BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Smishing & Vishing — Phishing über SMS und Telefon

SMS-Phishing und Anruf-Phishing kombinieren oft technische Tricks mit menschlicher Manipulation. Wir zeigen, woran Sie beide Varianten erkennen — und warum Rückrufe gefährlich sind.

min Lesezeit: 7 min **Aktualisiert:** 14. März 2026 **Risiko:** Hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/smishing-vishing

Was ist Smishing & Vishing?

Smishing (SMS + Phishing) und **Vishing** (Voice + Phishing) sind Varianten des klassischen Phishings, die den E-Mail-Kanal bewusst umgehen. Angreifer setzen auf SMS und Anrufe, weil Mitarbeitende dort weniger misstrauisch sind — kein Spam-Filter, keine URL-Vorschau im Hover, keine "External Sender"-Banner.

Smishing-Nachrichten tarnen sich als Paketdienst, Bankalert, Steuerbehörde oder IT-Helpdesk. Vishing-Anrufe kommen scheinbar von der eigenen Bank, vom Microsoft-Support, von der Personalabteilung oder vom Vorstandsbüro. In beiden Fällen steht ein Mensch am anderen Ende — oder seit 2025 immer häufiger eine KI-generierte Stimme, die kaum von einer echten zu unterscheiden ist.

Der kombinierte Angriff ist besonders gefährlich: Eine Smishing-SMS kündigt einen Anruf an ("Ihr Konto wurde kompromittiert, unser Sicherheitsteam meldet sich gleich") — und erhöht so die Bereitschaft, beim folgenden Anruf zu kooperieren.

Auf einen Blick

01

Kein Filter greift

SMS und Anrufe passieren E-Mail-Gateways, SPF/DKIM und Spam-Filter ohne Prüfung.

02

Nummer leicht fälschbar

CLI-Spoofing ermöglicht es, jede beliebige Absender-Nummer anzuzeigen — auch die Ihrer eigenen IT-Hotline.

03

Zeitdruck als Waffe

Im Telefongespräch bleibt keine Zeit zum Nachdenken. Genau das nutzen Angreifer aus.

Woran erkennen Sie Smishing & Vishing?

Smishing und Vishing lassen sich mit wenigen Faustregeln enttarnen:

! **Gespoofte Absender-Nummer**
Die angezeigte Nummer stimmt mit einer bekannten überein — aber der Kontext passt nicht. Ihre Bank sendet keine PIN-Anfragen per SMS.

! **Drängen auf Code-Weitergabe**
Niemand mit legitimem Auftrag fragt nach Ihrem MFA-Code, Passwort oder einer TAN — weder per SMS noch am Telefon.

! **Vermeintliche Bank- oder IT-Hotline**
Eingehende Anrufe von "Ihrer Bank" oder "Microsoft-Support" sind fast immer Betrug. Legitime Institutionen rufen selten unangekündigt an.

! **WhatsApp-Nachricht von "Mitarbeiter in Not"**
"Ich bin gerade im Ausland, Handy kaputt, kannst du kurz CHF 800 vorstrecken?" — oft erste Kontaktaufnahme per unbekannter Nummer.

! **Aufforderung zur App-Installation**
SMS mit Link zu einer "Sicherheits-App" oder "Tracking-App" — meist Spyware oder ein gefälschtes Banking-App.

Angebliche Steuernachzahlung
Behörden versenden Bescheide schriftlich. Anrufe unter Androhung sofortiger Pfändung sind ein klassisches Vishing-Muster.

So schützen Sie sich

Für Mitarbeitende

- **Rückruf über offizielle Nummer:** Wenn jemand behauptet, von Ihrer Bank oder IT anzurufen, legen Sie auf und rufen Sie über die auf der Website oder Karte angegebene Nummer zurück.
- **MFA-Codes niemals am Telefon nennen.** Kein legitimer Dienst fragt danach.
- **Unbekannte Nummern nicht zurückrufen:** Eine SMS mit "Bitte rufen Sie +49 … zurück" kann zu Mehrwertdiensten oder Vishing-Hotlines führen.
- **Kollegen direkt kontaktieren:** Bei WhatsApp-Nachrichten von unbekannten Nummern, die einen bekannten Kollegen vorgeben, kurz anrufen und verifizieren.

Für Administratoren

- **DMARC-ähnliche Maßnahmen für Telefonie:** Soweit möglich, ausgehende Nummern in STIR/SHAKEN-Registern verifizieren lassen.
- **Awareness-Kampagne spezifisch für Smishing/Vishing** integrieren — viele Schulungen fokussieren nur auf E-Mail.
- **Meldeprozess für verdächtige SMS/Anrufe** etablieren (Screenshot + Meldung an SOC).
- **Mobilfunk-Richtlinie:** Unternehmens-SIM-Karten mit Sperre für internationale Weiterleitungen und Premium-Nummern.
- **Mobile-Threat-Defence-Lösung** (MTD) für Unternehmensgeräte prüfen, die Smishing-Links in SMS erkennt.

Echte Beispiele

FALL 01 · LOGISTIKUNTERNEHMEN · DE · Q3/2025

Ein Disponenten-Mitarbeiter erhielt eine SMS, scheinbar von DHL: "Ihre Sendung wartet auf Zollgebühr — jetzt bezahlen." Der Link führte zu einer täuschend echten DHL-Seite, auf der Kreditkartendaten eingegeben wurden. Kurz danach folgten drei Abbuchungen über insgesamt EUR 2.400.

Schaden: EUR 2.400 · **Erkennung:** Kreditkarteninhaber meldete die Abbuchungen am nächsten Tag · **Lehre:** DHL verlangt keine Zollgebühren per SMS-Link. Offizielle Tracking-URLs beginnen mit dhl.com oder dhl.de.

FALL 02 · ANWALTSKANZLEI · CH · Q4/2025

Eine Kanzlei-Assistentin erhielt einen Anruf von "Microsoft", der einen Virus auf ihrem Rechner ankündigte. Der Anrufer bat sie, AnyDesk zu installieren und ihm Fernzugriff zu gewähren. Innerhalb von 20 Minuten wurden aus dem Outlook-Postfach Mandantenkommunikation exfiltriert.

Schaden: Datenschutzverletzung, Meldepflicht nach DSG · **Erkennung:** Kanzlei-Partner bemerkte ungewöhnliche Verbindung · **Lehre:** Microsoft, Google und Apple rufen nicht unaufgefordert an. Fernzugriff niemals an unbekannte Personen gewähren.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Gespräch beenden** oder Link nicht öffnen — aber Nachricht/Nummer dokumentieren (Screenshot).
2. **Sofort melden:** IT-Helpdesk oder ISB. Auch wenn "nichts passiert ist" — Meldungen helfen beim Erkennen von Kampagnenwellen.
3. **Zugangsdaten ändern,** wenn diese am Telefon oder auf einer verlinkten Seite eingegeben wurden — von einem sicheren Gerät aus.
4. **Bank kontaktieren,** wenn Zahlungsdaten oder TAN-Codes weitergegeben wurden. Frühzeitige Sperrung kann Schäden begrenzen.
5. **MFA-Geräte prüfen:** Wurden neue Geräte ohne Ihr Wissen registriert?
6. **Kein Fernzugriff-Tool deinstallieren, bevor IT es untersucht hat** — die laufende Sitzung liefert forensische Spuren.

Häufige Fragen

Kann ich eine gefälschte Absender-Nummer erkennen?

Nicht zuverlässig. CLI-Spoofing zeigt jede beliebige Nummer an — auch Nummern, die in Ihrem Telefonbuch gespeichert sind. Der einzige verlässliche Check ist der Rückruf über eine unabhängig recherchierte Nummer.

Ist eine SMS-Zwei-Faktor-Authentifizierung noch sicher?

SMS-OTP gilt als schwächste MFA-Methode, ist aber deutlich besser als kein zweiter Faktor. SIM-Swapping und SS7-Angriffe sind real, aber aufwendig. Für sensible Systeme sollten FIDO2/Passkeys bevorzugt werden.

Was ist der Unterschied zwischen Smishing und einer gewöhnlichen Spam-SMS?

Spam bewirbt Produkte oder Dienstleistungen. Smishing zielt darauf ab, Zugangsdaten, Geld oder persönliche Daten zu stehlen. Der Unterschied liegt in der kriminellen Absicht und oft auch in der Personalisierung der Nachricht.

Dürfen Mitarbeitende einen Vishing-Anruf einfach auflegen?

Ja. Jede Organisation sollte die Norm etablieren: Unverlangte Anrufe, die sensible Daten oder Zugriffsrechte fordern, werden beendet und gemeldet. Das ist professionelles Verhalten, keine Unhöflichkeit.

Weitere Themen

Smishing und Vishing sind häufig Einstiegskanäle für komplexere Angriffe. CEO-Fraud kombiniert oft E-Mail mit Vishing-Anrufen; Deepfakes machen Stimmen für Vishing-Kampagnen noch überzeugender.