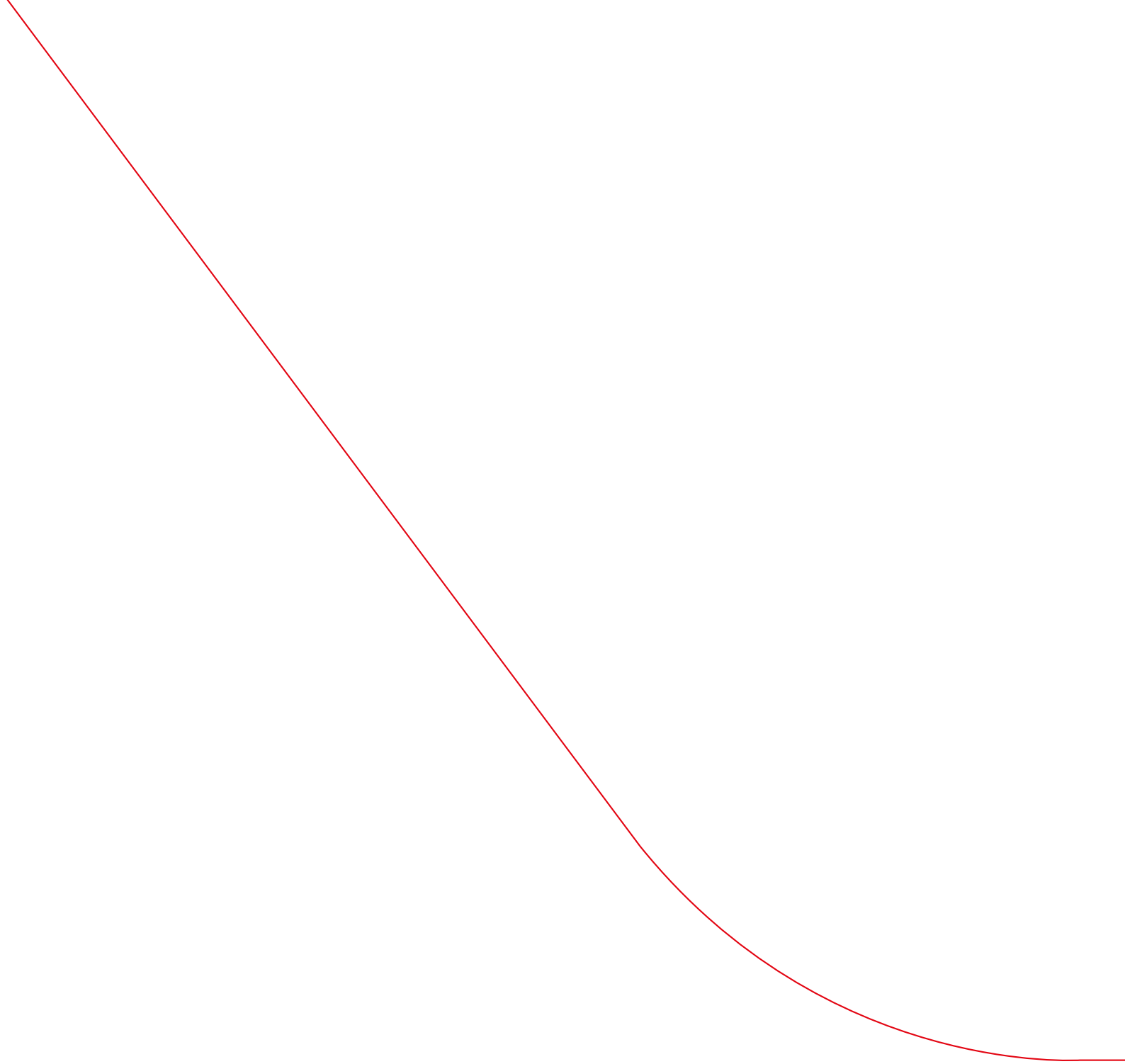
Christian Prantner
Benedikta Rupprecht
Arif Kaya

# MASSNAHMENPAKET GEGEN PHISHING

## Betrug an Bankkund:innen

AK WIEN



Christian Prantner
Benedikta Rupprecht
Arif Kaya

# MASSNAHMENPAKET GEGEN PHISHING

## Betrug an Bankkund:innen

Verlag Arbeiterkammer Wien
Mai 2025

# INHALTSVERZEICHNIS

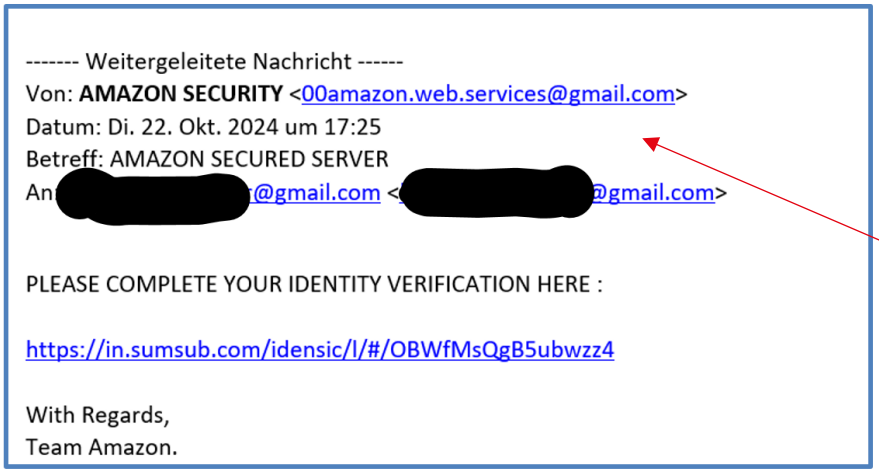
Die Arbeiterkammern (AK), der Verein für Konsumenteninformation (VKI) sowie die Ombudsstelle für Zahlungsprobleme (eingerichtet im österreichischen Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz) registrieren seit vielen Jahren in zunehmendem Ausmaß Beschwerden über Schäden von Bankkund:innen, die daraus resultieren, dass es Betrüger:innen gelingt, Geldbeträge von den Girokonten oder Zahlungskarten (Debit- und Kreditkarten) von Kund:innen abzubuchen. Diese Betrugsmethoden fallen unter die Kategorie von Phishing.

# 1. WAS IST PHISHING?

Der Begriff Phishing (Password + Fishing) stellt eine spezifische Art des Hackings da, es gibt jedoch noch weitere Formen wie zB Spoofing, Smishing, Vishing oder Quishing. Es gibt also eine Reihe von Hackingmethoden, die nachfolgend kurz dargestellt werden:

Dieser **Phishing**-Betrug begründet sich darauf, dass sich Betrüger:innen durch verschiedene, teils sehr fein gesponnene Betrugsmaschen, Zugang zu einem Girokonto verschaffen, in der Folge oft sehr hohe Geldbeträge abbuchen und auf Empfängerkonten transferieren, die unwiederbringlich verloren sind, da sie weder den Hausbanken der Konsument:innen noch Straf- bzw. Exekutivbehörden einen Zugriff bzw. eine Rückholung erlauben.

Mit Phishing-Nachrichten versuchen Kriminelle Ihre Daten zu stehlen. Meist fordern Betrüger:innen mittels Mitteilungen (wie insbesondere E-Mails, SMS) dazu auf, Links zu folgen oder Dateianhänge zu öffnen. Das Ziel der Betrüger:innen lautet, dass Sie persönliche Daten eingeben und – je nach Variante – Schadsoftware herunterladen. Kriminelle

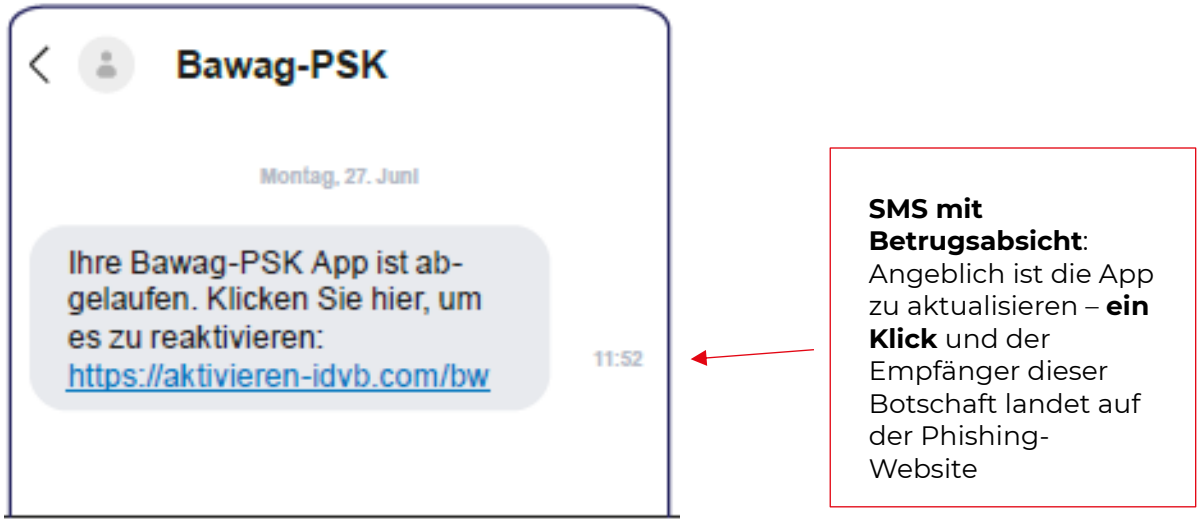



Betrügerische E-Mail: Kaum wahrzunehmender Hinweis auf Betrug: Amazon schickt **keine** E-Mails von einer (Gratis-)Gmail-Adresse

verwenden zunehmend **SMS (Smishing)**, **Telefonanrufe (Vishing)**, QR-Codes (Quishing) sowie diverse Social Media-Kanäle.

Abbildung 1: Vermeintliches E-Mail von Amazon, um Kundendaten zu aktualisieren

Die Methoden sind mittlerweile höchst raffiniert und der Datenklau gestaltet sich auch schon derart, dass eine der Website einer Bank täuschend ähnlich wirkende Betrugsseite auf diversen Suchmaschinen online gestellt und mittels bezahlter Anzeige hervorgehoben wird. Die Website gleicht dabei eins zu eins der tatsächlichen, zumeist bis auf einzelne Buchstaben in der Adressleiste genau wie etwa .ar statt .at (für Österreich) oder „Bamk“ statt „Bank“.




Selbst

Abbildung 2: SMS mit Betrugsabsicht. Darin findet sich ein Link zu einer Fake-Website

Auf den zweiten Blick ist die Betrugsseite nicht als solche zu identifizieren. Die Kennzeichnung mit dem SSL-Verschlüsselungssymbol (kleines „Bügelschloss“) wird schon länger von Betrügern einprogrammiert.

Es kommt auch vor, dass im gleichen Chatverlauf mit der Bank durch Vortäuschung der echten Telefonnummer der betrügerische Link von den Betrügern geteilt wird. In der Annahme, dass es sich um eine verschlüsselte seriöse Kommunikation mit der Bank handelt, wird man auf eine Fake-Website geleitet, um die Daten preiszugeben.

Sie finden hier einen detaillierten, **exemplarisch** aufbereiteten **Ablauf einer Phishing-Attacke**:
https://www.arbeiterkammer.at/beratung/konsument/AchtungFalle/AK_Warnung_vor_Datenklau_bei_Bankkunden.pdf

Die Betrugsmaschen entwickleln sich ständig weiter – **neuerdings auch mit QR-Code**; https://help.orf.at/stories/3228704/

Unter den Betrugsopfern finden sich Menschen quer durch alle Bildungs-, Gesellschafts- und Altersschichten. Programmierer:innen, IT-Techniker:innen und sogar vereinzelt Bankangestellte, die betrogen werden, sind in der Beratung keine Seltenheit mehr.

Die Schäden beim Cyberbetrug steigen sukzessive enorm an, was auch insofern unbefriedigend ist, als die Banken die Schäden Großteils auf die Kund:innen abwälzen. Das geht auch aus einem Bericht der Europäischen Bankenaufsicht hervor, der besagt, dass bei betrügerischen Überweisungen 86% des entstandenen Schadens durch die Kund:innen getragen werden muss (1. Halbjahr 2023).[1]

# 2. BETRUGSMASCHEN

Es gilt zum „Abfischen" von Bankdaten einige Begriffe bzw Anglizismen zu klären. Sehr häufig fällt der Begriff Spoofing.

**Spoofing** ist eine Technik, bei der ein/e Angreifer:in („Spoofer") **Daten oder Identitäten** missbräuchlich verwenden. Betrüger:innen nutzen real existierende E-Mailadressen oder Telefonnummern, die Banken/öffentlichen Einrichtungen/Unternehmen/Stellen wirklich gehören. Diese Methode ist deswegen besonders raffiniert, weil genau diese Telefonnummer am Display des Handys angezeigt wird, wenn die/der Betrüger:in anruft. Damit erhält ein/e Empfänger:in eines Anrufes, einer SMS odereines E-Mails den Eindruck, dass die Nachricht aus einer vertraueswürdigen Quelle oder von einem bekannten Unternehmen stammt – wie zum Beispiel die Hausbank, das Finanzamt, Google, Amazon oder Microsoft. Diese Betrugsanbahnung wird immer häufiger mit Methoden der künstlichen Inteligenz unterstützt, indem zB Bilder oder Videos reproduziert werden.[2] Sie führt zum Teil dazu, dass gefälschte Mitteilungen am Endgerät im selben Ordner landen, wie echte Nachrichten einer Bank oder öffentlichen Einrichtung.

Das Ziel eines Spoofing-Angriffes ist, zuerst **das Vertrauen der Zielperson** zu gewinnen, um letztlich **vertrauliche Informationen zu ergaunern**.In den meisten Fällen geht es darum, die Zugangsdaten zu einem Bankkonto zu erhalten, wie insbesondere den Verfügernamen, das Passwort und letztlich die Transaktionsnummern (TAN) für die Abbuchungen von einem Girokonto oder um (missbräuchliche) Transaktionen mit einer Zahlungskarte (Debit-, oder Kreditkarte) durchzuführen. Zum Teil wird dafür auch vom ahnunglosen Opfer Schadsoftware am eigenen Smartphone oder Laptop installiert, die Kriminellen Zugriff auf das Gerät ermöglicht.

Die Erfahrung zeigt, dass die Überweisungen oder Transaktionen, die auf Empfängerkonten der Betrüger:innen landen, in den allermeisten Fällen verloren sind. **Denn Überweisungen vom Zahlungskonto oder Kreditkartenabbuchungen** können nicht rückgängig gemacht

[1] EBA_ECB 2024 Report on Payment Fraud.pdf

[2] Weitere Informationen zu finden im Bericht von Europol: s. Europol Bericht https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

werden. In der letzten Zeit nutzen die Betrüger:innen Sofortüberweisungen, die binnen maximal zehn Sekunden auf einem Empfängerkonto landen müssen – das sind die Vorgaben der Verordnung über Sofortüberweisungen (VO 2024/886). [3]

**Arten von Spoofing:**

Die Absenderadresse einer Netzwerkverbindung wird gefälscht (zB erfolgt die Fälschung der Quelladresse einer Website), damit die/der Empfänger:in glaubt, dass der Datenverkehr bzw die (digitale) Kommunikation von einer vertrauenswürdigen Quelle stammt (**IP-Spoofing**).

Es kann auch eine **Ruf- bzw Telefonnummer eines Anrufers gefälscht** sein, um Empfänger:innen glauben zu lassen, dass der Anruf von einer vertrauenswürdigen Organisation oder einem namhaften Unternehmen stammt. Dabei nutzen die Anfgreifer:innen eine Software zur Fälschung der Telefonnummer – der betrügerische Anrufer gibt sich etwa als Mitarbeiter:in der Bank aus, um eine angebliche Kontosperre oder ein Sicherheitsupdate für das Girokonto durchzuführen (**Caller ID-Spoofing**). Der Gesetzgeber in Österreich ist tätig geworden, um betrügersiche Anrufe zu verhindern:

https://www.rtr.at/TKP/presse/pressemitteilungen/presseinformationen_2023/pinfo21122023tkp.de.html

Eine sehr häufige Variante des Betrugs erfolgt über die **Fälschung einer E-Mailadresse** einer Organisation oder eines namhaften Unternehmens, um Seriosität vorzutäuschen. Diese Form der Betrugsanbahnung kann auch über ein SMS erfolgen, in dem es etwa heißt, dass ein Sicherheitsupdate vorzunehmen ist.

[3] Verordnung (EU) 2024/886 des Europäischen Parlaments und des Rates vom 13. März 2024 zur Änderung der Verordnungen (EU) Nr. 260/2012 und (EU) 2021/1230 und der Richtlinien 98/26/EG und (EU) 2015/2366 im Hinblick auf Echtzeitüberweisungen in Euro

Häufig erfolgt eine **Kombination aus verschiedenen Betrugsmethoden**: Wenn ein/e Bankkund:in auf einen Link klickt, der in einer betrügersichen SMS oder einem E-Mail angeführt ist, dann erfolgt entweder die Weiterleitung auf eine betrügerische Webseite, die darauf angelegt ist, dass persönliche Daten – Passwörter – abgefragt werden, siehe nachfolgendes Beispiel:

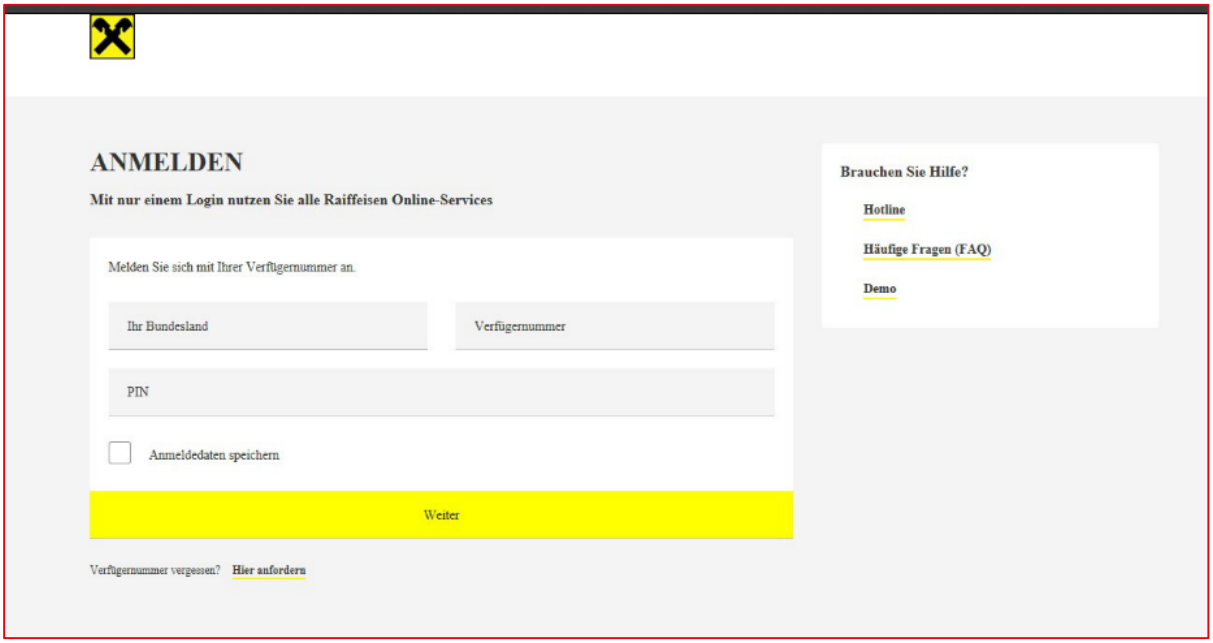



Abbildung : Fake-Login-Bereich durch Eingabe-Abfrage des Passwortes

Oder der Klick auf einen Link bringt mit sich, dass **Schadsoftware auf einem Gerät oder mehreren Geräten** des Betrugsopfers installiert wird. Dann kann es passieren, dass persönliche Informationen wie Sozialversicherungsnummern, Kreditkartendaten oder Anmeldedaten zum Girokonto ausgelesen und abgesaugt werden. Angenommen, die Betrüger:innen sind auf diese Weise zur Verfügernummer (bzw. zum Verfügernamen) und zum Passwort für das Online-Banking gelangt, dann können sie bereits ins Konto einsteigen und Transaktionen beauftragen. In diesem Fall fehlt nur ein oder mehrere Transaktionsnummern (TAN), um die Transaktion freizugeben. Daher erfolgt – **denn auch die Handynummer ist im Online-Banking ersichtlich** - oft ein Anruf beim anvisierten Betrugsopfer, um diesem die Transaktionsnummer (kurz: TAN) herauszulocken, den die Bank an das Smartphone des Opfers schickt. Der letzte Schritt ist also beispielsweise das Herauslocken der Transaktionsnummer durch **geschicktes Social Engineering,** also das kommunikativ ausgeklügelte „Bearbeiten" des anvisierten Betrugsopfers durch gekonnt manipulative Gesprächsführung des Anrufers. Ebenso kommt es vor, dass Kriminelle direkt Zugriff auf ein mit Schadsoftware infiziertes Gerät haben und den TAN-Code, die Push-Benachrichtigung etc selbst auslesen können, ohne dass das Opfer davon etwas merkt.

Ein im Bericht des Sozialministeriums **häufig stattfindendes Betrugsszenario** wird so beschrieben: im Nachrichtenverlauf der Bank am Mobiltelefon des anvisierten Betrugsopfers taucht eine SMS auf, die zum Inhalt hat, dass die Zugangsdaten zum Online Banking oder zur Zahlungs App aktualisiert werden müssen. **In der SMS ist ein Link**, der auf die Phishing-Webseite führt, die der echten Bankwebsite oft täuschend echt nachgemacht ist. In einigen

Browsereinstellungen wird die Adresszeile unterdrückt (es ist ein Hineinklicken in die Adresszeile notwendig).

Auf dieser Phishing-Webseite können nicht nur die Zugangsdaten zum Konto abgefragt werden, sondern auch eine **versteckte Zustimmung der (neuen) Registrierung des Mobiltelefons** der Betrüger:innen, was dazu führt, dass diese einen uneingeschränkten Zugriff auf das Online Banking, die Zahlungskarte und ein Mobiltelefon haben, auf dem sie einen selbstgewählten Code, ihren Fingerabdruck oder Face-ID-Daten[4] hinterlegen. Die Betrüger:innen können also nicht nur Bezahllimits für Transaktionen für Überweisungen und Kartenzahlungen erhöhen, sondern auch selbst Transaktionen beauftragen **und freigeben**. Die Opfer werden zwar von der Registrierung des neuen Telefons verständigt (SMS, E-Mail). Aber es kann sein, dass die Benachrichtigung zu spät kommt – denn der Betrug findet häufig innerhalb weniger Minuten nach Registrierung des neuen Telefons und/oder der Limiterhöhung statt. [5] Die Verbraucherzentrale in Deutschland hat zudem erhoben, dass solche Warnmeldungen von vielen Konsument:innen als verwirrend und unverständlich eingeschätzt werden. Nur 16 % verstanden den Inhalt der Warnmeldung, was belegt, dass diese meistens ihren Zweck verfehlen.[6]

Eine Variation des Telefon-Betruges ist, wenn es die Betrüger schaffen, eine Telefonnummer von der **ursprünglichen SIM-Karte des Betrugsopfers auf eine E-Sim** zu übertragen. Die E-SIM ist keine physische Karte mehr, sondern der Vertrag wird auf einem Chip im Smartphone aktiviert.

Es spielt den Betrüger:innen in die Hände, wenn **ein einzelnes Zahlungskonto (zB ein Gehalts- oder Pensionskonto) mit mehreren Bankprodukten** verknüpft ist. Das ist nämlich häufig der Fall. Wenn sich also Betrüger:innen Zugang zum Konto verschaffen, indem sie die (einzige) Verfügernummer (bzw. einen Verfügernamen) und das Passwort zum Zahlungskonto vom Betrugsopfer abfischen, dann haben sie auch Zugang zum Beispiel **zu einem mit dem Konto verknüpften Sparkonto (oder Sparkonten) und/oder einem Wertpapierdepot**. Sie finden also noch größere Beträge vor, die sie vom Konto abzweigen können.

[4] Fingerabdruck und Face-ID, also das Erkennen des Gesichts, sind Methoden körpereigener Merkmale, die dazu herangezogen werden, um ein Mobiltelefon zu entsperren, Zahlungstransaktionen oder Einkäufe im Internet freizugeben.

[5] https://www.konsumentenfragen.at/konsumentenfragen/Aktuelles/Konsumentenfragen/Taetigkeitsbericht-der-Ombudsstelle-fuer-Zahlungsprobleme.html , S. 5.

[6] 24-10-10 Bericht_vzbv_Sorgfaltspflichten Banken_final.pdf, S 6

# 3. FALLZAHLEN UND FALLBEISPIELE

Dieser Datenklau hat eine erhebliche Dimension angenommen und betrifft grundsätzlich alle Bankkund:innen. Die Beschwerdezahlen in den Konsumentenberatungseinrichtungen der Arbeiterkammern und in der Ombudsstelle für Zahlungsprobleme im Sozialministerium belegen dies. **Zwei aktuelle Fallbeispiele** aus der AK-Beratung, die einen häufig geschilderten Verlauf aufweisen – samt einer abschlägigen Antwort seitens der Bank:

**Fallbeispiel Beratung 1**

Herr S. schreibt der AK-Wien im Dezember 2024 (Bank anonymisiert):

*Ich habe ein Konto bei der X-Bank.* Am 9.12.2024 habe ich über Online-Banking *meiner Hausbank zwei Anfragen für Abbuchungen bekommen. Obwohl ich auf „Zahlung abgelehnt" gegangen bin, waren am nächsten Tag (10.12.) drei Beträge abgebucht. Für die dritte Abbuchung habe ich keine Zustimmungsanfrage erhalten. Die Firma, die die Abbuchungen vorgenommen hat, kenne ich nicht. Insgesamt hat sie drei Abbuchungen von meinem Konto getätigt. Ich habe noch am 9.12. in der App mein Konto gesperrt und war am 11.12. bei der Bank direkt in der Filiale. Dort hieß es, dass ich zur Polizei muss, um eine Anzeige zu machen, was ich auch getan habe. Am 13.12. habe ich von der Bank folgende Nachricht per E-Mail erhalten:*

*Guten Tag Peter S., wir möchten Sie darüber informieren, dass dieser Umsatz mittels eBanking App bestätigt wurde. Da nur der Karteninhaber Zugriff auf die App hat, können wir keine Reklamation aufgrund von Missbrauch durch eine dritte Person durchführen. Freundliche Grüße Ihr Bank Service Center*

*Herr S. betont, dass er den Überweisungen nicht zugestimmt habe. Die AK hat Herrn S. Unterstützung zugesagt.*

**Fallbeispiel Beratung 2**

**Herr W., selbst Bankangestellter, schreibt der AK Wien** (Bank anonymisiert)**:**

*Am 7.1.2025, circa gegen 23 Uhr, loggte ich mich auf meinem in die Banking-App ein, um die Entwicklung meines Wertpapierdepots zu überprüfen. Beim Scrollen fiel mir auf, dass bei meiner Kreditkarte ein ungewöhnlich hoher Minusbetrag von über 1.300 Euro vermerkt war. Ich klickte auf die entsprechende Kachel und fand zu meinem Entsetzen eine Transaktion von EUR 1.260,44 an das Unternehmen "XY Travel" - ein Unternehmen, das mir bis dahin gänzlich unbekannt gewesen war. Ich reklamierte die Transaktion umgehend mittels vorgefertigter eidesstattlicher Erklärung im Online-Banking und ließ die Kreditkarte sperren. Am darauffolgenden Tag schrieb mir eine Bankmitarbeiterin in meiner Banking-App, dass meine Rückerstattungsanfrage abgelehnt sei, da ein Autorisierungsprozess dokumentiert wurde. Anhand des beigefügten Dokuments sah ich, dass die Freigabe am 1.1. um rund 11:02 Uhr gestartet worden war. Zu diesem Zeitpunkt war ich daheim und hatte gerade auf meinem Tablet das Neujahrskonzert eingeschaltet. In der Banking App*

*war ich nicht eingeloggt und habe daher auch niemals eine Freigabeanfrage, SMS oder sonstiges erhalten. Nachdem ich also die Nachricht von der Bankmitarbeiterin gelesen hatte, telefonierte ich mit der Ombudsstelle der Bank, die die Transaktion als möglichen Betrugsfall markierte. Anschließend ging ich zur nächsten Polizeistation und erstattete Anzeige wegen Kreditkartenmissbrauchs. Es folgten noch weitere Korrespondenzen in der Banking App); darüber hinaus kontaktierte ich das Unternehmen XY Travel, die offenkundig keinen Eingang der EUR 1.260,44 feststellen konnten. Vonseiten der Bank wird nun behauptet, dass ich die Freigabe zweifelsfrei erteilt hätte, weswegen ich jetzt nicht nur grobe Sicherheitsbedenken hinsichtlich sämtlicher Zahlungsaktivitäten habe, sondern dies auch als Unterstellung zum Betrug meinerseits und einer damit einhergehenden Rufschädigung werten muss.*

**Herr W.** hat betont, dass er diese Transaktion definitiv nicht freigegeben habe, was die Bank bestreitet („Die gegenständliche Transaktion wurde mittels starker Kundenauthentifizierung freigegeben“).

**Fazit: Die von den Banken eingewendete a) grobe Fahrlässigkeit und/oder b) von Kund:innen vorgenommene Autorisierung einer Transaktion können Kund:innen ohne rechtlichen Beistand kaum wirksam entgegnen. Die Umstände der groben Fahrlässigkeit sind im Einzelfall zu beurteilen.**

Es gibt zahlreiche Fälle wir die von Herrn A. und S. Die Arbeiterkammern haben österreichweit im Jahr 2024 1054 Beschwerdefälle zum Betrug im Zahlungsverkehr registriert; der überwiegende Teil dieser Betrugsfälle betraf Phishing-Attacken.[7]

Im **Bericht des Sozialministeriums** bzw. der **Ombudsstelle für Zahlungsprobleme** ist – in systematischer Form aufbereitet - nachzulesen, dass die Phishing-Attacken viele Banken betreffen und durch alle gesellschaftlichen Schichten gehen.[8]

Im Berichtszeitraum von 1.1.2023 bis 30.9.2024 registrierte und bearbeitete die Ombudsstelle 457 Fälle von Phishing; daraus entstanden 377 Interventionen bei Banken, wovon die Hälfte der Fälle auf eine einzige Bank entfielen.[9] Der durchschnittliche Schaden belief sich laut Auswertung der Ombudsstelle auf fast 4.000 Euro[10]; pro Schadensfall gab es im Durchschnitt 5 missbräuchliche Buchungen. Die Interventionen der Ombudsstelle führten in 62 Prozent zu einer außergerichtlichen Einigung.[11]

[7] AK-Beratungsstatistik österreichweit, 2024: „Betrügerische Geschäftspraktiken im Zahlungsverkehr“

[8] https://www.konsumentenfragen.at/konsumentenfragen/Aktuelles/Konsumentenfragen/Taetigkeitsbericht-der-Ombudsstelle-fuer-Zahlungsprobleme.html

[9] ebendort, S. 6.

[10] ebendort, S. 9

[11] Ebendort, S. 15

Interessant sind gemäß Bericht der Ombudsstelle die Arten der Transaktionen, die zum Betrug führten. Demnach entfielen auf die Interventionen folgende Transaktionen:

- 60 % waren nicht autorisierten Transaktionen
- 40 % waren autorisierte Transaktionen[12]

Bei den **nicht autorisierten Zahlungen** gelingt es den Betrüger:innen im Zuge des Phishing-Angriffs, sich unmittelbaren Zugriff auf das Konto und/oder die Zahlungskarte des Opfers zu verschaffen und dadurch die von der Bank zum Schutz gegen Betrügereien getroffenen Sicherheitsmaßnahmen zu umgehen. Der Anteil solcher Betrugsfälle kann daher als ein Indikator für das Sicherheitsniveau bei der jeweiligen Bank angesehen werden.

Das Gegenstück sind die **autorisierten Zahlungen**, die zum Betrug führen: Eine Zahlung ist dann autorisiert, wenn der:die Konsument:in der Zahlung unter Verwendung seiner:ihrer Authentifizierungsmerkmale zugestimmt hat und ihm:ihr vor der Freigabe die notwendigen Informationen zum Zahlungsauftrag (Betrag, Empfänger, Währung) angezeigt wurden. Als Authentifizierungsmerkmale fungieren in der Regel das Mobiltelefon des:der Konsument:in in Verbindung mit dem geheimen PIN/dem Fingerabdruck/der Gesichtserkennung.[13]

Diese Betrugsmasche erfolgt durch **„Social Engineering", was** bedeutet, dass das Betrugsopfer auf geschickte Art und Weise insbesondere durch Anrufer:innen mit Betrugsabsicht dazu gebracht wird, eine letztlich betrügerische Transaktion selbst freizugeben. Das Opfer wird also manipuliert **(„Authorised Push Payment Fraud").**

Die wichtige **Unterscheidung zwischen autorisierter und nicht autorisierter Transaktion** besteht darin, dass die gesetzlichen Haftungsbestimmungen unterschiedlich ausgestaltet ist. Denn bei der nicht autorisierten Zahlung haftet die Bank bzw der Zahlungsdienstleister, während bei autorisierten Zahlungen hingegen der:die Konsument:in den Schaden zu tragen und allenfalls Schadenersatzansprüche gegen die Bank geltend machen kann.

**Wie ist die Haftung der Banken geregelt?**

**Es gibt im Zahlungsverkehr im Wesentlichen zwei Betrugsfelder:**

**Erstens: Der physische Kartenmissbrauch, vor allem wenn der PIN-Code einer Debit- bzw Bankomatkarte ausgespäht, die Karte dann entwendet wird und danach missbräuchliche Abbuchungen an Geldbehebungsautomaten stattfinden.**

**Mehr dazu:**

Vorsicht vor ausgespähten PIN-Codes | Arbeiterkammer

[12] ebendort, S. 6

[13] ebendort, S. 17

**In den letzten Jahren gab es mehrere Urteile, die die Haftung der Bank bzw. des Karteninhabers bei Missbrauch einer Zahlungskarte – vor allem nach Ausspähen des Codes und darauffolgendem Diebstahl – zum Gegenstand hatten. Banken machen oft vom so genannten "Anscheinsbeweis" Gebrauch, wenn nicht bewiesen werden kann, ob Konsument:innen tatsächlich den PIN-Code gemeinsam mit der gestohlenen Karte aufbewahrt bzw. auf der Karte notiert hatten und behaupten, dass der Anschein für diese Tätigkeit spricht. Gerichte akzeptieren diesen von den Banken getätigten Anscheinsbeweis oft, wenn andere plausible Begründungen fehlen, wie die Täter den geheimen PIN-Code sonst hätten erfahren können. Durch die mit dem Kontoauszug belegbare zeitnahe Abhebung vor dem Betrug verlieren Banken die Möglichkeit des Anscheinsbeweises. denn Geschädigte können in diesen Fällen das Ausspähen glaubhaft machen. Die Folge: die Beweislast ändert sich - die Bank hat ihrerseits den vollen Beweis zu erbringen, dass der PIN-Code gemeinsam mit der Karte aufbewahrt wurde. Diesen Nachweis zu führen, ist schwierig.**

**Der Oberste Gerichtshof (OGH) stellte zudem fest, dass die Bank im Normalfall für den Schaden durch den Missbrauch einer Bankomatkarte nach Ausspähung des Codes und Diebstahl der Karte aus dem Rucksack des Karteninhabers haftet („Rucksack- Urteil“). Aus Entscheidungen des Obersten Gerichtshofs (OGH) ging hervor, dass Besitzer von Bankomatkarten den ihnen von den Banken zur Verfügung gestellten PIN-Code für die Bankomatkarte sehr wohl auch aufschreiben dürfen. Der Code muss aber an einem für Dritte nicht zugänglichen Ort sorgfältig verwahrt werden. Auch ist es grundsätzlich nicht verboten, die Bankomatkarte in einem abgestellten Fahrzeug aufzubewahren. Diese Form des Betruges hat in den letzten Jahren stark abgenommen und ist von Internet-Betrugsfällen abgelöst worden.**

**Zweitens: Betrugsfälle durch Phishing haben die oben angesprochenen Bankomat-Betrügereien (dh Ausspähen/Ablesen des Codes, Entwendung der Debitkarte, Abbuchungen vom Konto etc.) fast vollständig abgelöst.**

**Das Zahlungsdienstegesetz sieht vor (§ 67 ZaDiG), dass die Bank einen Schaden bei missbräuchlicher Verwendung eines Zahlungsinstruments zu tragen hat. Genauer gesagt: die Bank haftet bei nicht-autorisierten Transaktionen – die betrogenen Bankkunden haften also nicht, wenn keine Authentifizierung einer bzw- mehrerer Zahlungen stattgefunden hat.**

**§ 68 sieht vor, dass die Bank nicht haftet, wenn grobe Fahrlässigkeit oder gar Vorsatz der:des Bankundin/-kunden vorliegt. Liegt hingegen leichte Fahrlässigkeit vor, dann haftet die:der Bankkundin/-kunde mit (höchstens) 50 Euro. Das bedeutet, dass für die Schadenstragung der Grad des Verschuldens maßgeblich ist, der nach den allgemeinen Maßstäben des österreichischen Schadensersatzrechtes in jedem Fall individuell zu beurteilen ist.**

**Was bedeutet das für die Bankkund:innen?**

**Zur Klärung der Fragen zur groben Fahrlässigkeit sind oberstgerichtliche Entscheidungen notwendig, die teilweise noch ausstehen. Es ist jedenfalls aufwändig, die grobe Fahrlässigkeit im Einzelfall (zB vor Gericht) feststellen zu lassen.**

**Das Zahlungsdienstegesetz – und damit die zugrundeliegende EU-Zahlungsdiensterichtlinie – ist lückenhaft, weil der in den letzten Jahren explodierende Anteil von Betrugsfällen mittels Social Engineering – die missbräuchlichen Transaktionen werden aktiv von Konsument:innen freigegeben**

**und damit rein formal autorisiert – nicht angemessen geregelt ist. Das bedeutet, dass es notwendig ist, dass die Haftungsbestimmungen für diesen von Betrügern geschickt initiierten autorisierten Betrug erweitert (Authorised Push Payment Fraud) werden.**

Die Arbeiterkammern registrieren – seit der Corona-Pandemie – verstärkt Konsument:innenbeschwerden zum Phishing. Das ist deshalb nicht verwunderlich, denn in in der Betrugsanbahnung werden betrügerische SMS oder E-Mails breit gestreut und erreichen somit eine große Anzahl an möglichen Betrugsopfern. Es ist ein Phänomen, dass selbst achtsame Bankkund:innen auf elektronische Nachrichten oder betrügerische Anrufe – getätigt von professionell-geschulten Anrufer:innen mit Betrugsabsicht - hereinfallen und letztlich – durch geschickt aufgebaute Gespräche, die auf **Angst und Besorgnis beim Opfer** abzielen - ihre Zugangskonten zum Konto bekannt geben oder die Transaktionen selbst freigeben. Die Erfahrung zeigt, dass die freigegebenen Transaktionen auf Empfängerkonten im Ausland landen und rasch in nicht nachvollziehbaren Kanälen versickern.

Die allerorts kursierenden Schutzmaßnahmen[14] reduzieren sich immer auf Verhaltensmaßnahmen für Konsument:innen – aber **niemals auf die Pflichten der Banken**, die Internet Banking als Feature ihres Girokontoangebotes entwickelt haben und in immer stärker werden Ausmaß die Digitalisierung propagieren, siehe zB https://www.oesterreich.gv.at/themen/onlinesicherheit_internet_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/2/2/Seite.1720530.html

In der **AK-Broschüre „Sicher bezahlen“** sind Hinweise auf die H**aftung beim Missbrauch von Zahlungsinstrumenten** zu finden: https://www.arbeiterkammer.at/sicher-bezahlen

Banken und Mobilfunkunternehmen sowie Nachrichtendienste, die in diesem Betrugsschema tragende Rollen einnehmen, sind bei Maßnahmen nur unzureichend adressiert, wenn es darum geht, dass Phishing-Attacken erst gar nicht stattfinden oder rechtzeitig unterbunden werden. Es kommt hinzu, dass Banken ihren Kund:innen Online-Banking-Apps sowie Freigabemöglichkeiten für Überweisungen für ein- und dasselbe Endgerät zur Verfügung stellen. Damit fehlen jedoch zwei Kommunikationswege, die eine sichere Authentifizierung von zwei voneinander unabhängigen Elementen ermöglichen sollen. Das geschieht auf Kosten der Kund:innen und der Sicherheit, denn im Schadensfall werden ihnen die Vorwürfe eines falschen Verhaltens gemacht, obwohl das Problem die von den Banken bereitgestellten Online-Banking-Lösungen sind.

[14] Erwähnenswerte Initiativen und Beispiele: https://www.bundeskriminalamt.at/news.aspx?id=4A77742B31664E706336733D (abgerufen am 4.2.2025)
https://www.sicher-bezahlen.at/

Die AK ist der Ansicht, dass reine Informationskampagnen zu kurz greifen und dass eine Reihe von Forderungen an Banken, Mobilfunkbetreiber und dem Gesetzgeber zu stellen sind:

# 4. FORDERUNGEN UND LÖSUNGSVORSCHLÄGE

## 4.1. ADRESSATEN MOBILFUNKUNTERNEHMEN UND NACHRICHTENDIENSTE

**Mobilfunkunternehmen und Nachrichtendienste** sollten technische Möglichkeiten in Anspruch nehmen, die es ermöglichen, „Massen-Phishing-SMS“ zu erkennen und diese abzufangen, zum Beispiel durch die Nutzung von Big Data und Künstlicher Intelligenz (KI) zur Analyse von Phishing-Mustern. Es müssen also Maßnahmen ergriffen werden, dass Phishing-SMS und Phishing-E-Mails erst gar nicht zugestellt werden. Wichtig beieiner derartigen technischen Lösung ist, dass Anbieter das Telekommunikationsgeheimnis wahren. Denkbar sind beispielsweise Lösungen, bei denen verdächtige Links mit bekannten Betrugs-Links abgeglichen oder einem Text sogenannte Hashwerte gegeben werden: dadurch kann festgestellt werden, ob eine SMS betrügerisch ist oder nicht. Eine weitere Möglichkeit zum Verhindern von SMS-Phishing ist das Führen einer Datenbank sicherer Absender von Massen-SMS. Das kann den Versand von betrügerische Massen-Phishing-SMS durch unbekannte Absender verhindern. Die AK spricht sich für eine Lösung aus, die das Telekommunikationsgeheimnis bestmöglich wahrt.

Zum Schutz vor Phishing-Angriffen gehört auch, dass ohne qualifizierten Identitätsnachweis keine e-Sims ausgestellt werden, die es Betrüger:innen erlauben, die Online Banking Authentifizierung völlig ahnungsloser Opfer auf ein Fremdgerät umzuleiten. Weitere denkbare Maßnahmen:

- Bei der Registrierung von neuen Handys bzw. Smartphones durch die Betrüger:innen – auf diese Weise verschaffen sie sich Zugang auf ein (neues) Endgerät der betrogenen Konsument:innen - sollte es eine **„Karenzfrist“** – beispielsweise zwei Stunden – sowohl für Limiterhöhungen als auch für die Registrierung neuer Geräte geben, dass vor allem plötzliche und mehrmalige Limiterhöhungen für Überweisungen/Buchungen nicht möglich sind.
- Der Betrug mit neu registrierten Handys/Smartphones durch Betrüger:innen ist auffallend. Es ist daher überlegenswert, dass bei der Neuregistrierung von Handys zusätzlich höhere Sicherheitsanforderungen – zum Beispiel durch einen **zusätzlichen Authentifizierungsschritt** – gestellt werden (zum Beispiel durch die Vorlage eines digitalen Personalausweises).
- Die anscheinend oft zu einfache Möglichkeit **zur Hinterlegung von Kredit- oder Debitkarten** auf neuen Endgeräten bzw. auf mehreren Geräten bzw. auf Smartphones/Smartwatches könnte durch zusätzliche Sicherheitsmaßnahmen erschwert werden.
- Die Rundfunk- und Telekom Regulierungs-GmbH (RTR) hat mit Wirksamkeit ab dem 1. September 2024 die sogenannte **RTR-Anti-Spoofing-Verordnung** erlassen. Diese Verordnung stellt sicher, dass bei Anrufen mit österreichischen Rufnummern

tatsächlich ein österreichischer Anschluss dahintersteht. Die Verordnung sieht vor, dass österreichische Telefonanbieter bei Anrufen aus dem Ausland, die eine österreichische Nummer vortäuschen, eine Verifizierung der Rufnummer durchführen müssen. Wenn eine Verifizierung fehlschlägt, dann wird die Rufnummer am Handy-Display der angerufenen Person nicht angezeigt; oder sie wird in eindeutigen Fällen blockiert. Dadurch soll verhindert werden, dass Betrüger:innen nicht mit „gestohlenen" Telefonnummern bei den Anrufer:innen den Anschein erwecken, es handle sich um eine legitime österreichische Telefonnummer.

- Die Verordnung hat dazu beigetragen, dass viele tausend betrügerische Anrufe mit österreichischen Telefonnummern geblockt wurden. Die AK setzt sich dafür ein, dass diese gesetzlichen Vorschriften zu Anrufen mit missbräuchlich gebrauchten Telefonnummern europaweit gelten soll. Für Österreich ist wichtig, **dass auch gespoofte Nummern mit deutschen Telefonnummern geblockt werden**.
- Die AK setzt sich auch dafür ein, dass nicht nur Anrufe mit Betrugsabsicht, sondern auch **SMS-Nachrichten am Handy** geblockt werden. Dabei ist das Telekommunikationsgeheimnis zu beachten.

## 4.2. ADRESSATEN BANKEN UND ZAHLUNGSDIENSTLEISTER

Die **Banken** streifen die Verantwortung nach erfolgreichen Phishing-Attacken im Regelfall ab und erklären geschädigte Konsument:innen als „grob fahrlässige" Kund:innen, die für den Schaden alleine haftbar sind. Die Haftung wird auch regelmäßig abgelehnt mit dem Hinweis, dass die Kontoinhaber:innen eine (oder mehrere) Transaktionen autorisiert und damit aktiv freigegeben haben. Diese Praxis der Banken nimmt keine Rücksicht auf die Tatsache, dass der Betrug – vor allem eingeleitet durch psychologisch geschickt agierende Anrufer:innen mit Betrugsabsicht - immer ausgeklügelter wird („Social Engineering"). Die AK ist der Ansicht, dass Banken die Digitalisierung im Zahlungsverkehr seit vielen Jahren stark forcieren, aber unfairerweise Bankkund:innen die mit der Digitalisierung verbundenen Risiken des Cyberbetrugs höchst einseitig aufbürden.

Wie aus dem **Bericht der Ombudsstelle für Zahlungsprobleme** hervorgeht, finden pro Betrugsfall im Schnitt 5 missbräuchliche Abbuchungen statt – in einem Extremfall jedoch 140 Transaktionen. Das lässt den Schluss zu, dass die Systeme der Transaktionsüberwachung der Banken, die verdächtige oder höchst ungewöhnliche Transaktionen identifizieren sollen, nicht effektiv genug ausgestaltet sind.[15] Daher haben die Banken dafür Sorge zu tragen, dass die Programme, die verdächtige Zahlungsverkehrstransaktionen anzeigen, effektiver gestaltet sein müssen. Konkrete Punkte von der AK geforderten Punkte:

- Einführung eines engmaschigeren und rechtlich **verpflichtenden Transaktionsmonitorings** (Einführung höherer Mindeststandards; Künstliche Intelligenz, also KI könnte auch zur Entwicklung von Frühwarnsystemen beitragen). Aus

[15] Auch der VZBV in Deutschland hat in einem Positionspapier die mangelnde Transaktionsüberwachung in Deutschland bemängelt, siehe Näheres im Kapitel 1.4 24-10-10 Bericht_vzbv_Sorgfaltspflichten Banken_final.pdf

der Beratungserfahrung über die Schadensfälle kann der Schluss gezogen werden, dass die Qualität dieser Transaktionsüberwachung bei den verschiedenen Bankinstituten variiert. Die europäische Dachorganisation der Verbraucherorganisationen BEUC fordert, dass die **Haftung** für eine missbräuchliche Transaktion automatisch auf die Bank übergeht, wenn sich herausstellt, dass die Bank **kein Transaktionsmonitoring** vorgenommen hat.

- Bei der Transaktionsüberwachung ist auf den Umstand Bedacht zu nehmen, dass die überwiegende Mehrzahl der (betrügerischen) Empfänger:innen im **außereuropäischen Ausland** liegt.
- Jedes Bankinstitut sollte automatisch für das mit einem Girokonto verbundenem Sparkonto, Wertpapierdepot etc. **einen eigenen Verfügernamen** einrichten. So könnte vermieden werden, dass beim Hacking des Online-Bankings auch das Sparkonto „abgefischt" wird. Derzeit ist es so, dass mit einem einzigen Verfügernamen der Zugang zu allen Produkten, das mit dem Girokonto verknüpft ist, gegeben ist. Es ist daher unter Sicherheitsaspekten sinnvoll, dass für die mit dem Konto verbunden Produkte **eigene Verfügernamen** eingeführt werden.
- Banken sollten abschreckende Strafen erhalten, wenn sie sich nicht an die gesetzlichen Bestimmungen halten (zB keine Richtigstellung des Bankkontos innerhalb eines Bankwerktages gemäß § 67 Zahlungsdienstegesetz - ZaDiG ). Wichtig wäre es, wenn die österreichische **Finanzmarktaufsicht (FMA)** auch erhebliche Strafen verhängen kann (zB auch dafür, wenn Phishingfälle nicht an die FMA gemeldet werden).
- Die Anforderungen an Konsument:innen hinsichtlich technischer Voraussetzungen und IT-Kenntnissen steigen zunehmend. Ist ein Hackerangriff auf das Konto erfolgt, sind **viele Konsument:innen** völlig **überfordert**, ob sie Maßnahmen an ihren Geräten setzen müssen oder sollten, um erneuten Schaden zu verhindern. Daher ist überlegenswert, dass es technische Angebote von zertifizierten Beratungsstellen gibt, die Überprüfungen des Geräts auf mögliche Manipulation oder Hackings anbieten.

## 4.3. ADRESSAT GESETZGEBER (NATIONAL, EU-GESETZGEBUNG)

Das **Zahlungsdienstegesetz** – basierend auf der EU-Zahlungsdienste-Richtlinie – sieht zwar vor, dass die Haftung bei missbräuchlichen Zahlungsinstrumenten grundsätzlich beim Zahlungsdienstleister liegt: in der Praxis jedoch lehnen die Banken bzw. Zahlungsdienstleister die Haftung nach Betrugsfällen zumeist ab, weil die geschädigten Kund:innen durch grobe Fahrlässigkeit den Betrug ermöglicht hätten oder eine Zahlung zugunsten betrügerischer Dritter selbst autorisiert hätten. Der Schaden müsse daher – in beiden zuvor genannten Fällen - vom Kunden selbst getragen werden. Es ist daher aus der Sicht der AK sinnvoll, wenn OGH-Urteile zur Klärung wichtiger Rechtsfragen im Zusammenhang mit dem Vorhalt der Fahrlässigkeit beitragen. Zudem ist es wesentlich, dass die zugrunde liegenden gesetzlichen Regelungen auf europäischer Ebene im Sinne des Konsument:innenschutzes weiterentwickelt werden.

Tatsächlich werden in der EU – Stand Jänner 2025 - im Rahmen der **Payment Services Regulation (PSR)** neue Haftungsbestimmungen diskutiert. Die EU-Kommission hat

vorgeschlagen, die derzeitigen Haftungsbestimmungen zu ändern, allerdings nur für ein eng gefasstes Betrugsszenario. Demnach soll die Bank haften, wenn die/der Konsument:in von einem Betrüger kontaktiert wird, der sich als Bankmitarbeiter:in ausgibt, den Betrug initiiert und die/der Konsument:in in der Folge eine Transaktion autorisiert. Allerdings besteht das Erstattungsrecht nur dann, wenn eine polizeiliche Anzeige vorliegt und die/der Konsument:in nicht grob fahrlässig war.

Das **Europäische Parlament** hat den Legislativvorschlag dahingehend erweitert, dass das Erstattungsrecht auch dann besteht, wenn **sich Betrüger:innen als Mitarbeiter:innen eines anderen Unternehmens – privat oder öffentlich – ausgibt.** Bei der Ablehnung des Erstattungsanspruchs soll die Bank der Behörde eine begründete Rechtfertigung übermitteln. Dieser Vorschlag ist zu begrüßen, denn in vielen Fällen würden Konsument:innen im Rahmen des von der Europäischen Kommission vorgeschlagenen neuen Rechtsrahmens keine Rückerstattung erhalten (z. B. Identitätsbetrug als Steuerbeamter/Polizist, Familienmitglied, Kollege, gefälschte Geschäfte/gefälschte Investitionsplattformen). Aus Konsument:innensicht gibt es zwischen diesen Fällen keinen Unterschied und daher es ist daher sachlich gerechtfertigt, dass es in allen Fällen eine Rückerstattung geben kann.

Die AK meint, dass diese Definition der Fahrlässigkeit dazu führen, dass die Banken sich in praktisch in allen Betrugsfällen von der Haftung befreien können. Im Jahr 2020 war der Wert der Schadenstragung durch Konsument:innen bei 68 %, 2022 stieg er auf 79 % und der aktuelle Wert mit den Zahlen des 1. Halbjahr 2023 beträgt 86 %. Durch diese vorgeschlagene Definition der groben Fahrlässigkeit steigt der Grad der Schadensfälle weiter an, in denen die betrogenen Konsument:innen den Schaden selbst tragen müssten.

**Die AK schlägt vor, dass die Ausgestaltung der gesetzlichen Vorgaben zur (groben) Fahrlässigkeit konsument:innenfreundlich ausgestaltet wird. So sollte im Erwägungsgrund 82 der Payments Services Regulation (PSR) folgendes festgelegt werden:**

*“Criteria to assess the degree of negligence should include the level of sophistication (e.g. use of spoofing, AI tools), the level of personalisation (e.g. prior data leaks allowing the fraudster to personalise the fraud attempt) and the individual characteristics of the consumer (e.g. digital skills, age, other factors of vulnerability).”*

AK-Textvorschlag zum Erwägungsgrund 82 auf Deutsch: „Zu den Bewertungskriterien des Grades der Fahrlässigkeit sollten der Grad der Raffinesse (z. B. Einsatz von Spoofing, KI-Tools), der Grad der Personalisierung (z. B. vorherige Datenlecks, die es dem Betrüger ermöglichen, den Betrugsversuch zu personalisieren) und die individuellen Merkmale der/des Verbraucherin/des Verbrauchers (z. B. digitale Fähigkeiten, Alter, andere Faktoren der Anfälligkeit) gehören.“

Die **Payment Services Regulation (PSR)** sieht weitere Maßnahmen vor, die zu begrüßen sind:

- Die Zahlungsdienstleister (Banken) haben **eine stärkere Transaktionsüberwachung** von Umsätzen von Kunden – im Sinne des Identifizierens verdächtiger bzw. missbräuchlicher Transaktionen – vorzusehen.
- Das Ziel von Artikel 83 PSR besteht darin, dass **missbräuchliche Zahlungen aufgespürt und vermieden werden**. Zu diesem Zweck soll der Informations- bzw Datenaustausch zwischen den Zahlungsdienstleistern bzw. Banken erleichtert werden.
- Außerdem soll es **stärkere Warnpflichten** durch die Banken über neue Betrugsformen an Konsument:innen geben. (Artikel 84).

## 4.4. SONSTIGE VORSCHLÄGE ZUR BETRUGSVERMEIDUNG

Weitere diskussionswürdige Punkte zur Betrugsvermeidung:

- Die **Europäische Bankenaufsicht (EBA)** soll ein Konzept erarbeiten, was unter grober Fahrlässigkeit zu verstehen ist.
- Verpflichtendes Angebot von Zahlungsdienstleistern und Banken **Bezahllimits** bei Zahlungsinstrumenten und Transaktionen anzubieten
- Einführung von **Cooling off-Perioden** nach Änderung von Bezahllimits, die von Konsument:innen initiiert wurden
- Die Banken sollen angehalten werden, massiv in die **Betrugsprävention** zu investieren. Die Banken sind dazu angehalten, dass sie angesichts der beträchtlichen Digitalisierungsgewinne auch nachweislich **Investitionen in die digitale Sicherheit** tätigen müssen.
- Die Finanzmarktaufsicht muss ausreichend **Ressourcen** erhalten, damit die Zahlungsdienstleister und Banken effektiv überwacht werden.
- Zahlungsinstrumente und Bezahlmethoden sollen sich an den **Bedürfnissen von Menschen** mit Beeinträchtigung orientieren. So soll es weitere Verbesserungen bei der starken Kundenauthentifizierung geben, um Barrieren für Menschen mit Behinderungen bzw. Beeinträchtigungen oder ohne Smartphone zu vermeiden.
- Die Banken sollen weiterhin **persönliche, effektive Beratung** anbieten, um nicht immer mehr Kund:innen bei den immer intensiver werdenden Digitalisierungsschritten zurückzulassen.

# 5. TIPPS FÜR KONSUMENT:INNEN[16]

- Kein Kreditkarteninstitut, keine Bank und kein seriöses Unternehmen fordert Sie per E-Mail, SMS oder Anruf auf, vertrauliche Zugangsdaten (Verfügernummer, PIN, Passwort etc.) preiszugeben.
- Überprüfen Sie stets die **Adressleiste Ihrer Bank etc. in Ihrem Browser**.
- Klicken Sie niemals auf **Links in einer dubiosen Textnachricht**. Versuchen Sie im Zweifelsfall stattdessen, die im Text genannte Information auf die Startseite Ihrer Bank, Kreditkartefirma, Organisation etc zu finden – tippen Sie jedoch nicht den angegebenen Link in der dubiosen Textnachricht in die Adresszeile des Browsers ein.
- Wenn Sie sich nicht sicher sind, **fragen Sie am besten telefonisch** bei Ihrer Bank, Kreditkartenfirma oder bei dem genannten Unternehmen (wie zB Amazon, Google, Post etc.) oder Organisation (zB Finanzamt, Sozialversicherung, Polizei etc.) nach. Verwenden Sie dafür die auf offiziellen Dokumenten, Websites etc angeführte Telefonnummer.
- Geben Sie **keinesfalls persönliche Daten wie Passwörter, Kreditkarten- oder Transaktionsnummern via E-Mail, SMS etc** preis.
- **Sobald Ihnen irgendetwas seltsam auf einer von Ihnen besuchten Website vorkommt**, beenden Sie die Verbindung sofort und kontaktieren Sie den regulären Website-Betreiber.
- **Starten Sie niemals einen Download-Link direkt aus einer Textnachricht** heraus, auf deren Echtheit Sie sich nicht hundertprozentig verlassen können. Starten Sie, wenn möglich, einen Download stets direkt von der Anbieter-Website/dem offiziellen App-Store für Ihr Endgerät.
- Öffnen Sie insbesondere niemals Dateien im **Anhang einer verdächtigen E-Mail**.
- Beenden Sie jede **Online-Session durch einen regulären Log-out** – statt einfach nur das Browserfenster zu schließen.
- Kontrollieren Sie regelmäßig den **Saldo Ihres Bankkontos sowie Umsätze** zum Beispiel von Internetzahlungsdienstleistern. So können Sie bei unbefugten Abbuchungen schneller reagieren.
- Geben Sie niemals persönliche Daten auf Webseiten mit unverschlüsselter Verbindung ein. Ob eine Website verschlüsselt mit Ihrem Browser kommuniziert, erkennen Sie an der Abkürzung **"https://"** in der Adresszeile sowie an dem kleinen Vorhängeschloss- Symbol neben der Adresszeile des Browsers.
- Achten Sie stets darauf, dass Ihre **Antivirus-Software aktuell und die Firewall aktiv** ist.
- Speichern Sie keine unbekannten Apps auf Ihrem Smartphone – darin kann sich ebenfalls Schadsoftware verbergen.
- Verhalten im Schadensfall bzw nach einem Betrug: Phishing und Trojaner | Arbeiterkammer Oberösterreich

- **Tipps zu Passwörtern**

- Speichern Sie **keine Passwörter im Browser** – diese könnten nämlich durch eine Schadsoftware, die auf Ihrem Endgerät installiert wurde, ausgelesen werden.

[16] Angelehnt an Quelle: (Deutsches) Bundesamt für Sicherheit in der Informationstechnik (BSI) - https://www.bsi.bund.de

- Besser Passwörter-Sätze – also die Anfangsbuchstaben in Groß-/Kleinschreibung eines prägnanten Satzes – also keine (durch Angriffssoftware leicht zu entschlüsselnden) Kurzpasswörter, die sich aus Namen und/oder Geburtsdatum zusammensetzen. Am besten jährlich ändern!“
- Verwenden Sie keine Passwörter doppelt.
- Verwenden Sie beim Online-Banking ein anderes System als für den täglichen Gebrauch
- Auf der Webseite www.phishen-impossible.at finden Sie die Videos, die aktuelle Phishing-Methoden aufgreifen

# KURZBIOGRAFIEN

## Mag. CHRISTIAN PRANTNER

Arbeiterkammer Wien / Abteilung Konsument:innenpolitik
Teamleiter Finanzdienstleistungen (Banken, Versicherungen)

Studium der Handelswissenschaften in Wien (Mag. rer. soc. oec.), Ausbildung als gewerblicher Vermögensberater und Hypothekarkreditvermittler, Versicherungskaufmann, Weiterbildung als Investmentfonds-Berater, gewerblich geprüfter Versicherungsmakler.

War zunächst Bankentester beim Verein für Konsumenteninformation (1992–2000), danach leitender Content-Redakteur bei Kurier-Online und trend-Online. Seit 2002 Referent für Bank- und Versicherungsdienstleistungen in der konsumentenpolitischen Abteilung der Arbeiterkammer Wien. Teamleiter Finanzdienstleistungen seit 2010.

Zuständig für www.bankenrechner.at; Stellungnahmen zu Verordnungen, Gesetzen und Gesetzesvorhaben im Finanzdienstleistungsbereich (nationale, EU), Studien, Vorträge und

Gremienarbeit zu Bank- und Versicherungsthemen aus Sicht der Verbraucher:innen; Beratung von Konsument:innen (Telefon, persönliche Beratung) in Fragen zu Finanzdienstleistungen; Öffentlichkeitsarbeit und Vertretung von Verbraucher:inneninteressen auf nationaler und internationaler Ebene (beratende Gremien der EU-Kommission): Mitglied in der Financial Services User Group (FSUG) in Brüssel von 1/2011 bis 11/2013 sowie Mitglied im Crowdfunding-Stakeholderforum (ECSF) in Brüssel.

## Mag.ª BENEDIKTA RUPPRECHT, BA

Arbeiterkammer Wien / Abteilung Konsument:innenpolitik, Team Finanzdienstleistungen (Banken, Versicherungen)

Studium der Rechtswissenschaften und Kunstgeschichte an der Universität Wien. Seit 2007 Referentin in der konsumentenpolitischen Abteilung der Arbeiterkammer Wien im Bereich Finanzdienstleistungen. Primär zuständig für Stellungnahmen zu Verordnungen, Gesetzen und Gesetzesvorhaben im Finanzdienstleistungsbereich (nationale, EU), Studien, Gremienarbeit zu Bank- und Versicherungsthemen aus Sicht der Verbraucher:innen. Unterstützende Tätigkeit bei der Zuführung von Verbraucheranliegen zur gerichtlichen Klärung.

## Mag. ARIF KAYA

Arbeiterkammer Wien / Abteilung Konsument:innenpolitik,
Team Finanzdienstleistungen (Banken, Versicherungen)

Studium der Rechtswissenschaften in Wien (Mag. iur.), Schwerpunktausbildung im Banken- und Versicherungsrecht.

Nach Absolvierung der Gerichtspraxis und einer Verwaltungspraxis im Finanzamt (Fachbereich) von 2016 bis 2019 als „In-House“ Jurist in einer Rechtsschutzversicherung tätig. Von 2019 bis 2023 beim Verein VertretungsNetz zunächst als Erwachsenenvertreter und zuletzt als Mitarbeiter in der Rechtsabteilung überwiegend für versicherungsrechtliche Agenden zuständig.

Zuständig für Stellungnahmen zu Verordnungen, Gesetzen und Gesetzesvorhaben im Finanzdienstleistungsbereich (nationale, EU), Studien, Gremienarbeit zu Bank- und Versicherungsthemen aus Sicht der Verbraucher:innen; Beratung von Konsument:innen (Telefon, E-Mail und persönliche Beratung) in Fragen zu Finanzdienstleistungen; Öffentlichkeitsarbeit und Vertretung von Verbraucherinteressen auf nationaler Ebene, sowie unterstützende Tätigkeit bei der Zuführung zur gerichtlichen Klärung von Verbraucheranliegen.

**ALLE RATGEBER ZUM DOWNLOADEN**
https://wien.arbeiterkammer.at/service/Ratgeber/index.html

**BERATUNGSTERMIN VEREINBAREN UNTER**
https://wien.arbeiterkammer.at/ueberuns/kontakt/index.html

**ALLE STUDIEN ZUM DOWNLOADEN**
https://emedien.arbeiterkammer.at/

**WEITERE SERVICES UND INFORMATIONEN UNTER**
https://wien.arbeiterkammer.at/

**FOTOCREDITS**
Porträtfotos Christian Prantner, Benedikta Rupprecht, Arif Kaya: © Lisi Specht

**DER DIREKTE WEG ZU UNSEREN PUBLIKATIONEN**
https://wissenschaft.arbeiterkammer.at/
https://emedien.arbeiterkammer.at/

**ZITIERFÄHIGER LINK ZUR STUDIE**
https://emedien.arbeiterkammer.at/resolver?urn=urn:nbn:at:at-akw:g-7135698

**CREATIVE COMMONS CC BY-SA**
Sofern nicht anders ausgewiesen, steht der Inhalt dieses Werks unter der Creative Commons Lizenz CC BY-SA 4.0 zur Verfügung: https://creativecommons.org/licenses/by-sa/4.0/deed.de

Bei Verwendung von Textteilen wird um Zusendung eines Belegexemplars an die AK Wien / Abteilung Konsument:innenpolitik ersucht.

**IMPRESSUM**
Medieninhaberin: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65 0
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Auftraggeberin: AK Wien / Abt. Konsument:innenpolitik
Rückfragen an: Christian Prantner (christian.prantner@akwien.at)
Gestaltung: Alexander Ullrich | A SQUARED
Verlags- und Herstellungsort: Wien
Druck: AK Wien
ISBN: 978-3-7063-1137-3
© 2025 AK Wien

# UNSER SERVICE FÜR IHR RECHT

Was bleibt netto von brutto?
Wie behalte ich den Überblick über Arbeitszeiten?
Oder was muss ich über meinen Mietvertrag wissen?
Ob durch unsere Services, Ratgeber oder unser Expertenteam in Ihrer Arbeiterkammer:
Wir helfen Ihnen weiter!

**Klicken Sie rein:** wien.arbeiterkammer.at







AK WIEN
GERECHTIGKEIT MUSS SEIN

# MASSNAHMENPAKET GEGEN PHISHING

**Betrug an Bankkund:innen**

Mai 2025

9 783706 311373