

Tägliche Bedrohungen - Betrug im Finanzbereich

Andreas Schaupp

CIS Compliance Summit, Sept. 2026

Bankensektor Intern

Motivation für diesen Vortrag

- Finanzinstitute waren schon immer beliebte Angriffsziele.
- Während manche Cyber-Attacken direkt gegen Banken gerichtet sind, werden zunehmend Angriffe gegen die Kundenbasis der Finanzinstitute ausgeführt.
- Aktuell sehen wir durchdachte mehrstufige Betrugsversuche, die jeden Kontoinhaber treffen können.
- Unsere Erfahrung zeigt, dass
 - Daten aus früheren Attacken als Basis für spätere Angriffe genutzt werden
 - Aktuelle Telekom-Systeme für Spoofing anfällig sind

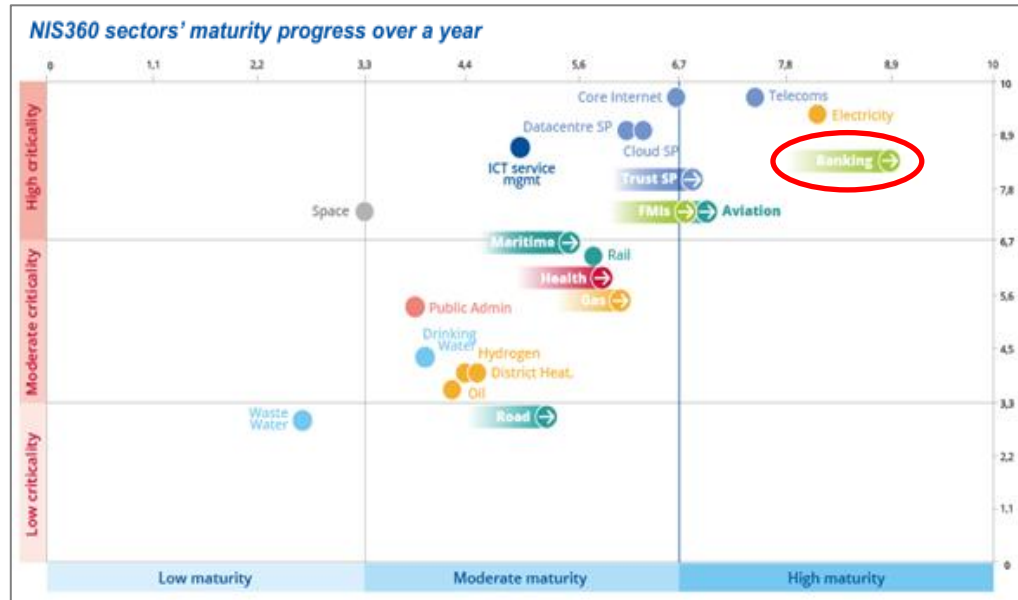
Persönliche Vorstellung



- **DI Andreas Schaupp** MMSc MAS
 - Group Chief Information Security Officer / CISO bei BAWAG Group
- Ausbildung
 - Nachrichtentechnik → IT Netzwerke → Informationssicherheit
 - Konzessionsprüfung Technisches Büro / Ingenieurbüro für Nachrichtentechnik & Telematik
 - Telematik Management MSc und Information Security Management MSc
 - Verschiedene IT-, Netzwerk- und Sicherheits-Zertifizierungen: CCIE, ITILv3, CISSP, CISA, ISO27001 Lead Auditor, CEH, CHFI, CSA, PCI-P, ...
- Erfahrung
 - 40+ Jahre Beschäftigung mit IT, Telekommunikation und Sicherheit
 - 20 Jahre IT, Netzwerk und Informationssicherheit Consulting
 - Leitende Mitarbeit beim Aufbau: Datennetz Datex-P, Vollelektronische Börse ÖTOB, ISP Chello, u.a.m.
 - 20 Jahre in der Finanzindustrie
 - 17 Jahre Head of Group Information Security Management / CISO bei Raiffeisen International, Erste Group und BAWAG Group
 - 35 Jahre nebenberufliche Vortragstätigkeit (zB kommerzielle Trainingsanbieter, Donau Universität Krems, FH St.Pölten, FH Technikum Wien, FH Campus Wien)

Cybersicherheit in NIS-Sektoren 2026

Kritikalität und Reifegrad laut ENISA sehr unterschiedlich

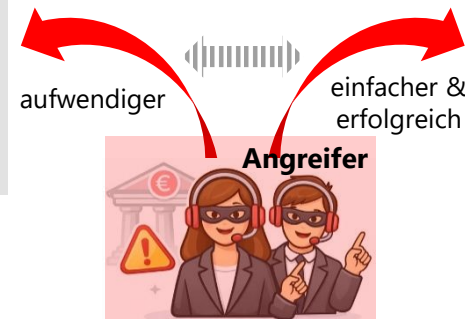


Quelle: ENISA, NIS360 05/2026

Finanzinstitute sind 300-mal häufiger von Cyberangriffen betroffen als andere Branchen, was auf den direkten finanziellen Gewinn zurückzuführen ist, ... Bankbetrug, Manipulationen bei Überweisungen und Eingriffe in Handelssysteme verursachen ... unmittelbare finanzielle Verluste. ...



Trotz hoher Investitionen in die Sicherheit führt die schiere Anzahl der Angriffe dazu, dass einige davon unweigerlich erfolgreich sind.



Phishing-Betrug in den News 2026

Worum geht es ?

27.02.2026



CHRONIK

FinanzOnline-Betrug: 100.000 Euro Schaden

Ein 70-Jähriger aus Leoben ist vor wenigen Tagen Opfer einer Betrugsmasche geworden, wodurch bei ihm ein finanzieller Schaden in der Höhe von knapp 100.000 Euro entstanden. Die Betrüger gaukelten dem Mann vor, dass FinanzOnline-Konto des Mannes ablaufen würde.

vorarlberg ORF.at



CHRONIK

Polizei warnt vor erfundenen Hackerangriffen

Aktuell kommt es wieder vermehrt zu Betrugsanzeigen in Vorarlberg. Bei diesen Fällen werden die Opfer von vermeintlichen Mitarbeitern ihrer Bank angerufen und zur Freigabe von Zugangsdaten im Onlinebanking aufgefordert, heißt es bei der Landespolizeidirektion. Als Grund wird ein Hackerangriff auf das jeweilige Konto angegeben.

1. Juni 2026, 11:42 Uhr (Update: 2. Juni 2026, 11:35 Uhr)

kaernten ORF.at

CHRONIK

Telefonbetrüger erbeuten Tausende Euro

Ein 48-jähriger Klagenfurter wurde Opfer eines Telefonbetrugs. Die Täter gaben sich als Bankmitarbeiter aus und erschlichen sich so mehrere Überweisungen, bis der Mann misstrauisch wurde. Die Ermittlungen laufen.

15.03.2026

Kronen Zeitung
Fr., 05.06.2026 15°C Wien

Politik Wirtschaft Chronik Sport Gericht Menschen Sonderthemen Wetter

AKTUELLE MASCH

Telefonbetrüger geben sich als Bankmitarbeiter aus

Vorarlberg | 02.06.2026 08:30



Symbolbild. (Bild: APA/HANS KLAUS TECHT)

Von Vorarlberg-Krone

Wer einen Anruf erhält und aufgefordert wird, seine Bankdaten offenzulegen, der sollte so schnell wie möglich auflegen: Die Masche „Hackerangriff auf Bankkonto“ macht derzeit in Vorarlberg verstärkt die Runde, warnt die Polizei.

Vom generischen Phishing zum Vishing-Betrug

Wie läuft der mehrstufige Betrug ?

- Generisches **Identitäts-Phishing** als Basis
 - Phishing im Namen bekannter Organisationen
 - mit eMails und SMS
 - Weiterleitung der gephashten Identitäts-Records

Nach Wochen
oder kurz danach

- **Vishing** gegen identifizierte Bank-KundINNen
 - Anbahnung / Ankündigung -> Vishing-Anruf
 - Manipulation / Überlisten des Bankkunden
 - Transaktion / Cashout

zB



09/2025

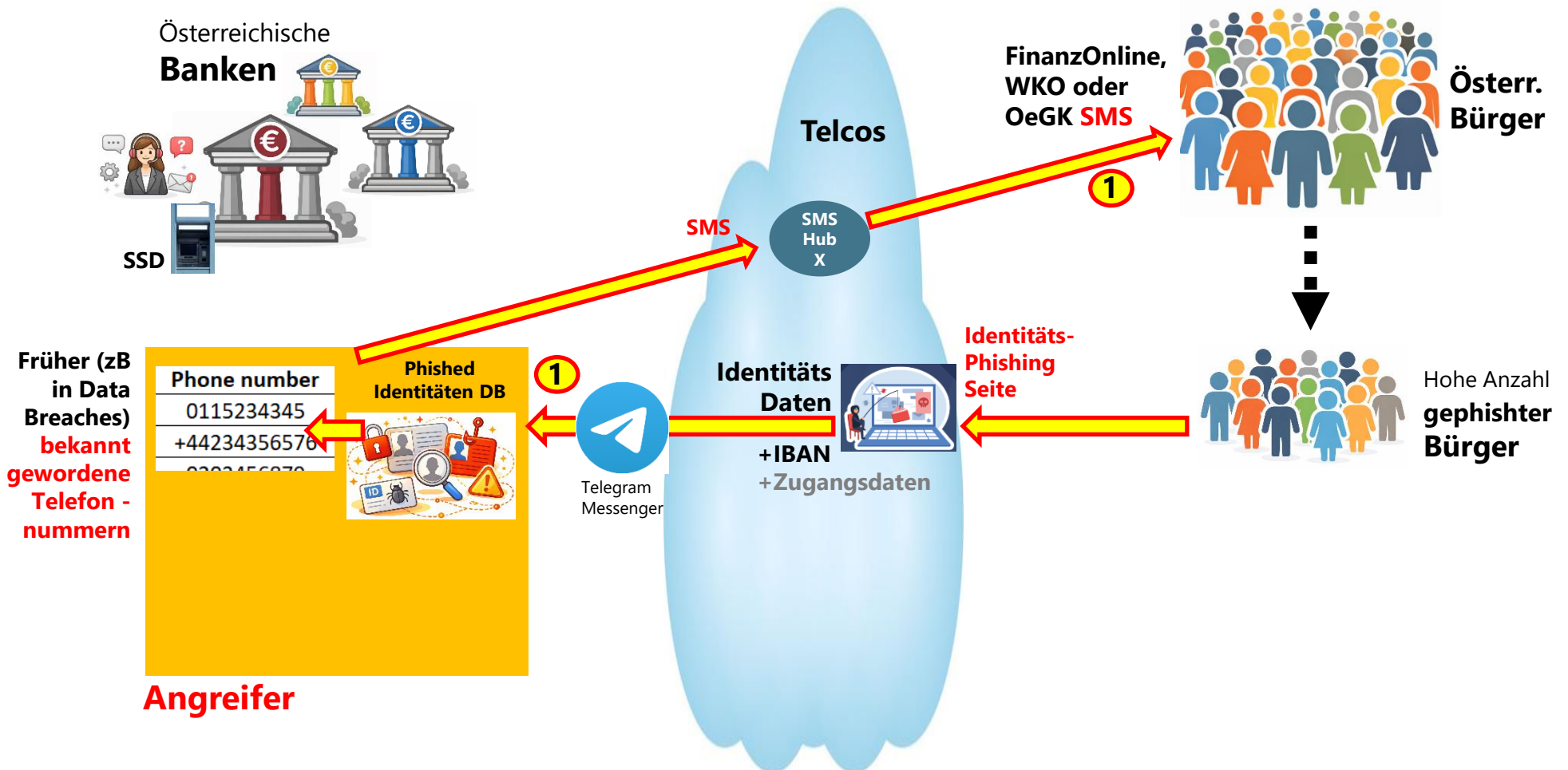
oder



08/2026

Generisches Identitäts-Phishing

... läuft unter dem Deckmantel bekannter österreichischer Institutionen



Identitäts-Phishing - Reloaded

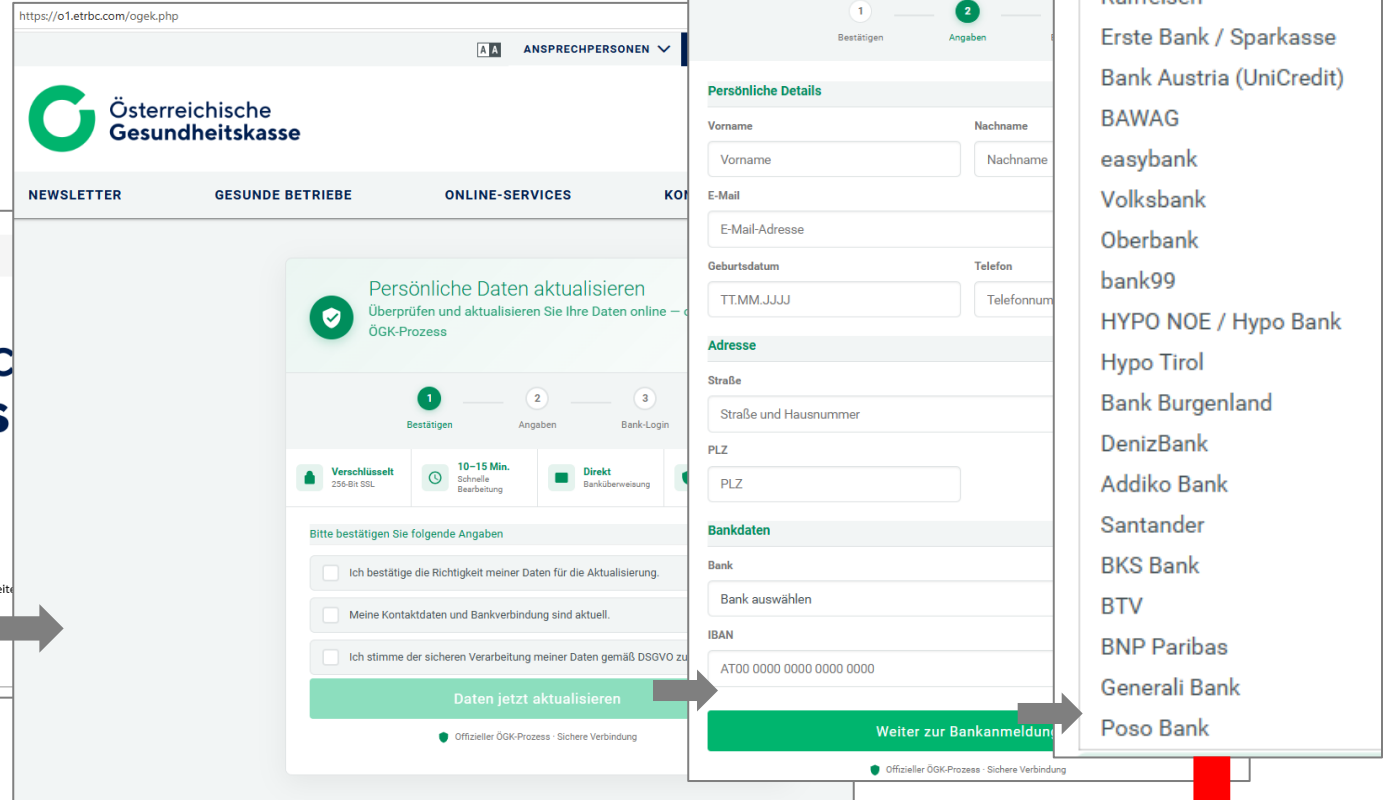
Phishing im Namen der ÖGK nahm im Q2/2026 zu

Betrüger ‚phishen‘

- 1) BankkundINNen-**Identitäten** und
- 2) Bank **Konto-Zugangsdaten**



Example content from a ÖGK Phishing site:



Es folgt der Fake (Vishing) Anruf von der Bank !

Nach ID Daten Phishing ?

Phishing von Zugangsdaten !



- Raitteisen Bank
- Erste Bank
- ✓ BAWAG P.S.K.
- Bank Austria
- Volksbank
- Easy Bank
- HYPO NOE
- OberBank
- Bank99
- Schelhammer
- Bankhaus Spängler
- Dolomiten Bank
- Sparda Bank
- Dadat Bank
- Bankhaus Marchfeld



finanz-id.live

BAWAG

eBanking Login

Wie wollen Sie sich einloggen?

Verfüger Mit der App

Verfügernummer

PIN (8 bis 16-stellig)

Login

> PIN vergessen oder Verfüger gesperrt?

Bank Austria
Member of UniCredit

24You

Verfügernummer

PIN

[PIN vergessen oder Verfügernummer](#)

LOGIN

Gefälschte Bank Austria Mails im Umlauf!
[Details anzeigen](#)

Bitte melden Sie sich an

Wählen Sie Ihr Bundesland und geben Sie Verfügernummer und PIN ein.

Bundesland oder Bank Wählen *

Verfügernummer eingeben *

PIN eingeben *

☐ Verfüger

George Login

Bitte geben Sie Ihre Verfügernummer oder Ihren selbst gewählten Benutzernamen ein.

Verfügernummer/Benutzernamen

Login starten

Aktivierungscode benötigt oder EB-PIN vergessen?
[Umsteigen auf George ID nach Fristablauf](#)

ERSTE SPARKASSE

VOLKSBANK
HAUSBANKING

hausbanking Login

Beim Login wird eine sichere Verbindung aufgebaut. Bitte achten Sie darauf, dass Sie Ihre Zugangsdaten auf keiner Ihnen unbekannten Seite eingeben und diese geheim halten.

Anmeldung mit Benutzernamen [Barrierefrei](#) | [English](#)

Durch die Eingabe Ihrer Zugangsdaten stimmen Sie den Nutzungsbedingungen der Bank ausdrücklich zu.

Weiter

[Benutzername vergessen?](#)
[Passwort vergessen?](#)

Oberbank

Kundenportal Login

Ihre PIN

Deutsch

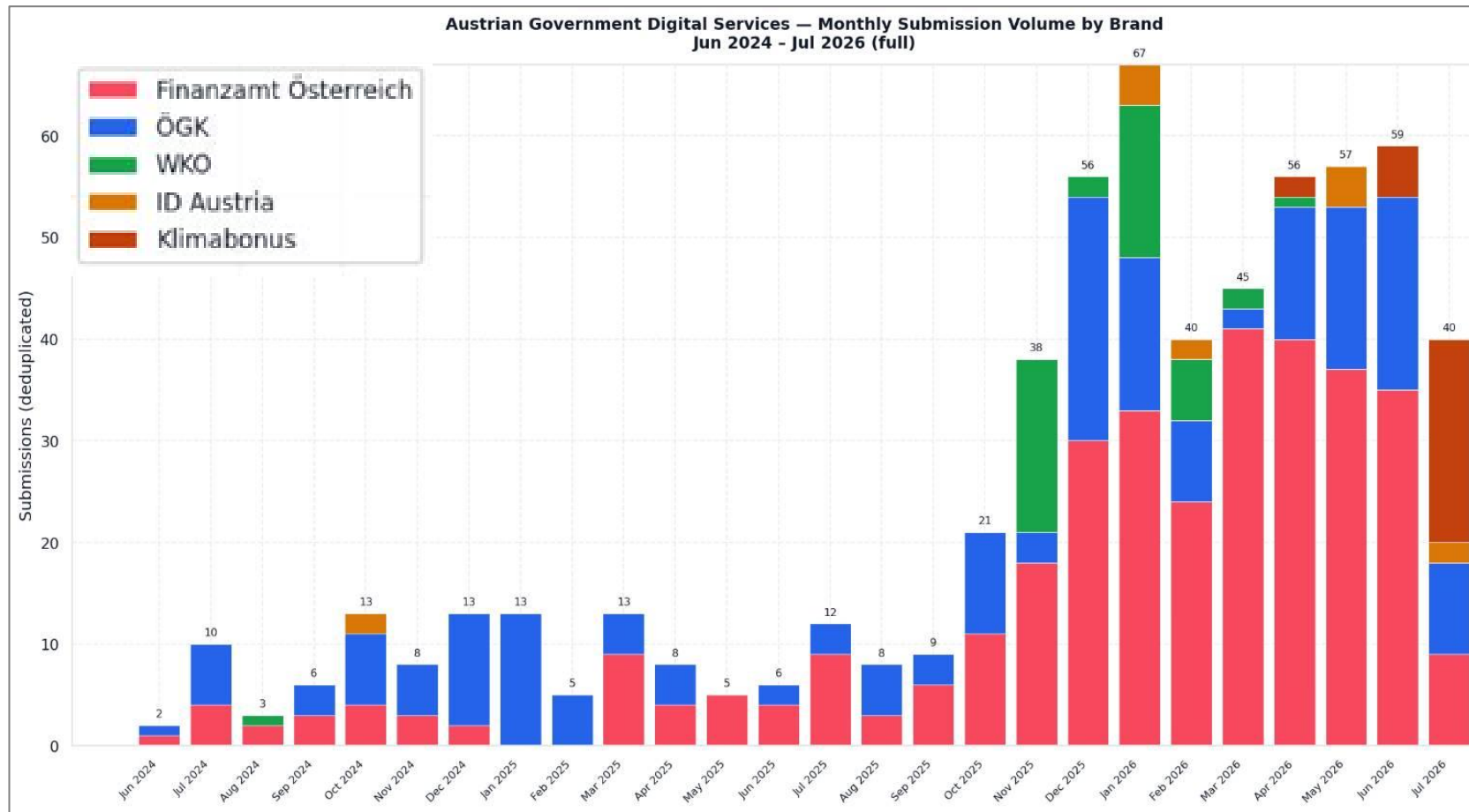
Ihre Anmeldung im Kundenportal geschieht über gesicherte SSL Verbindungen.

Weiter

Erstanmeldung

Identitäts-Phishing in AT über Zeit

Intensivierung der Phishing-Aktivitäten im letzten Jahr

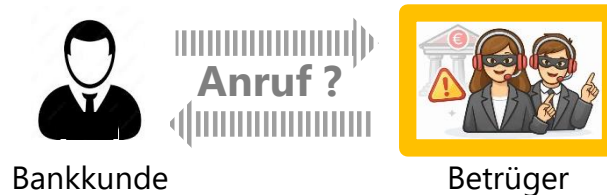


Voice-Phishing (Vishing) in 2 Varianten

Der eigentlich Betrugs-Angriff

- a) Tausende SMS-Nachrichten an ge phishingte Personen mit **Aufforderung im (Fake) Notruf Call Center anzurufen**

oder



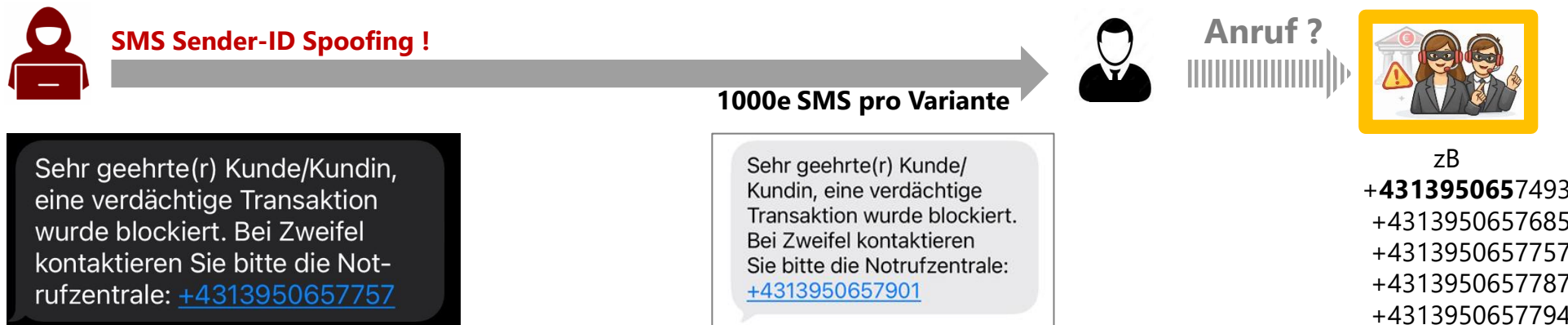
- b) Direkter **Anruf der Betrüger** (mit **CallerID-Spoofing**) beim potentiellen Betrugsoffer

Grund für
das Telefonat
ist eine
verdächtige
Transaktion

zB für Urlaub
in der Ukraine

Schritt 2 Variante a: Simple Vishing Methode

SMS an ‚identifizierte‘ Kunden – **Kunde soll anrufen**

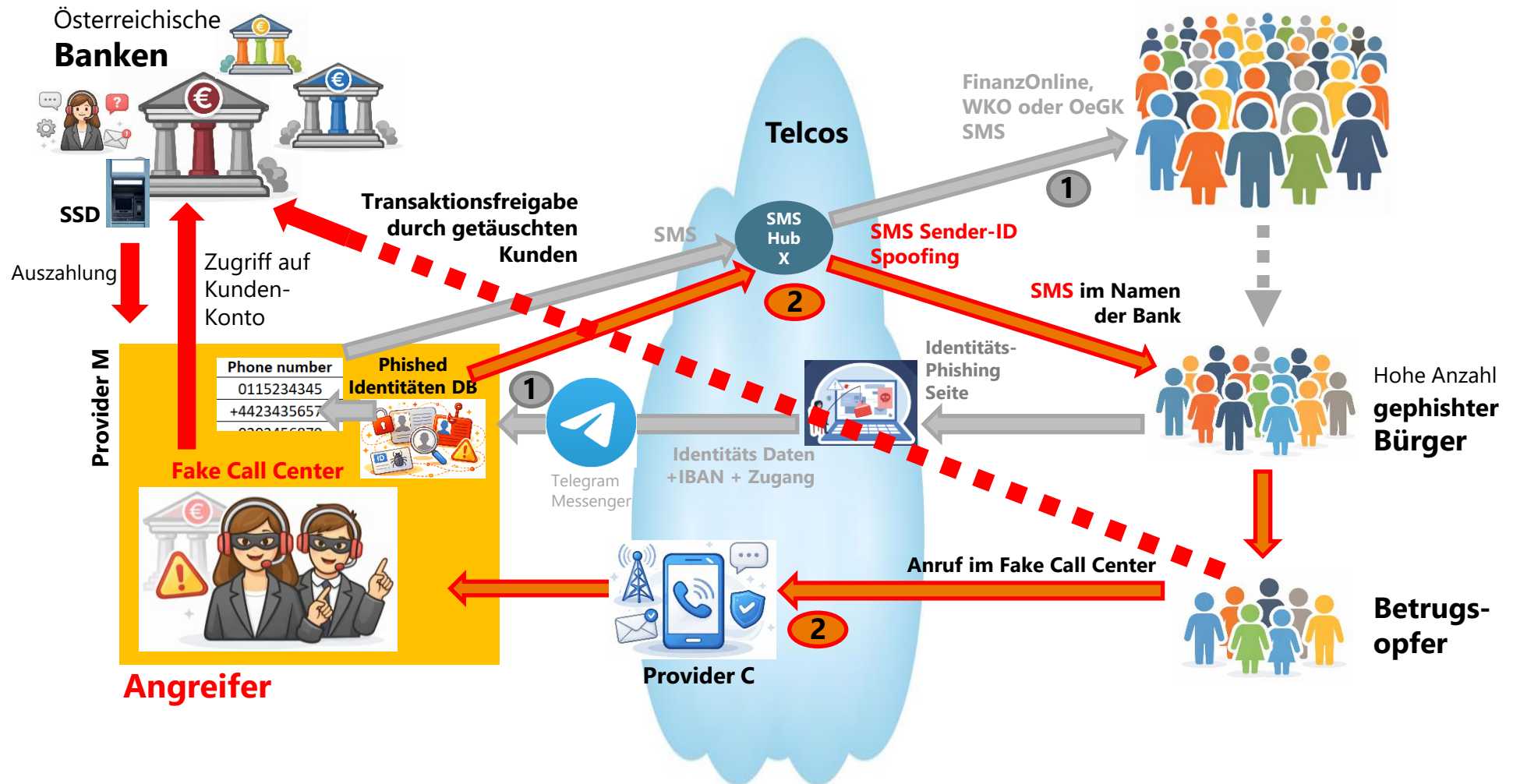


- Hinter angegebener Telefonnummer verbirgt sich ein **Fake-Bank Call Center**
 - meldet sich mit **‚kopierter‘ Ansage des echten Bank Call Centers**
- Fake Call Center Mitarbeiter **hinterfragt Namen des anrufenden Bankkunden**
 - prüft gegen die Liste der (zuvor gephishten) Bank KundINNen ?
 - **involviert ‚IT / Sicherheitsmitarbeiter‘**
 - hinterfragt das für Online Banking verwendete IT-System (PC oder ?) -> **Installation von Fernwartungssoftware**
- **Resilienz der Betrüger:** nach Deaktivierung der Fake-Call Center Nummer wird
 - das Fake-Call Center auf eine neue Nummer aufgeschalten
 - eine leicht adaptierte SMS an die erfassten Bank-KundINNen gesendet

Mehrere Fake
Call Center für
unterschiedliche
Finanzinstitute

Identitäts-Phishing --> Simple Vishing Methode

Schritt 2a: Verunsicherte Phishing-Opfer sollen (Fake) Call Center kontaktieren



Schritt 2 Var.b: Komplexes, mehrstufiges Vishing

Ankündigung des Vishing-Anrufs vor tatsächlichem Anruf

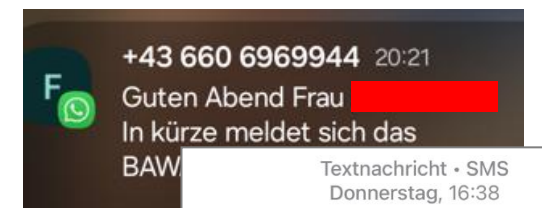


Individuelle Nachricht im Namen der Bank

WhatsApp oder SMS



- **b1) Angreifer kündigt ev. Vishing-Anruf mit kryptischer Textnachricht an**



Textnachricht • SMS
Donnerstag, 16:38

Sehr geehrter Kunde, wir haben eine verdächtige Transaktion festgestellt und kontaktieren Sie schnellstmöglich zur Verifizierung.

b2) Vishing mittels Sprach- oder WhatsApp-Anruf

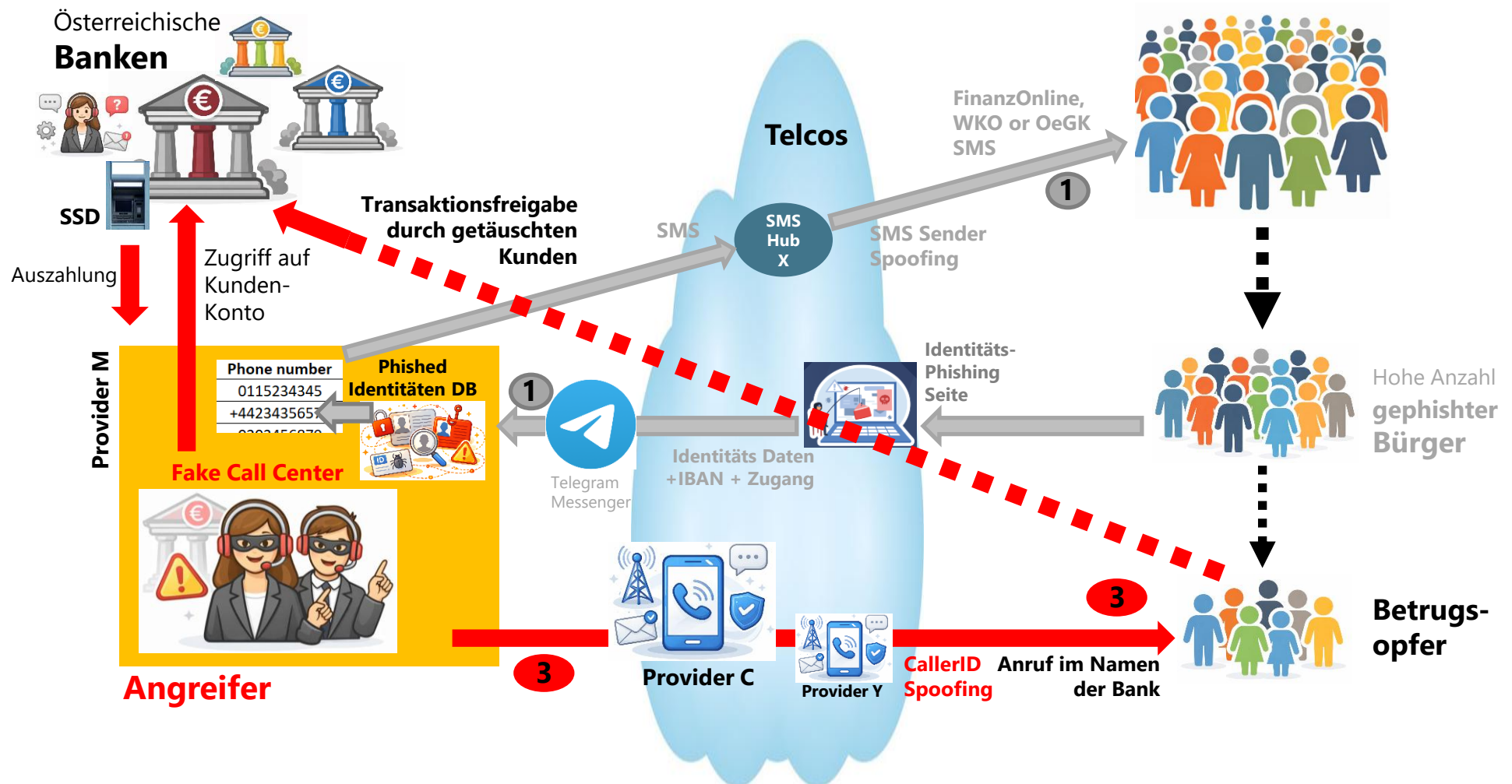
- Anrufe erfolgen zumeist **außerhalb der Bürozeiten**
- **Anrufe mittels CallerID Spoofing mit den echten Kopfnummern der jeweiligen Bank** scheinen von der Bank zu stammen
- Anrufer gibt vor, ein **Mitarbeiter der Sicherheitsabteilung** zu sein
-> eine verdächtige Transaktion wurde erkannt
- betrügerischer **Anrufer bietet Hilfe zur Stornierung der vorbereiteten Betrugstransaktion** an ... resultiert in **Tx-Freigabe**



Zur Bestätigung: Sie sind im Gespräch mit unserer Mitarbeiterin Melanie Müller von der IT-Sicherheitsabteilung

Identitäts-Phishing --> Komplexeres Vishing

Schritt 2b: Fake Call Center kontaktiert (potentielle) Opfer direkt

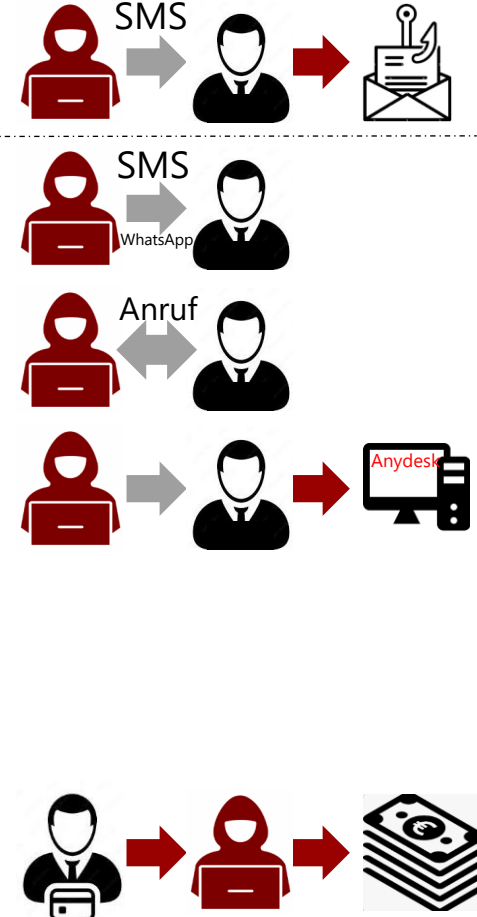


Beispiel eines realen Vishings Ende Q2/2026

Der bekannte Modus Operandi funktioniert (noch) immer

- ... Identitäts-Phishing ...
- Ich bekam eine **SMS**, ... **ich soll mich bei der Nummer +43660.... melden** – eine 'Katharina Klein' hat mich **zurückgerufen** und wollte das regeln
- Sie hat "gesehen,,, dass gerade bei einem Bankomaten Geld abgehoben wird - ich gab ihr **Zugang auf meinen Computer über anydesk.com**
- Während des Telefonats sah ich, dass **Geld von meinem Koto abgebucht** wurde. K.Klein meinte sie versucht das zu stornieren und hat **angeblich meine Karte gesperrt** - ich sollte das nicht auf meiner App machen
 - ... es wurde noch einmal abgehoben und noch einmal ...
- Danach sollte ich die (Bank-) **Karte in ein Kuvert geben** und einem Hr. Thomas Schuhmacher geben - er **kam und holte sie ab**
- ... sie wollte eine Überweisungsfreigabe mit erhöhtem Limit und fragte mich, ob ich Crypto habe - was ich verneinte - mir kam das komisch vor und **ich rief schließlich die Hotline** an

Transaktionen
wurden von
Transaktions-
Monitoring
geblockt



ID-Phishing & Vishing und gesetzlicher Rahmen

- Domains werden **ohne Prüfung der Namensrechte** auch in fremdem Namen registriert
- **Deaktivierung betrügerisch registrierter Domains** nicht durch Dritte möglich



- **Domain-registrierende Partei** wird nicht (mehr) bekanntgegeben



- **SMS Sender-ID Spoofing** funktioniert 4+ Jahre nach Flubot noch immer
- **Caller-ID Spoofing** funktioniert trotz RTR Verordnung (aus 9/2024)

Angreifer nutzen die Unzulänglichkeiten aus
versus

Angreifer nutzen die neuen Möglichkeiten aus

Banken haben umfangreiche Verpflichtungen gegenüber potentiell betroffenen KundINnen

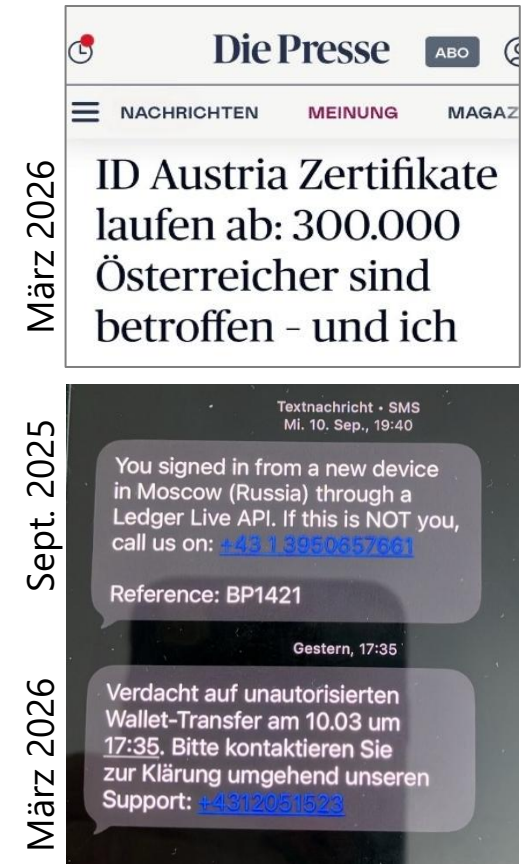


Betrügerische **Überweisungen** werden zB zu **Money Mule Konten** **unmittelbar ausgeführt** – erhaltene Beträge sofort weiterverschoben

Ein nicht optimistischer Ausblick

Identitäts-Phishing wirkt längerfristig / nach

- Mittlerweile müssen (zehn)tausende Identitäten gephisht sein und das ID-Phishing geht weiter
 - die Mehrzahl der gephishten **ID Daten sind statisch**
 - weitere Daten **ändert man eher nicht freiwillig**: zB Tel.nummer
- Mit dem weiter laufenden Identitäts-Phishing **reichern die Angreifer ihre Datenbanken** mit potentiellen Opfern weiter an
- Gephishte **Identitäten werden (weiter-) verkauft**
- (Bank-) KundINNen können **wiederholt angegriffen** werden
 - Wir sahen schon mehrfache Angriffsversuche



→ Erfolgreiches Identitäten-Phishing ist für Betroffene ein **längerfristiges Problem**

→ **Attacken-Optimierung** unter **Zuhilfenahme von KI** ?



ALLE Stakeholder sollten Eindämmung des Missbrauchs rasch & effektiv unterstützen

Betrug im Finanzbereich

Fragen und Antworten



Danke für Ihre Aufmerksamkeit 😊