THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Smishing & vishing — phishing via SMS and phone

SMS phishing and phone phishing combine technical tricks with human manipulation. We show how to spot both variants — and why calling back is dangerous.

min read: 7 min **Updated:** 14 March 2026 **Risk:** High risk
Source: awareness-as-a-service.com/en/resources/threats/smishing-vishing

What is smishing and vishing?

Smishing (SMS + phishing) and **vishing** (voice + phishing) are variants of classic phishing that deliberately bypass the email channel. Attackers favour SMS and phone calls because employees are less suspicious there — no spam filter, no hover-preview for URLs, no external-sender banner.

Smishing messages masquerade as parcel services, bank alerts, tax authorities, or IT helpdesks. Vishing calls appear to come from your own bank, Microsoft Support, HR, or the executive office. In both cases there is a human at the other end — or, since 2025, increasingly an AI-generated voice that is barely distinguishable from a real one.

The combined attack is particularly dangerous: a smishing SMS announces a call ("your account has been compromised, our security team will contact you shortly"), raising willingness to cooperate when the follow-up call arrives.

At a glance

01
No filter intervenes
SMS and phone calls pass through email gateways, SPF/DKIM checks, and spam filters without inspection.

02
Any number can be spoofed
CLI spoofing can display any caller ID — including your own IT helpdesk number.

03
Time pressure as a weapon
In a live phone call there is no time to think. That is exactly what attackers exploit.

How to recognise smishing and vishing

A few rules of thumb unmask smishing and vishing quickly:

Spoofed sender number
The displayed number matches a familiar one — but the context is wrong. Your bank does not send PIN requests by SMS.

Pressure to hand over a code
No legitimate service ever asks for your MFA code, password, or OTP — by SMS or over the phone.

Request to install an app
An SMS with a link to a "security app" or "tracking app" is usually spyware or a fake banking app.

Supposed bank or IT hotline
Unsolicited inbound calls from "your bank" or "Microsoft Support" are almost always fraud. Legitimate organisations rarely call without warning.

Alleged tax demand
Authorities send assessments in writing. Calls threatening immediate enforcement action are a classic vishing pattern.

WhatsApp message from a "colleague in trouble"
"I'm abroad, my phone broke, can you advance me CHF 800?" — often the first contact comes from an unknown number.

How to protect yourself

For employees

- **Call back on an official number:** If someone claims to be from your bank or IT, hang up and call the number on the official website or your bank card.
- **Never read out an MFA code over the phone.** No legitimate service asks for this.
- **Do not return calls to unknown numbers:** An SMS saying "please call +44..." may lead to premium-rate lines or vishing hotlines.
- **Verify colleagues directly:** If a WhatsApp message from an unknown number claims to be a known colleague, call them to check.

For administrators

- **STIR/SHAKEN verification** where carrier infrastructure supports it; raise awareness that caller ID is not trustworthy.
- **Awareness campaigns specifically covering smishing and vishing** — many training programmes focus only on email.
- **Establish a reporting process for suspicious SMS and calls** (screenshot + report to SOC).
- **Mobile policy:** Block international call forwarding and premium-rate numbers on corporate SIM cards.
- **Mobile Threat Defence (MTD)** solutions for company devices that detect smishing links in SMS messages.

Real cases

CASE 01 · LOGISTICS COMPANY · DE · Q3/2025

A dispatcher received an SMS apparently from DHL: "Your shipment is waiting for a customs fee — pay now." The link led to a convincing DHL lookalike page where credit card details were entered. Three charges totalling EUR 2,400 followed shortly afterwards.

Damage: EUR 2,400 · **Detection:** cardholder reported the charges the next day · **Lesson:** DHL does not request customs fees via SMS link. Legitimate tracking URLs start with dhl.com or dhl.de.

CASE 02 · LAW FIRM · CH · Q4/2025

A legal assistant received a call from "Microsoft" warning of a virus on her computer. The caller asked her to install AnyDesk and grant remote access. Within 20 minutes, client communications were exfiltrated from her Outlook inbox.

Damage: data breach, mandatory notification under the Swiss DSG · **Detection:** a partner noticed the unusual remote connection · **Lesson:** Microsoft, Google, and Apple do not call unsolicited. Never grant remote access to unknown parties.

What to do if it happens?

THE FIRST 15 MINUTES

1. **End the call** or do not open the link — but document the message or number (screenshot).
2. **Report immediately** to IT helpdesk or the information security officer. Even if "nothing happened" — reports help identify campaign waves.
3. **Change credentials** if they were provided on a call or on a linked page — from a secure device.
4. **Contact your bank** if payment data or OTP codes were shared. Early blocking can limit damage.
5. **Check MFA devices:** Were new devices registered without your knowledge?
6. **Do not uninstall any remote-access tool before IT investigates** — the active session contains forensic evidence.

Frequently asked questions

Can I tell whether a caller ID has been spoofed?

Not reliably. CLI spoofing can display any number — including numbers saved in your contacts. The only reliable check is to call back on a number you have found independently.

Is SMS two-factor authentication still secure?

SMS OTP is the weakest MFA method, but it is significantly better than no second factor at all. SIM swapping and SS7 attacks are real but complex to carry out. For sensitive systems, FIDO2/passkeys should be preferred.

What is the difference between smishing and ordinary spam SMS?

Spam advertises products or services. Smishing aims to steal credentials, money, or personal data. The difference lies in criminal intent and often in the personalisation of the message.

Are employees allowed to simply hang up on a vishing call?

Yes. Every organisation should establish the norm: unsolicited calls that demand sensitive data or access rights are ended and reported. That is professional behaviour, not rudeness.

Related topics

Smishing and vishing are frequently entry channels for more complex attacks. CEO fraud often combines email with vishing calls; deepfakes make voice imitation in vishing campaigns increasingly convincing.