Bundesministerium
Inneres

Bundeskriminalamt

PSA

# Gemeinsam gegen Phishing

## Plattform gegen Datendiebstahl im Internetbetrug



**INHALT**


| | |
|---|---|
| Vorwort | 3 |
| Intro **„Globale Herausforderung“** | 4 |
| Intro **„Immer einen Schritt voraus sein“** | 5 |
| Vortrag **„So viel wie möglich verhindern“** | 6 |
| Vortrag **„Die Wenigsten lesen, worauf sie klicken“** | 8 |
| Vortrag **„Opfer sind nicht dumm“** | 10 |
| Vortrag **„Social Engineering und Phishing mit SMS-Nachrichten“** | 12 |
| Vortrag **„Wenn der Käufer Betrüger ist“** | 14 |
| Vortrag **„Fallen erkennen, Bewusstsein stärken“** | 16 |
| Podiumsdiskussion | 18 |
| Ausblick & Agenda **„Wir müssen das Team erweitern!“** | 20 |


Der vorliegende Phishing Report präsentiert Ergebnisse und Befunde von Expertinnen und Experten, die bei der von Bundesministerium für Inneres/Bundeskriminalamt und PSA Payment Services Austria GmbH am 23. November 2023 im Bundeskriminalamt veranstalteten Auftaktkonferenz der Plattform gegen Datendiebstahl im Internetbetrug referiert haben.

# Mehr Kompetenz, bessere Prävention



Die wirksamsten Mittel im entschlossenen Vorgehen gegen den Internetbetrug sind Prävention und Aufklärung. Genau dieses Ziel verfolgen wir im Rahmen der neuen Plattform gegen Datendiebstahl im Internetbetrug. Im Fokus der Plattform steht vor allem am Beginn die enge Vernetzung zwischen Banken und der Polizei. Gemeinsam wollen und werden wir die Österreicherinnen und Österreicher bestmöglich vor Phishing schützen.

Das Thema Internetkriminalität ist jener Bereich, dem wir im Innenressort – neben dem Bereich Extremismus und dem Kampf gegen Schlepperei – auch im Rahmen der Kriminaldienstreform besondere Aufmerksamkeit widmen. In Zusammenarbeit mit dem Cybercrime Competence Center (C4) im Bundeskriminalamt und mit Cybercrime-Trainings-Centern in allen Bundesländern wird die Polizei bereits in der Grundausbildung viel stärker für diesen wichtigen Bereich geschult. Auch während des Dienstes wird es Fortbildungen geben. Kompetenz und Vernetzung sind im Kampf gegen Internetbetrug entscheidend.

**GERHARD KARNER**
Bundesminister für Inneres
der Republik Österreich

# Österreich noch sicherer machen



Als Payment Services Austria betreiben wir schon seit Jahren die Bezahlplattformen der Banken, egal ob es um Kartenzahlungen, Überweisungen oder Bargeldbehebungen geht. Natürlich kümmern wir uns auch um die Sicherheit der Systeme. Nicht nur um die technische Sicherheit, sondern auch, dass die Produkte sicher verwendet werden können. Dafür überprüfen und verbessern wir unsere Sicherheitssysteme fortwährend und teilen die Erfahrungen mit den Sicherheitsbehörden. Umgekehrt nehmen wir die Gelegenheit wahr, um die neuesten Erkenntnisse der Ermittler aus erster Hand zu erfahren. In diesem Sinn haben wir nun auch gemeinsam mit dem Bundesministerium für Inneres und den heimischen Banken die Plattform gegen Daten-Phishing ins Leben gerufen. Der Anti-Phishing-Gipfel und die gemeinsame Plattform gegen Phishing schaffen wertvolle Grundlagen für ein sicheres, digital erfolgreiches Österreich. Nur durch einen Schulterschluss aller Beteiligten kann es gelingen, die Gefahren für alle sichtbar zu machen und Gegenmaßnahmen zu kommunizieren. So verhindern wir, dass Menschen durch Betrügereien im digitalen Raum geschädigt werden.

**HARALD FLATSCHER**
Geschäftsführer
PSA Payment Services Austria GmbH

# Globale Herausforderung



Die Auswirkungen der Digitalisierung zeigen sich in nahezu allen Lebensbereichen. Damit einhergehende Technologien und deren positive Effekte sind aus unserem Alltag nicht mehr wegzudenken. Bringt dieser Fortschritt sicherlich viel Gutes mit sich, muss man frei nach Goethe leider auch feststellen, dass viel Licht auch viel Schatten bringt. Die digitale (Schatten-)Welt wird auch für kriminelle Aktivitäten genutzt. Der vermeintliche Deckmantel der Anonymität und die Möglichkeit, eine Vielzahl von Menschen mit einem Mouseclick zu kontaktieren, führen dazu, dass sich Straftäter zusehends in der virtuellen Welt bewegen. Die Internetkriminalität – Cybercrime – ist ein globales Problem, welches auch vor Österreich keinen Halt macht. Im Jahr 2022 verzeichneten wir rund 60.000 Anzeigen von Delikten, die in Zusammenhang mit dem Internet standen – Tendenz steigend.

Eines dieser neu aufgetretenen Phänomene, die mittlerweile schon zu einem Teil unseres Alltags wurden, ist das sogenannte Phishing. Wie ein Angler fischen die Täter im digitalen Raum nach potenziellen Opfern und deren Passwörtern. Der von ihnen ausgeworfene Köder wird dahingehend angepasst, dass er für die jeweilige Zielgruppe besonders attraktiv ist oder diese auf einer anderen Ebene anspricht. Sei es in Form einer Nachricht eines Paketzustellers, der zusätzliche Daten benötigt, die Bank, die Ungereimtheiten bei Kontobewegungen festgestellt habe, oder das Finanzamt, das über vermeintliche Steuerschulden informiert. Das sind nur einige der zahlreichen Varianten, die aber alle eines gemein haben: Auf täuschend echten Internetseiten sollen sie die Opfer dazu verleiten, ihre Daten, zumeist Bankdaten und Passwörter, anzugeben, um diese anschließend missbräuchlich zu verwenden und widerrechtliche Buchungen durchzuführen.

Die Mitarbeiterinnen und Mitarbeiter des Bundeskriminalamtes und der gesamten Kriminalpolizei in Österreich stehen tagtäglich im Einsatz – gehen sozusagen im Internet auf Streife –, um die Täter auszuforschen. Wichtig ist es jedoch, präventiv zu informieren und aufzuklären. Lassen Sie uns deshalb gemeinsam gegen diese Form der Kriminalität vorgehen. Gemeinsam mit anderen Stakeholdern stehen wir der Bevölkerung als starker Partner zur Seite und werden weiter vehement und entschlossen gegen jegliche Form der Kriminalität vorgehen. Denn das beste Delikt ist und bleibt jenes, das nie passiert ist.

**ANDREAS HOLZER**
Direktor Bundeskriminalamt

# Immer einen Schritt voraus sein



Sicherheit wird im Banksektor traditionell großgeschrieben. Das gilt auch für die Herausforderungen durch Phishing. Wir müssen das Finanzsystem gegen Phishing-Attacken und Online-Betrug verteidigen. Individuelle Anstrengungen – „jeder für sich" – reichen hier längst nicht mehr aus.

Nur durch intensive brancheninterne und branchenübergreifende Zusammenarbeit können wir effektive Maßnahmen gegen Cyberkriminalität durchsetzen und den Schaden minimieren. In einer zunehmend digitalisierten Wirtschaft ist diese Zusammenarbeit entscheidend. Innerhalb des Finanzsektors tauschen wir daher laufend Erkenntnisse, Strategien und Best Practices aus. Und darüber hinaus intensivieren wir die Zusammenarbeit über Branchengrenzen hinweg, um gemeinsame Lösungen zu entwickeln. Außerdem stärken wir unseren kollektiven Schutzschild durch die bereits heute sehr enge Zusammenarbeit mit den Strafverfolgungsbehörden. Denn nur gemeinsam können wir Lücken in unserer Verteidigungsstrategie schließen, Bedrohungen frühzeitig erkennen und möglichst vielen Tätern das Handwerk legen. Jeder einzelne Stakeholder spielt eine entscheidende Rolle in der gemeinsamen Verteidigung gegen Phishing und Online-Betrug. Die Plattform gegen Datendiebstahl im Internetbetrug ist dafür eine hervorragende Grundlage. Denn wir brauchen eine übergreifende Initiative und einen starken Austausch mit Strafverfolgungsbehörden und den Telekom-Unternehmen. Es geht darum, wie wir gemeinsam noch stärker zur Sensibilisierung für Phishing beitragen können und rascher Antworten auf künftige Herausforderungen finden. Mit dem vorliegenden Phishing Report wird ein wichtiger und sichtbarer Beitrag geleistet, um Erfahrungsaustausch und Vernetzung wichtiger Akteure beim Thema Phishing zu ermöglichen. Unser gemeinsames großes Ziel ist klar: Wir müssen den Cyberbedrohungen immer einen Schritt voraus sein und dem Vertrauen unserer Kundinnen und Kunden gerecht werden.

**ROBERT ZADRAZIL**
Stellvertretender Obmann der Bundessparte Bank und Versicherung der Wirtschaftskammer Österreich, Präsident des Bankenverbandes und CEO der UniCredit Bank Austria

ÖSTERREICH & EUROPA

# „So viel wie möglich verhindern.“

Was sind die gängigen Vorgangsweisen der Kriminellen? Ein Überblick über Phishing in Österreich und Europa von Manuel Scherscher und Horst Hakala vom Bundeskriminalamt.

60.195 Cybercrime-Delikte wurden in Österreich im Jahr 2022 angezeigt, die Hälfte davon entfällt auf das Thema Internetbetrug. Im November 2023 wurden bereits rund 90.000 Betrugsanzeigen verzeichnet.

Der Cybercrime-Gesamtschaden 2022 betrug rund 700 Millionen Euro. Fachleute gehen von einer Dunkelziffer von 90 bis 95 Prozent im Betrugsbereich aus.

***„Früher mussten Täter programmieren können, heute kann man sämtliche Komponenten im Darknet kaufen.“***

Aktuell beobachten wir rund 57 unterschiedliche Betrugsphänomene. Eines davon ist das sogenannte Phishing, das heuer einen Schaden von 24 Millionen Euro verursachen wird – Tendenz steigend.

## Formen von Phishing

Phishing bedeutet vor allem „Passwort-Fishing“. Es geht um das Herauslocken von Bank- und Kreditkarten-Daten, um damit Geld zu beheben.
Es gibt mehrere Varianten:

- Beim **klassischen Phishing** wird man dazu gebracht, auf Fake-Websites seine Daten einzugeben.
- Bei **Voice-Fishing („Vishing“)** wird man telefonisch dazu gebracht, Daten bekanntzugeben. Der Anrufer täuscht dazu vor, jemand anderer zu sein (z. B. Polizist, Bankmitarbeiter). Mittlerweile werden auch Stimmen unter Verwendung von Künstlicher Intelligenz nachgemacht.
- **Smishing** ist das Abfischen von Daten mittels SMS.

Die Modi der Täter wechseln sehr rasch. Früher mussten Täter programmieren können, heute kann man sämtliche Komponenten im Darknet kaufen. Phishing wird von den Tätern situationselastisch angepasst, etwa beim Black-Friday- oder im Weihnachtsgeschäft.



**24 Millionen Euro**
betrug 2023 der Schaden durch Phishing

### PHISHING AUF EINEN BLICK



Phishing ist der Versuch, über gefälschte Kommunikationswege (gefälschte Webseiten, E-Mails oder Kurznachrichten) sensible (persönliche) Informationen der Internetbenutzer zu erlangen.



Phishing stellt nicht nur ein technisches, sondern auch ein soziales Problem dar, da es auf die Manipulation und Ausnutzung menschlicher Schwächen abzielt.



Phishing ist ein internationales Phänomen. Darum ist die Notwendigkeit einer grenzüberschreitenden Zusammenarbeit zentral.

### AKTUELLE ERSCHEINUNGSFORMEN

- **Vishing**
  Amazon Security, Bankangestellter
- **Phishing**
  Fake-Seiten-Bank, Gewinnspiele
- **Smishing**
  Tochter/Sohn-Modus, Bezahllink, Paketzustellung, Bankenlinks
- **Dunkelziffer**
  Bank- und CC-Abbuchungen

## Kriminelle Dienstleister

Wer sind die Täter? Sie sind „Digital Natives“ zwischen 18 und 30 Jahren, semiprofessionell und haben hohe kriminelle Energie. Geografisch halten sich die Täter im Norden bzw. nordöstlichen Europa in digitalaffinen Ländern auf. Diese Angreifer sind aber nicht primäres Ziel der Ermittlungen, sondern Gruppen, die kriminelle Dienstleistungen zur Verfügung stellen. Es werden Domains, Simcards, Phishing-Seiten oder gefälschte Identitäten im Darknet angeboten. Für die Bekämpfung dieser Gruppen ist die Kooperation mit Europol von besonderer Bedeutung.

***„Man kann Bits und Bytes nur mit Bits und Bytes bekämpfen.“***

## Technische Tools und Prävention entscheidend

Zwei Erkenntnisse sind beim Kampf gegen Phishing besonders wichtig:

- **Man kann Bits und Bytes nur mit Bits und Bytes bekämpfen.** Dies erfordert entsprechende technische Tools. Gerade Künstliche Intelligenz und Deepfakes sind von großer Bedeutung und werden der Kriminalität einen weiteren Boost verleihen.

- **Der Prävention kommt sehr große Bedeutung zu.** Man kann Internetkriminalität nicht ganz aufklären, aber so viel wie möglich davon verhindern. Der Anti-Phishing-Gipfel und die Plattform gegen Datendiebstahl im Internetbetrug sind ein wichtiger Beitrag dafür.

**Manuel Scherscher**
Leiter der Abteilung für Wirtschaftskriminalität des Bundeskriminalamtes





*Dieser Vortrag wurde von Horst Hakala erstellt und von seinem Kollegen Manuel Scherscher vorgetragen.*

**Horst Hakala**
Leiter Lagebild Betrug
Bundeskriminalamt

### GEMEINSAM GEGEN PHISHING: DARAUF KOMMT’S AN!

**Aufklärung und Bewusstseinsschaffung**
Aufklärung ist entscheidend im Kampf gegen Phishing. Es ist wichtig, dass sowohl Privatpersonen als auch Unternehmen über die verschiedenen Formen von Phishing informiert sind. Dazu gehören Schulungen über sichere Online-Praktiken, das Erkennen von verdächtigen E-Mails oder Nachrichten und das sichere Verwalten von persönlichen Daten.

**Technologische Sicherheitsmaßnahmen**
Die Implementierung und Aktualisierung von technischen Sicherheitsmaßnahmen sind unerlässlich. Dies umfasst den Einsatz von Anti-Phishing-Software, regelmäßige Sicherheitsupdates und das Einrichten von Filtersystemen, die verdächtige E-Mails, SMS und sonstige Nachrichten erkennen und blockieren können.

**Internationale Zusammenarbeit**
Phishing ist ein grenzüberschreitendes Problem, das internationale Zusammenarbeit und Informationsaustausch erfordert. Behörden, Unternehmen, NGOs und Sicherheitsfirmen müssen zusammenarbeiten, um Informationen auszutauschen, gemeinsame Standards zu entwickeln und effektive Gegenmaßnahmen zu koordinieren.



ENTWICKLUNGEN & TRENDS

# „Die Wenigsten lesen, worauf sie klicken.“

Gegen eine Transaktion, die vom Opfer „gewollt“ wird, kann auch ein gut konzipiertes Sicherheitssystem wenig ausrichten: Robert Schischka von nic.at und CERT.at über Entwicklungen und Trends rund um Phishing.

Bei Phishing geht es in der Regel um eine Betrugshandlung oder deren Vorbereitung. Im Fokus steht nicht zwangsläufig ein technischer Ansatz. Für einen „guten Betrug“ braucht man eine „gute Geschichte“. Rein technische Maßnahmen dagegen greifen oft zu kurz. Es geht meistens um die Erlangung von Zugangs- und Identitätsdaten bzw. um das Installieren von Schadsoftware auf Geräten, um diese unter Kontrolle zu bringen. Sehr viele Betrugshandlungen nutzen Vertrauensbeziehungen aus. Man bekommt z. B. scheinbar ein Mail von seinem sehr guten Freund. Erpressung mit Ransomware beginnt mit einer unachtsam angeklickten Mail und ist mittlerweile ein Wirtschaftsfaktor in Österreich.

***„Für einen ‚guten Betrug‘ braucht man eine ‚gute Geschichte‘.“***

## Arbeitsteilige Tätergruppen

Phishing ist kein wirklich neues Thema. Es gab dieses Phänomen schon lange vor der Verbreitung des Internets. Per Mail verbreitete sich Phishing in den 1990er Jahren. Ein nächster Schritt war die Verbreitung von Schadsoftware, sogenannten Trojanern. Davon waren besonders Banken betroffen. Die Branche hat als erste auch die Bedeutung einer engen Kooperation und des Informationsaustauschs gegen Internetbetrug verstanden. In der Folge haben sich Spear-Phishing – das gezielte Heraussuchen von Zielgruppen – sowie Whaling entwickelt. Tätergruppen nehmen sich dabei Zeit, sich mit dem beruflichen und familiären Hintergrund von potenziellen Opfern genau auseinanderzusetzen. Diese Tätergruppen handeln auch arbeitsteilig. Es gibt Täter, die Werkzeuge bereitstellen oder vermieten, während andere Massenmails aussenden oder sich um hochkarätige Opfer „kümmern“.



**In den 1990er**
Jahren verbreitete sich Phishing per Mail

## Es geht um Vertrauen

Im Kern geht es um Vertrauen. „Social Engineering“ ist der erfolgversprechendste Angriff. Das zeigt sich etwa am Telefonbetrug mit Voice-over-IP-Technolo-

gie. Ein aktueller Trend ist die Nutzung von QR-Codes: Dahinter steht die Unmöglichkeit für Nutzer, einen Link zu prüfen. Die wenigsten Menschen sehen, dass sie an diesem Punkt schon ein Problem haben können. Täter springen auf Entwicklungen auf, wie etwa auf die Nutzung von QR-Codes im wirtschaftlichen Umfeld oder von WhatsApp im Familienumfeld. Auch eine schlecht formulierte Nachricht, die jedoch vorgibt, von einem Freund oder Familienmitglied zu kommen, oder die sich gar auf eine vorangegangene Kommunikation bezieht, hat eine hohe Erfolgswahrscheinlichkeit, wenn sie der Erwartungshaltung und Gewohnheiten des Opfers entspricht.

Letztlich geht es um die Frage, welcher Aufwand von den Tätern getrieben wird, um eine Geschichte zu erzählen. „Mir kann das nicht passieren" ist jedenfalls ein beliebter Denkfehler.

### Pflicht zur Sorgfalt vermitteln

Eine „erfolgreiche" Schadsoftware war Emotet – nicht unbedingt deshalb, weil sie technisch so hochstehend war, sondern weil sie einen perfiden Trick genutzt und die soziale Komponente mitgedacht hat: Sie hat Adressbücher und bestehende Geschäftskommunikation dazu verwendet, neue Beziehungen herzustellen. Das Phishing-Mail setzte auf eine vorher tatsächlich erfolgte (legitime) Kommunikation mit dem eigentlichen Opfer auf. In der Folge wurden Betroffene u. a. aufgefordert, eine andere Kontonummer zu verwenden.

Multifaktor-Authentifizierung ist heute in aller Munde. Die Frage, ob sie vor solchen Betrugsfällen schützt, ist mit „Jein" zu beantworten. Ohne Multifaktor-Authentifizierung hat man heute schon verloren – aber leider wähnen sich viele mit der Verwendung schon allzu sicher. Auch die Täter haben sich darauf eingestellt und bringen Opfer dazu, den zweiten Faktor bekanntzugeben. Die wenigsten Menschen lesen, worauf sie klicken. Man kann das mit Authentificator-Apps verbessern, wo man nicht einfach „Ja" klickt, sondern eine Nummer eingibt. Aber auch das ist nicht hundertprozentig sicher. **Die Zwei-Faktor-Authentifizierung entbindet Mitarbeiter und Kunden nicht davon, sorgfältig zu sein.**

**Robert Schischka**
Geschäftsführer
nic.at & CERT.at



***„Mir kann das nicht passieren' ist jedenfalls ein beliebter Denkfehler."***

### Zusammenarbeit und Informationsaustausch wirken

Der Verteidiger im Internet ist immer im Nachteil, er muss daher immer erfolgreich sein. Oft ist der Informationsaustausch für Verteidiger aus rechtlichen Gründen (DSGVO) nicht möglich. Tatsächlich muss man aber sehr schnell handeln können – und daher muss auch der Informationsaustausch weiter vorangetrieben werden. Zusammenarbeit und Informationsaustausch sind die wichtigsten Waffen gegen immer neue Betrugsmuster.

### DIE DREI WICHTIGSTEN PRIORITÄTEN IM KAMPF GEGEN PHISHING

- **breite Awareness und Aufklärung** in der Bevölkerung
- **bestmögliche Absicherung aller Online-Zugänge** durch Multifaktor-Authentifizierung als Mindeststandard
- **Kooperation und rascher Informationsaustausch** auf allen Ebenen (Finanz- und Telekommunikationsdienstleister, CERTs, Polizei, Konsumentenschutz, Watchlist Internet etc.)

KOMMUNIKATION & VERHALTEN

# „Opfer sind nicht dumm.“

Warum funktioniert Phishing? Wirtschaftskriminal- und Verhaltensanalytikerin Patricia Staniek erklärt im Interview die Hintergründe von Social Engineering.



**Wie funktioniert Social Engineering aus Sicht der Verhaltensanalyse?**
*Staniek:* Amateure hacken Systeme – Profis hacken Menschen: Darum geht es beim Social Engineering. Phishing-Betrüger arbeiten mit Zeitdruck, bauen also die Dringlichkeitsfalle ein. Sie nutzen Angststrategien, um Menschen zu schnellen Handlungen zu bewegen. Sie zielen darauf ab, persönliche Informationen wie Passwörter, Kreditkarteninformationen oder Bankdaten von ahnungslosen Empfängern zu erwirken. Was passiert, kann man als „Brainfucking“ bezeichnen.

***„Amateure hacken Systeme – Profis hacken Menschen.“***
*Bruce Schneier*

**Warum funktioniert das?**
*Staniek:* Die Betrüger sind oft psychologisch geschult und verwenden vorgefertigte Gesprächsleitfäden. Sie wissen genau, welche Taktik sie einsetzen müssen, um die Opfer in die Zielrichtung zu bewegen, um diese letztendlich vollkommen skrupellos abzuzocken.

***„Die meisten Opfer sind nicht dumm. Sie kennen lediglich die Betrugsmethoden nicht.“***

Der Mensch muss sich nicht vor der Technologie fürchten, sondern vor der Strategie. Die meisten Opfer sind nicht dumm. Sie kennen lediglich die Betrugsmethoden nicht. Wer weder die Betrugsform noch die Betrugsmethode kennt, lässt sich leicht über den Tisch ziehen.

**Was ist aus Ihrer Sicht für die Prävention wichtig?**
*Staniek:* Eigensicherheit ist ein wichtiges Thema. Prävention funktioniert dann, wenn wir nicht über etwas reden, sondern mit jemand reden – mit den Zielgruppen. Jeder hat eine Tante oder eine Oma oder andere, die betroffen sein können.

Nicht nur Naivität und Leichtgläubigkeit, auch autoritätshörige „People Pleaser“ und wenig internet- oder handyaffine Menschen sind gefährdet. Phisher und Hacker haben gute, geschulte Menschenkenntnisse. Sie wissen, was zu tun ist, wenn ein Opfer am Telefon so oder so reagiert.



**Welche Ansatzpunkte sind im Kampf gegen Phishing wichtig?**
*Staniek:* Wir brauchen erstens Sensibilisierung, Aufklärung und Schulung. Umfassende Schulungen für Mitarbeiter und die Öffentlichkeit sind entscheidend, um das Bewusstsein für Phishing-Angriffe zu schärfen.

Zweitens geht es um technologische Lösungen. Innovative Sicherheitslösungen, wie Anti-Phishing-Tools und E-Mail-Authentifizierungstechnologien, sind unerlässlich. Ein Vorteil der Künstlichen Intelligenz: Sie kann helfen, Muster von Phishing-Angriffen zu identifizieren.

Und drittens ist Zusammenarbeit und Infosharing zentral. Eine enge Zusammenarbeit zwischen Unternehmen, Behörden und Sicherheitsexperten ist von entscheidender Bedeutung für schnellere Reaktionen und präventive Maßnahmen.

**Was konkret bringt die bessere Zusammenarbeit im Kampf gegen Phishing?**
*Staniek:* Eine verbesserte Zusammenarbeit im Kampf gegen Phishing birgt zahlreiche Vorteile. Erstens ermöglicht sie einen effektiven Informationsaustausch über aktuelle Bedrohungen und Angriffsmuster.

Zweitens fördert sie die Entwicklung und Implementierung gemeinsamer Sicherheitsstandards, die die Widerstandsfähigkeit gegenüber Phishing erhöhen.

**Mag. Patricia Staniek**
Wirtschaftskriminal- und Verhaltensanalytikerin, BSc Betriebswirtin für Wirtschaftskriminalistik/-kriminologie, Certified Master Profiler & Ausbildnerin, Akademische Expertin für internationale Sicherheitsmanagements



***„Prävention funktioniert dann, wenn wir nicht über etwas reden, sondern mit jemand reden – mit den Zielgruppen."***

Drittens ermöglicht sie eine koordinierte Nutzung von Ressourcen und Expertise, um innovative Lösungen zu entwickeln. Insgesamt schafft eine verbesserte Zusammenarbeit eine robustere Verteidigung gegen Phishing-Angriffe, was sowohl Unternehmen als auch die breite Öffentlichkeit schützt.



BEISPIELE & TIPPS

# Social Engineering und Phishing mit SMS-Nachrichten

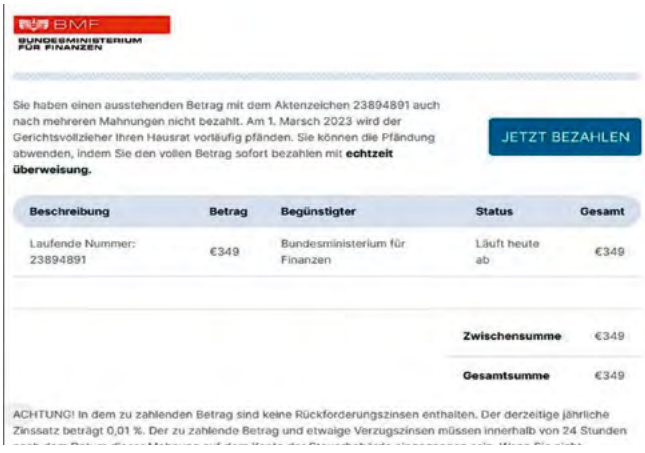
SMS-Phishing („Smishing“) ist ein vergleichsweise neuer Trend, der auch die Bankenwelt betrifft. Wolfgang Schwabl, CSO A1 Telekom Austria AG und Vorsitzender der Cyber Sicherheit Plattform des Bundeskanzleramtes, sowie Andreas Schaupp, Group CISO der BAWAG Group, haben dazu beim Anti-Phishing-Gipfel Fallbeispiele und Gegenmaßnahmen präsentiert.

**Beispiel: Das Finanzamt-SMS**

Dabei sind zwei Varianten zu beobachten. Eine Variante verspricht dem Empfänger eine Steuergutschrift. Wer auf den entsprechenden Link klickt, soll für die Gutschrift alle relevanten Kontodaten eingeben. Die andere Variante bezieht sich auf eine Forderung mit hoher Dringlichkeit. Um z. B. den Besuch des Gerichtsvollziehers zu vermeiden, soll man auf den übermittelten Link klicken und den entsprechenden Betrag bezahlen. Der „Bezahlen“-Button führt zu Banken. **Man loggt sich in das eigene Konto ein – und bezahlt eine Steuerschuld, die es gar nicht gibt.**

*Beispiel einer Forderung*

[FINANZAMT] Ihre offene Forderung mit der Nummer 23894891 wurde trotz mehrerer Mahnungen nicht beglichen. Am 28 Februar 2023 wird der Gerichtsvollzieher vorsorglich Ihren Hausrat pfänden. Sie können das Pfändungsverfahren vermeiden, indem Sie den vollen Betrag sofort über Ihren Zahlungslink bezahlen. https://finanzen-bundesministerium.info/BMF/23894891/


BMF
BUNDESMINISTERIUM FÜR FINANZEN

Sie haben einen ausstehenden Betrag mit dem Aktenzeichen 23894891 auch nach mehreren Mahnungen nicht bezahlt. Am 1. Marsch 2023 wird der Gerichtsvollzieher Ihren Hausrat vorläufig pfänden. Sie können die Pfändung abwenden, indem Sie den vollen Betrag sofort bezahlen mit **echtzeit überweisung.**

JETZT BEZAHLEN

| Beschreibung | Betrag | Begünstigter | Status | Gesamt |
|---|---|---|---|---|
| Laufende Nummer: 23894891 | €349 | Bundesministerium für Finanzen | Läuft heute ab | €349 |

| | |
|---|---|
| **Zwischensumme** | €349 |
| **Gesamtsumme** | €349 |

ACHTUNG! In dem zu zahlenden Betrag sind keine Rückforderungszinsen enthalten. Der derzeitige jährliche Zinssatz beträgt 0,01 %. Der zu zahlende Betrag und etwaige Verzugszinsen müssen innerhalb von 24 Stunden

## KAMPF GEGEN SMS-PHISHING: DARAUF KOMMT ES AN

**1. Sensibilisierung aller Beteiligten,** dass Phishing mittels SMS nicht nur die Banken betrifft, sondern ein Problem für unterschiedliche Industrien und die Gesamtbevölkerung ist – und als Initial-Vektor für verschiedene Social-Engineering-Angriffe wie „Hallo Mama/Papa" und Fake-Call-Center-Betrüge dient

**2. Wille zur Zusammenarbeit zwischen den Organisationen,** deren Kunden davon betroffen sein können (z. B. Finanzbranche, Telekommunikationsunternehmen, Logistikunternehmen, Cert.at)

**3. Schaffung einer rechtlich abgesicherten Möglichkeit für Telekommunikationsunternehmen,** die zahlreichen Spam- und Phishing-SMS nicht zustellen zu müssen bzw. blockieren zu dürfen

**4. Rechtssicherheit,** insbesondere beim Austausch von Fraud-relevanten Daten (z. B. zwischen Bankinstituten untereinander und mit Telekommunikationsunternehmen)

**5. Verbesserung bzw. Optimierung der Zusammenarbeit** Finanzindustrie mit der Exekutive bei erfolgten Betrugsfällen

**6. Entwicklung von Methoden für den Opferschutz** bei Identitätsklau



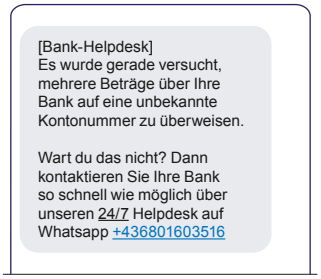
**Wolfgang Schwabl**
CSO A1 Telekom Austria AG
und Vorsitzender der Cyber Sicherheit Plattform (CSP)
des Bundeskanzleramtes

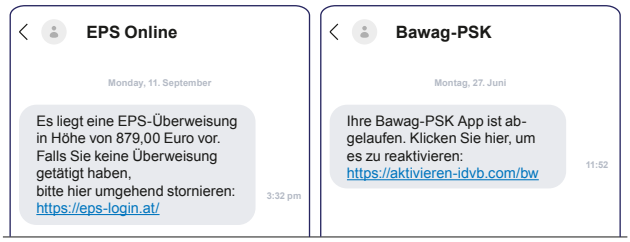


**Andreas Schaupp**
Group CISO der BAWAG Group

### Beispiel: Der direkte SMS-Angriff

Bei direkten Angriffen auf Bankkunden kommen neben E-Mails vermehrt SMS- oder auch WhatsApp-Nachrichten zum Einsatz. Angreifer besorgen sich gehackte, gültige Telefonnummern, die im Darknet gehandelt werden. Die Angreifer erwecken den Eindruck, dass die Nachricht direkt von der eigenen Bank oder von einem Logistikunternehmen kommt. Manche SMS verfügen über korrekt wirkenden Absendernamen statt der sendenden Telefonnummer. Im Idealfall für die Angreifer werden SMS-Nachrichten am empfangenden Smartphone in den SMS-Chatverlauf der jeweiligen Institution (z. B. Bank oder Logistikunternehmen) eingegliedert. Die Kunden denken, dass diese SMS legitim sein muss. Um offenbar falsche Überweisungen zu stornieren oder einen kleinen Kostenbetrag für eine Lieferung zu bezahlen, wird der Kunde aufgefordert, auf einen entsprechenden Link zu klicken – wo er in der Folge dann alle Bank- oder Kreditkartendaten selbst bekanntgibt.






***„Angreifer besorgen sich gehackte, gültige Telefonnummern, die im Darknet gehandelt werden.“***



**Beispiel: Smishing & Vishing**

Eine Kombination aus Smishing und Vishing startet ebenfalls mit dem Empfang einer SMS, die offenbar von der eigenen Bank stammt. Dabei werden Namen und Telefonnummer abgefragt. Der Angreifer ruft den Kunden „zurück“ und ersucht um Identifikation mit der Verfügernummer. Mit den Daten loggt sich der Angreifer ein und bereitet eine Transaktion vor. Der Kunde erhält in der Folge die Aufforderung zu einer Freigabe, die dann am Telefon nach Rückfrage des Angreifers storniert wird. In Wirklichkeit wird die Transaktion aber mit dem zur Stornierung übermittelten Code erst recht durchgeführt. Der Kunde führt somit die Transaktion im Sinn des Angreifers durch.

---

BETRUG UND KLEINANZEIGEN

# „Wenn der Käufer Betrüger ist.“

Kleinanzeigenportale bieten eine bequeme Plattform für Käufer und Verkäufer, ziehen aber auch Phishing-Kriminalität an: Maja Hoffmann, Head of Anti-Fraud Management der UniCredit Bank Austria, über die Vorgangsweise der Täter.

Eine weit verbreitete Betrugsform besteht darin, dass sich Betrüger als interessierte Käufer ausgeben und Täuschungstaktiken anwenden, um Verkäufer dazu zu bringen, vertrauliche Informationen preiszugeben, wie Kreditkartendaten und Internetbanking-Daten. Dafür erstellen Täter oft gefälschte Käuferprofile, die auf den ersten Blick legitim erscheinen. Sie bekunden starkes Interesse am Produkt oder Service des Verkäufers und bauen durch freundliche und überzeugende Kommunikation Vertrauen auf. Im Verlauf des Gesprächs geben die Betrüger möglicherweise vor, dass die Transaktion dringend abgeschlossen werden muss, oder nennen Gründe für eine sofortige Zahlung.

### Die Vorgangsweise der Täter auf einen Blick

1. Das Opfer registriert sich als Verkäufer auf der Kleinanzeigenplattform.
2. Ein Interessent meldet sich als Käufer.
3. Kontaktdaten werden seitens des vermeintlichen Käufers erfragt, um ab sofort über WhatsApp zu kommunizieren.
4. Das Opfer erhält eine Benachrichtigung per E-Mail, dass die Ware bezahlt wurde.
5. Zum Erhalt der Zahlung müssen auf einer Webseite, die vermeintlich zum Kleinanzeigenportal gehört, Daten eingegeben werden (Kreditkartendaten oder Internetbanking-Daten). Hierbei gibt es auch einen Chat-Support.
6. Zur finalen Bestätigung muss eine Freigabe erfolgen, bei der behauptet wird, dass es sich um keine Zahlungsfreigabe handelt.
7. Das Opfer wird beeinflusst, nicht auf den (warnenden) Inhalt des Zahlungsdienstleisters zu achten, sondern dennoch die finale Bestätigung abzugeben.
8. Die Freigabe bzw. Zahlung erfolgt.

***„Täter erstellen oft gefälschte Käuferprofile, die auf den ersten Blick legitim erscheinen."***

Um sich vor dieser Betrugsform zu schützen, sollten Verkäufer Vorsicht walten lassen und sich der üblichen Warnzeichen bewusst sein. Echte Käufer benötigen normalerweise keine sensiblen Informationen, die über das hinausgehen, was für die Transaktion notwendig ist. Nutzer (Verkäufer und Käufer) sollten ausschließlich über die sicheren Kanäle kommunizieren, die vom Kleinanzeigenportal bereitgestellt werden.



**Maja Hoffmann**
Head of Anti-Fraud Management
UniCredit Bank Austria



### TELEFONBETRUG „SPOOFING": SO GEBEN SICH BETRÜGER ALS UNTERNEHMEN AUS

Beim Spoofing wird eine vertrauenswürdige Nummer vorgetäuscht, um den Anruf so erscheinen zu lassen, als käme er von einer legitimen Quelle wie einer Bank, einer Regierungsbehörde oder einer angesehenen Organisation.

Gängige Szenarien sind:

**Finanzbetrug**
Betrüger können sich als Bankvertreter ausgeben und Opfer über unbefugte Transaktionen oder verdächtige Aktivitäten auf ihren Konten informieren. Um das Problem zu lösen, fordern sie sensible Informationen wie Kontonummern, Passwörter oder PINs an.

**Regierungsimitation**
Betrüger können behaupten, Vertreter von Behörden zu sein, die rechtliche Schritte oder Geldstrafen für angebliche Verstöße androhen. Diese Taktik spielt auf die Angst vor rechtlichen Konsequenzen ab, indem sie Opfer dazu bringt, den Forderungen des Betrügers nachzukommen.

**Technischer-Support-Betrug**
Indem sie sich als technische Supportmitarbeiter ausgeben, können Betrüger Einzelpersonen über angebliche Viren oder Sicherheitsbedrohungen auf ihren Geräten informieren. Sie fordern dann Fernzugriff oder Zahlungen für unnötige Dienstleistungen an, wodurch Opfer finanzielle Verluste und Identitätsdiebstahl riskieren.



PRÄVENTION
& STRATEGIE

# Fallen erkennen, Bewusstsein stärken

Was tun gegen Internetbetrug und Phishing? Welche Ansätze zur Prävention gibt es? Bernhard Jungwirth, Geschäftsführer des Österreichischen Instituts für angewandte Telekommunikation, und Thorsten Behrens, Projektleiter von Watchlist Internet, berichten im Interview, was Österreichs größte Informationsplattform zu Internetbetrug leistet – und empfiehlt.

**Watchlist Internet ist seit zehn Jahren in Österreich aktiv. Was ist Ihr Präventionsansatz?**
*Jungwirth:* Es geht einerseits um allgemeine Prävention: Wie kaufe ich sicher ein, wie kann ich Phishing-Nachrichten erkennen? Es geht aber auch um spezifische Warnmeldungen vor konkreten Fallen, wo wir z. B. warnen, dass ein bestimmter Webshop Fake ist. Unser Ziel ist es, Antworten auf die drei wichtigsten Fragen zum Thema Internetbetrug zu geben:

- Handelt es sich in einem konkreten Fall um Betrug?
- Was kann ich tun, wenn ich in eine Betrugsfalle geraten bin?
- Wie kann ich Internetbetrug selbst erkennen?

**PRÄVENTION**

| Allgemeine Prävention | Prävention zu konkreten Fällen |
|---|---|
| Medienarbeit<br>Social-Media-Kampagnen<br>Schulprogramme<br>Watchlist (Newsletter, App etc.) | AWARENESS – Zweifel haben<br>KNOWLEDGE – Wissen, wie man sich hilft<br>ACTION – Keine Daten eingeben, melden |

*Behrens:* Wir haben lange Listen mit Phishing-Domains. Die etwa 200 redaktionellen Warnmeldungen und 10.000 Domaineinträge pro Jahr basieren auf ca. 12.000 Meldungen von Nutzerinnen und Nutzern sowie von Partnern. Die Warnmeldungen und Domain-Listen mit Fake-Shops, problematischen Shops, Finanzbetrug, Abo-Fallen oder Phishing-Alarm sind suchmaschinenoptimiert, sodass sie im Moment des Zweifels – „ist das Betrug oder nicht?" – bei einer Internetsuche gefunden werden können. Die Watchlist Internet verzeichnet mehr als 3 Millionen Besuche und 12 Millionen Seitenaufrufe pro Jahr.

**Wie sprechen Sie Zielgruppen aktiv an?**
*Jungwirth:* Neben den Aufrufen über Suchmaschinen erreicht die Watchlist Internet ihre „Stammkunden" über E-Mail-Newsletter, Social Media und die Smartphone-App. Mit unserem Fake-Shop-Detector (*www.fakeshop.at*) und den Social-Media-Auftritten werden die Warnungen außerdem direkt im Umfeld der Fallen platziert.

Aktive Medienarbeit mit etwa 1.000 gezählten Medienbeiträgen in TV, Radio, Print und Web pro Jahr rundet die Präventionsarbeit der Watchlist Internet ab.

**Muss man erst in eine Falle tappen, damit man daraus lernt?**
*Behrens:* Am besten lernen Menschen durch eigene Erfahrung und aus eigenen Fehlern. Aber es muss ja nicht unbedingt eine echte Falle sein. Deshalb ahmen wir z. B. mit simulierten Fake-Investmentplattformen oder Fake-Shops (*www.watchlist-internet.at/vorsicht-falle*) betrügerische Webseiten nach. Wer in eine solche „Fake-Falle" tappt, erlebt vielleicht eine Schrecksekunde, ist für die nächste Falle aber besser gerüstet. Unsere Empfehlung: Das sollte man auch Verwandte und Bekannte testen lassen.




**Relevante Zielgruppe von Cyberkriminellen sind auch KMU. Wie unterstützen Sie deren Prävention?**
*Behrens:* Die Watchlist Internet für Unternehmen (*www.watchlist-internet.at/unternehmen*) ist ein eigener Bereich mit Warnmeldungen und Newsletter speziell für Unternehmen. Ergänzt wird der Bereich durch eine Phishing-Simulation für KMU und das Cybersecurity-Awareness-Playbook (*www.cybersecurity-awareness.at*), das CISOs und andere mit konkreten Maßnahmen-Ideen bei der Sensibilisierung der Kolleginnen und Kollegen unterstützt.

***„Im Kampf gegen Phishing und andere Formen von Internetbetrug gibt es nicht die eine ‚Wunderwaffe'."***

**Angesichts des massiv steigenden Bedarfs: Was sind Ihre Ziele für die nächsten Jahre?**
*Jungwirth:* Der Impact soll in den nächsten Jahren mittels Erhöhung der Anzahl der Warnungen und Verbreitungskanäle weiter gesteigert werden. Dazu sind Sourching-Tools wie der Fake-Shop-Detector und Crawler genauso wichtig wie Kooperationen mit relevanten Stakeholdern. Bei der Weiterentwicklung der Präventionsmethoden arbeiten wir neben der laufenden Suchmaschinenoptimierung vor allem daran, Warnungen auf unterschiedlichsten Kanälen so nah wie möglich an den Fallen zu platzieren.



**Bernhard Jungwirth**
Geschäftsführer Österreichisches Institut für angewandte Telekommunikation



**Thorsten Behrens**
Projektleiter Watchlist Internet
*watchlist-internet.at*

***watchlist-internet.at***
Die unabhängige Informationsplattform zu Internetbetrug und betrugsähnlichen Online-Fallen informiert über konkrete aktuelle Betrugsfälle im Internet und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann.

**Was erwarten Sie sich von besserer Zusammenarbeit im Kampf gegen Phishing?**
*Behrens:* Im Kampf gegen Phishing und andere Formen von Internetbetrug gibt es nicht die eine „Wunderwaffe". Es muss an vielen unterschiedlichen Stellschrauben gedreht werden. Dafür braucht es ein Bekenntnis aller Beteiligten zu einer gemeinsamen Verantwortung, ein Verständnis für die unterschiedlichen Perspektiven und einen fachlichen Austausch über Lösungen. Eine Plattform gegen Daten-Phishing kann dafür den idealen Rahmen bieten.

## DIE WICHTIGSTEN PRIORITÄTEN IM KAMPF GEGEN PHISHING

1. Präventionsmethoden weiterentwickeln
2. Verbreitungswege von Betrugsfallen erschweren (z. B. Werbung für Fallen auf Plattformen)
3. Fallen automatisiert erkennen und das Datenmanagement zwischen den Stakeholdern verbessern

# Gemeinsam gegen digitale Bedrohungen

Im Rahmen der Auftaktveranstaltung zur Plattform gegen Datendiebstahl im Internetbetrug diskutierten unter der Leitung von Thomas Von der Gathen (PSA Payment Services Austria GmbH), Verhaltensanalytikerin Patricia Staniek, Head of Fraud-Management Birgit Langeder (Erste Bank), Bundeskriminalamt-Experte Mohamed Ibrahim (Cybercrime Competence Center C4) und CSO Wolfgang Schwabl (A1 Telekom Austria AG und Vorsitzender CSP des BKA) gemeinsame Antworten auf die Phishing-Gefahr.

Head of Fraud-Management **Birgit Langeder** von der Erste Bank erklärte, dass man die gruppenweiten Maßnahmen der Banken zur Vermeidung von Betrug nicht unterschätzen dürfe. Neben der verpflichtenden Zwei-Faktor-Authentifizierung wurden auch Fraud-Management-Systeme etabliert, um Schäden für Kunden und Institute zu verhindern. Neben der Schaltung von Warnhinweisen und einem Warning-Screen bei gleichzeitigem Telefonieren und Online-Bankgeschäften betonte Langeder auch die gute Zusammenarbeit mit Watchlist Internet. Die gesetzten Maßnahmen kämen bei den Kundinnen und Kunden sehr gut an.

Langeder unterstrich die Wichtigkeit der Zusammenarbeit zwischen Banken und Polizei. Man versuche, die Kunden überall zu erreichen und zu sensibilisieren.

**Zusammenarbeit unterstützt Prävention**

Bundeskriminalamt-Experte **Mohamed Ibrahim** (Cybercrime Competence Center) nannte als Herausforderungen bei der Bekämpfung von Internetbetrug die Komplexität des Themas, internationale Hürden bei der Zusammenarbeit und die hohe Zahl von Anzeigen. Den aktuell 28.000 Anzeigen pro Jahr stehe eine noch höhere Dunkelziffer gegenüber. Der Großteil betreffe Phishing. Ziel müsse es sein, durch bessere Prävention Fälle zu verhindern. Die Zusammenarbeit mit Banken und Mobilfunkanbietern und die gemeinsame Plattform gegen Phishing helfe, mehr in die Prävention zu investieren, betonte der Bundeskriminalamt-Experte.



**Wissen über Opfer wichtig**

Verhaltensanalytikerin **Patricia Staniek** sprach sich dafür aus, Menschen noch besser zu informieren. Kein Polizist holt an der Haustür Geld und Schmuck ab. Die potenziellen Opfer müssen auf allen möglichen Ebenen erreicht werden, durch Medien, durch Institutionen, Vereine und Familienangehörige.

Letztlich könne man in der Prävention Menschen nur erreichen, wie es die Täter selbst bei Social Engineering tun – „in ihr Gehirn einsteigen“. Man müsse wissen, wie Opfer ticken, um Präventivmaßnahmen richtig weiterzuentwickeln.




*Bild v. l. n. r.: Wolfgang Schwabl, Mohamed Ibrahim, Thomas Von der Gathen, Patricia Staniek, Birgit Langeder*

**Rechtliche Weiterentwicklung nötig**

**Wolfgang Schwabl,** CSO A1 Telekom Austria AG und Vorsitzender der Cyber Sicherheit Plattform des Bundeskanzleramtes, machte in der Diskussion auf rechtliche Lücken aufmerksam: Es sei den Telekom-Anbietern nicht erlaubt, Phishing-SMS zu stoppen, weil das Telekom-Gesetz dies nicht erlaube.

Die rechtliche Regelung, die sich am traditionellen Briefgeheimnis orientiert, sei nicht mehr zeitgemäß. Die Kommunikation laufe schließlich nicht mehr – wie per Brief und Telefon – von Mensch zu Mensch. SMS würden heute von Computerprogrammen versendet. Angesichts dieser maschinengenerierten Attacken müsse man den Rechtskontext überlegen, sagte Schwabl: „Ist nicht der Schutz der Empfänger vor bösartigen Nachrichten wichtiger?“ Er verwies auf die Notwendigkeit eines breiten gesellschaftlichen Konsenses in dieser Frage.



Im Bereich alphanumerischer SMS biete das Urheberrecht einen Ansatz für mehr Schutz. Noch besser wäre allerdings eine Registrierungspflicht für alle alphanumerischen Absender. Für diese Frage brauche es jedenfalls einen Konsens zwischen Parteien und Behörden. Man werde das Gespräch in diesem Sinn weiter vertiefen, kündigte der Vorsitzende der Cyber Sicherheit Plattform des Bundeskanzleramtes an.

**Zusammenarbeit weiterführen**

Bundeskriminalamt-Experte **Mohamed Ibrahim** unterstrich abschließend die Wichtigkeit von Anzeigen: Mit jeder Anzeige könne man Verbindungen herstellen. Es gebe immer wieder Ermittlungserfolge.

Head of Fraud-Management **Birgit Langeder** wünschte sich, dass die Zusammenarbeit mit Polizei und Banken weitergeführt werden soll. Auch sie plädierte für rechtliche Weiterentwicklungen, um den Austausch zu verbessern. Derzeit würde dies der Datenschutz noch behindern.

Es gebe allerdings Bemühungen, dies zu verbessern. Der legale Austausch sei wichtig, damit nicht noch mehr Geld in organisierte Kriminalität fließe, sagte die Expertin.

Auch Verhaltensanalytikerin **Patricia Staniek** begrüßte die forcierte Zusammenarbeit. Großes Ziel sei die Eigensicherheit der Menschen.



AUSBLICK
& AGENDA

# „Wir müssen das Team erweitern!“

**Mit der Plattform gegen Datendiebstahl im Internetbetrug wird ein entscheidender Schritt für bessere Zusammenarbeit und wirksame Prävention gesetzt: Thomas Von der Gathen (PSA Payment Services Austria GmbH) und Bernhard Schafrath (Bundeskriminalamt) über die Agenda der Plattform ab 2024.**

Der Ursprung des neuen Anti-Phishing-Gipfels geht auf das sogenannte „Kreditkartenseminar“ zurück. Das ist eine Expertenrunde von Bankenvertretern und Kriminalbeamten, die seit 28 Jahren aktiv ist und sehr gut zusammenarbeitet. Cybercrime ist allerdings ein weites Land ohne Grenzen. Wir sehen, dass sich das Thema Phishing immer stärker und vielfältiger entwickelt. Der Modus hat sich grundlegend geändert. Heute bringen Kriminelle Menschen dazu, Transaktionen selbst zu tätigen. Vieles, was bisher in technische Sicherheitsmaßnahmen investiert wurde, funktioniert daher nicht mehr ausreichend.

## Gemeinsam weiterkommen

Wir müssen das Team im Kampf gegen Phishing über Banken und Polizei hinweg erweitern und brauchen weitere Teammitglieder. Daher haben wir die Plattform gegen Phishing initiiert. Gemeinsam werden wir einen guten Schritt weiterkommen. Wesentlich sind auch gesetzliche Maßnahmen, damit Banken Daten austauschen dürfen, um Betrug zu verhindern.

## Folder als erstes Ergebnis

Erstes Arbeitsergebnis der „Plattform gegen Phishing“ ist ein gemeinsamer Folder zur Bewusstseinsbildung, der im Zuge der Vorbereitungsarbeiten zur Plattform entwickelt wurde.




Die Polizei verteilt dieses Produkt bereits. Einzelne Banken haben den Folder bereits selbst gebrandet und übermitteln ihn an ihre Kundinnen und Kunden.

## Regelmäßiger Austausch

Ziel unserer Agenda (s. Kasten) ist es, in regelmäßiger Zusammenarbeit, bei Tagungen und Arbeitsgruppen einen raschen Informationsaustausch aller



Stakeholder sicherzustellen. Gemeinsam sollen Maßnahmen erarbeitet werden, welche die Bürgerinnen und Bürger noch weiter für die Bedrohungen sensibilisieren und sie so bestmöglich vor jeglichem Datendiebstahl schützen.

Wir werden auch Empfehlungen für Politik und Gesetzgebung entwickeln, damit die Rahmenbedingungen für den Kampf gegen Phishing zeitgemäß weiterentwickelt werden können.

**Thomas Von der Gathen**
General Counsel Payment Services Austria (PSA Payment Services Austria GmbH)





**Bernhard Schafrath**
Leiter Büro für Kriminalprävention und Opferschutz im Bundeskriminalamt

Wir bedanken uns bei allen, die bis jetzt am Anti-Phishing-Gipfel und an der Gründung der Plattform mitgearbeitet haben – und laden alle weiteren Stakeholder ein, unsere gemeinsame Plattform zu unterstützen.

# AGENDA 2024

**Auf der Agenda für 2024 stehen drei erklärte Ziele:**

Erarbeitung von gemeinsamen **Bewusstseinsbildungs- und Präventionsmaßnahmen**, um die bestehenden Potenziale zu bündeln und zu verstärken.

Erarbeitung von **zukünftigen technischen Möglichkeiten** zur Verhinderung von Phishing-Angriffen, wobei auch entsprechende legistische Änderungsnotwendigkeiten adressiert werden.

**Erarbeitung von Empfehlungen** nach internationalem Beispiel für Entscheidungsträger, um Politik und Gesetzgebung zu unterstützen.

# Danke!

Für die bisherige Mitwirkung am Gipfel und der Plattform gegen Phishing bedanken wir uns in alphabetischer Reihenfolge bei:

**BEHRENS Thorsten,**
Projektleiter von Watchlist Internet

**FLATSCHER Harald,**
Geschäftsführer PSA Payment Services Austria GmbH

**FRITZ Robert,**
COO/CIO, Mitglied des Vorstandes Card Complete

**GRAF-MARSCHALLEK Markus,** Head of
Card Service & Fraudmanagement Card Erste Bank

**HAKALA Horst,**
Leiter Lagebild Betrug des Bundeskriminalamtes

**HOFFMANN Maja,** Head of
Anti-Fraud Management UniCredit Bank Austria

**HOFSTÄTTER-POBST Gregor,**
CFO/CRO Wüstenrot Gruppe/Wüstenrot Bank

**HOLZER Andreas,** Direktor Bundeskriminalamt

**HOLZINGER-BURGSTALLER Gerda,**
Vorstandsvorsitzende Erste Bank Österreich

**IBRAHIM Mohamed,** Bundeskriminalamt-Experte,
Cybercrime Competence Center C4

**JESTÄDT Guido,** Vorstandsmitglied BAWAG Group

**JUNGWIRTH Bernhard,**
Geschäftsführer Österreichisches Institut
für angewandte Telekommunikation

**KARNER Gerhard,**
Bundesminister für Inneres der Republik Österreich

**LANGEDER Birgit,**
Head of Fraud-Management Erste Bank

**MECHTLER Roland,**
Vorstandsdirektor Effizienz, Technology und Treasury
Raiffeisenbank Niederösterreich-Wien

**NISSL Christoph,** Head of Compliance
Financial Crime Prevention Wüstenrot Group Austria

**OSTAH David,**
Geschäftsführer PSA Payment Services Austria GmbH

**PILLER-MAYERHOFER Diana,**
Head of Operations & Corporate Fraud Card Complete

**RENNER-ROHRBECK Nikolaus,**
Head of Anti-Fraudmanagement Card Complete

**SCHAFRATH Bernhard,** Leiter Büro für
Kriminalprävention und Opferschutz, Bundeskriminalamt

**SCHAUPP Andreas,** Group CISO BAWAG Group

**SCHERSCHER Manuel,** Leiter Abteilung für
Wirtschaftskriminalität, Bundeskriminalamt

**SCHISCHKA Robert,** Geschäftsführer nic.at & CERT.at

**SCHWABL Wolfgang,**
CSO A1 Telekom Austria AG, Vorsitzender der
Cyber Sicherheit Plattform (CSP), Bundeskanzleramt

**STANIEK Patricia,**
Wirtschaftskriminal- und Verhaltensanalytikerin

**VON DER GATHEN Thomas,**
General Counsel PSA Payment Services Austria GmbH

**ZADRAZIL Robert,** stellvertretender Obmann der
Bundessparte Bank und Versicherung der Wirtschafts-
kammer Österreich, Präsident des Bankverbandes und
CEO UniCredit Bank Austria

---

**IMPRESSUM**

Herausgeber
PSA Payment Services Austria GmbH
Handelskai 92, Gate 2, 1200 Wien
gemeinsam mit dem
Bundeskriminalamt (BK)
Josef-Holaubek-Platz 1, 1090 Wien

Verantwortlich für den Inhalt
Thomas Von der Gathen/PSA
Bernhard Schafrath/BK

Fotografie
iStockphoto, BMI/BK, BMI/Karl
Schober, Fotostudio Semrad, Anna
Rauchenberger, Andrea Sojka, ÖIAT

Gestaltung
GPK public GmbH

Druck
oha-druck GmbH

© 2024 PSA und BMI/BK
Alle Rechte vorbehalten.

# Auftakt-konferenz der Plattform gegen Datendiebstahl im Bild

23. November 2023





























Bundesministerium
Inneres

Bundeskriminalamt

**bmi.gv.at**

PSA

**psa.at**