



# Bei Anruf Betrug

## Von perfiden Telefontricks und wirksamen Gegenmaßnahmen

Wien, Oktober 2023

Durchgeführt im Auftrag von: Dr. Armin Kaltenegger

# Bei Anruf Betrug

## Von perfiden Telefontricks und wirksamen Gegenmaßnahmen

**Verfasst von**

Patricia Jeßner, BA

**Unter Mitarbeit von**

Mag. Eveline Wögerbauer

**Fachliche Verantwortung**

Patricia Jeßner, BA

**Im Auftrag von**

Dr. Armin Kaltenegger

# Inhaltsverzeichnis

<b>1. Einleitung</b>	<b>4</b>
<b>2. Situation in Österreich – Trends und Tendenzen</b>	<b>6</b>
2.1. Aktuelle Trends belästigender Anrufe und SMS	6
2.2. Angezeigte Fälle von Internetbetrug	7
<b>3. Aktuelle Arten von Telefonbetrug</b>	<b>8</b>
<b>4. KFV-Dunkelfeldstudie: Telefonbetrug in Österreich</b>	<b>11</b>
4.1. Telefonnutzung in Österreich	12
4.1.1. Handy versus Festnetz	12
4.1.2. Tägliche Internetnutzung	12
4.1.3. Private Telefonnutzung pro Woche	13
4.1.4. Eintrag privater Nummern im Telefonbuch	14
4.2. Risikoverhalten rund ums Telefon	15
4.2.1. Angabe der eigenen Telefonnummer	15
4.2.2. Annahme von Anrufen mit unbekannter Rufnummer	16
4.2.3. Angabe der Telefonnummer in der E-Mail-Signatur	17
4.3. Telefonbetrug in Österreich	18
4.3.1. Bekanntheit von Telefonbetrug	18
4.3.2. Persönliche Betroffenheit von Telefonbetrug	18
4.3.3. Viktimisierung im engeren Sinn	20
4.3.4. Reaktion nach Betrugsversuch	21
4.3.5. Bekanntheit und Akzeptanz von Informations- und Beratungsstellen	22
4.4. Fact Box	23
<b>5. Tipps zum Schutz vor Telefontricks</b>	<b>24</b>
<b>6. Conclusio</b>	<b>28</b>

## 1. Einleitung

„Hallo, wer spricht?“

„Hier spricht Susi, eine Freundin Ihrer Tochter. Ich habe leider schlechte Nachrichten: Ihre Tochter hat einen Unfall mit Personenschaden verursacht, wurde festgenommen und braucht nun dringend 20.000 Euro für die Kautions. Ich schick Ihnen gleich die Kontonummer für die Überweisung ...“

„Hallo, Tante Fini! Rat mal, wer da spricht!“ – „Der Lorenz?“ – „Ja, genau! Geht's dir gut? Du, ich bräuchte dringend Geld für meine neue Wohnung. Kannst du mir bitte was borgen? Ich hol's nachher ab – aber bitte nix Mama und Papa sagen ...“

„Guten Tag, Polizeikommissariat XY, Revierinspektor Z. Eine Diebsbande treibt gerade in unserer Stadt ihr Unwesen, und wir haben Ihre Wohnung auf einer Zielliste der Täter gefunden. Wir können Ihre Wertsachen aber abholen und in Sicherheit bringen. Bitte legen Sie Bargeld, Schmuck und Goldmünzen bereit – wir kommen gleich vorbei, holen die Wertgegenstände ab und verwahren sie sicher ...“

So oder so ähnlich beginnen ausgefeilte Telefontricks schauspielerisch begabter Krimineller, die mit dreisten Lügengeschichten Schock, Verzweiflung und Hilfsbereitschaft am anderen Ende der Leitung ausnutzen wollen, um in betrügerischer Absicht zu hohen Geldsummen zu kommen. Dabei sind es längst nicht mehr nur ausländische Nummern aus exotischen Gefilden wie den Kleinen Antillen, die Unbill mit sich bringen – gekaperte und harmlos gewöhnlich wirkende 0664- oder 0676-Nummern lassen aktuell vertrauensvoll abheben.

Es muss nicht immer Naivität oder Gutgläubigkeit sein, die Menschen zu Opfern macht. Oft sind die Maschen der Anrufer\*innen so raffiniert gestrickt, dass die Szenarien durchaus real wirken. Dann heißt es kühlen Kopf bewahren und die Plausibilität der Lage klären – was nicht immer leichtfällt, wenn das Chaos des Kopfkinos über einen hereinbricht. Tatsache ist: Telefonbetrug liegt voll im Trend – und kann uns alle treffen, Menschen jeder Alters-, Berufs- und Bildungsschicht: Ob Arbeiter oder Akademikerin, ob Teenager oder Seniorin, jede\*r von uns kann in den gefährlichen Sog akribisch inszenierter Anrufe geraten und in der perfide verursachten Panik die Orientierung zwischen Sein und Schein verlieren.

Warum ist Telefonbetrug derart en vogue? Wie präsent ist dieses Thema in Österreich? Welche psychologischen Tricks wenden die Täter\*innen an? In welchem Ausmaß ist die österreichische Bevölkerung bereits konkret betroffen? Um Antworten auf diese und weitere Fragen zu erhalten, führte das IFES – Institut für empirische Sozialforschung im Auftrag des Kuratoriums für Verkehrssicherheit (KFV) im Zeitraum November/Dezember 2022 unter 1.007 Österreicher\*innen ab 17 Jahren eine repräsentative Telefon- und Online-Umfrage zum Thema Telefonbetrug durch. Die Ergebnisse dieser österreichweiten Befragung wurden vom KFV-Forschungsbereich

Eigentumsschutz detailliert unter die Lupe genommen, die essenziellsten Erkenntnisse der KfV-Dunkelfeldstudie fanden Eingang in den vorliegenden Bericht.

Vom klassischen Neffentrick im neuen Kleid – die Stimmen von Telefonbetrüger\*innen klingen im Jahr 2023 fallweise mittels KI-Support bereits wie jene der echten Nichten, Neffen und Enkelkinder – bis zum monströsen Millionenbetrug unter dem Deckmantel international vernetzter Cyber-Trading-Plattformen: Wie funktioniert die Psychologie hinter dem Verbrechen? Welche Methoden werden von den meist hochprofessionell agierenden Täter\*innen angewendet? Wo sind unsere typisch menschlichen Schwachstellen, die kriminelle Geister gezielt anvisieren und gekonnt ausnutzen? Wie können wir uns gegen diese Strategien wehren und uns selbst- und sicherheitsbewusst vor Telefonbetrug schützen? Wie erkennen wir: Was ist Fakt und was ist Fake?

Die neue KfV-Studie beleuchtet das Thema Telefonbetrug aus mehreren Perspektiven, schafft einen Überblick über Muster und Methoden, berichtet über Betroffenheit und Bewusstsein der Bevölkerung und liefert probate Gegenmaßnahmen.

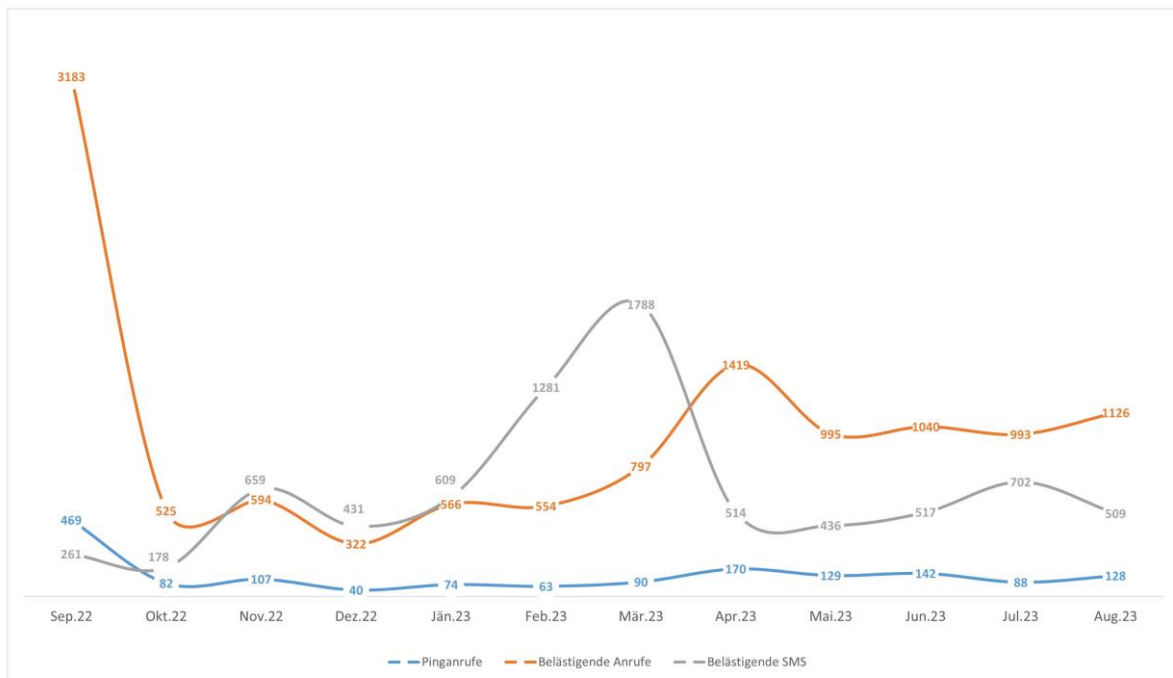
## 2. Situation in Österreich – Trends und Tendenzen

### 2.1. Aktuelle Trends belästigender Anrufe und SMS

Wie viele Zahlen belästigender Anrufe mit Betrugsabsicht werden in Österreich offiziell verzeichnet? Die Verlaufskurve der von der Rundfunk und Telekom Regulierungs-GmbH (RTR) veröffentlichten Zahlen belästigender Anrufe auf österreichischem Gebiet zeigt: Nach einem Peak im September 2022 und einem starken Rückgang im Herbst/Winter 2022 steigen die Zahlen der belästigenden Anrufe mit Betrugsziel wieder stetig an.

Die Hochzeit der belästigenden SMS war im März 2023, nach einer starken Abwärtskurve im April 2023 plätschert die Kurve auf und ab.

Ping-Anrufe liegen dagegen nicht mehr so stark im Trend – die Zahlen der Ping-Fälle haben sich auf einem niedrigen Niveau eingependelt – mit minimalem Auf und Ab.



© RTR

Abbildung 1: Belästigende Anrufe und SMS in Österreich, 02/2022 - 08/2023, Quelle: RTR

## 2.2. Angezeigte Fälle von Internetbetrug

In Form polizeilicher Anzeigen wird in Österreich nur ein Bruchteil der Telefonbetrugszahlen verzeichnet, die Dunkelziffer der Fälle ist groß. **Scham und Resignation der Betroffenen spielen in dieser Hinsicht eine große Rolle.** Dennoch spiegelt die Statistik der Anzeigen von Internetbetrug den Boom der Netz-Kriminalität in Österreich **erschreckend deutlich** wider.

**Hoch wie nie:** Die folgende Grafik dokumentiert die stark steigende Tendenz der Anzeigen von Internetbetrug in Österreich im Zeitraum 2006 bis 2022.

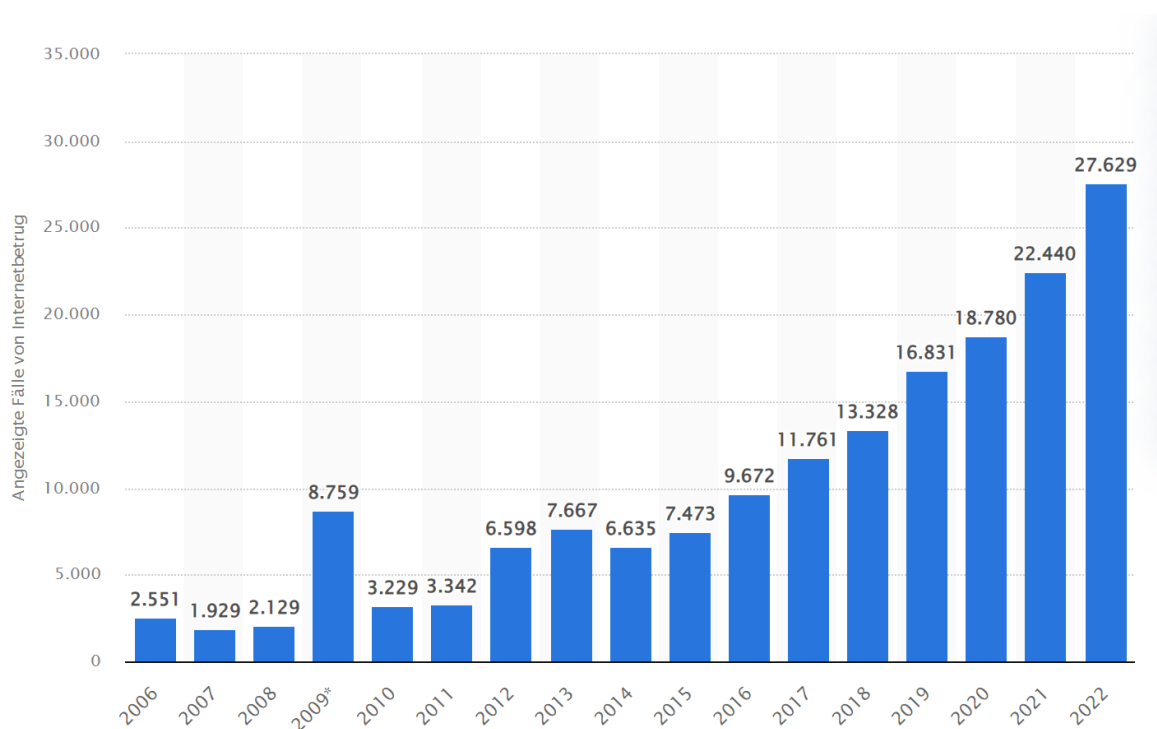


Abbildung 2: Anzeigen von Internetbetrug in Österreich 2006 bis 2022, Quelle: Statista, 2023

### 3. Aktuelle Arten von Telefonbetrug

Telefonbetrug im 3. Jahrtausend: Alte Maschen in neuem Kleid oder atemberaubend innovative Methoden krimineller Energie? Alles ist möglich – die Palette der beim Fernsprechen eingesetzten Fakes und Finten ist vielfältig und groß. Vom simplen Neffentrick in gruselig neuer Verpackung bis zum spektakulären Cyber Trading Fraud: Allen via Telefon begangenen Betrugsarten gemeinsam ist das Motiv der Gier nach fremdem Geld.

**Internationale Recherchen zeigen: Täter\*innen gehen in ihren Machenschaften und Methoden kompromiss- und gewissenlos vor – Telefontricks von heute sind meist akribisch inszeniert und psychologisch durchdacht bis ins letzte Detail.** Besonders bemerkenswert: Falsche Telefonberater\*innen, im Fall von Cyber Trading Fraud oft von professionell organisierten Call-Centern aus agierend, sind nicht immer voll informiert über das wahre Ziel großer Geldtransfers – sie sind oft ebenso ahnungslos wie ihre betrogenen Kund\*innen. Das große Ding, das unter der Regie der abgebrühten Masterminds über ihren Köpfen gedreht wird, führt auch für unfreiwillig kriminelle Mittäter\*innen nicht selten zu einem Ende mit Schrecken: **So manchen Telefonist\*innen wird ihr verbrecherisches Treiben erst nach Call-Center-Großrazzien schmerzlich bewusst.**

Wer Hintergründe, Triebfedern und Vorgangsweisen von Verbrecher\*innen kennt, ist und bleibt im Fall des Falles auf der sicheren Seite. Die gängigsten Muster und Methoden aktueller Telefonbetrugsarten beschreibt der folgende Kurzüberblick.

#### Bei Anruf Fraud – die populärsten Telefonbetrugsmaschen von heute:

- **Scam- und Phishing-Anrufe:** Unter Vortäuschung einer falschen Identität (Polizei, Tech-Support-Teams, Finanzinvestoren etc.) versprechen die Anrufer\*innen – oft sogar unter Nutzung gehackter bzw. gekapeter bekannter Telefonnummern – ihren Opfern bestimmte **Scheinvorteile** (etwa die vermeintliche Überweisung eines Gewinns), um an sensible persönliche Daten zu gelangen. Mitunter werden die Anrufe als **Umfragen** getarnt, zu Allerweltsthemen wie Urlaubsgestaltung oder Genussmittelkonsum, wie etwa die auch in Österreich lancierte Wein-Umfrage, die in Wahrheit eine Betrugsmasche war. Manchmal wird auch mit **angeblich offenen Schulden** der Betroffenen oder anderen Bedrohungsszenarien künstlich Druck erzeugt.

Der berühmteste Telefon-Scam ist wohl der altbekannte **Neffentrick** – er erlebt gerade ein atemberaubend großspuriges Revival. Bevorzugt ältere, allein lebende Menschen erhalten Anrufe angeblicher Neffen, Nichten oder Enkel, die ihre Namen meist in subtiler Weise



erraten lassen: „Rat mal, wer da spricht!“ Aus der genannten Auswahl an Namen wird dann ein Name ausgewählt – unter dieser Fake-Identität wird nach Geld verlangt, da man sich in einer angeblichen Notsituation befinde und dringend eine hohe Geldsumme brauche. Falls der gewünschte Betrag nicht zu Hause vorrätig ist, wird die ältere Person massiv unter Druck gesetzt, noch am selben Tag zur Bank zu gehen und das Geld sofort abzuheben. Ein Bote oder eine Botin werde die so dringend benötigte Barschaft dann abholen, da man selbst aus triftigen Gründen verhindert sei.

Im Zuge des Neffentricks wird sehr oft auch moralischer Druck ausgeübt: Man habe der Tante, dem Onkel, den Großeltern doch schon so oft geholfen – nun sei es an der Zeit für eine Gegenleistung. Traurig, aber wahr: In unzähligen Fällen haben ältere Menschen auf diese Weise ihre gesamten Lebensersparnisse an Kriminelle verloren. Buchstäblich unerhört und in atemberaubend neuen Dimensionen kommt der Neffentrick am Telefon im Jahr 2023 daher: Der Einsatz revolutionärer KI-Programme lässt die Stimmen der jüngeren Deep-Fake-Verwandten täuschend echt aus dem Hörer erklingen.

Der **Kautions-Trick** ist artverwandt: Eltern erhalten von vermeintlichen Freund\*innen oder Anwält\*innen ihrer Kinder oder falschen Polizist\*innen einen schockierenden Anruf. Ein Unfall mit Personenschaden sei passiert, der Sohn/die Tochter sei am Steuer gesessen und nun in Untersuchungshaft. Nur eine Kautions in Höhe einer großen Geldsumme könne die rasche Wiedererlangung der Freiheit ermöglichen. Ein besonders übler Trick, der immer wieder folgenschwere Kurzschlussreaktionen bewirkt. Der entsetzte Vater, die verzweifelte Mutter stellt so schnell wie möglich, völlig ferngesteuert irrational handelnd, die gewünschte Summe zur Verfügung – um das geliebte Kind aus der vermeintlichen Notlage zu befreien. Der Blick der Betroffenen ist einzig und allein auf die versprochene Problemlösung fokussiert, der Wahrheitsgehalt der geschilderten Geschehnisse wird in der hochemotionalen Ausnahmesituation kaum in Frage gestellt.

Auch der klassische **Polizisten-Trick** reiht sich in die Kategorie von pure Panik auslösendem Telefonbetrug ein: Falsche Polizist\*innen rufen an – mit der Hiobsbotschaft, dass die Wohnung/das Haus der angerufenen Person auf der Zielliste einer Diebsbande aufscheine, die gerade in der Umgebung ihr Unwesen treibe. Aber man könne Abhilfe schaffen: Alle daheim befindlichen Bargeldsummen, Schmucksachen und Wertgegenstände mögen bitte umgehend gesammelt an der Tür übergeben werden – dem „Polizisten“, der gleich vorbeikomme und die Schätze „in Sicherheit“ bringen werde. Mit raffiniert gehackten Nummern und großem Psycho-Druck gelangen auf diese Weise immer wieder spontane Übergaben astronomischer Geldsummen und wertvoller Familienschätze an die dunkle Seite der Macht.

Die Königsklasse des Telefonbetrugs spielt in schwindelerregenden Höhen verlorener Geldsummen: Betrug mittels vorgetäuschter Internet-Handelsplattformen – kurz und international: **Cyber Trading Fraud**. Potenzielle Anleger werden zu vermeintlich lukrativen Investitionen verleitet – meist von sympathisch klingenden Telefonberater\*innen, die in eigens geschaffenen Call-Centern, oft von Osteuropa aus, illegal und kriminell agieren. Die vorgegaukelten hohen Gewinnsummen gibt es in Wirklichkeit nicht, der sehnsüchtig

erwartete Geldregen ist eine Fata Morgana, ein Luftschloss aus leeren Versprechungen: Das investierte Vermögen wandert über dunkle Geldwäschekanäle durch ein verschachteltes Konzern-Netzwerk von Tarn- und Scheinfirmen rund um den Globus, bis zu Briefkastenfirmen in der Karibik – und in die Taschen von hochprofessionell agierenden Kriminellen.

Wie kriminelle Cyber-Trading-Plattformen ihren Opfern Investitionen in Millionenhöhe abluchsen, illustriert der Fall eines deutschen Unternehmers, eindrucksvoll recherchiert und dokumentiert in der Podcast-Reihe „Call me Günther“, einer Co-Produktion von Deutschlandfunk und Ö1.

- **Scam- und Phishing-SMS:** Mittels betrügerischer SMS vermeintlicher Bankunternehmen, Paketzusteller etc. wird über einen mitgeschickten Link versucht, an persönliche Daten zu kommen. Der Link ist eine als App getarnte Malware oder Umleitung auf eine Website, auf der die privaten Daten bekannt gegeben werden sollen.

In manchen Fällen ist die SMS auch getarnt als Tochter/Sohn-Nachricht („Hallo Mama/Papa, mein Handy ist ins Wasser gefallen, ich habe jetzt ein neues Telefon und eine neue Nummer ... Bitte schreib mir auf WhatsApp!“)

- **Ping-Anrufe:** Das Telefon läutet nur kurz – zum Beispiel mit tunesischer Vorwahl. Wen kennt man denn dort? Ruft man die meist ausländische Nummer zurück, fallen hohe Kosten an. Mittels Tonbandansagen wird versucht, die ahnungslosen Rückrufer\*innen möglichst lange in der Leitung zu halten – eine tückische Kostenfalle, bei der mehrere Euro pro Minute in der Kassa der Kriminellen klingeln. Wer dabei länger – wortwörtlich – auf der Leitung steht, zahlt teures Geld für den gut gemeinten Rückruf.
- **Call-Bot-Anrufe:** Im Falle eines Call-Bot-Anrufs wird man in meist englischsprachigen Tonbandansagen dazu aufgefordert, eine bestimmte Tastenkombination am Handy zu drücken. Daraufhin melden sich die Täter\*innen, die sich u.a. als Polizeibeamte ausgeben und erfundene Kriminaldelikte vortäuschen oder der angerufenen Person eine Beteiligung an kriminellen Delikten vorwerfen. Die Betroffenen werden zum Downloaden einer Software oder zu einer Überweisung von Geld aufgefordert.
- **Cold Calls / Cold SMS:** Hierbei handelt es sich meist um Kontaktaufnahme von Unternehmen mittels unerbetener Werbeanrufe oder SMS, zu deren Durchführung man nicht vorab eingewilligt hat. Diese gesetzlich unzulässige Form der Kaltakquise dient meist zur Gewinnung von Neukund\*innen und hat in einigen Fällen bereits kriminellen Charakter angenommen: Betroffene berichten von Drohungen via Telefongespräch oder SMS.

## 4. KFV-Dunkelfeldstudie: Telefonbetrug in Österreich

Wie sieht die Lage in puncto Telefonnutzung und Telefonbetrug in Österreich aus? Im Auftrag des KFV führte das österreichische IFES – Institut für empirische Sozialforschung von Mitte November bis Mitte Dezember 2022 unter 1.007 Österreicher\*innen ab 17 Jahren eine Umfrage zum Thema Telefonbetrug durch. Im Fokus dieser österreichweiten Telefon- und Online-Befragung standen die Informiertheit, das Risikoverhalten und die persönliche Betroffenheit der Bevölkerung in puncto Telefonbetrug.

Wie und wie oft nutzen die Österreicher\*innen das Kommunikationsmedium Telefon und das Internet im Allgemeinen? Wie viele Personen sind – mit Handy- und/oder Festnetznummer – im Telefonbuch eingetragen? Wie viele Österreicher\*innen gehen mit der Nennung ihrer privaten Telefonnummer freigiebig um? Wie oft klingelt in Österreich das Handy mit unterdrückter Nummer am Display – und wie oft wird dann abgehoben? Wie viel Prozent der Österreicher\*innen haben bezüglich der Erfassung ihrer elektronischen Daten Sicherheitsbedenken? Welche Telefonbetrugsformen sind in Österreich bekannt? Wie viele Menschen waren hierzulande bereits von Telefonbetrug betroffen – und wie viele mit konkret entstandenem Schaden?

All diese und weitere wesentliche Fragen rund um Telefonnutzung und Telefonbetrug in Österreich beantwortet die neue KFV-Dunkelfeldstudie. Hier die wichtigsten Ergebnisse.

## 4.1. Telefonnutzung in Österreich

### 4.1.1. Handy versus Festnetz

Die KfV-Dunkelfeldstudie zeigt: **Fast alle Österreicher\*innen besitzen ein privates Mobiltelefon (98 %)**, der Anteil der Personen mit Festnetzanschluss ist allerdings deutlich geringer. Festnetz nutzen 36 % der Befragten in der Arbeit, 34 % privat von zu Hause aus.

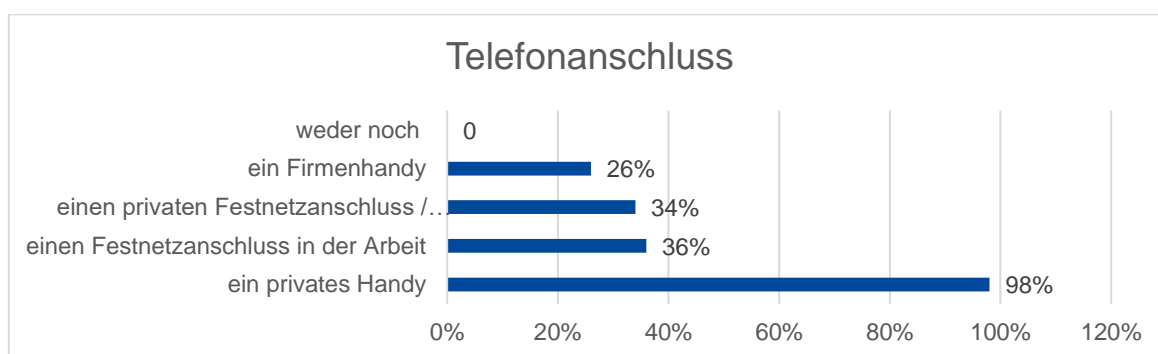


Abbildung 3: Telefonnutzung in Österreich, in Prozent, Mehrfachauswahl

### 4.1.2. Tägliche Internetnutzung

Auch die allgemeine Internet-Affinität der Österreicher\*innen war Gegenstand der IFES-Umfrage: 15 % der Menschen hierzulande nutzen das Internet mindestens 6 Stunden pro Tag, 22 % tun dies 4-5 Stunden täglich, 16 % der Befragten sind immerhin 3 Stunden pro Tag online unterwegs. **26 % der Befragten, der größte Anteil der Antworten, nannten lediglich 2 Stunden als tägliche Nutzungsdauer.** 18 % der Befragten tummeln sich täglich bis zu einer Stunde im Netz, von 2 % der befragten Personen kam bei dieser Frage kein Feedback.

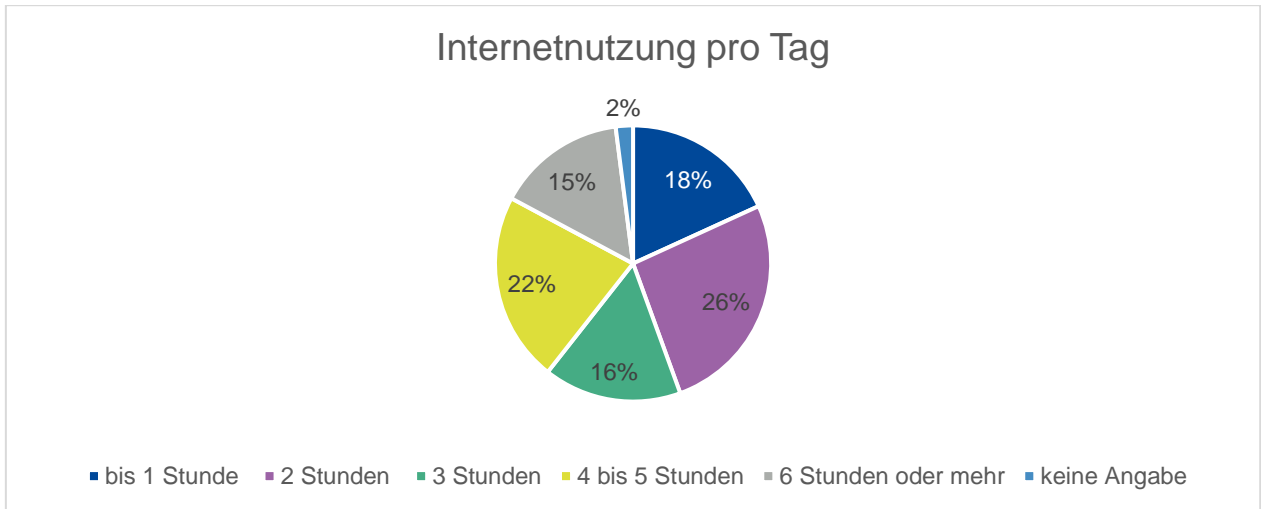


Abbildung 4: Tägliche Internetnutzung

#### 4.1.3. Private Telefonnutzung pro Woche

Was die durchschnittliche Häufigkeit privater Telefonate betrifft, so nutzen 15 % der Befragten ihr privates Handy und/oder Festnetz 11 Stunden oder mehr pro Woche. 30 % tun dies 3 bis 10 Stunden wöchentlich, 16 % sprechen etwa 2 Stunden pro Woche in privater Sache fern, der Löwenanteil von 34 % telefoniert allerdings nur bis zu einer Stunde pro Woche privat. 4 % der Befragten hielten sich zu diesem Thema bedeckt.

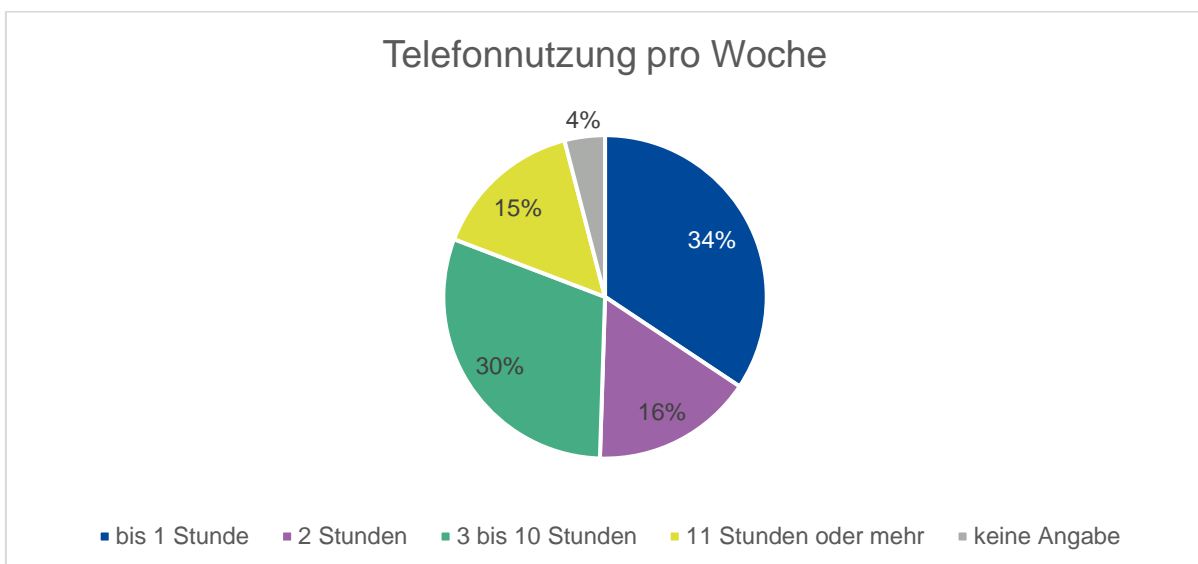


Abbildung 5: Telefonnutzung pro Woche

#### 4.1.4. Eintrag privater Nummern im Telefonbuch

Fast 6 von 10 Befragten stehen weder mit ihrer privaten Handynummer noch mit ihrer privaten Festnetznummer im Telefonbuch. **22 % der Österreicher\*innen sind mit ihrer privaten Handynummer, 13 % mit privater Festnetznummer eingetragen.**

Ein Fünftel (20 %) der über 50-Jährigen steht mit der privaten Festnetznummer im Telefonbuch. Beim Telefonbucheintrag der privaten Handynummer steigt der Anteil der Generationen 50+ auf 28,5%. Mit beiden Anschlüssen sind etwas mehr Männer als Frauen im Telefonbuch eingetragen.

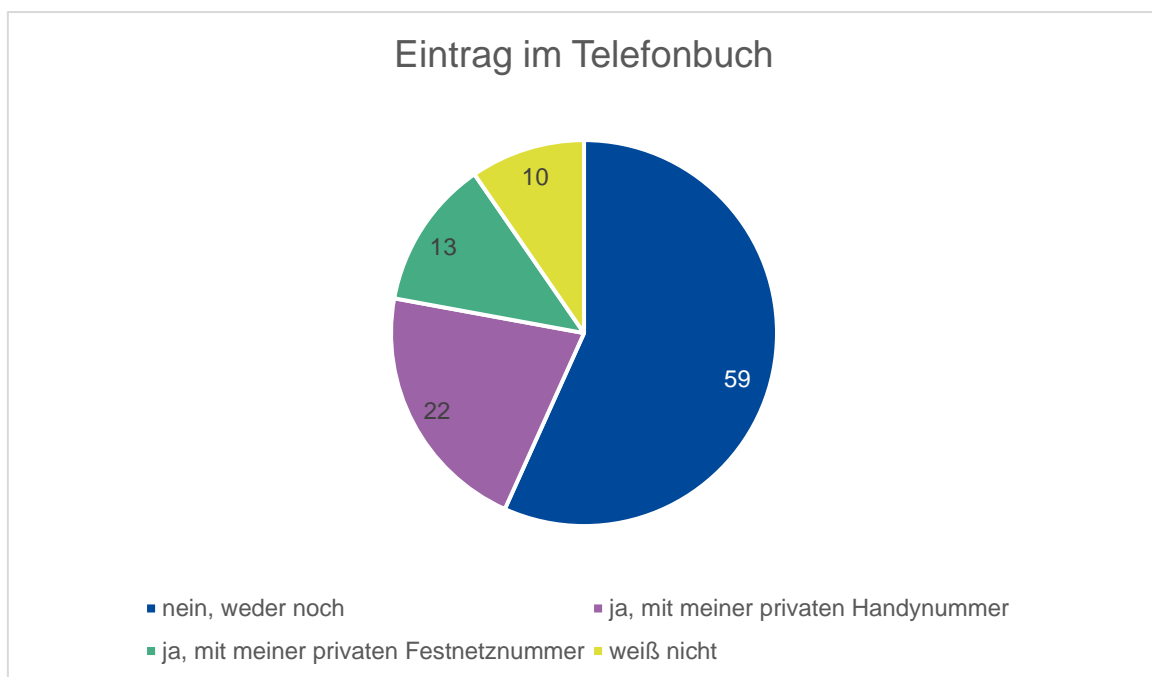


Abbildung 6 Eintrag mit privater Nummer, Angaben in Prozent, Mehrfachauswahl

## 4.2. Risikoverhalten rund ums Telefon

### 4.2.1. Angabe der eigenen Telefonnummer

Ein Viertel der vom KFV befragten Personen gibt auf entsprechende Anfragen (fast) immer bis häufig die eigene Telefonnummer an, etwa bei Online-Registrierungen, Benutzerkonten etc.

Mit steigendem Lebensalter geben Menschen seltener ihre Telefonnummer preis – teils wohl aus vermehrter Skepsis und höherer Lebenserfahrung, teils aufgrund geringerer Nachfrage.

Weibliche Vernunft zeigt sich in vorsichtigerem Umgang mit persönlichen Daten: Frauen nennen ihre Nummer etwas seltener als Männer.

Die junge Generation scheint unbesorgter und freigiebiger im Umgang mit persönlichen Daten – Menschen unter 30 Jahren geben ihre Telefonnummern vergleichsweise häufig an.

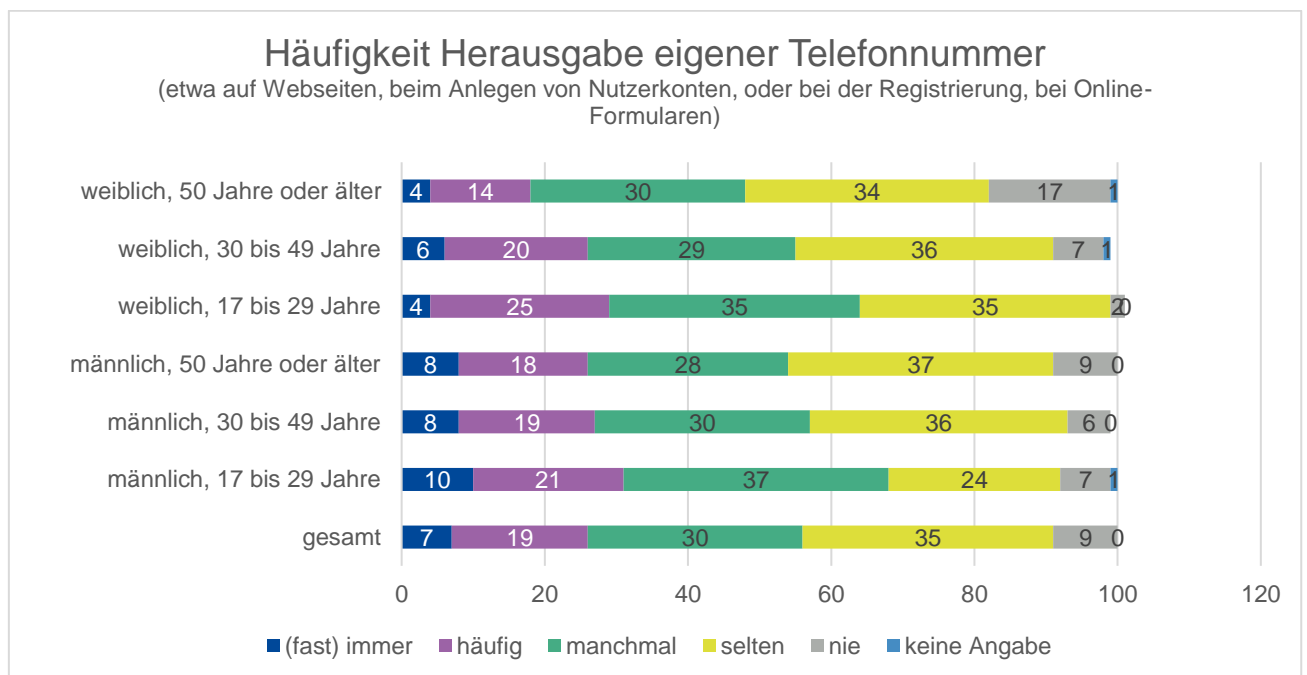


Abbildung 7: Häufigkeit Herausgabe eigener Telefonnummer

#### 4.2.2. Annahme von Anrufen mit unbekannter Rufnummer

„Unbekannte Nummer“, „Rufnummer unterdrückt“: Derart anonyme Display-Info weist auf Geheimnummern hin – legal oder illegal erworbene.

Ein Fünftel (20 %) der vom KFV befragten Österreicher\*innen bekommt zumindest häufig Anrufe von unbekanntem oder unterdrückten Rufnummern. **35 % der Befragten heben dann zumindest hin und wieder ab.**

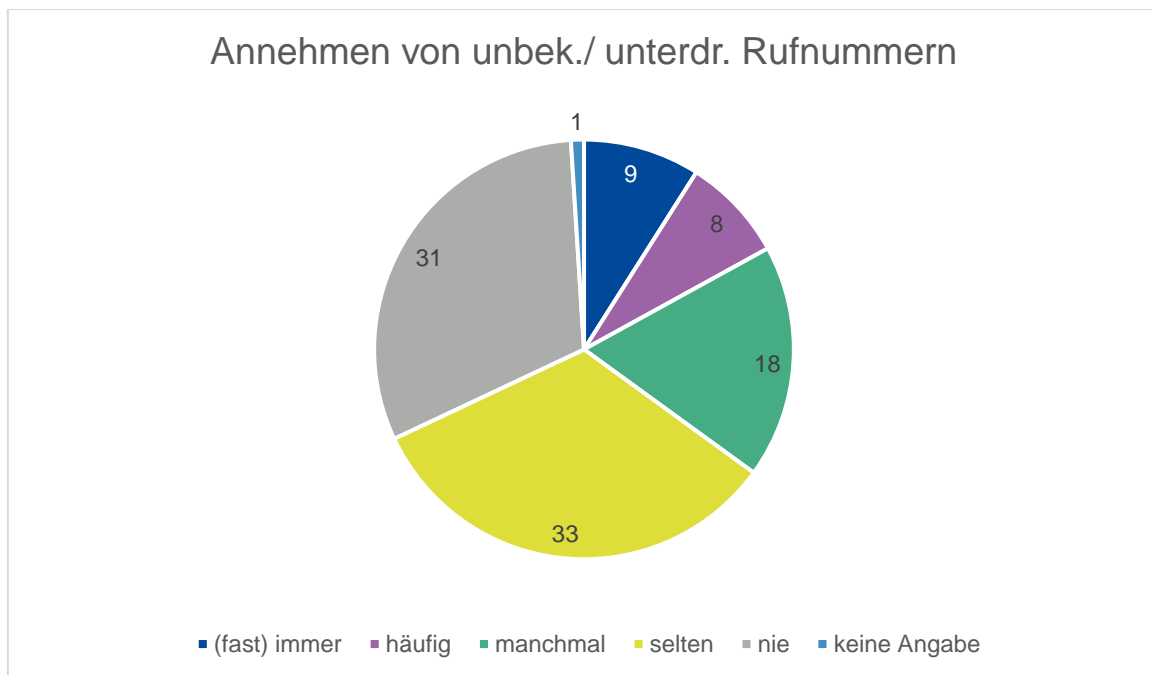


Abbildung 8: Annahme von Anrufen unbek. Nummern, Angaben in Prozent



#### 4.2.3. Angabe der Telefonnummer in der E-Mail-Signatur

**29 %** der Befragten nennen ihre **Telefonnummer in ihrer persönlichen E-Mail-Signatur**, **41 %** tun dies allerdings nicht. **30 %** der befragten Personen verwenden gar keine E-Mail-Signatur.

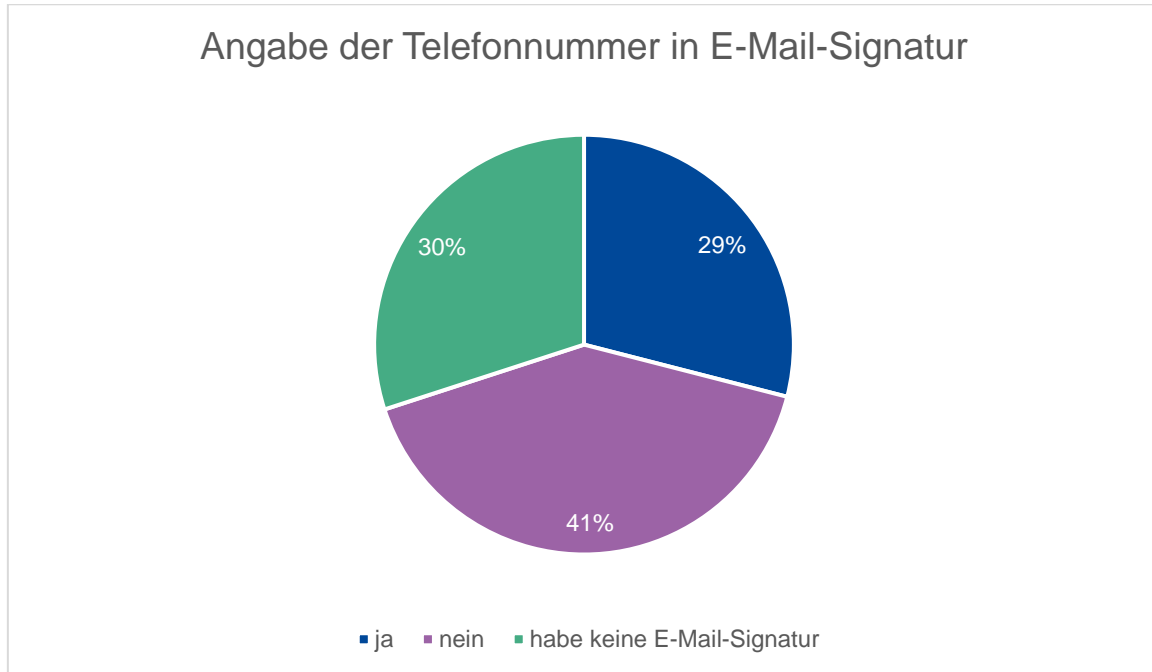


Abbildung 9: Angabe der Telefonnummer in E-Mail-Signatur

## 4.3. Telefonbetrug in Österreich

### 4.3.1. Bekanntheit von Telefonbetrug

Wissen Österreichs Bürger\*innen über Telefonbetrugsmaschen ausreichend Bescheid? Telefonbetrug ist in Österreich grundsätzlich wohlbekannt: Fast alle Respondent\*innen haben schon einmal von Telefonbetrug in verschiedenen Varianten gehört oder gelesen (96 %).

Am bekanntesten sind den Österreicher\*innen **Phishing-SMS (83 %)** und **Ping-Anrufe (82 %)**, gefolgt von **Cold Calls/Cold SMS (75 %)** und **Phishing-Anrufen (74 %)**. Etwas weniger stark verbreitet ist dagegen noch das Wissen über **Call-Bot-Anrufe (55 %)**.

Die Umfrage zeigt also: Das grundsätzliche Wissen um Telefonbetrugsformen ist in Österreich bereits weitverbreitet. Dennoch kommt es immer wieder zu Fällen mit drastischen Folgen.

### 4.3.2. Persönliche Betroffenheit von Telefonbetrug

Gemäß den Ergebnissen der KFV-Befragung sind die in Österreich am weitesten verbreiteten Deliktformen von Telefonbetrug Phishing-SMS (Lebenszeit-Prävalenz: 63 %) und Cold Calls/SMS (Lebenszeit-Prävalenz: 47 %). Eher selten war jedoch damit auch tatsächlicher Schaden finanzieller oder emotionaler Natur verbunden. Weniger häufig erlebt wurden hierzulande Phishing-Anrufe (Lebenszeit-Prävalenz: 29 %), Ping-Anrufe (Lebenszeit-Prävalenz: 21 %) und Call-Bot-Anrufe (Lebenszeit-Prävalenz: 19 %).

Die persönlichen Erfahrungen der Befragten mit verschiedenen Arten von Telefonbetrug im Detail:

#### **Phishing-SMS**

Telefonbetrug kommt besonders oft in Form von Phishing-SMS vor. Fast zwei Drittel der befragten Personen (63 %) haben bereits ein- oder mehrmals eine Phishing-SMS erhalten. Hier sind vor allem Männer und Frauen mittleren Alters betroffen.

Fast die Hälfte der Befragten (46 %) war in den letzten 12 Monaten mit Phishing-SMS konfrontiert. Phishing-SMS zählen aber nicht unbedingt zu jenen Formen von Telefonbetrug, mit denen finanzieller und/oder emotionaler Schaden verbunden ist.

## Phishing-Anrufe

Etwa 3 von 10 Personen haben ein- oder mehrmals Phishing-Anrufe erhalten. Jüngere Befragte sind dabei häufiger betroffen als ältere. Betrugsopfer im engeren Sinn (Personen mit entstandenem Schaden) waren doppelt so oft davon betroffen. In den vergangenen 12 Monaten vor dem Zeitpunkt der Umfrage hatten 13 % der Befragten Phishing-Anrufe erhalten, vor allem Männer der unteren und mittleren Alterskategorie waren häufiger davon betroffen.

## Ping-Anrufe

Ein Fünftel der Österreicher\*innen hat bereits unliebsame Erfahrungen mit Ping-Anrufen gemacht – von den Betrugsopfern im engeren Sinn, also mit erlittenem Schaden, sogar die Hälfte. Jüngere Befragte und vor allem Männer waren häufiger betroffen als Ältere.

8 % der Befragten waren in den 12 Monaten vor der Befragung davon betroffen. In der Gruppe der durch Telefonbetrug Geschädigten liegt der Anteil sogar bei 25 %.

## Call-Bot-Anrufe

Call-Bot-Anrufe sind in Österreich weniger weit verbreitet als andere Deliktformen. Die Lebenszeit-Prävalenz liegt in diesem Bereich bei 19 %, bei den Opfern im engeren Sinn (Personen mit entstandenem Schaden) bei 48 %. Auch hier sind Jüngere wieder stärker betroffen als Ältere.

In den letzten 12 Monaten vor der Befragung hatte fast ein Zehntel einen oder mehrere Call-Bot-Anrufe erhalten, Jüngere und Befragte der mittleren Alterskategorie waren auch hiervon stärker betroffen, junge Frauen stachen besonders als Adressat\*innen von Call-Bot-Anrufen hervor.

## Cold Calls / Cold SMS

Fast die Hälfte der Befragten (47 %) hatte bereits Cold Calls oder Cold SMS erhalten. Personen mittleren Alters waren häufiger mehrmals von dieser Form des Telefonbetrugs betroffen. Bei 7 von 10 Betroffenen entstand dabei sogar konkreter Schaden.

In den letzten 12 Monaten vor dem Zeitpunkt des Interviews hatte mehr als ein Viertel (27 %) Cold Calls oder Cold SMS erhalten. Vor allem Männer und Frauen der mittleren Alterskategorie waren Ziele der Kaltakquise. Bei mehr als einem Drittel der Betroffenen (37 %) entstand dabei konkreter Schaden.

### 4.3.3. Viktimisierung im engeren Sinn

**83 % der betroffenen Befragten konnten den Betrugsversuch rechtzeitig entdecken, es entstand kein finanzieller oder materieller Schaden.**

Menschen mit erlittenem Schaden durch Telefonbetrug (Opfer im engeren Sinn) erfuhren zu nahezu gleichen Teilen finanziellen (6 %) und emotionalen Schaden (5 %).

Von Phishing-, Ping- oder Call-Bot-Anrufen Betroffene berichteten überdurchschnittlich oft von konkret erlittenem Schaden.

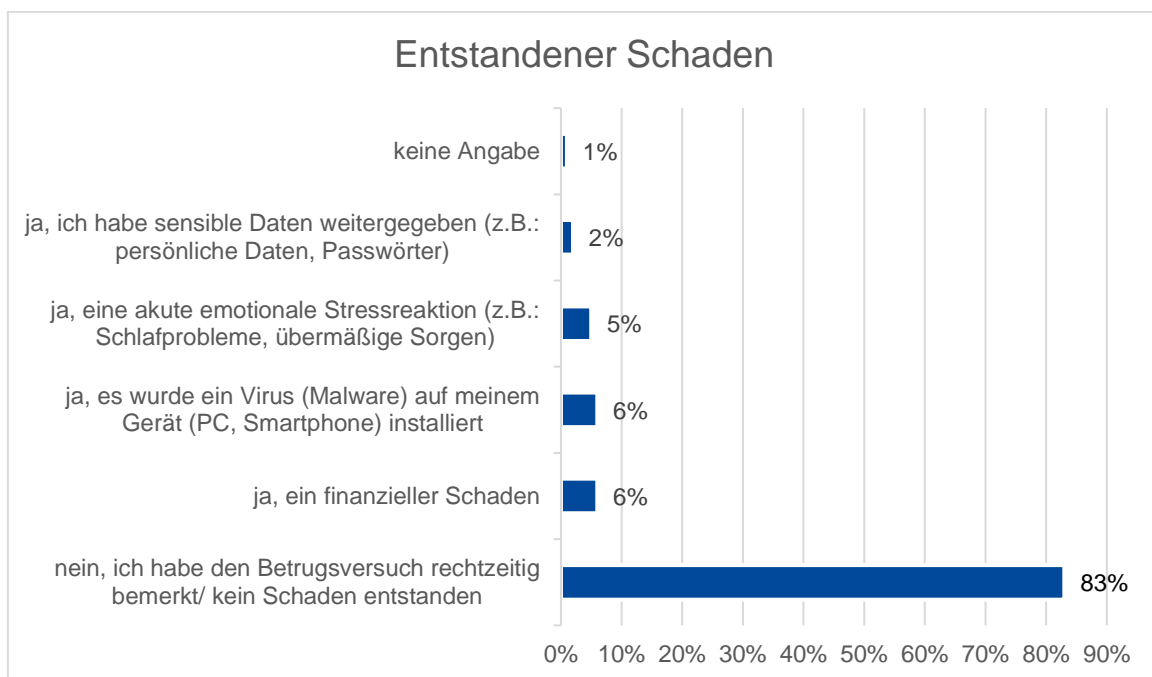


Abbildung 10: Viktimisierung im engeren Sinn

#### 4.3.4. Reaktion nach Betrugsversuch

Nach Entdecken des Telefonbetrugs wurden einige Betroffene aktiv, **die Mehrheit (61 %) der Betroffenen setzte allerdings keine Reaktionsmaßnahmen.**

Die häufigsten Reaktionen betroffener Personen: Der Betrug wurde im Internet öffentlich gemacht (16 %). 22 % der Betroffenen wollten die Tat der Polizei melden, 11 % waren de facto bei der Polizei, haben aber von einer Anzeige schlussendlich Abstand genommen.

**Nur 8 % der Betroffenen erstatteten tatsächlich Anzeige**, weiteren 8 % wurde in der Polizeidienststelle mitgeteilt, dass derartige Delikte nicht in den Zuständigkeitsbereich der Polizei fielen. 11 % der Betroffenen wendeten sich an eine Beratungsstelle, 5 % nahmen psychologische Beratung in Anspruch.

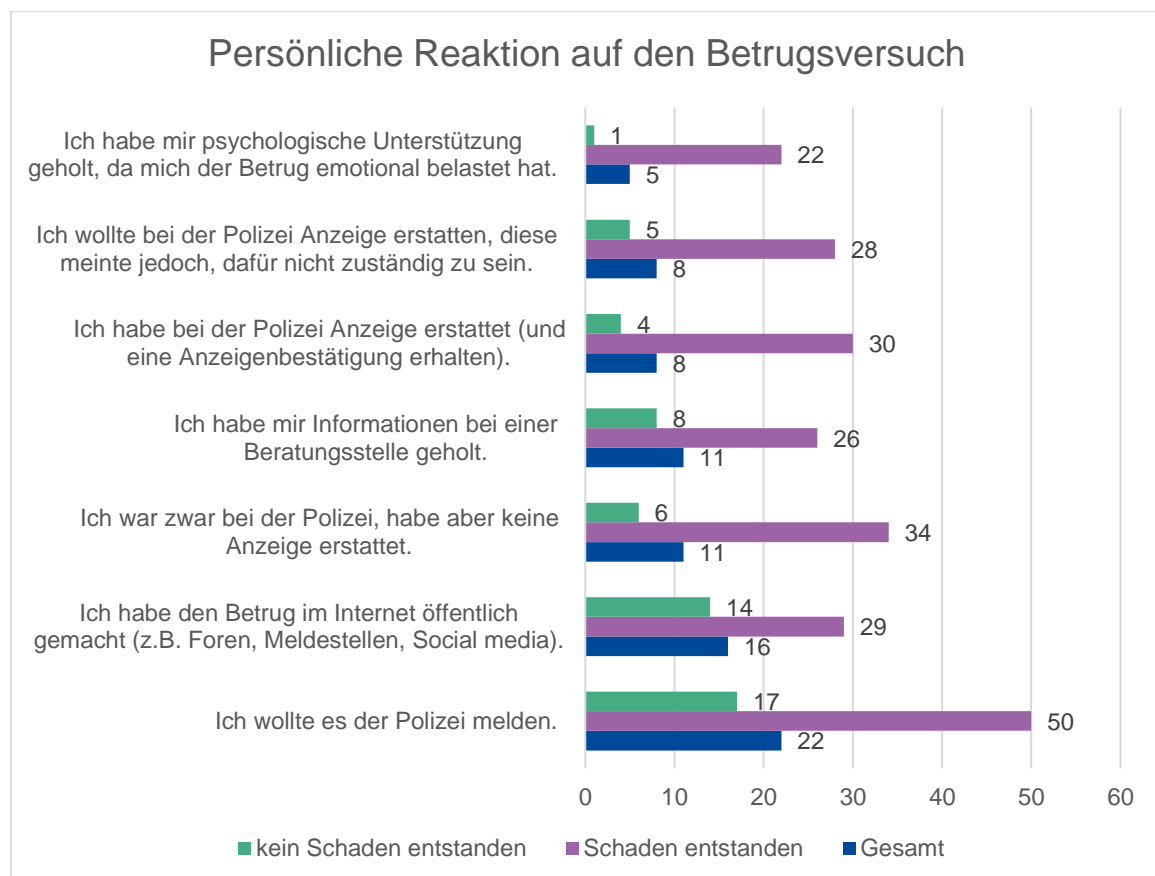


Abbildung 11: Persönliche Reaktion nach Betrugsversuch

#### 4.3.5. Bekanntheit und Akzeptanz von Informations- und Beratungsstellen

Die Antworten der KfV-Befragung lassen wissen: **Die in Österreich bekanntesten Informations- und Beratungsstellen im Bereich Telefonbetrug sind das Bundeskriminalamt (32 %), oesterreich.gv.at (28 %) und der Weiße Ring (21 %).**

Beim Wissen um die Existenz von Hilfsorganisationen gibt es allerdings noch Luft nach oben: Ein Drittel der Befragten – und auch der Betrugsopfer – kennt keine einzige der genannten Beratungsstellen. Dennoch: 26 % der Opfer im engeren Sinn – der von Telefonbetrug Betroffenen mit dabei entstandenem Schaden – haben bei Beratungsstellen Informationen eingeholt. 22 % der von Telefonbetrug betroffenen Menschen nahmen psychologische Unterstützung in Anspruch, da sie sich nach dem Betrugsfall emotional belastet fühlten.

Die Ergebnisse der Befragung zeigen: Mehr Information über hilfreiche Anlaufstellen ist ein absolutes Muss, der Bedarf an verstärktem psychologischem Support ist bei offensichtlich steigenden Betrugsfallzahlen und künftig höherem Informationsgrad über derartige Hilfsangebote wohl eindeutig gegeben.

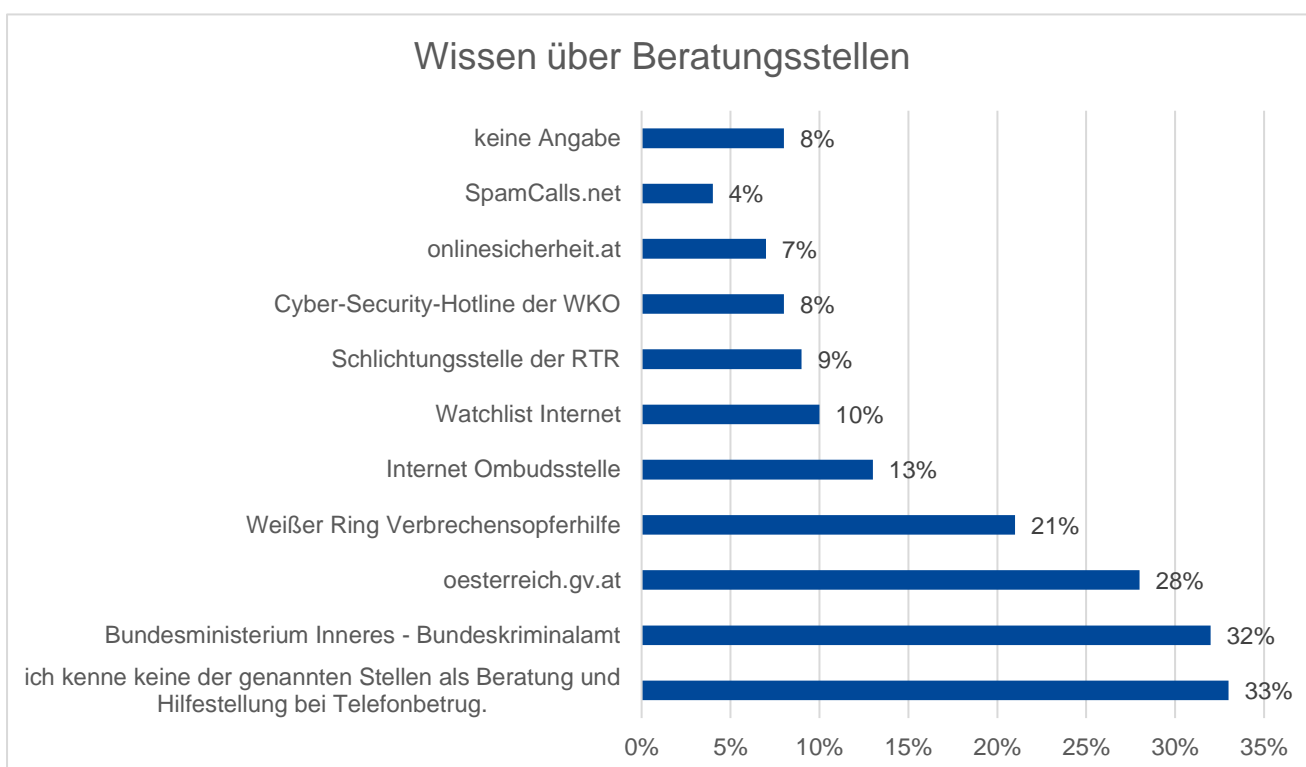
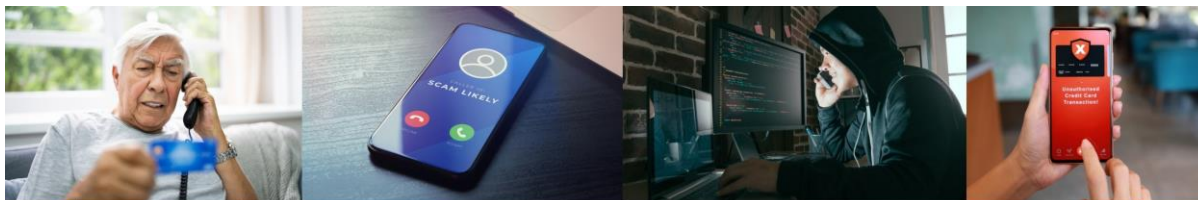


Abbildung 12: Wissen über Beratungsstellen, Mehrfachauswahl möglich

## 4.4. Fact Box



### Fact Box Telefonbetrug

- **98 %** der Österreicher\*innen besitzen ein **privates Mobiltelefon**.
- 36 % nutzen **Festnetz-Telefone** im Job, 34 % daheim.
- 15 % der Befragten **nutzen das Internet** mindestens 6 Stunden pro Tag, 22 % tun dies 4 bis 5 Stunden täglich, 16 % der Befragten sind immerhin 3 Stunden täglich online unterwegs.
- 15 % der Österreicher\*innen **nutzen ihr privates Handy und/oder Festnetz** 11 Stunden oder mehr pro Woche. 30 % tun dies 3 bis 10 Stunden wöchentlich, 16 % sprechen wöchentlich etwa 2 Stunden in privater Sache fern.
- 22 % der Österreicher\*innen sind mit ihrer privaten Handynummer, 13 % mit privater Festnetznummer **im Telefonbuch eingetragen**.
- Ein Viertel der vom KfV befragten Personen **gibt auf entsprechende Anfragen** (fast immer bis häufig **die eigene Telefonnummer** an, etwa bei Online-Registrierungen, Benutzerkonten etc. – junge Menschen unter 30 sind in dieser Hinsicht sorgloser.
- Ein Fünftel der vom KfV befragten Österreicher\*innen bekommt zumindest häufig Anrufe **von unbekanntem oder unterdrückten Rufnummern**. Fast 6 von 10 Befragten heben dann zumindest hin und wieder ab. Junge Menschen und Personen mittleren Alters heben Anrufe unter unbekannter Nummer häufiger ab.
- 29 % der Befragten nennen ihre **Telefonnummer in ihrer persönlichen E-Mail-Signatur**.
- Fast alle Respondent\*innen haben schon einmal **von Telefonbetrug in verschiedenen Varianten gehört oder gelesen** (96 %). Am bekanntesten sind den Österreicher\*innen Phishing-SMS (83 %) und Ping-Anrufe (82 %), gefolgt von Cold Calls/Cold SMS (75 %) und Phishing-Anrufen (74 %). Etwas weniger stark verbreitet ist dagegen noch das Wissen über Call-Bot-Anrufe (55 %).
- Fast zwei Drittel der befragten Personen (63 %) haben bereits **ein- oder mehrmals eine Phishing-SMS erhalten**.
- Etwa 3 von 10 Personen haben bereits ein- oder mehrmals **Phishing-Anrufe** erhalten.
- Ein Fünftel der Österreicher\*innen wurde bereits von **Ping-Anrufen** belästigt.
- Von Call-Bot-Anrufen wurden bislang 19 % der Österreicher\*innen erreicht.
- Fast die Hälfte der Befragten (47 %) hat bereits **Cold Calls** oder **Cold SMS** erhalten.
- 83 % der betroffenen Befragten konnten den **Betrugsversuch rechtzeitig entdecken**, es entstand kein finanzieller oder materieller Schaden.
- 6 % der Telefonbetrugsopfer im engeren Sinn erfuhr **finanziellen Schaden**, 5 % erlebten emotionale Beeinträchtigungen.
- Die Mehrheit der Betroffenen (61 %) setzte **keinerlei Maßnahmen als Reaktion** auf den Betrug.
- Die **häufigsten Reaktionen** betroffener Personen: 22 % der Betroffenen wollten die **Tat der Polizei melden** – doch nur **8 % erstatteten tatsächlich Anzeige**. 16 % **berichteten im Internet über ihre leidvolle Erfahrung**.
- 11 % der Betroffenen wendeten sich an eine **Beratungsstelle**, 5 % nahmen **psychologische Unterstützung** in Anspruch.

## 5. Tipps zum Schutz vor Telefontricks

„Hallo, wer spricht? Na, sicher nicht!“ Das omnipräsente Risiko von Telefonbetrug erfordert von mündigen Menschen bewusst gesetzte Gegenstrategien: Maßnahmen, die vom simplen Auflegen oder strikten „Nein“ am Telefon über gefinkelte Gegenfragen, umfassende Internet-Recherchen und familiäre Rücksprache bis zur polizeilichen Anzeige und aktiven Mitarbeit im Rahmen der Strafverfolgung reichen.

Der folgende Leitfaden liefert die wichtigsten Handlungsempfehlungen für ein kompetentes Verhalten im Fall von (versuchtem) Telefonbetrug.

### So reagieren Sie auf Telefontricks richtig – die wichtigsten Tipps zur Vermeidung von Telefonbetrug:

#### Allgemeine Achtsamkeit, hallo!

- Vorsicht ist die Mutter der Telefonleitung: Legen Sie beim Telefonieren **Achtsamkeit** und eine gesunde Portion **Skepsis** an den Tag! Erkennen Sie beim Anruf unbekannter Personen den feinen Unterschied zwischen Dichtung und Wahrheit!
- Hören Sie auch beim Telefonieren auf Ihr **Bauchgefühl!** Nicht immer ist alles echt, was sich nach Wirklichkeit anhört. Oft ist die via Telefon geschilderte Realität nur konstruiert – ein geschickt gestricktes Lügenmärchen, das Sie zur Zahlung von Geld drängen soll.
- Bleiben Sie möglichst **sachlich** und bewahren Sie **kühlen Kopf** – auch wenn am anderen Ende der Leitung scheinbar die Welt untergeht.
- Wenn Sie sich **bei seltsam wirkenden Telefongesprächen unwohl fühlen, legen Sie ganz einfach auf!**
- Halten Sie nach zweifelhaften Telefonbegegnungen **Rücksprache mit Vertrauenspersonen aus dem Familien- und Freundeskreis!**
- **Rufen Sie in Not- und Zweifelsfällen die Polizei: 133!**

#### Neffentrick? Nein, danke!

- Formulierungen wie **"Rat mal, wer da spricht!"** oder **"Erkennst du mich denn nicht?"** sollten stutzig machen. Lassen Sie sich auf kein Namen-Raten ein! **Verlangen Sie, dass die anrufende Person von sich aus ihren Namen nennt!** Wenn es sich tatsächlich um eine nahestehende Person handelt, wird sie dieser Bitte nachkommen.



- Auch wenn die anrufende Person ihren Namen genannt hat und um Geld bittet, ist Vorsicht angebracht. **Lassen Sie sich nicht unter Druck setzen!** Vergewissern Sie sich, ob es sich bei der anrufenden Person tatsächlich um ein Familienmitglied handelt: **Stellen Sie ihr eine persönliche Frage, die nur im vertrauten Familienkreis beantwortbar ist!**
- Wenn das **Bauchgefühl Nein sagt, antworten Sie mit einem klaren „Nein“!** **Beenden Sie das Gespräch und rufen Sie Ihre Nichte/Ihren Neffen/Ihr Enkelkind unter der gewohnten Nummer zurück!** Nur so können Sie die zuvor am Telefon gehörte Version gegenchecken und sich von den Tatsachen überzeugen.

### Kautionstrick? Nicht mit Ihnen!

- Die **Story mit dem schweren Verkehrsunfall und der erforderlichen Kaution zur Freilassung des Sohnes/der Tochter** ist eine **lupenreine Telefonlüge**. Gehen Sie dieser atemberaubend frechen Forderung nicht auf den Leim!
- **Bleiben Sie cool, legen Sie auf und rufen Sie Ihren Sohn/Ihre Tochter unter der gewohnten Handynummer zurück.** Nur so bringen Sie Klarheit in Ihr Gefühls-Chaos und Licht in das dunkle Strickwerk eiskalt servierter Lügenmärchen.

### Falsche Polizisten müssen draußen bleiben

- Auch wenn Sie den **Anruf einer angeblichen Amtsperson** erhalten haben: **Lassen Sie keine fremde Person in Ihr Haus!** Sagen Sie, dass für die genannte Sache gerade **kein günstiger Zeitpunkt** ist. Echte Exekutivbeamte haben Verständnis dafür, Betrüger\*innen erhöhen dagegen den Druck, damit Sie in der Leitung bleiben und dem geplanten Verbrechen Tür und Tor öffnen.
- Falls Sie der anrufenden Person bereits telefonisch **Zusage erteilt** haben und danach aber **Zweifel** aufkommen, **rufen Sie die Polizei (Telefonnummer 133) an!** Diese wird mit Ihnen die weitere Vorgangsweise abstimmen und eventuell versuchen, die kriminelle Person bei der fingierten Geldübergabe zu stellen.
- **Gewähren Sie niemals fremden Personen Zutritt in Ihr Haus oder Ihre Wohnung!**
- **Übergeben Sie niemals unbekanntem Personen Geld oder Wertgegenstände!** Echte Polizeibeamte und -beamtinnen holen niemals Geld, Schmuck & Co. von Privathaushalten ab.

### Datenklau und wie man ihn verhindern kann

- **Vorsicht bei WhatsApps, SMS und E-Mails von unbekanntem Absender\*innen!** Klicken Sie nicht auf unbekannte Links, öffnen oder installieren Sie keine unbekanntem Dateien und Programme!
- Wehren Sie **Phishing-Anrufe** mit einem freundlichen, aber bestimmten „Danke, nein!“ ab und legen Sie so schnell wie möglich auf!

- Wenn der **Mama-Papa-Hilfe-neue Nummer-Trick** anklopft: **Rufen Sie Ihr Kind unter seiner gewohnten Handy-Nummer zurück und checken Sie die Echtheit der Notsituation!**
- **Melden Sie Phishing-Vorfälle der Polizei (133)!**

### **Call-Bot-Anrufe: Sag dem Tonband leise Servus!**

- Wenn die automatische, spooky klingende **Stimme vom Tonband seltsame Handlungsanweisungen** gibt: **Legen Sie auf!**
- **Lassen Sie sich mit Pseudo-Polizist\*innen auf keine Gespräche über Fake-Delikte ein, die Sie angeblich begangen haben!**
- **Laden Sie keine Software herunter, überweisen Sie kein Geld!**

### **Zeigen Sie Cold Calls & Cold SMS die kalte Schulter!**

- **Brechen Sie bei Cold Calls eiskalt das Gespräch ab** – Sie haben ein Recht darauf, nicht belästigt zu werden.
- **Reagieren Sie nicht auf unerwünschte Werbe-Messages!**
- Sollte Ihre **Privatsphäre nachhaltig gestört** werden: **Melden Sie die Sache der Polizei (133)!**

### **Rückruf bei Ping-Anrufen? Sicher nicht!**

Das Telefon **klingelt nur ganz kurz** – und die Rufnummer hat eine **ausländische – meist osteuropäische oder afrikanische – Ländervorwahl?**

- **Heben Sie bei Anrufen unbekannter Nummern aus dem Ausland nicht ab und rufen Sie auch nicht zurück!** Denn bei dieser Art von Abzocke aus dem Ausland sollten bei Ihnen die Alarmglocken schrillen: Ein Rückruf landet auf einer kostenpflichtigen Hotline – danke, nein!
- **Smartphones bieten die Möglichkeit, Anrufe mit bestimmten Rufnummern zu unterdrücken – nutzen Sie bei Bedarf diese Option, um sich vor lästigen Anrufen zu schützen!**

### **Cyber Trading Fraud kritisch durchschauen!**

Und ewig lockt das Geld. Doch **schnellen Cash-Flow und hohe Gewinnchancen gibt es auch im Internet nicht zu erhaschen.** Wenn etwas zu schön erscheint, um wahr zu sein, ist es höchstwahrscheinlich waschechter Betrug.

- Checken Sie die **Website der Trading Plattform** genau: Gibt es ein **Impressum**? Gibt es eine **Kontaktadresse**, einen verantwortlichen **Ansprechpartner**? Klingen die **Allgemeinen Geschäftsbedingungen (AGBs)** schlüssig und seriös?
- Recherchieren Sie im Internet, ob es bereits **Beschwerden oder Warnungen** die jeweilige Plattform oder Gesellschaft betreffend gibt!
- Überprüfen Sie die (nicht) vorhandene **Konzession der Finanzmarktaufsicht** für die betreffende Trading Plattform bzw. ihre Betreibergesellschaften – oder eine eventuelle **Warnung vonseiten der FMA**! Nähere Infos finden Sie auf der FMA-Website: [www.fma.gv.at](http://www.fma.gv.at)
- **Wenn irgendein Detail nicht passt: Lassen Sie die Finger davon!**
- **Bei bereits erlittenem Schaden: Erstellen Sie Anzeige bei der Polizei!** Ihre Mitarbeit kann die Chancen eines Ermittlungserfolgs erhöhen. Melden Sie den Vorfall auch der FMA.

**Für alle Not- und Zweifelsfälle in Sachen Telefonbetrug gilt:**

**Rufen Sie die Polizei unter der Nummer 133!**

## 6. Conclusio

Die KfV-Dunkelfeldstudie zeigt: Österreich ist gut informiert – aber noch immer nicht gut genug. In viel zu vielen Fällen haben Telefonbetrüger\*innen allzu leichtes Spiel. Mit psychologischen Tricks wird massiver emotionaler Druck angewendet, um gutgläubige Bürger\*innen um ihr Hab und Gut zu bringen. Ältere, allein lebende Menschen sind besonders oft Ziel betrügerischer Anrufe. Das Thema Telefonbetrug muss daher vermehrt im Bewusstsein der Bevölkerung verankert werden, um den dreisten Kriminellen einen Strich durch die Rechnung zu machen.

Der Schlüssel zu mehr Sicherheit heißt „Information“. Denn Wissen ist Macht – und schützt vor Schaden: Mit der aktuellen Dunkelfeldstudie will das KfV-Forschungsteam das Problem des modernen Telefonbetrugs in den Fokus der öffentlichen Aufmerksamkeit rücken, Information über kriminelle Taktiken liefern und wertvolles Bewusstsein für diese Bedrohung schaffen. Vom simplen Neffentrick bis zum ausgeklügelten Cyber Trading Fraud: Wir müssen Bescheid über den unsichtbaren Feind am Ende der Leitung wissen.

Gegenwehr statt Opferwerdung ist angesagt: Wenn statt der Goldmünzen nur Kieselsteine und statt der Geldscheine nur alte Hemden übergeben werden – und ein paar Sekunden später die Handschellen klicken: Dann haben sich die Betrüger\*innen wohl leicht verkalkuliert. Telefonbetrug muss nicht immer klappen, oft stoßen Lügengeschichten auf taube Ohren und umso wacheren Geist, dies lassen spannende Medienberichte über brillant gelungene Gegenmaßnahmen wissen. Von so manchem Scharf- und Spürsinn ihrer Leider-nein-Opfer können zur Strecke gebrachte Schmalspur-Kriminelle hinter schwedischen Gardinen nur träumen.

Kriminelle Energie braucht eine starke, selbstbewusste Antwort – in puncto Telefonbetrug ist diese Antwort für die meisten Menschen mit minimalem Aufwand möglich. Ein simples Nein zur rechten Zeit schützt vor fatalen Folgen, eine Anzeige unterstützt Polizei- und Präventionsarbeit. Die Suche nach den Täter\*innen gestaltet sich meist schwierig und ist dennoch in so manchen Fällen von Erfolg gekrönt. Oft ist die Beute aber bereits in dunklen Kanälen verschwunden. Umso stärker gilt der Grundsatz: Sicherheit beginnt im Kopf – Aufklärung muss sein: Informierte, sensibilisierte Menschen gehen betrügerischen Tricks nicht so leicht auf den Leim.

Doch wohlgermerkt: Telefonbetrug passiert täglich, rund um die Welt – und kann grundsätzlich alle von uns treffen. Wer von Täter\*innen via Telefon hinters Licht geführt wurde, erlebt also kein Einzelschicksal, sondern hat – wie tausende andere Menschen – im falschen Moment falsch reagiert. Eine menschliche Fehlreaktion im Affekt, die – aus Sorge, Wunschdenken oder Überforderung – allen von uns einmal passieren kann. Folgeschwerer Vertrauensmissbrauch hinterlässt tiefe seelische Spuren – der Verlust der gesamten Lebensersparnisse ist eine niederschmetternde Schockerfahrung mit finanziellen, sozialen und psychischen Konsequenzen.

„Du bist nicht allein“: Dieses Gefühl muss Betroffenen daher umfassend vermittelt werden, um die emotionalen Folgen des erlebten Traumas abzufedern. Psychologische Betreuung sollte

Betroffenen in Extremsituationen wie diesen mit Rat und Tat zur Seite stehen. Auch wenn so mancher Fall Sensationscharakter hat: Mitgefühl und Solidarität sind angebracht – denn die perfiden Tricks der Täter\*innen zielen direkt auf unsere im Ernstfall allzu leicht steuerbaren Emotionen ab. Mitten ins Herz.

Fazit des KFV-Forschungsteams: Das beste Gegenrezept zur Vermeidung von Telefonbetrug sind verstärkte Aufklärung und Bewusstseinsbildung. Das kriminelle Spiel mit unseren menschlichen Gefühlen – Ängsten, Hoffnungen, Sehnsüchten, Sorgen, Wünschen – muss mit der wirksamsten aller Gegenmaßnahmen unterbunden werden: Information.

Information schafft Sicherheit: Die Ohnmacht potenzieller Opfer muss der Macht des Wissens weichen. Wenn aufgeklärte Kompetenz den Anruf entgegennimmt, haben Kriminelle in ihren muffigen Hinterhofzimmern oder strahlend hellen Call-Centern keine Chance. Die richtige Antwort auf alles, was zu schön oder zu wild erscheint, um wahr zu sein, lautet also frei nach Georg Danzer: „Ruaf mi ned au!“

Irren ist menschlich – Information ist ein Muss. Mit verstärkter Bewusstseinsbildung zum Thema Telefonbetrug kann Täter\*innen das dunkle Treiben erschwert oder gar das Handwerk gelegt werden. Unzählige leidvolle Erfahrungen können vermieden werden – und das Familiensilber bleibt, wo es ist.

## Abbildungsverzeichnis

Abbildung 1: Belästigende Anrufe und SMS in Österreich, 02/2022 - 08/2023, Quelle: RTR.....	6
Abbildung 2: Anzeigen von Internetbetrug in Österreich 2006 bis 2022, Quelle: Statista, 2023....	7
Abbildung 3: Telefonnutzung in Österreich, in Prozent, Mehrfachauswahl .....	12
Abbildung 4: Tägliche Internetnutzung .....	13
Abbildung 5: Telefonnutzung pro Woche .....	13
Abbildung 6 Eintrag mit privater Nummer, Angaben in Prozent, Mehrfachauswahl .....	14
Abbildung 7: Häufigkeit Herausgabe eigener Telefonnummer .....	15
Abbildung 8: Annahme von Anrufen unbek. Nummern, Angaben in Prozent.....	16
Abbildung 9: Angabe der Telefonnummer in E-Mail-Signatur.....	17
Abbildung 10: Viktimisierung im engeren Sinn.....	20
Abbildung 11: Persönliche Reaktion nach Betrugsversuch .....	21
Abbildung 12: Wissen über Beratungsstellen, Mehrfachauswahl möglich .....	22
Abbildung 13: Beispieldiagramm Balken .....	<b>Fehler! Textmarke nicht definiert.</b>
Abbildung 14: Beispieldiagramm Kreis.....	<b>Fehler! Textmarke nicht definiert.</b>

## Literaturverzeichnis

Bundeskriminalamt, Bundesministerium für Inneres: **Vorsicht: Betrügerische Anrufe**,  
<https://bundeskriminalamt.at/news.aspx?id=73623334725656744D41413D> (abgerufen am 21.9.2023)

Bundesministerium für Inneres: **Anrufkriminalität**,  
[https://bmi.gv.at/magazin/2022\\_03\\_04/Anrufkriminalitaet.aspx](https://bmi.gv.at/magazin/2022_03_04/Anrufkriminalitaet.aspx)

Rundfunk und Telekom Regulierungs-GmbH (RTR): **Aktuelle Beobachtungen und Warnungen**,  
[https://www.rtr.at/TKP/was\\_wir\\_tun/telekommunikation/konsumentenservice/meldestelle\\_rufnummernmissbrauch/aktuelle\\_Beobachtungen.de.html](https://www.rtr.at/TKP/was_wir_tun/telekommunikation/konsumentenservice/meldestelle_rufnummernmissbrauch/aktuelle_Beobachtungen.de.html)

Statista: **Angezeigte Fälle von Internetbetrug in Österreich von 2006 bis 2022**,  
<https://de.statista.com/statistik/daten/studie/527857/umfrage/angezeigte-faelle-von-internetbetrug-in-oesterreich/> (abgerufen am 21.9.2023)



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](mailto:kfv@kfv.at)

[www.kfv.at](http://www.kfv.at)

**Medieninhaber und Herausgeber:** Kuratorium für Verkehrssicherheit

**Verlagsort:** Wien

**Herstellung:** Eigendruck

**Redaktion:** Patricia Jeßner, BA

**Grafik:** eigene/Canva

**Copyright:** © Kuratorium für Verkehrssicherheit, Wien. Alle Rechte vorbehalten.

**SAFETY FIRST!**