Die Evolution des Online-Betrugs

Vom klassischen Internetbetrug zur KI-gestützten Täuschung

Wien, Oktober 2024

Die Evolution des Online-Betrugs

Vom klassischen Internetbetrug zur KI-gestützten Täuschung

Verfasst von
Patricia Rosenauer
Valentine Auer (Watchlist Internet)

Unter Mitarbeit von
Thorsten Behrens (Watchlist Internet)

Fachliche Verantwortung
Patricia Rosenauer

Im Auftrag von
Dr. Armin Kaltenegger

Inhaltsverzeichnis

1. Einleitung: Die vielschichtige Welt des Online-Betrugs

In einer Zeit, in der unser Leben zunehmend digital wird, lauern Gefahren oft dort, wo wir sie am wenigsten erwarten. Online-Betrug hat viele Gesichter, und die Methoden der Kriminellen werden immer raffinierter. Von gefälschten Online-Shops über massenhaft versendete Phishing-Nachrichten bis hin zu ausgeklügelten KI-gestützten Täuschungen – **die Betrüger sind erfinderisch und passen sich schnell an neue Technologien an.**

"Das würde mir nie passieren." Ein Gedanke, den viele von uns schon einmal hatten. Doch die Realität sieht anders aus: Laut den Ergebnissen einer aktuellen KFV-Umfrage zum Thema Online-Betrug haben **83 % der Befragten in den letzten 12 Monaten Betrugsversuche** bemerkt.

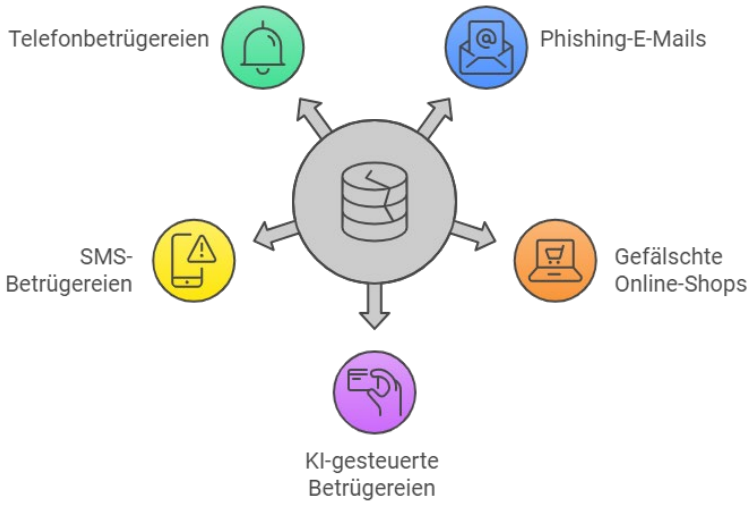


Abbildung 1: Betrug mit Medien

Die vorliegende Studie – eine Kooperation des KFV-Fachbereichs Eigentumsschutz und der Watchlist Internet – soll die dramatische Entwicklung einer facettenreichen Form von Internet-Kriminalität in den Fokus rücken: die Evolution des Online-Betrugs.

Die Geschichten von Rita, Mario, Milena und Claus, die wir in den folgenden Kapiteln kennenlernen werden, sind zwar **fiktiv**, spiegeln aber die **tägliche Realität vieler Menschen** wider. Sie zeigen, wie selbst vorsichtige und informierte Personen in einem Moment der Unachtsamkeit oder emotionalen Verletzlichkeit Opfer von Betrügern werden können. Besorgniserregend ist auch der **Einsatz von künstlicher Intelligenz (KI) in Betrugsmaschen**, vor allem hinsichtlich der rasanten Entwicklungen in diesem Bereich.

In den folgenden Kapiteln werden wir tiefer in die verschiedenen Formen des Online-Betrugs eintauchen, von klassischen Phishing-Attacken bis hin zu hochentwickelten KI-gestützten Täuschungen. Wir werden die Erfahrungen unserer Protagonist:innen analysieren, statistische Daten präsentieren und praktische Tipps zur Prävention geben. Denn eines ist klar: **In der digitalen Welt ist Wachsamkeit unser bester Schutz.**

2. Methodik

Um ein umfassendes Bild der aktuellen Betrugslandschaft zu zeichnen, wurde im August 2024 im Rahmen der KFV-Studie in Zusammenarbeit mit Watchlist Internet eine repräsentative Online-Umfrage durchgeführt. Die Methodik dieser Studie basierte auf folgender Struktur:

Stichprobe

Die Umfrage umfasste **1.033 Teilnehmende im Alter von 14 bis 75 Jahren** und spiegelte die österreichische Bevölkerung hinsichtlich Alter, Geschlecht und Wohnsituation wider. Die erzielte Diversität ermöglichte es, verlässliche Rückschlüsse auf die Erfahrungen und Wahrnehmungen der Bevölkerung in Bezug auf Online-Betrug zu ziehen.

Erhebungsmethode

Die Datenerhebung erfolgte durch einen strukturierten **Online-Fragebogen**, der sowohl geschlossene als auch offene Fragen beinhaltete. Die behandelten Themen umfassten Online-Aktivität, Erfahrungen mit verschiedenen Betrugsarten, Wissen über Betrugsmaschen, insbesondere jene mit Einsatz von künstlicher Intelligenz, sowie Präventionsmaßnahmen.

Analyseverfahren

Die gesammelten **Daten wurden statistisch ausgewertet**, wobei Häufigkeiten, Prozentsätze und Mittelwerte berechnet wurden. Besondere Aufmerksamkeit galt der statistischen Schwankungsbreite, um die Zuverlässigkeit der Ergebnisse zu gewährleisten.

Integration von Fallbeispielen

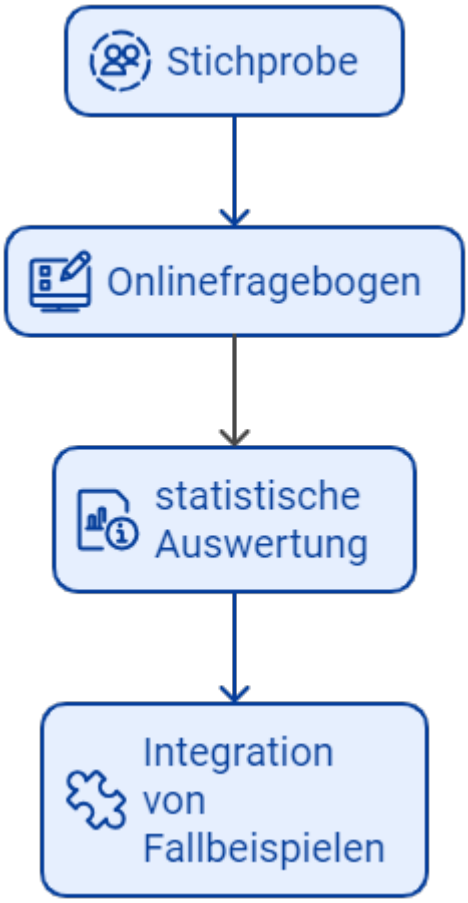


Abbildung 2: Methodik

Um die statistischen Ergebnisse greifbar zu machen, werden in den folgenden Kapiteln die Geschichten von fiktiven Personen wie Claus, Milena, Rita und Mario erzählt. **Diese Fallbeispiele veranschaulichen die verschiedenen Betrugsmaschen und deren Auswirkungen auf das Leben der Betroffenen.** Durch die Verbindung von Daten und persönlichen Geschichten wird die Thematik des Online-Betrugs anschaulicher und nachvollziehbarer.

Diese methodische Herangehensweise ermöglichte es dem Forschungsteam, fundierte Erkenntnisse über die Verbreitung von Online-Betrug, das Wissen der Bevölkerung und die Wirksamkeit von Präventionsmaßnahmen zu gewinnen.

3. Die wichtigsten Ergebnisse der Studie

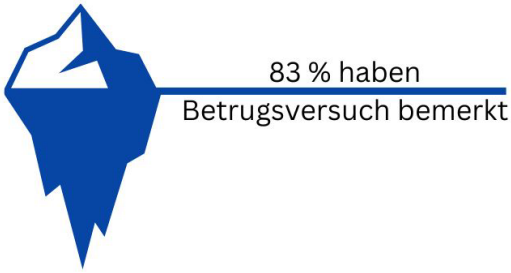


Abbildung 3: Betrugseisberg

Die Umfrage hat gezeigt, **dass 83 % der Befragten in den letzten 12 Monaten auf Betrugsversuche aufmerksam wurden**. Diese hohe Zahl verdeutlicht, dass Betrüger immer raffinierter vorgehen und sich an die neuen Möglichkeiten der digitalen Welt anpassen. Klar ist aber auch, dass es sich dabei nur um die Spitze des Eisbergs handelt. Es ist davon auszugehen, dass nahezu **jeder Internetnutzer** irgendwann einem **Betrugsversuch** ausgesetzt ist, selbst wenn er diesen nicht bewusst wahrnimmt oder nicht darauf hereinfällt. Oftmals werden solche Versuche direkt in Spam-Ordnern abgefangen oder als verdächtige Nachrichten in Messengerdiensten gelöscht, **ohne dass sie als Betrugsversuche erkannt werden**. Dies führt dazu, dass viele Betrugsversuche unbemerkt bleiben, obwohl sie potenziell Schaden anrichten könnten.

3.1. Betrugsversuche

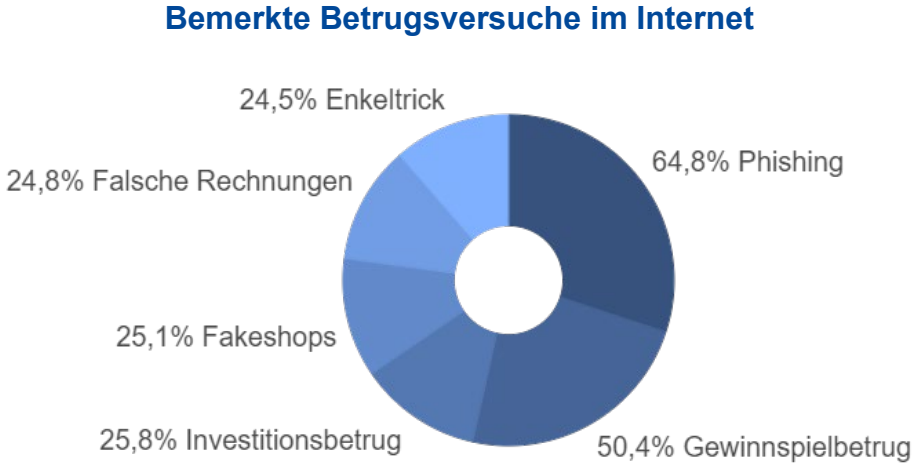


Abbildung 4: Bemerkte Betrugsversuche im Internet, Mehrfachnennung

Die häufigsten Kontaktwege, über die Betrugsversuche im Internet stattfanden, wurden im Zuge der Befragung klar erkennbar. An erster Stelle stehen **E-Mails**, die von **68 %** der Befragten als Hauptkommunikationsmittel für betrügerische Angriffe genannt wurden. **Kurzmitteilungen (SMS)**

folgen dicht dahinter, da **60 %** der Teilnehmenden angaben, auf diesem Weg mit betrügerischen Inhalten konfrontiert worden zu sein. Auch **Telefonanrufe** sind ein beliebter Kanal für Betrüger: **50 %** der Befragten berichteten, auf diese Weise kontaktiert worden zu sein.

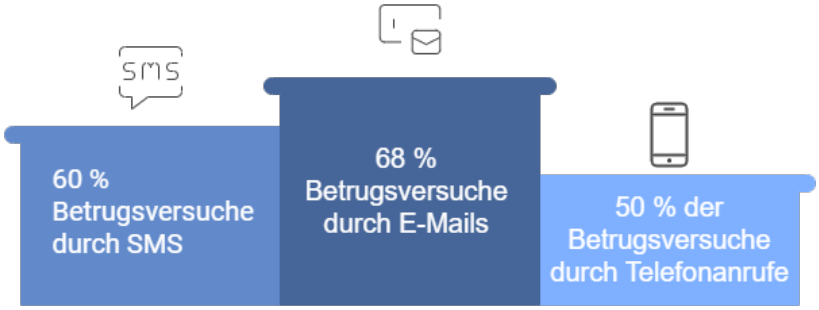
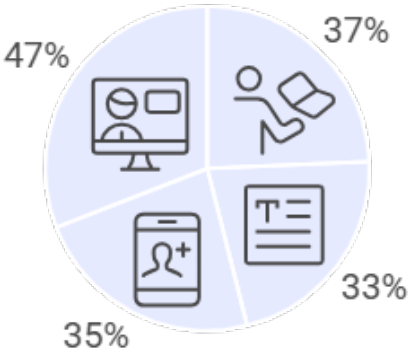


Abbildung 5: Top 3 Kontaktwege Betrug

69 % der Befragten schätzten ihr Wissen über Betrugsmaschen als sehr gut oder zumindest eher gut ein. Diese hohe Selbsteinschätzung zeigt, dass sich viele Menschen der verschiedenen Betrugsstrategien durchaus bewusst sind und meinen, betrügerische Tricks erkennen zu können. Dennoch wurde eine erhebliche Anzahl der Befragten bereits selbst Opfer von Betrugsversuchen. **Jede fünfte befragte Person (20 %) wurde bereits Opfer eines Betrugs im Internet**. Dabei waren Männer häufiger betroffen als Frauen.

Auffallend ist, dass zwei Drittel der Befragten KI-Betrugsmaschen kennen. **5,5 % wurden bereits Opfer eines KI-unterstützten[1] Betrugs**. Die Informationsquellen über KI-Betrugsmaschen sind vielfältig:



- **47 %** erfahren darüber aus **Berichten im TV**
- **37 %** aus **Zeitungen/Magazinen**
- **35 %** über **soziale Medien**
- **33 %** über **Online-Portale**
- **27 %** über **Berichte im Radio**
- **25 %** von **Freunden, Bekannten oder Familie**
- **11%** im Zuge von **Ausbildung oder Arbeit**

Abbildung 6: Top 4 Infoquellen KI-Betrug

[1] Dabei ist allerdings zu bedenken, dass für einen Laien die Unterscheidung zwischen Robocalls, also automatisierten Telefonanrufen, die vorab aufgezeichnete Nachrichten abspielen, und KI-gestützten Telefonanrufen schwer ist, da beide Betrugsarten automatisierte Systeme nutzen, die natürliche Stimmen simulieren.

3.2. Präventionsmaßnahmen

Die Umfrageergebnisse zeigen ein hohes Bewusstsein für Sicherheits- und Präventionsmaßnahmen innerhalb der Bevölkerung. So geben **77 % der Befragten** an, zu wissen, dass **niemals auf unbekannte Links geklickt werden sollte**, da diese Links potenziell schädliche Inhalte oder betrügerische Absichten verbergen könnten. **76 % der befragten Personen sind sich darüber im Klaren, dass persönliche Daten niemals am Telefon weitergegeben werden sollten**, da Betrüger häufig diese Methode nutzen, um an sensible Informationen zu gelangen. **75 % der Teilnehmenden** der Umfrage sind sich der Gefahr bewusst, die von Anhängen in E-Mails unbekannter Absender ausgehen kann. Diese Zahlen zeigen, dass ein breites Verständnis für grundlegende Sicherheitsregeln vorhanden ist.

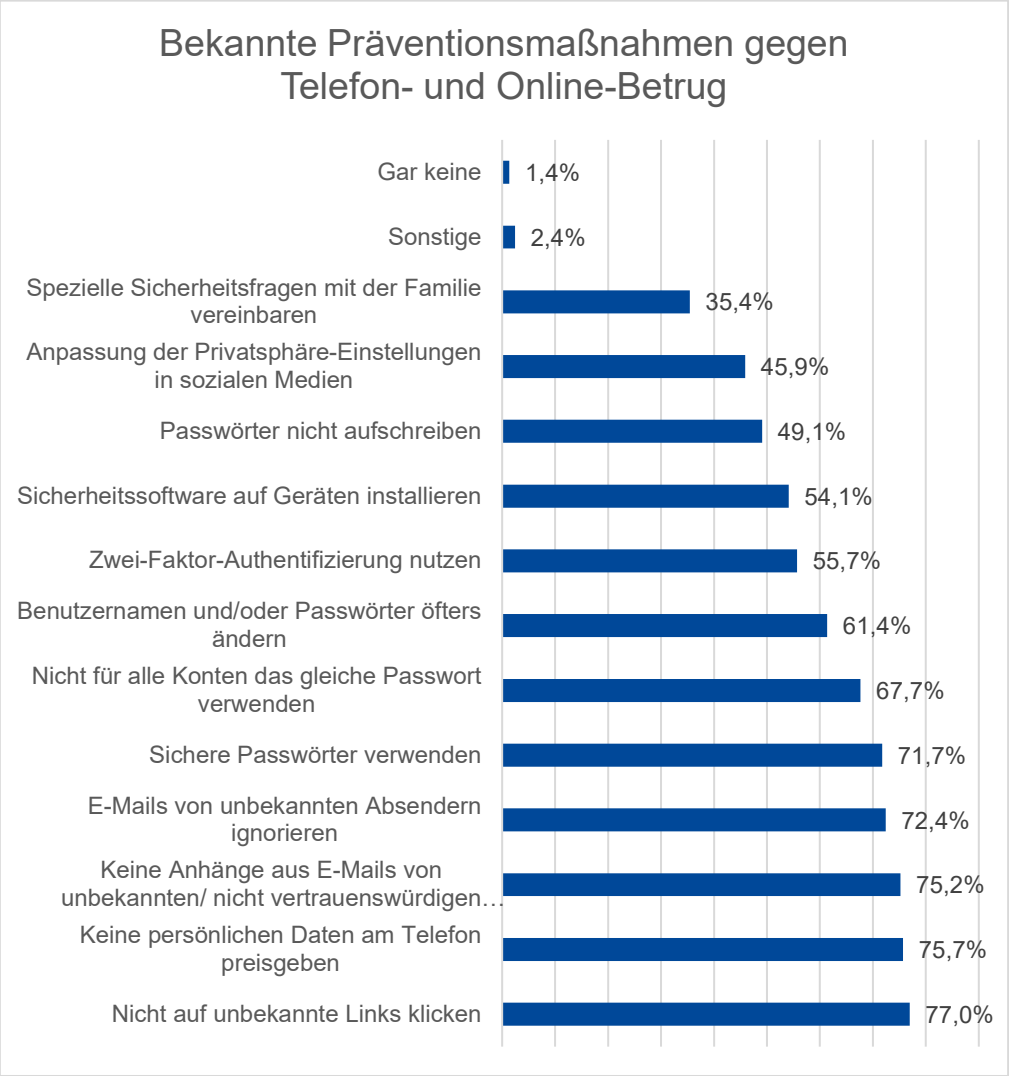


Abbildung 7: Bekannte Präventionsmaßnahmen

Erfreulicherweise ergreifen nach Eigenaussage **bereits 60 % der Befragten konkrete Maßnahmen zum Schutz vor Betrug**:

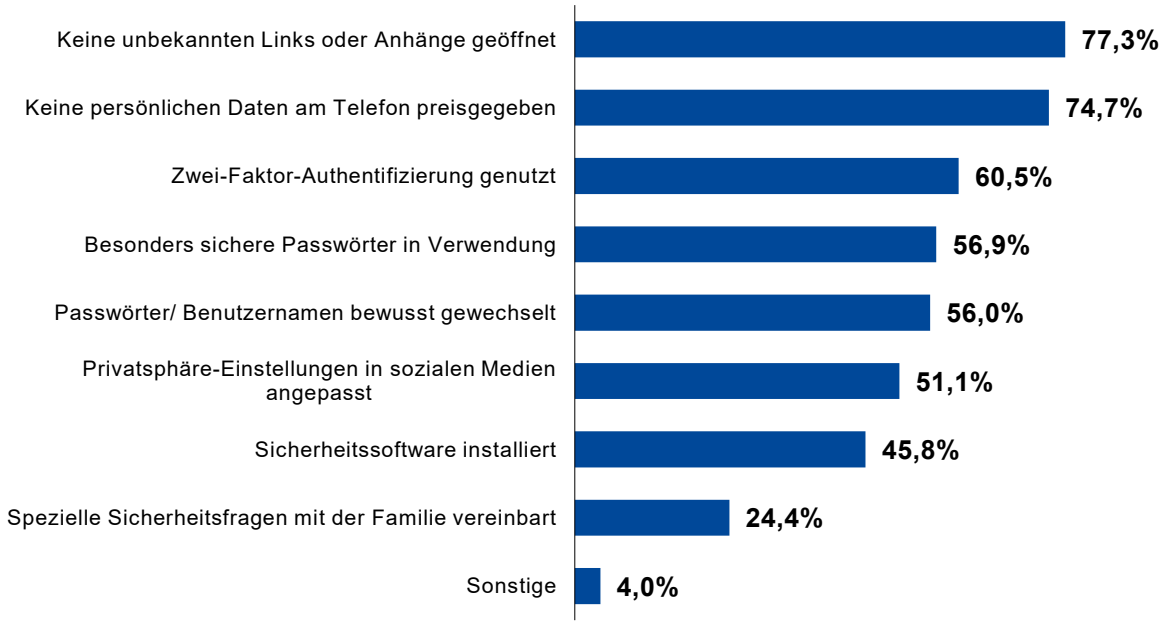


Abbildung 8: Ergriffene Maßnahmen gegen Betrug

Diese Zahlen belegen: Viele Menschen kennen die Basics der digitalen Sicherheit nicht nur, sondern setzen sie auch um. Trotzdem gibt es noch Verbesserungspotenzial. **Immerhin 40 % haben bisher keine Vorkehrungen getroffen und sind dadurch anfälliger für Betrugsversuche**. Hier gilt es anzusetzen, das Problembewusstsein zu stärken und mehr Menschen zu motivieren, sich aktiv zu schützen.

Abbildung 9: Anteil der Befragten mit bereits ergriffenen Schutzmaßnahmen

3.3. Datenlecks und Datenschutz

Datenlecks stellen eine erhebliche Bedrohung in Sachen Datenschutz dar, da sie oft sensible, persönliche oder vertrauliche Informationen unbefugt zugänglich machen. **Bei einem Leck bzw. Leak können Namen, Adressen, finanzielle Details, Passwörter oder auch Gesundheitsdaten in falsche Hände geraten und für kriminelle Zwecke missbraucht werden**. Identitätsdiebstahl oder finanzielle Verluste aufgrund gezielter Phishing-Angriffe sind eine allgegenwärtige Gefahr in der digitalen Welt von heute. Unternehmen und Organisationen stehen daher in der Verantwortung, ihre Systeme und Datenbanken ausreichend zu sichern, um unbefugten Zugriff zu verhindern. Neben den direkten Folgen für Betroffene kann ein Datenleck auch das Vertrauen in Institutionen massiv beschädigen und zu rechtlichen Konsequenzen führen. Die aktuelle Befragung zeigt:

22 % der Befragten waren bereits von einem Datenleck oder einer Datenpanne betroffen.

Personen, die von einem Leak betroffen waren, haben folgende Maßnahmen ergriffen:

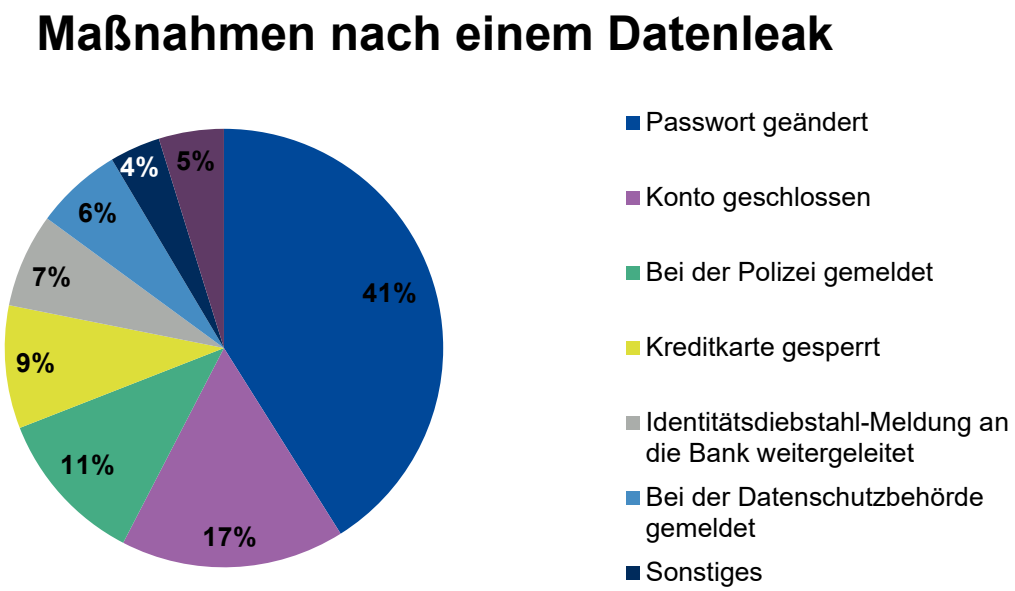


Abbildung 10: Maßnahmen nach einem Datenleck

Nach einem Datenleak haben Betroffene unterschiedliche Maßnahmen ergriffen, um ihre Daten nachträglich bestmöglich zu schützen und weiteren Schaden abzuwenden. **Die wichtigste Maßnahme war, das Passwort zu ändern**. Dies taten **41 % der Betroffenen**, da ein neues Passwort verhindert, dass Unbefugte weiterhin Zugriff auf ihre Konten haben. Diese Sicherheitsmaßnahme ist entscheidend, um persönliche Informationen zu schützen und eine weitere Kompromittierung der Konten zu verhindern.

17 % der Betroffenen entschieden sich, das betroffene Konto zu schließen. Durch diese drastische, aber wirksame Maßnahme entzogen sie Angreifern jegliche Möglichkeit, weiterhin auf sensible Daten zuzugreifen oder diese zu missbrauchen.

Eine weitere Maßnahme, die **11 % der Betroffenen ergriffen**, war eine **Meldung bei der Polizei**. Eine Anzeige kann helfen, rechtliche Schritte gegen die Täter einzuleiten und unterstützt die Strafverfolgungsbehörden bei der Bekämpfung von Cyberkriminalität. Auch wenn eine polizeiliche Anzeige den Vorfall nicht rückgängig machen kann, setzt sie ein klares Signal gegen digitale Straftaten.

Zum Schutz vor finanziellem Verlust **sperrten 9 % der Betroffenen vorsorglich ihre Kreditkarten** – eine sinnvolle Reaktion, da diese Sperrung unautorisierte Transaktionen verhindert und den Betroffenen finanzielle Sicherheit bietet.

Einige Betroffene, etwa **7 %, haben eine Meldung über den möglichen Identitätsdiebstahl an ihre Bank weitergeleitet.** Die Bank informiert zu halten, ist besonders wichtig, da sie in der Lage ist, notwendige Schutzmaßnahmen zu ergreifen und möglichen finanziellen Schaden zu minimieren.

Weitere **6 % der Betroffenen meldeten den Vorfall der Datenschutzbehörde**. Eine solche Meldung dokumentiert den Vorfall offiziell und ermöglicht es, das Datenleck rechtlich zu verfolgen und zusätzliche Schutzmaßnahmen einzuleiten.

Um sich vor zukünftigen Datenlecks zu schützen, wurden folgende Maßnahmen ergriffen:

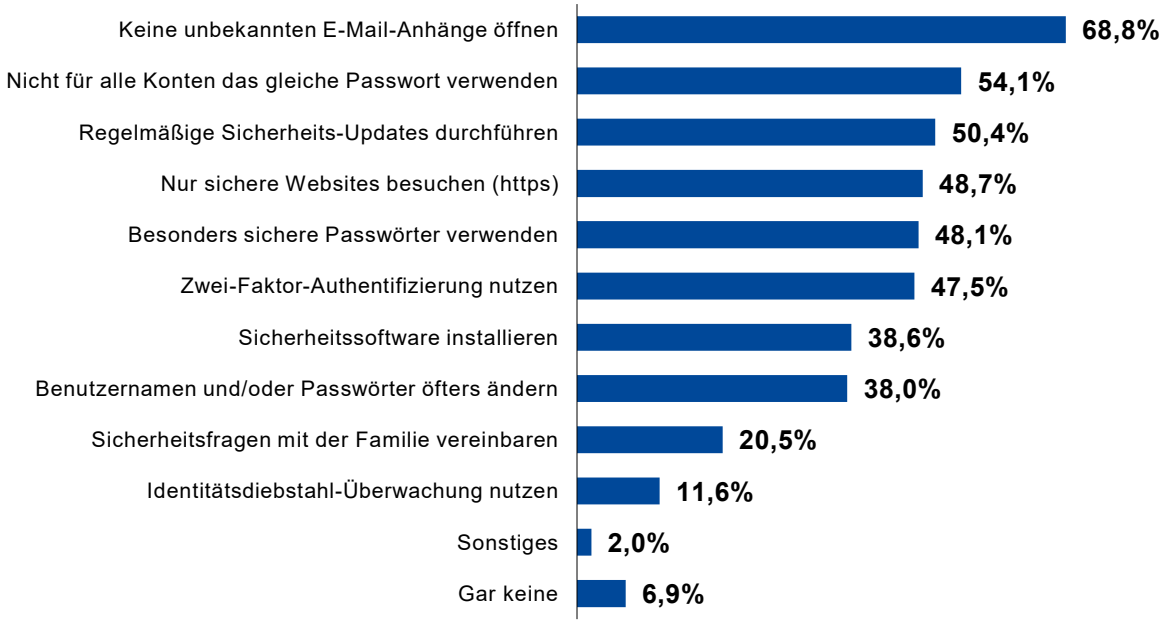


Abbildung 11: Schutz vor zukünftigen Datenlecks

4. Investmentbetrug

Investmentbetrug ist eine raffinierte Form des Betrugs, bei der Kriminelle gezielt Vertrauen aufbauen, um ihre Opfer zu einer Investition zu verleiten, die letztlich in den Taschen der Betrüger verschwindet. Typisch ist, dass die Betrüger professionelle und überzeugende Methoden einsetzen: **Sie verwenden gefälschte Videos, sogenannte Deepfakes, in denen prominente Persönlichkeiten scheinbar für die betreffende Investition werben.** Dazu kommt oft eine persönliche „Beratung“, die den **Eindruck von Seriosität** vermittelt und den Druck auf das Opfer erhöht, mehr Geld zu investieren.

Der Betrug bleibt meist so lange verborgen, **bis das Opfer seine Gewinne auszahlen lassen möchte.** Dann fordern die Betrüger plötzlich hohe Gebühren oder zusätzliche Zahlungen, um angebliche Auszahlungsprozesse zu decken. Bei genauerer Recherche stellt sich heraus, dass die Plattform eine lupenreine Fälschung ist. Häufig folgen auf den ersten Betrug später weitere Täuschungsmanöver: Kriminelle geben sich als Behörden oder Firmen aus, die Hilfe bei der Rückholung des verlorenen Geldes anbieten, verlangen dafür jedoch erneut Geld. Diese perfide durchdachte Masche zeigt, wie ausgeklügelt moderne Betrüger vorgehen, um Vertrauen zu gewinnen und emotionale Schwachstellen gutgläubiger Menschen auszunutzen.

4.1. Fallbeispiel: Claus und der Investmentbetrug

Claus surft gerade auf Facebook. Er liest von einem Datenleck bei der Firma „Seriousity“. Cyberkriminelle haben es geschafft, in das IT-System der Firma zu gelangen. E-Mail-Adressen, Telefonnummern, Namen, … – die Daten von über 23 Millionen Kunden sind jetzt in den Händen von Kriminellen.

„Wahnsinn“, denkt Claus, scrollt aber schon weiter und muss lächeln. Ein Video von seinem Lieblingsschauspieler erscheint auf dem Handy. Christoph Waltz erzählt begeistert davon, wie er reich geworden ist. Noch vor seiner Karriere hat er mit Bitcoins gehandelt, musste dafür kaum etwas tun und hatte innerhalb weniger Wochen ein Vermögen auf seinem Konto.

Claus wird neugierig, klickt auf den Link, der zu einer Plattform führt und liest sich alles genau durch. Er braucht nur 250 Euro zu zahlen – und schon ist er dabei. Eine machbare Summe, die ihn überzeugt. Er registriert sich, fängt an zu investieren, hat sogar einen persönlichen Berater, mit dem er fast täglich telefoniert. Die Gewinne steigen. Er investiert mehr.

Alles läuft gut – zumindest bis Claus entscheidet, dass er genug Geld hat und aufhören will. Er bittet seinen Berater, ihm seine Gewinne auszuzahlen. „Natürlich. Du brauchst nur eine Gebühr von 1.000 Euro zu zahlen, und das Geld ist auf deinem Konto“, antwortet der Berater.

Und da dämmert es Claus: Investmentbetrug. Er hatte doch schon mal von dieser Masche gehört. Aber das Video von Christoph Waltz, die Betreuung, die unglaublichen Gewinne. Es klang alles so plausibel. Er recherchiert, wie man Investmentbetrug erkennt, und nach und nach setzt sich das Puzzle zusammen.

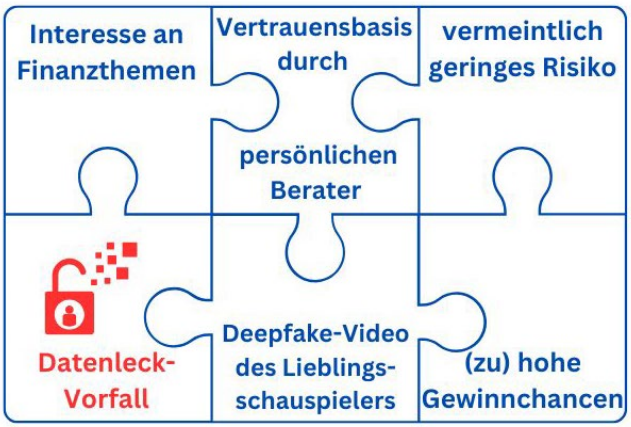


Abbildung 12: Investmentbetrug-Puzzle

Im Internet findet er auch Warnungen vor genau dieser Plattform. Ihm bleibt nur noch der Weg zur Polizei. Dort wird er informiert, dass er auf die Verhinderung von Folgebetrug achten muss: Oft melden sich die Kriminellen nach einigen Monaten oder sogar Jahren erneut und geben sich als Behörden oder Unternehmen aus, die dabei helfen können, das verlorene Geld zurückzuholen. Auch hier würde Claus nur dazu gedrängt werden, Geld auf das Konto der Kriminellen zu überweisen. Das Geld jedenfalls ist weg.

Die Geschichte von Claus illustriert eindrucksvoll, wie selbst Menschen mit vermeintlich gutem Wissen über Betrugsmaschen in die Falle tappen können. Claus, der sich für Finanzthemen interessiert, stieß auf ein verlockendes Angebot für Bitcoin-Investments, scheinbar beworben von seinem Lieblingsschauspieler Christoph Waltz.

Das professionell gestaltete Deepfake-Video und die persönliche Betreuung durch einen "Berater" weckten sein Vertrauen.

Erst als Claus seine vermeintlichen Gewinne abheben wollte und dafür eine hohe Gebühr zahlen sollte, wurde ihm der Betrug bewusst. Dieses Beispiel zeigt, **wie Kriminelle moderne Technologien wie Deepfakes nutzen, um ihre Opfer zu täuschen und emotionale Bindungen auszunutzen**.

4.2. Erkennungsmerkmale und Warnsignale

Beim Investmentbetrug versuchen Kriminelle, Menschen dazu zu bringen, in vermeintlich lukrative Geldanlagen zu investieren. Dabei werden meist **unrealistisch hohe Renditen in kurzer Zeit** versprochen, die ein normales Investment nicht bieten kann. Diese betrügerischen Angebote werden oft als risikofrei dargestellt, obwohl sie tatsächlich mit erheblichen finanziellen Verlusten verbunden sind. Das Ziel der Betrüger ist es, das Vertrauen ihrer Opfer zu gewinnen, um an deren Geld zu kommen.

Wichtige Warnsignale für Investmentbetrug

Abbildung 13: Erkennungsmerkmale Investmentbetrug

- **Hohe Gewinnversprechen bei kleinen Investitionen**: Angebote, die hohe Gewinne in kurzer Zeit garantieren und keine Risiken erwähnen, sind oft betrügerisch. Es gibt keine risikofreien Investitionen mit hohen Renditen.
- **Persönliche Betreuung durch angebliche Berater:** Betrüger geben sich als erfahrene Berater aus, ohne Qualifikation. Ihr Ziel ist es, Vertrauen aufzubauen, um an das Geld der Opfer zu gelangen.

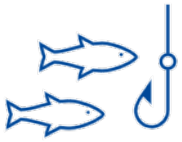
- **Zusätzliche Gebührenforderungen:** Häufig werden zusätzliche Überweisungen für „Transaktionsgebühren“ oder „Steuern“ gefordert, bevor eine Auszahlung angeblich freigegeben wird – ein klares Warnsignal.
- **Professionelle Videos oder Inhalte mit Prominenten:** Betrüger nutzen manipulierte Videos (etwa Deepfakes) und Inhalte mit bekannten Persönlichkeiten oder Logos seriöser Medien, um Vertrauen zu erwecken.
- **Werbung in sozialen Medien oder über Suchmaschinen:** Werbung über Social Media und Suchmaschinen, oft unter Verwendung bekannter Namen und Marken, soll Vertrauen erwecken und Opfer in die Falle locken.
- **Lockangebote mit kleinen Investitionen:** Kleine Investitionen mit unrealistisch hohen Gewinnversprechen sollen Vertrauen wecken. Tatsächlich werden diese Gewinne meist nicht ausgezahlt.
- **Pflicht zur Angabe einer Telefonnummer und „persönliche Beratung“:** Opfer werden kontaktiert und beraten, meist von geschulten Betrügern, die zu weiteren Investitionen drängen.
- **Fehlendes oder unvollständiges Impressum:** Seriöse Anbieter geben immer vollständige Kontakt- und Unternehmensinformationen an. Fehlen diese auf der Webseite, ist Vorsicht geboten.

4.3. Empfehlungen und Präventionstipps

Abbildung 14: Prävention von Investmentbetrug

5. Phishing und Datensicherheit

Phishing ist eine der **häufigsten Formen des Online-Betrugs.** Es handelt sich um den Versuch, über gefälschte E-Mails, Webseiten oder Nachrichten persönliche Daten wie Passwörter oder Kreditkartendaten zu stehlen. In der digitalen Welt von heute ist es unerlässlich, sich mit den Methoden und Risiken von Phishing auseinanderzusetzen, um sich effektiv zu schützen.



Der Begriff Phishing stammt aus dem Englischen und setzt sich aus **„password harvesting“ (Passwörter sammeln) und „fishing“ (Angeln, Fischen)** zusammen. Im übertragenen Sinne kann Phishing also als das Angeln von Passwörtern mit einem Köder verstanden werden. Aber nicht nur Passwörter werden mit dieser Methode erbeutet, auch Kreditkartendaten oder andere persönliche Daten sind bei Kriminellen beliebt.

Phishing-E-Mails gibt es schon sehr lange und sie sind – zumindest für die Kriminellen – immer noch effektiv. Sie **werden sogar immer professioneller**, da Kriminelle dank generativer KI-Anwendungen wie ChatGPT, Gemini oder Claude AI über Tools verfügen, mit denen sie fehlerfreie und überzeugende Nachrichten in vielen verschiedenen Sprachen verfassen können, darunter auch in weniger verbreiteten Sprachen. Auffällige Rechtschreib- oder Grammatikfehler gehören damit der Vergangenheit an.

Unter einem Vorwand (Köder) **werden die Opfer dazu gebracht, auf einen Link zu klicken und dort ihre Daten einzugeben** – die dann direkt in den Händen der Kriminellen landen. Haben Sie beispielsweise Ihre Zugangsdaten für Ihr E-Mail-Konto eingetippt, können sich die Kriminellen nun in Ihr Konto einloggen und in Ihrem Namen betrügerische E-Mails versenden.

Phishing-Angriffe können über verschiedene Kanäle erfolgen. E-Mails sind nach wie vor der häufigste Weg (68 % der Betrugsversuche), gefolgt von SMS (60 %) und Telefonanrufen (50 %). Die Kriminellen passen ihre Methoden ständig an und nutzen zunehmend auch soziale Medien und Messaging-Apps.

Die aktuelle Studie zeigt, dass 65 % der Befragten bereits einmal bemerkt haben, dass sie Ziel eines Phishing-Versuchs wurden. Diese hohe Zahl unterstreicht die Dringlichkeit, sich mit diesem Thema auseinanderzusetzen.

5.1. Fallbeispiel: Die Phishing-Falle, die doch noch zuschlug

Milena erhält seit Tagen E-Mails und SMS von Kriminellen, die sich als Banken, als Post und sogar als Finanzamt ausgeben. Sie kennt glücklicherweise die Tricks der Kriminellen und weiß, dass es sich um Phishing handelt: Sie überprüft bei E-Mails die Absende-Adressen und bemerkt somit schnell, dass diese nichts mit dem jeweils angeblichen Unternehmen zu tun haben. Generell sind Links in E-Mails immer verdächtig und sollten daher nicht voreilig angeklickt werden. Milena meldet sich also bei eventuellen Unsicherheiten direkt in ihrem Browser im Konto des jeweiligen Unternehmens an und folgt niemals einem Link in einer Mail.

Milena will aber wissen, wieso sie ausgerechnet jetzt massenhaft derartige Nachrichten erhält. Sie gibt auf der Seite havibeenpwned.com ihre E-Mail-Adresse ein, um zu überprüfen, ob es ein Datenleck gab, aufgrund dessen die Kriminellen ihre Daten haben. Und siehe da: Sie ist Kundin der Firma „Seriousity", die erst kürzlich von einem Datenleck betroffen war. Jetzt, wo sie Bescheid weiß, passt sie noch mehr auf als sonst. Aber leider funktionieren solche guten Vorsätze nicht immer ...

Als Milena an ihrem Arbeitsplatz gefühlt fünf Sachen gleichzeitig machen muss, erhält sie eine SMS von der Post. „Oh, nein! Jetzt steckt meine bestellte Kamera auch noch im Zoll fest", ist ihr erster Gedanke. Sie wartet schon so lange auf diese neue Kamera und will, dass das ersehnte Produkt endlich daheim ankommt.

Also unterbricht sie die Arbeit kurz, klickt auf den Link in der SMS, um ihre Daten zu bestätigen und die geforderten Gebühren zu zahlen. Zuhause kann sie es nicht fassen, als ihre Mitbewohnerin ihr freudig das Paket mit der Kamera darin überreicht. Unglaublich, aber wahr: Die sonst so umsichtige Milena ist doch noch in eine Phishing-Falle getappt. Sie überprüft ihr Konto – und tatsächlich: Statt 2,99 Euro hat sie 299 Euro freigegeben. Geld, das jetzt bei den Kriminellen liegt. Sie kontaktiert ihren Kreditkartenanbieter und lässt die Karte sofort sperren, bevor noch mehr abgebucht wird.

Milenas Geschichte zeigt, wie selbst informierte Menschen mit hohem Wissensstand zum Thema Phishing in einem Moment der Unachtsamkeit Opfer krimineller Energie werden können.

5.2. Erkennungsmerkmale und Warnsignale

Phishing-Mails zu erkennen und sich davor zu schützen ist heutzutage eine **zentrale Kompetenz**, um sicher im digitalen Raum zu agieren. Phishing-Attacken zielen darauf ab, **persönliche Daten wie Passwörter, Bankinformationen oder andere vertrauliche Angaben** zu erbeuten. Die Angreifer setzen dabei auf geschickt gefälschte E-Mails, die häufig wie legitime Nachrichten aussehen. Es gibt jedoch einige klare Erkennungsmerkmale und Warnsignale, die helfen können, solche betrügerischen Nachrichten zu entlarven.

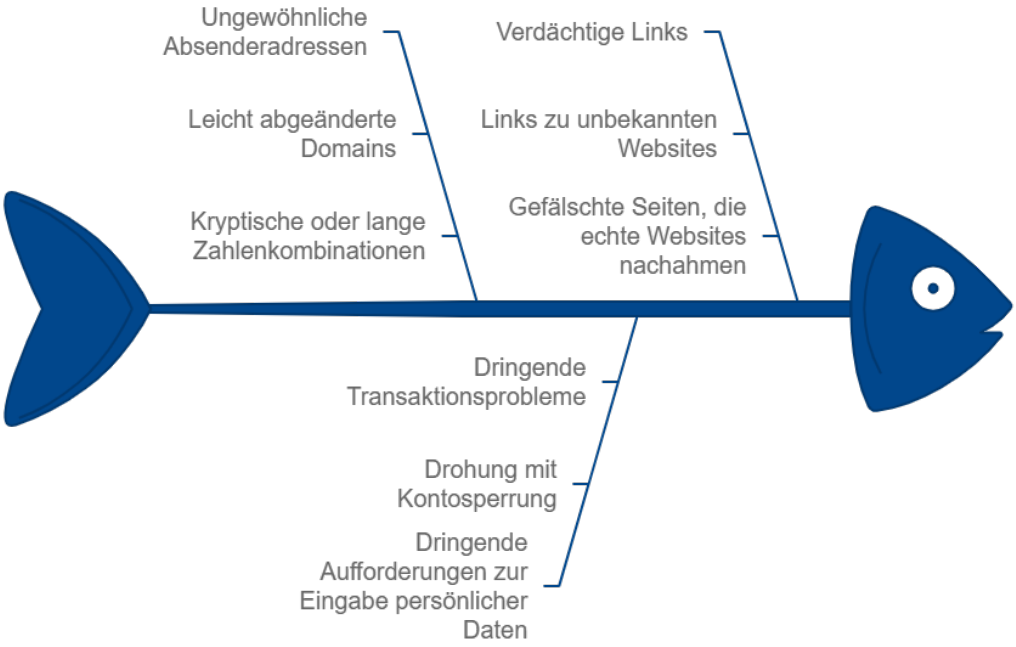


Abbildung 15: Erkennungsmerkmale Phishing

1) Ungewöhnliche Absenderadressen

Eines der wichtigsten Details, auf die man bei einer verdächtigen E-Mail sofort achten sollte, ist die Absenderadresse. Phishing-Mails kommen oft von Absendern, die auf den ersten Blick vertrauenswürdig wirken, aber bei genauerer Betrachtung **auffällige Unterschiede zu echten Adressen aufweisen**. Häufig verwenden die Angreifer leicht abgeänderte Domains, die dem Original zum Verwechseln ähnlich sind, zum Beispiel statt „@bank.de“ wird „@bank-sicherheit.de“ genutzt. Auch kryptische oder lange Zahlenkombinationen in der Absenderadresse sind ein häufiges Zeichen für Phishing-Versuche.

2) Dringende Aufforderungen zur Eingabe persönlicher Daten

Phishing-Mails beinhalten oft eine dringende Aufforderung, persönliche Informationen wie Passwörter, Kreditkartendaten oder Benutzernamen einzugeben. **Die Nachricht versucht**

häufig, Druck aufzubauen, indem behauptet wird, dass das Konto gesperrt wird oder wichtige Transaktionen nicht durchgeführt werden können, wenn nicht sofort gehandelt wird. Seriöse Unternehmen fordern niemals per E-Mail die Eingabe persönlicher Daten. Wenn eine Nachricht also dazu auffordert, sensible Informationen preiszugeben, sollte man **besonders misstrauisch werden.**

3) Links zu unbekannten oder verdächtigen Webseiten

Ein zentrales Warnsignal bei Phishing-Mails sind verdächtige Links. In den Mails werden oft Aufforderungen eingebaut, auf Links zu klicken, die angeblich zu einer vertrauten Webseite führen. Diese Links können jedoch zu gefälschten Seiten weiterleiten, die fast identisch mit den echten Webseiten aussehen, um sensible Daten abzugreifen. Um die Echtheit eines Links zu überprüfen, sollte man immer mit der Maus über den Link fahren (ohne zu klicken), um die tatsächliche URL in der Statusleiste des Browsers zu sehen. Wenn diese URL seltsam oder unbekannt aussieht, sollte der Link keinesfalls angeklickt werden.

5.3. Empfehlungen und Präventionstipps

Abbildung 16: Prävention von Phishing

- Nutzen Sie **Zwei-Faktor-Authentifizierung**
- Halten Sie Ihre **Software und Antivirusprogramme aktuell**
- Seien Sie **vorsichtig** bei **unerwarteten Nachrichten** oder **Anfragen.** Folgen Sie nie dem Link, sondern **überprüfen Sie direkt im Konto des jeweiligen** Anbieters ob tatsächlich eine Aktion notwendig ist.
- **Überprüfen** Sie regelmäßig Ihre **Kontobewegungen**

6. Fake-Shops

In der digitalen Einkaufswelt lauern viele Gefahren für Konsumenten. Betrügerische Online-Shops sind ein wachsendes Problem, das sowohl finanzielle Verluste als auch den Verlust persönlicher Daten zur Folge haben kann. Diese Shops nutzen oft verlockende Angebote, um ahnungslose Käufer in die Falle zu locken. Dabei gibt es unterschiedliche Arten von Fake-Shops:

Klassische Fake-Shops: Diese Fake-Shops sind sehr professionell gestaltet. Angeboten werden meist hochpreisige Waren wie Fahrräder und E-Bikes, Laptops und Monitore oder teure Haushaltsgeräte – meist zu Schleuderpreisen. Häufig wird auch auf sehr beliebte und daher bereits ausverkaufte Produkte gesetzt. Diese Shops verfügen über ein Impressum, das jedoch von seriösen Unternehmen kopiert wurde. Bezahlt wird meist per Vorkasse per Banküberweisung, Ware wird aber keine geliefert.

Markenfälscher-Shops: Wie der Name bereits verrät, werden hier vermeintliche Markenprodukte angeboten, oft bis zur Hälfte des Originalpreises. Impressum, Kontaktdaten oder andere Informationen über das Unternehmen sind auf der Seite nicht zu finden. Geliefert wird entweder gar nichts oder etwas, das mit dem bestellten Produkt gar nichts zu tun hat. Bezahlt wird mit Kreditkarte, da die Kriminellen in einigen Fällen auch die Kreditkartendaten beim Bezahlvorgang stehlen.

Problematische Online-Shops: Neben den Fake-Shops gibt es eine immer größer werdende Grauzone von Shops, die nicht eindeutig als betrügerisch einzustufen sind. Meist haben diese Online-Shops ihren Sitz im Ausland oder sie lassen direkt aus dem Ausland liefern (Dropshipper). Die Produktpalette reicht von orthopädischen Schuhen über stylische Wohnaccessoires oder witzige Haushaltsgadgets bis hin zu Nischenprodukten. Konsument:innen berichten von zahlreichen Problemen wie ausbleibenden Lieferungen, Lieferverzögerungen, minderwertiger Qualität, zusätzlichen Liefer- und Zollkosten oder der Verweigerung von Retouren.

Bei dieser Vielzahl an Variationen verwundert das Ergebnis der aktuellen Umfrage nicht: **Jede vierte befragte Person (25,1 %) wurde bereits auf einen Fake-Shop aufmerksam.**

6.1. Vom einmaligen Betrug zur langfristigen Problematik

Fake-Online-Shops stellen ein komplexes und anhaltendes Sicherheitsrisiko dar, das weit über den Verlust eines einzelnen bestellten Artikels hinausgeht. Neben der Gefahr, dass entweder keine Ware geliefert oder minderwertige Produkte versendet werden, liegt die wahre Bedrohung in der **Weitergabe sensibler Informationen**, die ahnungslose Kunden in betrügerische Bestellformulare eingeben. Sobald persönliche und finanzielle Daten in die Hände krimineller Akteure gelangen, steigt das Risiko für nachfolgende Betrugsversuche und vielfältige Formen des Identitätsmissbrauchs erheblich.

Betroffene sind oft nicht nur mit einem einmaligen finanziellen Verlust durch den Kauf konfrontiert, sondern geraten im Anschluss häufig in das Visier von **Phishing-Kampagnen, gefälschten Anrufen, betrügerischen E-Mails und anderen Arten digitaler Angriffe.** Die erlangten Daten ermöglichen es Betrügern, gezielt und wiederholt auf das Opfer einzuwirken, indem sie unter anderem den Anschein erwecken, dass weitere Transaktionen notwendig seien oder Sicherheitsmaßnahmen ergriffen werden müssten.

Der Missbrauch dieser Daten kann weitreichende Folgen haben: Kriminelle nutzen gestohlene Identitäten, um beispielsweise unter falschem Namen Bankkonten zu eröffnen oder Kredite aufzunehmen, was nicht nur zu einem langfristigen finanziellen Schaden führt, sondern auch einen erheblichen Aufwand und Stress für die Opfer bedeutet. Dieser Form des Betrugs geht somit eine Kette von betrügerischen Handlungen voraus, die aufeinander aufbauen und die Opfer über einen langen Zeitraum in einem Zustand der Unsicherheit halten können.

6.2. Fallbeispiel: Rita und der Online-Shop-Pflanz

Rita sucht online nach einem Geschenk für ihre beste Freundin Milena. Sie will Milena eine Freude machen und sie aufheitern, nachdem sie in die Phishing-Falle getappt ist.

Rita findet einen Online-Shop, der wunderschöne Zimmerpflanzen verkauft und das zu einem mehr als fairen Preis. Versandkosten gibt es auch keine, und in zwei Tagen ist die Pflanze da. „Perfekt“, freut sich Rita. Sie bestellt, zahlt per Klarna und wartet. Und wartet. Und wartet. Doch anstelle des Pakets kommt nur ein unerwarteter Anruf – und das ausgerechnet dann, als sie ziemlich gestresst kocht. Ein Bankmitarbeiter ist dran, angeblich wurde eine ungewöhnliche Abbuchung auf Milenas Konto festgestellt. Eine Sicherheitsprüfung genügt, um diese zu stoppen. Sie folgt den Anweisungen des Bankmitarbeiters.

Und merkt erst zu spät, dass es kein Bankmitarbeiter war. Beim Essen denkt sie nochmals in Ruhe über den Anruf nach und bekommt ein schlechtes Gefühl … und tatsächlich: Ein Blick auf ihr Konto bestätigt, dass sie keine Zahlung gestoppt, sondern eine Zahlung freigegeben hat.

Sie vermutet sogar einen Zusammenhang mit dem Shop. Sie recherchiert – und ihre Vermutung wird bestätigt: Ihre Daten wurden beim Zahlen abgegriffen, Kriminelle kennen ihren Namen, ihre Kontodaten, ihre Adresse. Kein Wunder, dass alles so überzeugend wirkte!

Später erinnert sie sich, wie sie sich über den „perfekten“ Zufallsfund gefreut hat. Jetzt weiß sie: Wenn etwas zu schön wirkt, um wahr zu sein, ist es das auch oft. Denn Kriminelle locken gerne mit unschlagbaren Angeboten – auch bei betrügerischen Online-Shops.

6.3. Erkennungsmerkmale und Warnsignale

Beim Online-Einkauf auf Fake-Shops zu stoßen, stellt ein immer größer werdendes Problem dar. Um sich vor Betrug zu schützen, ist es wichtig, typische Erkennungsmerkmale und Warnsignale solcher unseriösen Websites zu kennen. Die folgenden Hinweise können helfen, verdächtige Shops zu identifizieren und finanzielle Verluste zu vermeiden:

1. Unrealistisch niedrige Preise für hochwertige Produkte

Ein häufiges Warnsignal für einen Fake-Shop sind **auffallend niedrige Preise**, insbesondere bei Produkten, die normalerweise deutlich teurer sind. Wenn ein hochwertiges Markenprodukt zu einem Bruchteil des üblichen Preises angeboten wird, sollten Sie misstrauisch werden. Fake-Shops locken oft mit solchen verführerischen Angeboten, um potenzielle Kunden zum Kauf zu bewegen. Realistische Preise liegen selten weit unter dem Marktwert – Schnäppchen ja, aber in Maßen.

2. Fehlendes oder gefälschtes Impressum

Ein weiteres wichtiges Erkennungsmerkmal unseriöser Online-Shops ist das Fehlen eines vollständigen und korrekten Impressums. In Österreich und vielen anderen Ländern sind Händler **gesetzlich dazu verpflichtet, ein Impressum anzugeben**, das die vollständigen Kontaktdaten des Unternehmens enthält. Fake-Shops versuchen, diesen rechtlichen Anforderungen oft zu entgehen oder geben unvollständige, falsche oder irreführende Informationen an. Überprüfen Sie

die Adresse und gegebenenfalls die Telefonnummer, um die Seriosität des Anbieters zu verifizieren.

3. Zahlungsaufforderungen per Vorkasse oder Banküberweisung

Seriöse Online-Shops bieten in der Regel mehrere Zahlungsmethoden an, darunter sichere Optionen wie Kreditkarten, PayPal oder andere treuhänderische Dienste. Ein Shop, der **ausschließlich Vorkasse per Banküberweisung** verlangt, sollte mit Vorsicht betrachtet werden. Fake-Shops nutzen diese Methode, um das Geld schnell und unkompliziert zu kassieren, ohne eine Ware zu liefern. Zahlungen per Vorkasse sind schwer zurückzuverfolgen, sodass der Kunde bei einem Betrug kaum Chancen auf Rückerstattung hat.

4. Negative Bewertungen oder Warnungen im Internet

Eine **gründliche Internetrecherche** kann viel über die Seriosität eines Online-Shops verraten. Suchen Sie nach Erfahrungsberichten und Bewertungen anderer Kunden. Fake-Shops bewirken oft viele negative Bewertungen oder Warnungen von Verbraucherschutzportalen, die auf Probleme wie nicht gelieferte Waren, schlechte Kommunikation oder Schwierigkeiten bei der Rückerstattung hinweisen. **Achten Sie auch darauf, ob der Shop in Warnlisten geführt wird, die von Verbraucherschutzorganisationen herausgegeben werden.**

6.4. Empfehlungen und Präventionstipps

- **Website prüfen:** Achten Sie auf vollständiges Impressum, seriöse Domain und ein SSL-Zertifikat.
- **Realistische Preise:** Sehr günstige Angebote könnten betrügerisch sein – Preise vergleichen! Häufig werden ähnlich klingende Namen wie bekannte Marken verwendet, mit nur kleinen Abweichungen, daher besonders bei extrem günstigen Angeboten aufpassen!
- **Sichere Zahlungen:** Vermeiden Sie Vorkasse und bevorzugen Sie Zahlungen mit Käuferschutz.
- **Bewertungen hinterfragen:** Lesen Sie Bewertungen kritisch und prüfen Sie unabhängige Portale.
- **Shop recherchieren:** Domainalter und Firmenname online überprüfen.
- **Technische Sicherheit:** Nutzen Sie Sicherheitssoftware und 2-Faktor-Authentifizierung.
- **Kontaktmöglichkeiten:** Seriöse Shops bieten leicht erreichbaren Kundenservice.
- **AGB und Sprache:** Achten Sie auf klare AGB und eine professionelle Sprache.

7. Vishing und Robocalls

In einer Welt, in der sich Technologie rasant entwickelt, haben auch Betrüger ihre Methoden verfeinert. Das Internet und künstliche Intelligenz (KI) bieten ihnen neue Möglichkeiten, ihre Opfer zu täuschen.

Vishing setzt sich aus den englischen Wörtern **„Voice“ und „Phishing“** zusammen. Im Gegensatz zum Phishing stehen bei dieser Betrugsmasche nicht E-Mails im Vordergrund. Stattdessen versuchen Kriminelle, über einen Telefonanruf an Zugangsdaten zu gelangen oder ihre Opfer direkt zu einer Überweisung zu bewegen. Vishing wird bei einigen Kriminellen zunehmend beliebter, da sich am Telefon noch leichter emotionaler Druck aufbauen lässt.

Dazu kommt, dass die Täter **Rufnummern-Spoofing betreiben, also ihre Rufnummer so manipulieren, dass beispielsweise eine österreichische Rufnummer** angezeigt wird, obwohl der Anruf aus dem Ausland kommt: Durch die Nutzung eines VoIP-Dienstes (Voice over Internet Protocol) können die Kriminellen beliebige Zahlen- oder Buchstabenkombinationen am Display des Empfangsgerätes erscheinen lassen.

Die gute Nachricht: Seit September 2024 wird solches Spoofing in Österreich erschwert. Denn mit der neuen Anti-Spoofing-Verordnung müssen Mobilfunkbetreiber Anrufe aus dem Ausland mit österreichischen Rufnummern verifizieren. Ist eine Verifizierung nicht möglich, wird die Rufnummer am Display unterdrückt, bei Spoofing-Verdacht wird der Anruf sogar blockiert.

Aktuell erscheinen die meisten Vishing-Anrufe als **automatisierte Robocalls**, die oft als vermeintliche Anrufe von Behörden oder Familienmitgliedern getarnt sind. Diese täuschenden Anrufe nutzen einfache, **vorab aufgezeichnete Nachrichten**, die darauf abzielen, das Vertrauen der Opfer zu gewinnen und sie zur Herausgabe sensibler Informationen oder zur Durchführung bestimmter Handlungen zu bewegen. **In Zukunft wird jedoch erwartet, dass Künstliche Intelligenz diese Art des Betrugs wesentlich weiterentwickelt**. Mithilfe von KI-gesteuerten Systemen könnten die Betrüger personalisierte Gespräche führen, die auf Basis umfangreicher Datenbanken oder öffentlich zugänglicher Informationen speziell auf die Zielperson abgestimmt sind. So könnten KI-basierte Stimmen beispielsweise individuelle Sprachmuster oder persönliche Details imitieren und somit noch glaubhafter auftreten. Diese Weiterentwicklung erhöht das Risiko erheblich, da die Anrufe noch überzeugender und schwerer zu erkennen sein werden, was die Herausforderung für Verbraucher und Sicherheitsexperten weiter verschärft.

7.1. Mario und die Entdeckung krimineller Effektivität

Mario ist ein weiterer „Seriousity“-Kunde und damit eine weitere Person, deren Daten an Kriminelle verkauft wurden.

Wie Milena merkt er das an den vielen E-Mails, die er immer wieder in seinen Spam-Ordner verschiebt. Seine Hoffnung: Irgendwann lernt das E-Mail-Programm, dass solche Nachrichten von vornherein im Spam-Ordner landen sollen.

Rrrring. Rrrrrring. Rrrrrrring.

Das schrille Klingeln seines Handys unterbricht Marios Gedanken. Er hebt ab. Eine blecherne Stimme meldet sich: „Es gibt einen Haftbefehl auf Ihren Namen, und Ihr Eigentum wird beschlagnahmt. Drücken Sie die 1, um mit einem Bundesbeamten zu sprechen und weitere Informationen zu erhalten."

Seine Gedanken überschlagen sich: Wie ein Mensch klingt das nicht … Was heißt hier Haftbefehl? Mein Eigentum soll beschlagnahmt werden? Was will ein Bundesbeamter von mir …? Und schon drückt er die 1. Eine nun menschliche Stimme stellt sich als österreichische Polizeibeamtin vor und fragt nach Namen, Adresse und Kreditkartendaten. Das würde helfen, alles aufzuklären. Verwirrt, aber doch froh über das Missverständnis, folgt er den Anweisungen der Polizistin und bedankt sich, als alles erledigt ist.

Nach all der Anspannung ist Entspannung angesagt. Also Füße hoch, Fernseher an. So zumindest der Plan. Als Mario die Nachrichten einschaltet, wird über einen neuen Telefonbetrug berichtet, der ihm verdammt bekannt vorkommt. Irgendwas mit Taste 1, Polizei und Kreditkartendaten. „Mit diesem Trick werden nur Menschen an die Kriminellen weitergeleitet, die grundsätzlich anfällig für Internetbetrug sind", tönt es aus dem Fernseher. „Toll. Wie effektiv", ergänzt Mario. Als der Moderator erklärt, wie man solche Anrufe als Betrug enttarnt, hängt Mario an seinen Lippen:

- *Kurz innehalten und überlegen: Warum sollte es einen Haftbefehl geben? Und selbst wenn es ihn gäbe, würde die Polizei ihn nicht so kommunizieren.*

- *Keine persönlichen Daten preisgeben: Polizeibeamte fordern niemanden am Telefon auf, seine Kreditkartendaten preiszugeben.*

Mario nimmt sich fest vor – sollte er nochmals in eine derartige Situation kommen –, die Ruhe zu bewahren und die Sachlage logisch zu hinterfragen.

7.2. Erkennungsmerkmale und Warnsignale

Robocalls sind automatisierte Telefonanrufe, die mithilfe vorab aufgezeichneter Nachrichten oder computergenerierter Stimmen ablaufen. Ursprünglich wurden Robocalls von Unternehmen für legitime Zwecke genutzt, etwa um Kunden an Termine zu erinnern oder Angebote zu teilen. Kriminelle haben diese Technik jedoch adaptiert, um betrügerische Anrufe im großen Stil durchzuführen und sensible Informationen zu erbeuten.

Betrügerische Robocalls nutzen computergesteuerte Anrufsprogramme, um in kurzer Zeit tausende Menschen anzurufen. Die Anrufe beginnen oft mit einer automatisierten Nachricht, die eine dringende oder emotionale Situation schildert – etwa, dass das Bankkonto des Opfers gesperrt sei oder dass das Finanzamt sofortige Zahlung fordere, um Konsequenzen zu vermeiden. Das Ziel ist, das Opfer zu einem Rückruf oder zur Eingabe vertraulicher Daten zu drängen.

Im Gegensatz zu direkten Vishing-Anrufen werden bei Robocalls häufig die folgenden Elemente verwendet:

1. **Automatisierte Nachrichten**

Robocalls spielen standardisierte Nachrichten ab, die das Opfer in Stress versetzen sollen. Dies geschieht häufig in einem autoritären Ton oder durch die Darstellung einer vermeintlich kritischen Situation.

2. **Interaktive Anweisungen**

Viele betrügerische Robocalls nutzen Tastenoptionen, etwa "Drücken Sie 1, um einen Mitarbeiter zu sprechen". So werden die Opfer an einen echten Betrüger weitergeleitet, der das Gespräch fortführt und gezielt nach vertraulichen Informationen fragt.

3. **Gefälschte Anruferkennung**

Robocalls nutzen oft „Spoofing“-Technologie, um eine vertrauenswürdige Rufnummer auf dem Display des Opfers anzuzeigen, etwa von einer Bank oder Behörde. Das soll das Opfer dazu bringen, den Anruf als seriös wahrzunehmen.

4. **Betrügerische Szenarien**

Typische Szenarien in Robocalls sind angebliche Sicherheitswarnungen von Banken, falsche Steuerbescheide oder Lotteriegewinne, die nur durch eine Vorauszahlung freigegeben werden können. Ziel ist immer, das Opfer emotional unter Druck zu setzen und zur schnellen Herausgabe von Informationen oder Geldern zu drängen.

7.3. Präventionstipps

- **Keine Reaktion auf verdächtige Anrufe**
  Legen Sie bei unbekannten, automatisierten Anrufen sofort auf. Wenn der Anruf angeblich von einer Institution stammt, können Sie über die offizielle Rufnummer zurückrufen, um die Echtheit zu überprüfen.
- **Automatische Anrufblockierung verwenden**
  Viele Telefonanbieter bieten Schutzdienste, die verdächtige Anrufe blockieren können. Die Installation spezieller Apps kann zusätzlich helfen, verdächtige Robocalls herauszufiltern.
- **Keine persönlichen Daten weitergeben**
  Seriöse Unternehmen und Behörden fragen niemals am Telefon nach sensiblen Daten. Bleiben Sie wachsam und hinterfragen Sie jede Situation, bei der vertrauliche Informationen verlangt werden.
- **Verständnis für Spoofing entwickeln**
  Machen Sie sich bewusst, dass die Anzeige einer bekannten Telefonnummer keine Garantie dafür ist, dass der Anruf auch tatsächlich von dieser Nummer stammt.
- **Emotionale Anfragen hinterfragen**
  Betrügerische Robocalls nutzen oft emotionale Manipulation. Seien Sie vorsichtig bei Anrufen, die Sie unter Druck setzen oder mit drastischen Konsequenzen drohen.
- **Keine Weitergabe sensibler Daten am Telefon**
  Betrüger fragen häufig nach sensiblen Daten wie PIN-Nummern oder Passwörtern, die seriöse Unternehmen niemals am Telefon erfragen würden.

8. KI-unterstützter Betrug: Die neue Bedrohung

Künstliche Intelligenz (KI) revolutioniert viele Bereiche unseres Lebens. Sie birgt nicht nur Chancen, sondern auch erhebliche Risiken, insbesondere im Bereich des Online-Betrugs. KI-unterstützte Betrugsmaschen nutzen fortschrittliche Technologien wie Deepfakes und Voice Cloning, um Menschen zu täuschen und zu manipulieren. Diese neuen Methoden sind besonders gefährlich, da sie schwer zu erkennen sind und das Vertrauen der Opfer gezielt ausnutzen. Zwei von drei Befragten (66 %) sind solche KI-unterstützten Betrugsversuche bekannt. Dies zeigt, dass das Bewusstsein für diese neue Form des Betrugs in der Bevölkerung wächst.

8.1. Fallbeispiel: Der Deepfake-Tochtertrick

Mario hat aus seinem Fehler gelernt – auch zwei Jahre später denkt er noch an seinen unerfreulichen Fauxpas. Vieles hat sich verändert, die Tricks der Kriminellen sind noch professioneller geworden und immer schwerer zu durchschauen.

Noch einmal will er nicht in die Falle tappen. Deshalb hält er sich mit Hilfe der Watchlist Internet über Internet-Betrügereien auf dem Laufenden. Gerade als Mario auf watchlist-internet.at einen neuen Artikel über irreführende Abofallen liest, bekommt er wieder einen Anruf. „Papa, ich bin's!", schluchzt seine Tochter Anais verzweifelt ins Telefon. Aufgewühlt berichtet sie, dass sie in einen Unfall verwickelt war – und das im Urlaub: ihr Auto Totalschaden, ihre Nerven blank und ihr Bankkonto leer. Sie braucht dringend Hilfe und bittet ihren Vater, ihr Geld zu überweisen. Noch bevor Anais erklären kann, warum sie jetzt sofort Geld braucht, unterbricht Mario sie: „Wie lautet das Geburtsdatum deiner ersten Katze?“ Anais ignoriert die Frage und schluchzt weiter ins Telefon. „Du bist nicht meine Tochter", sagt Mario darauf und legt eiskalt auf. Ganz so eiskalt war es dann doch nicht … Seine Hände schwitzen, und sein Herz schlägt ihm bis zum Hals.

Die Masche mit dem Deepfake-Enkeltrick ist mittlerweile mehr als bekannt: Kriminelle klonen mit Hilfe künstlicher Intelligenz die Stimmen von Verwandten und Bekannten und geben sich am Telefon als diese aus. Dass das ausgerechnet Anais passiert, wundert Mario überhaupt nicht. Als renommierte Wissenschaftlerin ist sie im Internet mit zahlreichen Audioaufnahmen ihrer Stimme präsent. Mehr als genug, um Verbrechern die Möglichkeit zu bieten, ein überzeugendes Deep Fake ihrer Stimme zu erstellen. Das ist auch der Grund, weshalb sich Mario und seine Tochter eine Sicherheitsfrage für genau solche Fälle überlegt haben: das Geburtsdatum von Anais‘ erster Katze. Wenn die Person am Telefon nicht darauf antwortet, weiß Mario: Hier stimmt was nicht. Um aber wirklich auf Nummer sicher zu gehen, ruft Mario sofort seine Tochter an, diesmal die echte. Sein Verdacht bestätigt sich: Alles in Ordnung. Lachend erzählt Anais ihrem Vater die Höhepunkte ihres bisherigen Urlaubs. Ein Unfall gehört nicht dazu.

Wie die genannten Beispiele zeigen, spielt künstliche Intelligenz bereits heute eine wichtige Rolle bei Online-Betrug: Deepfakes von Prominenten werden erstellt, um Autorität und Seriosität vorzutäuschen, und Phishing-Nachrichten, aber auch Malware können mit Hilfe von künstlicher Intelligenz professionalisiert werden.

8.2. Erkennungsmerkmale und Warnsignale

Der Enkel- oder Tochtertrick, auch als „Verwandtentrick“ bekannt, ist eine der beliebtesten Betrugsmethoden, die vor allem auf ältere Menschen abzielt. Ziel ist es, das Vertrauen der Opfer zu gewinnen, indem sich die Anrufer als nahe Verwandte in einer akuten Notlage ausgeben. Doch diese Betrugsmethoden entwickeln sich stetig weiter und werden durch die Nutzung moderner Technologien immer raffinierter. Robocalls und gefälschte Anruferkennungen („Spoofing“) helfen Tätern, sich authentisch darzustellen und das Vertrauen der Opfer schneller zu gewinnen.

Der Enkeltrick: Wie läuft die Masche aktuell ab?

Beim klassischen Enkeltrick gibt sich der Anrufer als Verwandter des Opfers aus, der oder die sich in einer verzweifelten Situation befindet – häufig geht es um einen plötzlichen Unfall, eine dringende medizinische Behandlung oder eine akute finanzielle Notlage. Der Betrüger schildert das Szenario emotional und bittet um schnelle finanzielle Unterstützung. **Durch den Einsatz einer vertraut klingenden Anrede und gezielte Manipulationen wird beim Opfer Mitgefühl und Hilfsbereitschaft geweckt.**

Aktuelle Betrugsmethoden nutzen dabei jedoch modernste Technologie, um noch glaubwürdiger aufzutreten. Einige Täter verwenden gefälschte Telefonnummern, um auf dem Display eine bekannte Nummer anzeigen zu lassen – etwa die eines Krankenhauses, einer Behörde oder einer Familiennummer. Oft werden diese Anrufe mit automatisierten Nachrichten (Robocalls) eingeleitet, die das Opfer vorwarnen, um das Vertrauen zu gewinnen, bevor ein Betrüger persönlich übernimmt und das Gespräch fortsetzt.

Zusätzlich wird häufig eine dritte Person ins Spiel gebracht, die als vermeintlicher „Mitarbeiter“ auftritt, der die Geschichte untermauert. So kann etwa jemand behaupten, ein Anwalt oder Arzt zu sein, der das Problem bestätigt, um das Opfer emotional weiter unter Druck zu setzen.

Betrug durch angebliche Behörden und Banken

Kriminelle geben sich auch häufig als Mitarbeiter von Behörden oder Banken aus, um Vertrauen zu gewinnen. Ein typisches Szenario ist ein angeblicher Sicherheitsvorfall, bei dem der Anrufer sich als Bankmitarbeiter oder Polizist ausgibt und behauptet, es gäbe verdächtige Aktivitäten auf dem Konto des Opfers. **Häufig wird erklärt, das Konto sei Ziel eines Diebstahls oder einer Phishing-Attacke geworden.** Durch „Spoofing“ kann der Anruf scheinbar von einer offiziellen Telefonnummer der Bank oder Polizei stammen. Oft erhalten die Opfer die Anweisung, Geld abzuheben und es an eine vermeintlich sichere Stelle zu übergeben, um es „zu schützen“.

Diese Formen des Betrugs entwickeln sich jedoch kontinuierlich weiter, und die Täter werden immer raffinierter in ihren Methoden. Mit der fortschreitenden Technologie und dem stärkeren Einsatz künstlicher Intelligenz (KI) eröffnen sich Betrügern neue Möglichkeiten, die herkömmlichen Methoden anzupassen und noch gezielter auf ihre Opfer einzugehen. KI bietet die Fähigkeit,

riesige Datenmengen in kürzester Zeit zu analysieren, was den Betrügern erlaubt, Informationen über ihre Zielpersonen zu sammeln und damit ihr Verhalten zu verstehen und vorherzusagen.

So können betrügerische Systeme mittlerweile spezifische Details über eine Person aufnehmen und diese Details in einem täuschend echten Kontext verwenden. **Beispielsweise können Betrüger durch KI-gestützte Sprachsynthese-Techniken die Stimme von Familienmitgliedern oder Freunden des Opfers imitieren**. Diese Technologie ermöglicht es ihnen, gezielt und sehr glaubwürdig in die Rolle einer vertrauten Person zu schlüpfen, was das Vertrauen des Opfers verstärkt und die Wahrscheinlichkeit erhöht, dass es auf die Betrugsmasche hereinfällt.

Zusätzlich ermöglicht KI, emotionale Manipulationstechniken genauer abzustimmen und auf das Verhalten und die Reaktionen des Opfers anzupassen. Indem das System auf bestimmte Antworten und Emotionen reagiert, kann es das Gespräch in Echtzeit dynamisch verändern und genau die Informationen liefern, die das Opfer emotional beeinflussen und unter Druck setzen. So wird es für die Opfer immer schwieriger, zwischen einem echten Hilferuf oder einer authentischen Nachricht und einem gut ausgeklügelten Betrug zu unterscheiden.

Der Einsatz von KI ermöglicht es Betrügern auch, „Spoofing"-Technologien mit einer bislang unerreichten Präzision anzuwenden. Durch die Manipulation der Anruferkennung kann der Anruf für das Opfer so wirken, als käme er von einer bekannten Telefonnummer, etwa von der Bank oder einer Behörde. **Diese Technologien werden immer ausgefeilter, sodass auch gängige Sicherheitsmaßnahmen, wie die Überprüfung der Anrufer-ID, nicht mehr ausreichen, um einen Betrugsversuch zu erkennen.**

Der technologische Fortschritt in Verbindung mit KI verleiht den Tätern also die Möglichkeit, immer individuellere und glaubwürdigere Geschichten zu erzählen. Das Ziel besteht dabei stets darin, das Opfer in eine emotionale Lage zu versetzen, in der es aus Sorge oder Angst handelt und rationale Überlegungen zurückstellt. **Diese technologische Anpassung macht es nötig, dass auch die Präventionsmaßnahmen und die Wachsamkeit der potenziellen Opfer sich kontinuierlich weiterentwickeln.** Erkennungsmerkmale dieser Betrugsform sind:

Ungewöhnliche oder unerwartete Anrufe von Bekannten oder Familienmitgliedern

Betrüger rufen häufig im Namen eines vermeintlich vertrauten Familienmitglieds oder Bekannten an. Die Anrufe kommen meist völlig unerwartet und zu ungewöhnlichen Zeiten. Oft gibt sich der Anrufer als Enkelkind, Neffe oder enge Freundin aus und nutzt dabei das Überraschungsmoment. Dies soll den Angerufenen verunsichern und dazu führen, dass er dem Anrufer eher glaubt.

Emotionale Geschichten oder dringende Bitten um finanzielle Unterstützung

Betrüger setzen darauf, dass ein emotionaler Appell das kritische Denkvermögen übersteuert. Häufig schildern sie dramatische Situationen, wie zum Beispiel einen Unfall, einen finanziellen Notfall oder eine dringende Reise, für die sofort Geld benötigt wird. Sie setzen den Angerufenen

bewusst unter Druck und appellieren an dessen Hilfsbereitschaft. Dies ist eine besonders perfide Taktik, die ältere Menschen schnell emotional belastet und in die Irre führen kann.

Anrufer verwenden bekannte Stimmen oder persönliche Informationen

Betrüger nutzen inzwischen häufig persönliche Informationen aus sozialen Netzwerken oder anderen Quellen im Internet, um Vertrauen aufzubauen. Sie nennen beispielsweise den Namen eines Verwandten, sprechen über gemeinsame Erinnerungen oder erwähnen Orte, an denen die Familie früher oft war. Diese Informationen helfen den Tätern, ihre Glaubwürdigkeit zu erhöhen.

Verwendung von KI-generierten Inhalten wie Deepfakes

Mittels KI können Betrüger Stimmen imitieren und sogar visuelle Deepfakes erstellen. So können sie einen Videoanruf vortäuschen, bei dem das Gesicht und die Stimme einer vertrauten Person nahezu perfekt nachgeahmt werden. Die neuen Technologien erschweren es, die Identität des Anrufers zu überprüfen. Besonders bei älteren Menschen, die mit diesen Techniken oft nicht vertraut sind, können solche KI-Manipulationen großen Schaden anrichten.

8.3. Empfehlungen und Präventionstipps

1. Bei unerwarteten Anrufen misstrauisch sein

Wenn ein Anruf von einem Verwandten oder Bekannten ungewöhnlich erscheint, ist es ratsam, den Anrufer höflich zu hinterfragen und auf unlogische oder inkonsistente Antworten zu achten.

Halten Sie inne und lassen Sie sich nicht von emotionalen Appellen unter Druck setzen.

2. Rückruf unter der bekannten Nummer

Beenden Sie das Gespräch und rufen Sie den vermeintlichen Verwandten oder Bekannten unter seiner bekannten Telefonnummer zurück. Häufig reicht ein Rückruf, um festzustellen, ob der Anruf tatsächlich von dieser Person kam.

3. Codewort oder Kennfrage vereinbaren

Mit Familienmitgliedern und engen Freunden kann ein geheimes Codewort oder eine Kennfrage vereinbart werden, die nur echte Verwandte kennen. Falls ein solcher Anruf kommt, fragen Sie nach dem Codewort.

4. Persönliche Informationen schützen

Geben Sie keine persönlichen Informationen an Unbekannte weiter und beschränken Sie Ihre Angaben in sozialen Medien. Betrüger nutzen häufig öffentlich zugängliche Informationen, um Vertrauen aufzubauen.

5. Auf KI-gestützte Täuschungstechniken achten

Wenn Sie einen Anruf über einen Videochat erhalten und Ihnen die Person merkwürdig vorkommt, seien Sie wachsam. Deepfake-Videos und -Stimmen können täuschend echt wirken. Achten Sie auf kleine Verzögerungen oder unnatürliche Bewegungen, die manchmal bei Deepfakes auftreten.

6. Gespräch unterbrechen und Hilfe holen

Wenn der Anrufer Sie unter Druck setzt, sollten Sie das Gespräch sofort beenden und eine Vertrauensperson zurate ziehen. Beraten Sie sich mit Freunden, Verwandten oder Nachbarn, bevor Sie auf Forderungen eingehen.

8. Keine Geldübergaben an Dritte

Betrüger geben manchmal vor, dass das Geld dringend an eine dritte Person übergeben werden muss, die „im Auftrag“ des Verwandten kommt. Nehmen Sie in keinem Fall Übergaben vor und holen Sie stattdessen einen unabhängigen Zeugen hinzu oder verständigen Sie die Polizei.

9. Angehörige sensibilisieren

Besonders ältere Familienmitglieder sollten regelmäßig über neue Betrugsmethoden informiert werden. Workshops oder Informationsveranstaltungen können dabei hilfreich sein.

10. Im Zweifelsfall die Polizei kontaktieren

Zögern Sie nicht, bei Verdacht auf Betrug die Polizei einzuschalten. Polizei und Behörden sind mit den neuesten Betrugsmethoden vertraut und können helfen, die Gefahr richtig einzuschätzen.

9. Was bringt die Zukunft?

Der Einfluss künstlicher Intelligenz auf die verschiedenen Methoden des Internetbetrugs wird künftig massiv zunehmen. Hier einige Zukunftsszenarien, die in diesem Zusammenhang zu erwarten sind:

Voice Cloning: Das Klonen von Stimmen funktioniert in vielen Fällen bereits sehr gut (z.B. bei Personen ohne Dialekt oder bei weit verbreiteten Sprachen). Neben dem Klonen von Stimmen aus dem familiären Umfeld sind auch Stimmenimitationen von Geschäftsführer:innen, um Mitarbeiter:innen zu Überweisungen zu überreden, oder Voice Cloning zur Aushebelung von Spracherkennungssystemen realistische Szenarien – erste Fälle, in denen KI in diesen Kontexten eingesetzt wird, sind bereits bekannt.

KI-generierte Videos: Auch Deepfake-Videos haben Anwendungsbereiche, die über die Bewerbung betrügerischer Angebote hinausgehen. So können – ähnlich wie beim Voice Cloning – Gesichtserkennungssysteme überlistet oder Personen aus dem familiären oder beruflichen Umfeld imitiert werden, um an Geld oder Informationen zu gelangen. Sogar Deepfakes in Echtzeit sind möglich, die beispielsweise bei Videokonferenzen am Arbeitsplatz oder beim Love Scamming eingesetzt werden können.

KI-generierte Bilder: KI-Modelle zur Bilderzeugung können so trainiert werden, dass das Ergebnis immer dieselbe Person abbildet. Diese Funktion ist vor allem bei der Erstellung von konsistenten Fake-Profilen hilfreich, beispielsweise für Love Scammer. Aktuell nutzen Kriminelle gestohlene Bilder aus dem Internet, um sich als eine bestimmte Person auszugeben. Eine umgekehrte Bildersuche würde die Kriminellen entlarven. Mit KI-generierten Bildern sinkt das Entdeckungsrisiko. Darüber hinaus gibt es zahlreiche KI-gestützte Tools, die es ermöglichen, auf einem Foto abgebildete Personen „auszuziehen“ (Deep Nudes). Solche Bilder (aber auch Videos) können unter anderem zur Erpressung der abgebildeten Personen verwendet werden.

AI-as-a-Service: Crime-as-a-Service ist ein illegales Geschäftsmodell, bei dem Tools, Dienstleistungen, Plattformen oder Know-how zur Durchführung krimineller Handlungen angeboten werden. Dadurch wird Cyberkriminalität auch für technisch weniger versierte Personen möglich. Zu erwarten ist, dass KI diesem Geschäftsmodell zusätzlichen Auftrieb geben wird. So kann KI beispielsweise zum Schreiben von Schadprogrammen oder zur Verbesserung von Hacking-Techniken eingesetzt werden. Im Darknet sind bereits erste Anwendungen aufgetaucht, die Kriminellen den Alltag erleichtern sollen – etwa KI-gestütztes Passwort-Guessing, CAPTCHA-Umgehungen, Prompt-Engineering-Tools oder Jailbreaking-Anwendungen zum Aushebeln von Schutzmaßnahmen.

Durch den Einsatz von KI durch Kriminelle werden Betrugsmaschen noch mehr zu Massenphänomenen. Das Gute daran: Massenphänomene erleichtern das Erkennen von Mustern und Regelmäßigkeiten und treiben damit auch die KI-basierte Betrugserkennung voran.

Für Strafverfolgungsbehörden, Betrugsbekämpfungsorganisationen und Verbraucherschutzverbände bietet KI neue Möglichkeiten. Durch die Entwicklung von KI-Tools können Betrugsmaschen nicht nur schneller, sondern auch quantitativ mehr Betrugsversuche detektiert werden als noch vor wenigen Jahren. Ein Beispiel ist der Fake-Shop Detektor der Watchlist Internet, der mit Hilfe von KI Online-Shops bewertet und Nutzer:innen per Browser-Plugin in Echtzeit vor betrügerischen Seiten warnt. Auch Antivirenprogramme setzen zunehmend auf KI und maschinelles Lernen, um ihre Systeme zu verbessern und so auch neue, bisher unbekannte Arten von Schadsoftware zu erkennen.

Im Rahmen der Studie „2024 Anti-Fraud Technology Benchmarking“ wurden Organisationen weltweit befragt, ob sie aktuell KI oder maschinelles Lernen zur Betrugsbekämpfung einsetzen. Das Ergebnis: 18 % nutzen KI, weitere 32 % werden KI in den nächsten Jahren implementieren. Gleichzeitig ist bekannt, dass Kriminelle zu den Early Adopters neuer Technologien gehören. KI ist also ein zweischneidiges Schwert, das sowohl Chancen für Innovation und Automatisierung in der Betrugsbekämpfung bietet als auch zur Professionalisierung von Betrugsmaschen beitragen kann. Beispiele für verbesserte Betrugsbekämpfung mittels KI-Anwendungen:

KI-gestützte Betrugserkennung: Systeme wie der Fake-Shop-Detektor der Watchlist Internet nutzen KI, um in Echtzeit vor betrügerischen Websites zu warnen.

Verbesserte Antivirenprogramme: KI und maschinelles Lernen werden zunehmend eingesetzt, um auch neue, bisher unbekannte Arten von Schadsoftware zu erkennen.

Automatisierte Analyse von Betrugsmustern: KI kann große Datenmengen analysieren, um neue Betrugstrends frühzeitig zu erkennen und Gegenmaßnahmen zu entwickeln.

10. Fazit

In einer Welt, in der Online-Betrug immer raffinierter wird, ist Prävention der Schlüssel zum Schutz. Die vorliegende Studie zeigt, dass viele Österreicher sich der Gefahren bewusst sind und aktiv Maßnahmen ergreifen, um sich zu schützen. 60 % der Österreicher:innen ergreifen bewusst selbst Maßnahmen, doch es bleiben 40 %, die zu leichten Opfern für geschickte Betrüger werden könnten.

10.1. Fallbeispiel: Vom Opfer zur Präventions-Expertin

Um die Bedeutung von Präventionsmaßnahmen zu veranschaulichen, betrachten wir die Geschichte von Tina:

Tina hat in den letzten Jahren viel gelernt. Nachdem sie Opfer eines Online-Betrugs wurde, hat sie sich intensiv mit dem Thema Internetsicherheit auseinandergesetzt. Heute gilt sie in ihrem Freundeskreis als Expertin für Prävention.

An einem Samstagnachmittag erhält Tina eine SMS: „Mama, mein Handy ist kaputt. Das ist meine neue Nummer. Kannst du mir bitte 2.500 Euro für eine dringende Rechnung überweisen? Ich melde mich später." Tina lächelt. Sie weiß sofort, dass es sich um einen Betrugsversuch handelt. Statt zu antworten, ruft sie ihre Tochter auf der alten Handy-Nummer an. Wie erwartet, ist alles in Ordnung.

Tina nutzt die Gelegenheit, um ihre Freunde über diese Betrugsmasche zu informieren. Sie postet in ihrer WhatsApp-Gruppe: „Achtung, Freunde! Ich habe gerade eine betrügerische SMS erhalten. Passt auf solche Nachrichten auf und überprüft immer die Identität des Absenders, bevor ihr Geld überweist."

Prävention ist der beste Schutz gegen Online-Betrug. Indem wir wachsam bleiben, uns informieren und aktiv Schutzmaßnahmen ergreifen, können wir das Risiko, Opfer von Betrug zu werden, erheblich reduzieren.

Wie Tinas Geschichte zeigt, kann jeder von uns nicht nur sich selbst schützen, sondern auch andere vor den Gefahren des Online-Betrugs bewahren.

Trotz aller technologischen Fortschritte bleibt die Aufklärung und Sensibilisierung der Bevölkerung ein Schlüsselelement in der Betrugsbekämpfung. Wie die Geschichten von Claus, Milena, Rita, Mario und Tina zeigen, können das Wissen über aktuelle Betrugsmaschen und ein gesundes Maß an Skepsis viele Betrugsfälle verhindern.

Die Zukunft des Online-Betrugs und seiner Bekämpfung wird ein Wettlauf zwischen Kriminellen und Sicherheitsexperten sein, bei dem KI sowohl Waffe als auch Schild sein wird. Es wird entscheidend sein, dass Technologieunternehmen, Strafverfolgungsbehörden und

Verbraucherschutzorganisationen eng zusammenarbeiten, um mit den sich schnell entwickelnden Bedrohungen Schritt zu halten.

Gleichzeitig müssen wir als Gesellschaft einen ausgewogenen Ansatz finden, der die Vorteile der KI in der Betrugsbekämpfung nutzt, ohne dabei grundlegende Rechte und Freiheiten zu gefährden. Nur durch ein Zusammenspiel von technologischem Fortschritt, rechtlicher Regulierung und individueller Verantwortung können wir eine sicherere digitale Zukunft gestalten.

11. Präventionstipps im Kurzüberblick

Hier die wichtigsten Tipps, die sich aus der vorliegenden Studie und den Erfahrungen von Claus, Milena, Rita, Mario und Tina ergeben:

1. **Seien Sie skeptisch:** Wenn etwas zu schön klingt, um wahr zu sein, ist es das wahrscheinlich auch. Dies gilt besonders für unerwartete Angebote, Gewinne oder dringende Anfragen.
2. **Überprüfen Sie Quellen, Absender und Links:** Klicken Sie nicht voreilig auf Links in E-Mails oder SMS. Überprüfen Sie sorgfältig die Absenderadresse und seien Sie vorsichtig bei unbekannten oder verdächtigen Absendern.
3. **Schützen Sie Ihre persönlichen Daten:** Geben Sie keine vertraulichen Informationen wie Passwörter, Kreditkartendaten oder TANs preis, besonders nicht am Telefon oder in E-Mails.
4. **Nutzen Sie starke Authentifizierung:** Aktivieren Sie die Zwei-Faktor-Authentifizierung, wo immer möglich. 61 % der Befragten, die aktiv Präventionsmaßnahmen ergriffen haben, nutzen diese Methode.
5. **Halten Sie Ihre Software aktuell:** Führen Sie regelmäßig Sicherheits-Updates durch. Die Studie zeigt: 50 % der Befragten nutzen derartige Updates als Schutzmaßnahme.
6. **Verwenden Sie unterschiedliche Passwörter:** Nutzen Sie nicht das gleiche Passwort für alle Konten. 54 % der Befragten befolgen diesen Rat bereits.
7. **Seien Sie vorsichtig bei Online-Shops:** Überprüfen Sie das Impressum, die Zahlungsmethoden und die Preise. Wenn etwas zu günstig erscheint, könnte es sich um einen Fake-Shop handeln.
8. **Bleiben Sie informiert:** Halten Sie sich über aktuelle Betrugsmaschen auf dem Laufenden. Nutzen Sie vertrauenswürdige Quellen wie die Watchlist Internet.
9. **Reagieren Sie richtig auf Datenlecks:** Wenn Sie von einem Datenleck betroffen sind, ändern Sie umgehend Ihre Passwörter. 68 % der Betroffenen haben dies getan.
10. **Seien Sie besonders wachsam bei KI-gestütztem Betrug:** Denken Sie daran, dass Stimmen und Videos gefälscht sein können. Verifizieren Sie wichtige Informationen immer über einen zweiten, vertrauenswürdigen Kanal.
11. **Teilen Sie Ihr Wissen**: Informieren Sie Freunde und Familie über neue Betrugsmaschen. Gemeinsam können wir ein Netzwerk der Prävention aufbauen.
12. **Vertrauen Sie Ihrem Instinkt:** Wenn Sie ein ungutes Gefühl haben, nehmen Sie sich die Zeit, die Situation genau zu überprüfen. Lassen Sie sich nicht unter Druck setzen.

Indem wir diese Tipps beherzigen und in unseren digitalen Alltag integrieren, können wir uns und andere besser vor Online-Betrug schützen. Denken Sie daran: Prävention ist ein kontinuierlicher Prozess. Bleiben Sie wachsam, informiert und teilen Sie Ihr Wissen. Gemeinsam können wir die digitale Welt sicherer machen.

Abbildungsverzeichnis

KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
T +43-(0)5 77 0 77-DW oder -0
F +43-(0)5 77 0 77-1186
E-Mail kfv@kfv.at
www.kfv.at

Medieninhaber und Herausgeber: Kuratorium für Verkehrssicherheit
Verlagsort: Wien
Herstellung: Eigendruck
Redaktion: Patricia Rosenauer
Grafik: eigen/Canva, eigen/napkin.ai und generiert durch Dall:E

SAFETY FIRST!