure and credibility.

Why It Matters

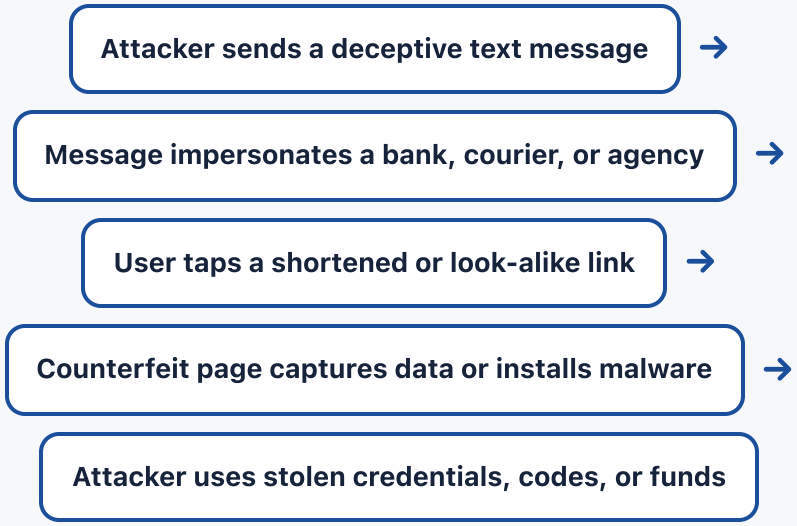
People tend to trust and respond to texts faster than email, and mobile devices make it harder to spot warning signs, so smishing can be highly effective. A single tap can lead to stolen banking credentials, account takeover, fraudulent charges, or malware on a device that also holds work data. For organizations that allow personal and work use on the same phones, a successful smishing attack can bridge into corporate accounts. Smishing also fuels larger schemes such as

multi-factor code theft and business fraud. For professionals, understanding this channel is increasingly important as attackers diversify beyond email, and defending mobile and messaging channels is now part of a complete security program.

How It Works

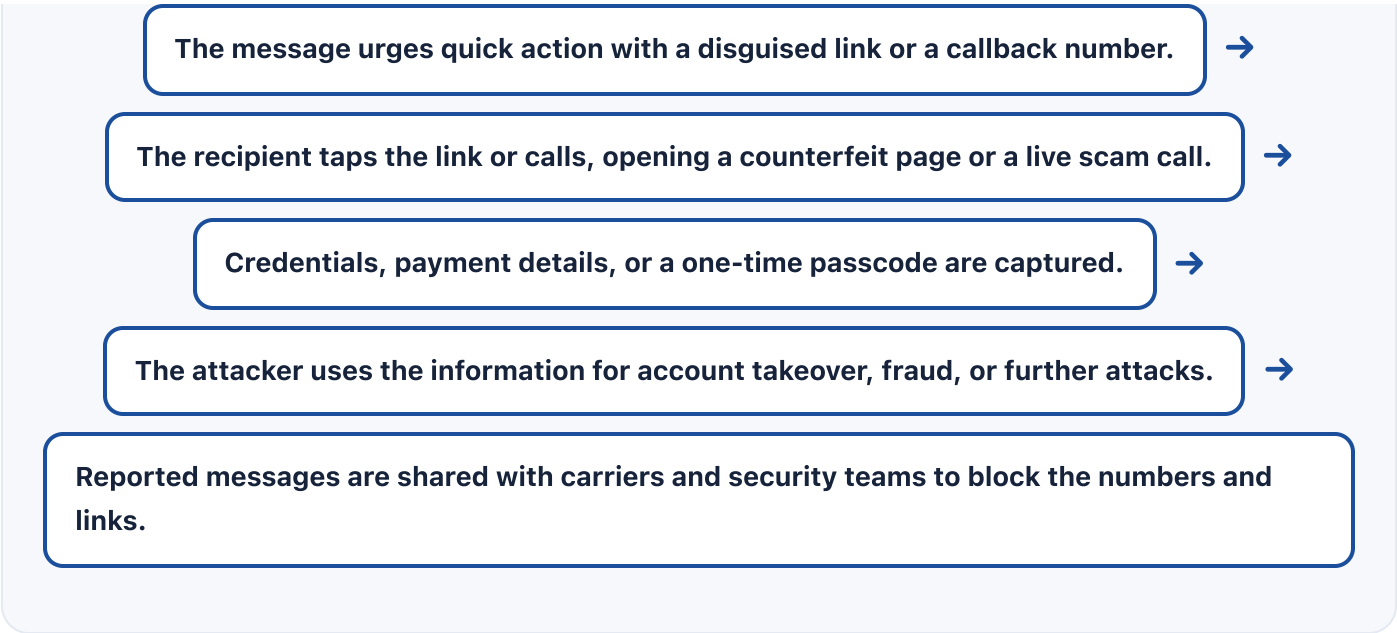
An attacker sends a text designed to look like a legitimate notification: a package cannot be delivered, an account is locked, a payment failed, or a verification code is needed. The message creates urgency and includes a shortened or look-alike link or a number to call. Tapping the link opens a counterfeit page that captures whatever is entered, or triggers a prompt to install a malicious app or grant permissions. In some schemes the attacker follows up by phone to walk the victim through handing over a one-time passcode, defeating certain forms of multi-factor authentication. Because sender numbers can be spoofed and links disguised, the message can look convincing, which is why caution with unexpected texts and independent verification are the core defenses.

Architecture Diagram



Smishing uses a deceptive text and a disguised link to capture information or install malware on a mobile device.

Visual Workflow



Common Attacks

- Fake package-delivery notices with a link to a counterfeit tracking page
- Bank or payment alerts claiming an account is locked or a charge failed
- Messages requesting a one-time passcode to defeat multi-factor authentication
- Impersonation of government agencies demanding urgent payment or information
- Links that install a malicious app or request excessive device permissions

Common Mistakes

- Trusting a text simply because it arrived on a personal, familiar device
- Tapping links in unexpected messages instead of visiting the service directly
- Sharing a one-time passcode with anyone who requests it by text or call
- Assuming a sender number is genuine because it looks local or familiar
- Mixing unprotected personal texting habits with work accounts on the same phone

Best Practices

- Never tap links in unexpected texts, navigate to the service directly instead
- Never share one-time passcodes, no legitimate party will ask for them
- Enforce multi-factor authentication, preferring phishing-resistant methods

- Report smishing to the carrier and, where available, to consumer protection channels
- Separate work and personal use with mobile device management where feasible
- Train staff to recognize smishing as part of broader awareness programs

Quick Checklist

- [x] Users trained to distrust unexpected text links and callback numbers
- [x] One-time passcodes never shared, reinforced in policy and training
- [x] Phishing-resistant multi-factor authentication used where possible
- [x] Mobile device management protecting work accounts on phones
- [x] Reporting path to carrier and security team communicated to staff
- [x] Incident process to reset credentials after a suspected smishing compromise

Recommended Tools

Mobile device management
Separates and protects work data and accounts on phones

Phishing-resistant MFA
Resists one-time-passcode theft that smishing enables

Carrier and message filtering
Blocks known scam numbers and malicious links at the network

Security awareness platform
Trains staff to recognize and report smishing attempts

Industry Standards

NIST SP 800-63
Digital identity guidance including stronger authentication methods

NIST SP 800-124
Guidance on securing mobile devices in the enterprise

CIS Critical Security Controls
Authentication and awareness safeguards

that reduce smishing impact

Career Relevance

Smishing extends phishing defense into mobile and messaging channels. SOC analysts investigate reported texts and related account takeovers, incident responders handle compromises that reach work systems through phones, and security awareness leads add smishing to training. Security engineers deploy mobile device management and stronger authentication, while GRC analysts assess mobile and messaging risk. For the AI-Governance-Jobs.com audience, smishing is an important and growing part of social engineering defense.

Interview Questions

- What is smishing, and why can it be more effective than email phishing?
- Why should a one-time passcode never be shared, even with a caller who seems official?
- How does mobile device management reduce the risk of smishing at work?
- What warning signs suggest a text message is a smishing attempt?
- How would you add smishing to an existing awareness program?

Related Certifications

CompTIA Security+ | **ISC2 Certified in Cybersecurity (CC)** | **GIAC Security Essentials (GSEC)**

Further Reading

- FTC: How to Recognize and Report Spam Text Messages
- CISA: Avoiding Social Engineering and Phishing Attacks
- NIST: Digital Identity Guidelines

Key Takeaways

- Smishing is phishing delivered through text messages.
- It exploits the trust and speed people give to texts on mobile devices.
- A single tap can lead to stolen credentials, codes, money, or malware.

- Never tap unexpected links or share one-time passcodes.
- Stronger authentication and mobile management reduce the impact.

FAQ

How is smishing different from phishing?

Why do attackers ask for a one-time passcode?

What should I do about a suspicious text?

Related Careers

RELATED ROLES

Soc Analyst

Security Awareness Lead

Incident Responder

Grc Analyst

RELATED CERTIFICATIONS

CompTIA Security+

ISC2 Certified in Cybersecurity (CC)

GIAC Security Essentials (GSEC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides

Role roadmaps

Salary data

Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Smishing**
3. Go deeper: Vishing
4. Go deeper: Phishing
5. Validate it: work toward **CompTIA Security+**

6. Find the role: browse current openings

RELATED SHEETS

CS-037 Vishing | CS-032 Phishing | CS-033 Spear Phishing | CS-025 Multi-Factor Authentication (MFA) | CS-010 Cyber Hygiene