HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Marie Köhler

Untersuchung der moralischen und ethischen Auswirkungen von Social Engineering Angriffen am Beispiel des Enkeltricks – analog und digital

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Untersuchung der moralischen und ethischen Auswirkungen von Social Engineering Angriffen am Beispiel des Enkeltricks – analog und digital

Autor:
Frau

Marie Köhler

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO19w2-B

Erstprüfer:
Herr Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Frau Michele-Nadine Wagner

Einreichung:
Mittweida, 14.08.2023

Verteidigung/Bewertung:
Mittweida, 2023

Faculty Applied Computer Sciences and Biosciences

BACHELOR THESIS

Investigation of the moral and ethical effects of social engineering attacks using the example of the “grandchild trick” – analogue and digital

author:
Ms.

Marie Köhler

course of studies:
General and Digital Forensic Science

seminar group:
FO19w2-B

first examiner:
Mr. Prof. Dr. rer. nat. Dirk Labudde

second examiner:
Ms. Michele-Nadine Wagner

submission:
Mittweida, 14.08.2023

defence/ evaluation:
Mittweida, 2023

Bibliografische Beschreibung:

Köhler, Marie:
Untersuchung der moralischen und ethischen Auswirkungen von Social Engineering Angriffen am Beispiel des Enkeltricks – analog und digital. - 2023. - 14, 53, 18 S.
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung von männlichen und weiblichen Sprechformen verzichtet. Sämtliche allgemeine Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Referat:

Verschiedenste telefonische Betrugsmaschen, die auf die ältere Generation abzielen, sind in den letzten Jahren in Deutschland exorbitant gestiegen. Ob Schockanruf, WhatsApp-Betrug oder Enkeltrick: die Folgen eines solchen Betrugsfalls werden nur selten aufgezeigt. Anhand einer quantitativen Umfrage und einem Interview mit einer Betroffenen werden in dieser Arbeit die Betrugspräsenz, die Trendentwicklung und der aktuelle Aufklärungsstand am Beispiel des Enkeltricks, sowohl analog als auch digital untersucht. Abschließend werden Handlungsempfehlungen für potenziell gefährdete Menschen ausgesprochen.

Abstract:

Various telephone scams aimed at the older generation have increased exorbitantly in Germany in recent years. Whether it’s a shocking phone call, WhatsApp fraud or the ‘Grandchild trick’: the consequences of such fraud cases are rarely shown. Based on a quantitative survey and an interview with an affected person, this work examines the presence of fraud, trend development and the current state of clarification using the example of the ‘Grandchild trick’, both analogue and digitally. In the end, recommendations for action are made for endangered people.

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

BMFSFJ	Bundesministerium für Familie, Senioren, Frauen und Jugend
SE	Social Engineering
BSI	Bundesamt für Sicherheit in der Informationstechnik
StGB	Strafgesetzbuch
KI	Künstliche Intelligenz

1 Einleitung

Ob Schockanruf, WhatsApp-Betrug oder der Enkeltrick: Verschiedenste Betrugsmaschen am Telefon oder an der Haustür älterer Menschen sind in den letzten Jahren in Deutschland exorbitant gestiegen. Und es tauchen immer neue abgewandelte Maschen auf. Allein in Sachsen wurden 2022 251 erfolgreiche Schockanrufe registriert, die über 1,92 Millionen Euro Schaden anrichteten [1]. Die Fälle des klassischen Enkeltricks scheinen in Sachsen rückläufig zu sein, in anderen Bundesländern hingegen steigen sie jährlich. Doch immer noch erbeuten die Täter jedes Jahr Tausende, wenn nicht Millionen an Euro durch Betrugsanrufe, und nur in 25% der Fälle würden die Täter ermittelt [2] [3].

Obwohl es keine eigenen statistischen Aufzeichnungen über den klassischen Enkeltrick gibt, sondern diese Form des Trickbetrugs unter die Kategorie Betrug allgemein fällt, ist davon auszugehen, dass die Dunkelziffer deutlich höher sein muss. Die Gründe dafür werden u.a. in dieser Bachelorarbeit thematisiert.

1.1 Motivation

Laut dem Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) zeigten polizeiliche Kriminalstatistiken, dass ältere Menschen nicht pauschal ein höheres Risiko haben, Opfer von Kriminalität zu werden, als jüngere. Jedoch gäbe es einige Kriminalitätsfelder, in denen sie gefährdeter sind und besonders ins Visier von Kriminellen geraten, wie zum Beispiel Betrug. Gerade Trickbetrug durch Vortäuschung falscher Identität wie dem Enkelkind, der Polizei oder dem Handwerker, ist bei den Betrügern sehr beliebt [4]. Leider werden die psychischen Auswirkungen eines solchen Betrugsfalls viel zu wenig thematisiert, daraus resultiert die Motivation für dieser Forschungsarbeit. Die wissenschaftliche Relevanz des Themas liegt in der Opferpsychologie, der Betrugsprävention und der Strafverfolgung. Das Verständnis der Auswirkungen auf die Opfer ist wichtig, um psychische und emotionale Folgen von Betrug und Täuschung zu erfassen. Es kann helfen, angemessene Maßnahmen für die Opfer zu entwickeln, die ihnen bei der Verarbeitung der traumatischen Erfahrung helfen können. Außerdem hilft die Aufklärung über die Vorgehensweise der Täter und die Folgen des Betrugs, potenziell gefährdete Menschen für verdächtige Faktoren zu sensibilisieren, sodass zukünftige Fälle vermieden werden können.

Anhand einer quantitativen Umfrage wird die Präsenz des Enkeltrick-Betrugs in analoger und digitaler Form analysiert und mithilfe eines Interviews mit einer Betroffenen werden Erfahrungen bezüglich des Themas Enkeltrick aufgezeigt. Anhand der Ergebnisse dieser beiden Methoden werden folgende aufgestellten Hypothesen beantwortet und kritisch betrachtet:

1. „Enkeltrick-Betrugsopfer haben Langzeitfolgen in Form von Depressionen, Angstzuständen und Vereinsamung.“
2. „Betroffene scheuen sich davor, sich anderen Menschen anzuvertrauen.“
3. „Frauen sind häufiger Enkeltrick-Betrugsopfer als Männer.“
4. „Es erfolgt eine Trendentwicklung des Enkeltrick-Betrugs auf die jüngere Generation.“
5. „Es muss mehr Aufklärungsarbeit geleistet werden.“

1.2 Zielstellung

Ziel der Bachelorarbeit ist es zu untersuchen, welche ethischen und moralischen Auswirkungen der Enkeltrick-Betrug auf die Opfer hat. Mithilfe der Methoden soll untersucht werden, ob und warum es ein Geschlecht gibt, das signifikant öfter zum Opfer wird und ob sich der Trend dieses Trickbetrugs auf die jüngere Generation verlagert hat. Außerdem wird der aktuelle Aufklärungsstand erörtert und Handlungsempfehlungen für potenzielle Opfer und deren Umfeld aufgezeigt.

2 Grundlagen Social Engineering

In der heutigen digitalen Welt werden Betrug und Abzocke immer häufiger über das Internet durchgeführt. Dabei setzen Kriminelle nicht nur auf technische Methoden, sondern nutzen auch soziale Techniken, um ihre Opfer zu manipulieren. In diesem Kapitel wird das Social Engineering (wörtlich: „soziale Manipulation“) [5] als Kommunikationstechnik ausführlich erklärt.

2.1 Definition Social Engineering

Christopher Hadnagy, ein Pionier auf diesem Gebiet, definiert Social Engineering (SE) als „jede Handlung, die jemanden dazu veranlasst, etwas auszuführen, was für ihn nicht unbedingt vorteilhaft ist.“ [6]. Der Mensch als Schwachstelle wird auf einer emotionalen Ebene manipuliert, was dazu führt, dass bestimmte Verhaltensweisen hervorgerufen werden. Ziel ist es zum Beispiel, Menschen dazu zu bringen, ein Produkt zu kaufen oder vertrauliche Informationen preiszugeben, die illegal verwendet werden können.

Kevin Mitnick, ein bekannter amerikanischer Social Engineer, beschreibt in seinem Buch „The Art Of Deception“ (deutsch: „Die Kunst der Täuschung“), dass technische Sicherheitssysteme wie Firewalls oder Zugangsbeschränkungen den Menschen ein falsches Sicherheitsgefühl vermitteln. Die Menschen glaubten, sie seien vor Dieben oder Angreifern geschützt, wenn sie Schlösser zur Diebstahlsicherung oder die besten technischen Abwehrsystem installierten. Trotzdem seien alle gut geschützten Hausbesitzer oder Unternehmen gefährdet, da die größte Schwachstelle in der Sicherheitskette der Mensch selbst ist. Die Unwissenheit des Menschen, meist verstärkt durch Ignoranz und Leichtgläubigkeit, würde immer mehr durch Social Engineers und Betrüger ausgenutzt, je weiter die technologische Entwicklung fortschreitet. Denn dadurch werden technische Schwachstellen immer weiter verringert und der Mensch als Schwachstelle immer beliebter [7].

2.2 Geschichte des Social Engineerings

Eine der ältesten Formen des Social Engineering ist die Kunst der Überzeugung. Schon in der Antike verwendeten Politiker und Redner rhetorische Fähigkeiten, um Menschenmassen zu beeinflussen und deren Meinung zu ändern. Diese Techniken werden auch heute noch von Propagandisten und Werbetreibenden genutzt, um die breite Öffentlichkeit zu beeinflussen. Mit der Weiterentwicklung der Technologie kamen jedoch neue Möglichkeiten des Social Engineerings hinzu. Schon im 19. Jahrhundert begannen Betrüger das Vertrauen und die Naivität ihrer Opfer auszunutzen, um an Geld zu gelangen. Ein berühmtes Beispiel ist der amerikanische Betrüger Charles Ponzi, der ein Betrugssystem entwickelte, bei dem Opfer dazu gebracht wurden ihm ihr Geld für Investitionen anzuvertrauen. Millionen von Menschen wurden mit seinem „Ponzi-Scheme“ (deutsch: „Ponzi-Masche“) um ihr Geld gebracht [8].

Im späten 20. Jahrhundert wurde die Technik des Social Engineering als „Phone Phreaking“ genutzt. Man gab sich damals als vermeintlicher Telefontechniker aus, um die Leitungen der Telefonnetze kostenlos zu nutzen. Die Angreifer nutzten ihre Kunst der Beeinflussung,

um Autorität vorzugaukeln [9] .Mit der Entwicklung des Internets in den 90er Jahren wurde das SE zu einer ernsten Bedrohung für die Cyber-Sicherheit, nicht nur von Unternehmen sondern auch von Privatpersonen. Hacker und Cyber-Kriminelle entwickelten raffinierte Techniken, um Passwörter und andere vertrauliche Informationen von ahnungslosen Nutzern zu stehlen. Phishing-Angriffe sind ein Beispiel für diese moderne Form des Social Engineerings, die in Kapitel 2.6.1 noch einmal aufgegriffen werden.

In den letzten Jahren hat diese Art der Manipulation auch politische Auswirkungen gehabt. Zum Beispiel wurde im Jahr 2016 bekannt, dass eine russische Trollfabrik namens „Internet Research Agency“ Social-Media-Plattformen wie Facebook und Twitter manipulierte, um die öffentliche Meinung und die Wahlkampagne in den USA zu beeinflussen [10].

2.3 Social Engineering in der Gesellschaft

Social Engineering wird in gewissem Maße täglich von jedem von uns angewendet. Begonnen wird damit sogar schon in jungen Jahren. Denn selbst Kinder beeinflussen ihre Eltern, um an das zu gelangen, was sie gern hätten. Sie schaffen emotionale Bindung durch Berührung oder liebe Worte und bewegen sie so dazu, dass sie ihre Wünsche erfüllt bekommen [6].

Ein anderes permanent präsentes Beispiel für Social Engineering ist Werbung. Hierbei wird beim Kunden mit perfekt abgestimmten visuellen und akustischen Mitteln ein Bedürfnis erschaffen, das durch Wiederholung immer wieder verstärkt wird. Verkäufer verwenden außerdem verschiedene Kommunikationsmethoden, die dem Kunden persönliche Informationen entlocken und ihm dann das Gefühl geben, ein bestimmtes Produkt passe genau zu seinen Bedürfnissen. Diese beiden Szenarien sind Beispiele für positives Social Engineering. Es zielt darauf ab, dass beide Parteien gewinnen und sie sich danach besser fühlen. Laut Hadnagy liege der Unterschied zwischen gutem und bösem Social Engineering in der Absicht: „Beim bösen Social Engineering will der Social Engineer nicht helfen oder Ihr Leben verbessern, sondern ihm geht es einzig darum, was er selbst bekommt.“ [6, S. 76] Unter böses Social Engineering fällt jede Art von Betrug und Trickserei, die einer Partei Schaden zufügt.

2.4 Manipulationsprinzipien

Im folgenden Abschnitt werden die notwendigen Prinzipien, also Vorgehensweisen des Social Engineerings genauer vorgestellt.

2.4.1 Informationsbeschaffung

Zunächst ist es wichtig, so viele Informationen über das potenzielle Ziel zu sammeln, wie nur möglich. Je mehr Informationen ein Social Engineer hat, desto größer ist die Angriffsfläche, die er nutzen kann. So kann er mehr Methoden entwickeln, um die Zielperson oder das Zielunternehmen zu infiltrieren. Es gibt viele Möglichkeiten, wie ein Social Engineer an Informationen gelangen kann. Viele Menschen teilen von sich aus viele in sozialen Netzwerken, die für jeden zugänglich sind. So wissen sie meist schon über Vorlieben oder

Hobbys einer Zielperson oder über Abläufe in Firmen Bescheid. Andere Wege, um an wichtige Informationen zu gelangen, sind Methoden wie das Dumpster Diving (oder „Information Diving“) oder das Shoulder Surfing. Beim Dumpster Diving durchsucht man den Müll einer Person, um Rückschlüsse auf deren Konsumverhalten, Gewohnheiten oder Interessen zu ziehen [11]. Als Shoulder Surfing wird das simple Beobachten von sensiblen Daten bezeichnet. Dabei wird der Person unmittelbar über die Schulter geschaut, wenn sie z.B. ihren PIN auf dem Handy oder an der Kasse eingibt [12].

Social Engineere nutzen auch gern eine persönliche Art der Informationsbeschaffung, das Elizitieren. Hierbei werden dem Opfer beim Gespräch unterschwellig Informationen entlockt, ohne ihm direkte Fragen zu stellen. Der Gesprächspartner sammelt einfach während einer Unterhaltung Informationen über Hobbys, Familie oder Arbeit und bringt den anderen dazu ihn zu mögen, indem er so tut, als hätte er genau dieselben Interessen [6].

2.4.2 Pretexting

Pretexting ist eine wichtige Vorgehensweise. Das Prinzip der Täuschung ist, jemandem die Unwahrheit zu erzählen. Der Pretext eines Social Engineers ist die Geschichte, die er sich ausdenkt, die das Opfer glauben soll. Er schlüpft in eine Schauspielrolle, die er glaubwürdig verkörpern muss. Dabei muss das äußerliche Auftreten wie die Kleidung und ggf. ein Nachweis wie ein Ausweis oder ein Namensschild, sowie Wortwahl, Körpersprache und das Hintergrundwissen miteinander übereinstimmen.

2.4.3 Rapport

Rapport nennt man das wohl wichtigste Prinzip: Vertrauen zur Zielperson aufzubauen. Denn nur auf dieser Basis kann Betrug überhaupt funktionieren. Vertrauen und Verbundenheit führen dazu, dass die Zielperson Informationen preisgibt oder Handlungen ausführt. Das kann mit verschiedenen Methoden erreicht werden. Grundlage hierfür ist, dass man bei der Zielperson ein Gefühl der Zugehörigkeit in Form von Gemeinsamkeiten hervorruft. Gibt der Social Engineer selbst ein paar Informationen über sich preis, vermittelt das dem Gegenüber nicht nur ein Gefühl von Sicherheit, sondern auch der Verpflichtung ebenso von sich zu erzählen.

2.4.4 Framing

Als Framing bezeichnet man die Persönlichkeitsstruktur eines Menschen. Es beschreibt das Zusammenspiel von persönlichen, emotionalen und psychologischen Eigenschaften, die uns zu dem Menschen machen, der wir sind. Unsere Erziehung und Erfahrungen sind der Grund dafür, dass wir auf eine bestimmte Art und Weise denken, handeln oder fühlen. Diese Eigenschaften lassen sich als „Frame“ (deutsch: Rahmen oder Struktur) bezeichnen. Ein Social Engineer muss den Frame seiner Zielperson verstehen, damit er eine Verbindung zu ihr aufbauen, und er zum „gleichen Stamm“ gehören kann. Nur so kann sich das Opfer ihm anvertrauen [6].

2.4.5 Manipulation

Durch ein paar geschickte Methoden der Gesprächsführung, kann das Opfer so manipuliert werden, dass es dem Social Engineer alles glaubt oder tut, was er will. Die Kunst dabei ist, dass das Opfer später glaubt, dass es sein eigener Wille gewesen sei [13]. Hadnagy beschreibt in seinem Buch unter anderem folgende Aspekte der Beeinflussung, die helfen, dies zu erreichen:

- **Reziprozität / Verpflichtung:** Reziprozität beschreibt das Gefühl der Verpflichtung, das beim Gegenüber erzeugt wird, wenn man (ihm) zuerst etwas preisgibt. Das Opfer hat das Gefühl, es stünde in der Schuld des Gesprächspartners und müsse sich als Zeichen der Dankbarkeit revanchieren.
- **Dringlichkeit:** Gerade zu Werbezwecken ist dieses Mittel sehr beliebt und wirkungsvoll. Wenn die Ware als limitiert, bald ausverkauft oder schwer erhältlich angepriesen wird, erzeugt das einen gewissen Kauf- bzw. Handlungsdruck. Durch die Erzeugung von Stress und Angst kann der Angreifer das Urteilsvermögen des Opfers beeinflussen und es dazu bringen, unüberlegte Entscheidungen zu treffen.
- **Autorität:** Ein Angreifer kann vorgeben, eine vertrauenswürdige Autoritätsperson zu sein, wie zum Beispiel ein Vorgesetzter, ein Techniker oder ein Polizist. Dadurch wird der Drang zu gehorchen ausgelöst, die uns von Geburt an gelehrt wird, ohne dass das Opfer die Autorität hinterfragt [6].
- **Zuneigung / Sympathie:** Das Gegenüber ist eher bereit Informationen preiszugeben, wenn es das Gefühl hat, gemocht zu werden. Ein wichtiger Faktor, der dafür sorgt, dass wir jemanden sympathisch finden, ist Ähnlichkeit. Gemeinsamkeiten wie die Herkunft oder ähnliche Interessen erzeugen Sympathie. Sympathiebekundungen wie Komplimente machen jemanden in der Regel noch schneller zugänglich [14].
- **Social Proof:** Social Proof ist, wenn ein Social Engineer der Zielperson glaubhaft versichert, dass es in Ordnung ist, eine bestimmte Handlung auszuführen oder Informationen preiszugeben, weil es andere auch tun. Der Mensch will sich einer Gruppe zugehörig fühlen und genau dieses Bedürfnis wird dabei aufgegriffen.

Insgesamt zielt Social Engineering darauf ab, das Opfer auf psychologischer Ebene zu manipulieren, indem es Freundschaft, Vertrauen, Mitleid, Angst oder andere Emotionen ausnutzt. Kevin Mitnick beschreibt dazu folgendes:

„Geschickte Social Engineers sind bei der Erfindung von Hochstapeleien sehr erfahren, bei denen auf der Klaviatur von Emotionen wie Angst, Aufregung oder Schuld gespielt wird. Sie nutzen dabei psychologische Auslöseimpulse – automatische Mechanismen, die andere dazu bringen, sogleich auf vorgebrachte Anliegen zu reagieren, ohne eine gründliche Analyse aller verfügbaren Informationen vorzunehmen.“ [7, S. 131]

Generell ist es so, dass feste Verhaltensmuster und Routinen dafür sorgen, dass menschliche Gedankenprozesse bei der Entscheidungsfindung vereinfacht werden. Als kontrolliertes Verhalten werden Reaktionen bezeichnet, die anhand gründlicher Analyse aller verfügbaren Informationen ausgelöst werden [15]. Das heißt, wenn wir genügend Zeit haben, alle Vor- und Nachteile einer Handlung zu bedenken und sie bei der Entscheidungsfindung einbinden, treffen wir eher Entscheidungen, hinter denen wir später auch stehen und dessen Konsequenzen wir seltener bereuen. Menschen treffen Entscheidungen außerdem viel

bewusster, wenn sie mental in einer guten Verfassung, also motiviert und gedanklich unbeschwert sind. So können mögliche Konsequenzen des Handelns vorher gedanklich abgewogen werden. Emotionen erzeugen eine verzerrende Wahrnehmung unserer Entscheidungsfindung, die eher als unkontrolliertes Verhalten bezeichnet wird. Ein interessanter Ansatz stammt von Daniel Kahneman, einem Verhaltensökonom und Nobelpreisträger. In seinem Buch „Schnelles Denken, langsames Denken“ beschreibt er zwei Denksysteme. Das intuitive und das reflektierende System. Das intuitive System wird stark von Emotionen beeinflusst, während das reflektierende System eher rational arbeitet. Er argumentiert, dass Emotionen oft das intuitive System dominieren und somit unsere Entscheidungen überdurchschnittlich beeinflussen [16].

Eine weitere Studie von Jennifer Lerner, eine Forscherin auf dem Gebiet der Sozialpsychologie, bestätigt, dass negative Emotionen wie Angst, Wut oder Traurigkeit die Entscheidungsfindung beeinträchtigen können. In Experimenten fand sie heraus, dass Menschen in einem negativen emotionalen Zustand überreagieren und risikoreichere Entscheidungen treffen. Positive Emotionen hingegen können dazu führen, dass wir risikoscheu werden und weniger Bereitschaft zeigen, gravierende Veränderungen vorzunehmen. Allerdings kann das nicht pauschal auf alle Emotionen angewandt werden. Beispielsweise bei der Emotion der Liebe wurde beobachtet, dass ein Mensch, durch die Ausschüttung verantwortlicher Hormone, auch risikofreudiger und impulsiver entscheidet, wenn er frisch verliebt ist [17].

Um bei seinem Opfer Angst auszulösen, nutzt der Social Engineer oben genannte Methoden wie Bedrohungen, Dringlichkeit und/oder Autorität. Er kann vorgeben, Mitarbeiter einer Regierungsbehörde zu sein und das Opfer sei in Gefahr, weil es Sicherheitsvorschriften verletzt habe oder sensible persönliche Daten veröffentlicht würden. Er kann den Druck zusätzlich erhöhen, indem er behauptet, das Opfer müsse schnell handeln, um negative Konsequenzen abzuwenden. Der Mensch neigt dazu, jeden Lösungsvorschlag dankbar anzunehmen, den ihn schnellstmöglich aus einer bedrohlichen Lage herausbringt. Vor allem von Personen, die vorgeben das nötige Hintergrundwissen zu haben. Genauso funktioniert die Vorgehensweise mit anderen starken Emotionen wie Mitleid oder Mitgefühl. Erzeugt ein Betrüger dieses Gefühl bei der Zielperson, indem er eine Geschichte erfindet, in der er vorgibt, in einer prekären Situation zu sein und dringend Hilfe zu benötigen, löst er in ihm das Gefühl der Verpflichtung aus. Gerade ältere Menschen wurden so erzogen, dass man sich gegenseitig hilft, da das der natürliche Trieb des Menschen ist, sich einer Gruppe zugehörig zu fühlen. Der Mensch könnte allein und ohne soziale Kontakte nicht überleben. Gibt der Täter sich nun auch noch als Familienmitglied aus, ist die stärkste Form der Hilfsbereitschaft aktiviert. Da man sich zu seiner Familie noch verbundener fühlt und man eher bereit ist, sich innerhalb vorhandener Beziehungen zu helfen, als bei Fremden. Der Täter appelliert somit an die Solidarität des Opfers. Social Engineere nutzen bewusst extra die stärksten Emotionen, bei denen sich der Mensch verwundbar und am beeinflussbarsten macht.

2.5 Kommunikation

Um zu verstehen, wieso Betrugsmaschen funktionieren, muss veranschaulicht werden, wie Kommunikation überhaupt funktioniert und wie die menschliche Psychologie von äußeren Faktoren verändert werden kann. Kommunikation ist ein komplexer Prozess, der auf einem Austausch von Informationen basiert. Dabei spielen verschiedene Modelle und Theorien eine Rolle, die nachfolgend erklärt werden.

Grundsätzlich werden bei Kommunikation mit einem Gesprächspartner Informationen verbal und nonverbal mithilfe von Signalen auf verschiedenen Kanälen vermittelt. Der Inhalt der Nachricht wird über verbale Kommunikation auf dem auditiven Kanal, also als hörbares Signal gesendet. Wie eine Information rübergebracht werden kann, richtet sich nach dem stimmlichen Ausdruck, also beispielsweise mittels Stimmlage, und dem nonverbalen Ausdruck - der Körpersprache. Der stimmliche Ausdruck erfolgt ebenso auf dem auditiven Kanal, die nonverbale Kommunikation meist über den visuellen Kanal als sichtbares Signal. Auch können über den taktilen Kanal, zum Beispiel über Körperkontakt bestimmte Signale kommuniziert werden. Wenn auditive, visuelle und/oder taktile Signale nicht miteinander übereinstimmen, kommt es zu Missverständnissen bei der Kommunikation. Deshalb sind diese Signale untrennbar verbunden [18].

2.5.1 SMCR-Modell nach Berlo

Ein bekanntes Kommunikationsmodell ist das SMCR-Modell von Berlo. Dabei steht die Abkürzung für Source (Quelle), Message (Nachricht), Channel (Kanal) und Receiver (Empfänger).

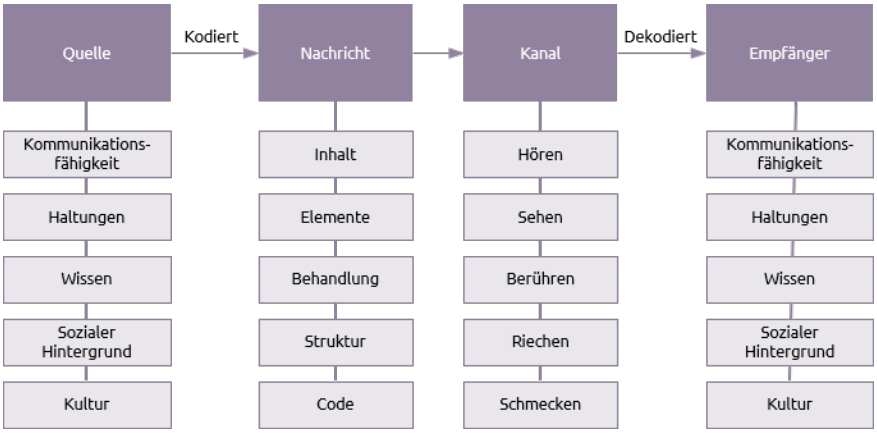


Abbildung 1: SMCR-Kommunikationsmodell nach Berlo (1960)

Quelle: Praxis Framework [19]

Das 1960 von David Berlo aufgestellte Modell, zu sehen in Abbildung 1, nimmt an, dass eine Nachricht vom Sender kodiert und über einen Kanal übertragen wird, um vom Empfänger wieder dekodiert zu werden. Die Quelle, also der Sender, kodiert eine Botschaft durch verschiedene Eigenschaften wie ihr inhaltliches Wissen, ihren sozialen Hintergrund und Kultur, sowie ihre Kommunikationsfähigkeiten. Der Inhalt der Nachricht beschreibt alles, was sowohl absichtlich als auch unabsichtlich kommuniziert wird. Dazu zählen z.B. die Sprache der Nachricht, Körpersprache wie Mimik und Gestik und die visuelle Gestaltung.

Der Sender muss die Nachricht so kodieren, dass die Absicht der Nachricht beim Empfänger deutlich wird, beispielsweise kann sie formell, informell, locker oder ernst gemeint sein.

Berlo beschreibt die Kanäle, die zur Überbringung der Botschaft gewählt werden können, als die fünf Sinne des Menschen. Worte können nicht nur über das Hören oder Lesen vermittelt werden, sondern auch über die nonverbale Kommunikation wie Körperhaltung, Gesichtsausdrücke oder Körperkontakt. Auch können über den Geruchs- und Geschmackssinn Botschaften überbracht werden. Wichtig ist, dass der Sender den richtigen Kanal zur Überbringung seiner Nachricht wählt, damit sichergestellt wird, dass der Empfänger sie auch dekodieren kann. Medien für visuelle und auditive Kommunikationskanäle können beispielsweise E-Mails, Videos, Bilder, Podcasts, Telefonanrufe oder das persönliche Gespräch sein. Letztendlich liegt es an den Fähigkeiten und dem Hintergrundwissen des Empfängers, die Botschaft zu entschlüsseln. Er muss die gleiche Sprache sprechen, den Kontext des Inhalts kennen sowie Zugriff auf die vom Sender gewählten Übertragungskanäle haben [19]. Beim Social Engineering nutzen Täter dieses Modell, um die Kommunikation zu ihrem Vorteil zu beeinflussen. Dabei kann er den Empfänger selbst oder den Kanal manipulieren. Es lassen sich bewusst falsche oder irreführende Informationen präsentieren oder Druck ausüben, um den Empfänger dazu zu bringen, etwas Bestimmtes zu tun. Dieser kann aufgrund von Erwartungen, Annahmen oder sozialen Normen beeinflusst werden und unwissentlich das Ziel des Angreifers unterstützen. Insgesamt ist dieses Modell sehr hilfreich zur Beschreibung menschlicher Interaktionen und bietet auch im Zusammenhang mit Social Engineering eine anschauliche Erklärungsgrundlage, um die Mechanismen der Manipulation und Täuschung zu verdeutlichen.

2.5.2 Vier-Seiten-Modell von Schulz von Thun

Ein anderes Kommunikationsmodell ist das Vier-Seiten-Modell von Friedemann Schulz von Thun. Es besagt, dass jede Nachricht vier Ebenen hat: Sachinhalt, Selbstoffenbarung, Beziehung und Appell. Beim Social Engineering können zum Beispiel Appelle so formuliert werden, dass die Opfer dazu verleitet werden, den Anweisungen der Täter Folge zu leisten, ohne die Konsequenzen zu hinterfragen.

- Der **Sachinhalt** bezieht sich auf die reinen Fakten und Informationen, die in einer Nachricht enthalten sind. Der Sachinhalt ist der wichtigste Teil der Arbeit eines Social Engineers, da darin die Hauptinformation steckt, mit dem sein Opfer beeinflusst werden soll. Das kann ein Gewinnversprechen oder ein angebliches Unfallszenario am Telefon sein.
- **Selbstoffenbarung** bezieht sich auf die Informationen, die der Sender über sich selbst preisgibt, wie zum Beispiel Gefühle, Meinungen, Werte und Einstellungen. Diese Informationen können bewusst oder unbewusst vermittelt werden. Nach vorangehender Recherche über das Opfer kann der Social Engineer seine Werte oder Meinung über im Gespräch relevante Themen dem des Opfers anpassen. So werden sie dem „gleichen Stamm“ zugehörig und das Opfer fühlt sich automatisch dem Täter verbunden, da Gemeinsamkeiten vorhanden sind. Dies schafft Vertrauen, das die Basis eines erfolgreichen Social Engineering Angriffes ist.
- **Beziehung** bezieht sich auf das Verhältnis zwischen Sender und Empfänger. Es beinhaltet die Art und Weise, wie die Nachricht die Beziehung beeinflusst oder spiegelt, wie der Sender den Empfänger wahrnimmt. Indem der Täter die Emotionen

seines Opfers beeinflusst, weil er vorgibt in einer engen Beziehung mit ihm zu stehen, zum Beispiel als Enkel oder Bekannter, verändert er seine Wahrnehmung beim Opfer. Er erzeugt gezielt Mitleid und falsche Verbundenheit, sodass es dem Opfer einfacher fällt, die Handlungen auszuführen, die von ihm verlangt werden.

- Der **Appell** bezieht sich darauf, was der Sender mit der Nachricht beim Empfänger erreichen will. Dies kann eine Bitte, eine Forderung oder eine Meinungsäußerung sein. Mit Worten wie: „Bitte hilf mir!“ wird das Opfer unter psychischen Druck gesetzt und zu einer bestimmten Handlung gedrängt [20].

2.5.3 Watzlawicks Metakommunikation

Ein weiteres wichtiges Kommunikationsmodell ist die axiomatische Kommunikationstheorie von Paul Watzlawick. Dieses beschreibt, wie Bedeutung bei Kommunikation zwischen Menschen geschaffen wird. „Man kann nicht nicht kommunizieren“, denn ob man spricht oder schweigt, in jedem Fall wird damit eine Nachricht übermittelt, die das Gegenüber interpretieren muss. Ähnlich wie beim Kommunikationsmodell von Friedemann Schulz von Thun bestimmt der Beziehungsaspekt einer Nachricht, wie der Gesprächspartner die Mitteilung auffassen soll. Watzlawick versteht diesen Beziehungsaspekt als Metakommunikation. Diese Metakommunikation ermöglicht es dem Menschen, über den Kommunikationsvorgang selbst zu sprechen und damit Missverständnisse aufzudecken und zu beseitigen [21].

Die nonverbale Kommunikation spielt ebenso eine wichtige Rolle beim Social Engineering. Gerade bei Betrugsmaschen am Telefon müssen Täter allein über den auditiven Kanal all ihre Manipulationsfähigkeiten bündeln, da die Opfer sich so nicht auf ihre visuellen oder taktilen Sinne verlassen können. Wie schon erwähnt, müssen die Kanäle und die Signale übereinstimmen. Ein Sanitäter beispielsweise, kann einen Hinterbliebenen nicht mit dem Tod eines Angehörigen konfrontieren und dabei lachen und ihm mit heiterem Gesicht gegenübertreten. Würde er dies tun, vermittelte er dem Gegenüber eine komplett falsche Botschaft. Gerade bei sensiblen Themen müssen Gesichtsausdruck, Tonlage und Körpersprache miteinander im Einklang sein. Für die Täter ist es am Telefon nur wichtig, dass er seine verbalen Merkmale aufeinander abstimmen muss. Laut Hadnagy bringt Lächeln Fröhlichkeit in die Stimme [6]. Forschern zufolge strahle dies Vertrauen aus, welches man sogar fühlen könne, wenn man es nicht sieht. Dies kann nicht nur auf das gesprochene Wort angewandt werden, sondern auch auf das geschriebene. Emoticons zum Beispiel, weisen bei schriftlichen Texten auf die auszulösende Emotion hin. Beim Schreiben eines simplen Ausdrucks wie: „Lustig! ☺“ wird mit dem Smiley deutlich, dass der Sender etwas wirklich amüsant findet. Würde er nur „Lustig!“ schreiben, hätte man das Gefühl, er meine es sarkastisch. Körperhaltung, Gesten sowie Tonhöhe, Lautstärke, Geschwindigkeit und Tonfall der Stimme wirkten sich Hadnagy zufolge ebenso darauf aus, wie die Person am anderen Ende der Leitung unsere Botschaft wahrnimmt. Die Wortwahl und der Ausdruck spielen eine genauso große Rolle dabei. Wiederholt der Täter öfter Wörter hintereinander oder stammelt, könnte das Opfer das Gefühl bekommen, der Täter stünde unter Druck oder sei gestresst, was seine Glaubwürdigkeit wiederum gefährden könnte. Der Tonfall kann Informationen über die Gefühle des Senders geben. Hadnagy beschreibt dies an einem schönen Beispiel: „Als Test schauen Sie mal Ihren Hund streng an und rufen zornig: ‚Ich liebe dich!‘ Dann beobachten Sie, wie er sich in eine Ecke verkriecht. Die Wörter sind nicht wichtig, sondern Ton und Ausdruck.“ [6, S. 43].

Zusammenfassend kann man sagen, dass sich Social Engineering nicht nur einem bestimmten Kommunikationsmodell zuordnen lässt. Es bedient sich aller Kanäle und Signale der Kommunikation, um sie im Sinne des Ausführenden zu beeinflussen.

2.6 Social Engineering Angriffe

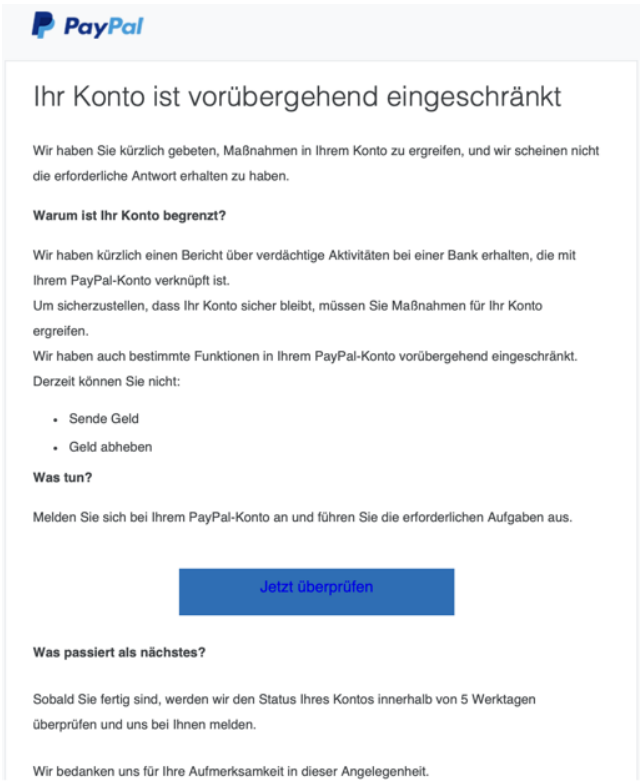
Um zu veranschaulichen, wie die verschiedenen Kanäle und Signale bei Betrug für Manipulation ausgenutzt werden, erfolgt nachfolgend eine nähere Beleuchtung verschiedener Social Engineering Angriffe, sowohl analog als auch digital.

2.6.1 Phishing

Die wohl bekannteste SE-Angriffsmasche ist das Phishing. Bei diesem Angriff werden massenhaft gefälschte E-Mails an potenzielle Opfer verschickt, die sich kaum vom Original unterscheiden lassen. Ziel ist es an Passwörter, Kreditkarteninformationen oder Kontodaten von Nutzern zu gelangen. Die Mails haben die Aufmachung von bekannten, vertrauenswürdigen Institutionen oder Unternehmen wie PayPal, Amazon oder Banken und sind meistens erst auf den zweiten Blick als gefälscht zu erkennen. Das Layout, das Logo, die Farben stimmen mit denen der Originale überein.

Die Opfer werden durch einschlägige Ansprache dazu verleitet, auf Links zu klicken, die es auf gefälschte Webseiten weiterleitet, wo das Opfer dann seine persönlichen Daten wie Passwörter oder Bankdaten eingeben soll. So gelangen die Täter an die Zugangsdaten und können sich so an den Daten der Opfer zu schaffen machen, ohne sich erst die Mühe zu machen, Passwörter zu hacken. Die Vorgehensweise ist hierbei immer gleich, doch die genaue Ausführung variiert ständig und die Täter lassen sich immer neue Abwandlungen einfallen, um ihre Opfer zu täuschen.

Die Empfänger der Phishing-Mails werden durch alarmierende Betreffzeilen oder Ansprachen dazu aufgefordert, eine bestimmte Handlung auszuführen, meistens eben das Anklicken eines Links (siehe Abbildung 2). Beispielsweise wird ein dringender Handlungsbedarf vorgegeben wie: „Wenn Sie Ihre Daten nicht umgehend aktualisieren, dann gehen sie unwiederbringlich verloren…“ oder „Wenn Sie das nicht tun, müssen wir Ihr Konto leider sperren…“.



PayPal

Ihr Konto ist vorübergehend eingeschränkt

Wir haben Sie kürzlich gebeten, Maßnahmen in Ihrem Konto zu ergreifen, und wir scheinen nicht die erforderliche Antwort erhalten zu haben.

Warum ist Ihr Konto begrenzt?

Wir haben kürzlich einen Bericht über verdächtige Aktivitäten bei einer Bank erhalten, die mit Ihrem PayPal-Konto verknüpft ist.
Um sicherzustellen, dass Ihr Konto sicher bleibt, müssen Sie Maßnahmen für Ihr Konto ergreifen.
Wir haben auch bestimmte Funktionen in Ihrem PayPal-Konto vorübergehend eingeschränkt.
Derzeit können Sie nicht:

- Sende Geld
- Geld abheben

Was tun?

Melden Sie sich bei Ihrem PayPal-Konto an und führen Sie die erforderlichen Aufgaben aus.

Jetzt überprüfen

Was passiert als nächstes?

Sobald Sie fertig sind, werden wir den Status Ihres Kontos innerhalb von 5 Werktagen überprüfen und uns bei Ihnen melden.

Wir bedanken uns für Ihre Aufmerksamkeit in dieser Angelegenheit.

Abbildung 2: Beispiel einer Phishing-Mail in PayPal-Aufmachung
Quelle: Verbraucherzentrale [24]

Vor einigen Jahren wurden solche verdächtigen Mails meist noch durch eine unpersönliche Anrede wie „Sehr geehrter Kunde…“ oder durch Rechtschreibfehler und eigenartige Umlaute im Text erkannt. Doch mittlerweile haben Kriminelle ihre Masche perfektioniert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet, dass rund 30% der in 2022 verschickten Spam Mails Phishing Angriffe waren [22]. Man schätze die volkswirtschaftlichen Schäden von Cyber-Delikten in Deutschland, die mit gezielten Phishing-Attacken beginnen, auf einen zweistelligen Millionenbetrag [23].

Während das „normale“ Phishing auf die massenhafte Verteilung dieser Betrugsmails abzielt, lässt sich noch eine andere gezielte Variante beobachten. Beim so genannten Spear-Phishing werden speziell angefertigte Mails an bestimmte Einzelpersonen oder kleinere Gruppen verschickt, nachdem vorher ausgiebige Recherche auf das Ziel vorgenommen wurde. So kann die Erfolgsquote deutlich erhöht werden [25].

2.6.2 Baiting

Beim Baiting-Angriff werden schädliche Gegenstände, wie beispielsweise mit Schadsoftware infizierte USB-Sticks, absichtlich an Orten platziert, wo potenzielle Opfer diese finden und an ihre Computer anschließen. Christopher Hadnagy begründet den Erfolg dieser Masche damit, dass der Angreifer bewusst mit Neugier erweckenden Bezeichnungen der USB-Sticks, wie „Privatfotos“ oder „Vertraulich“ lockt. Der Social Engineer instrumentalisiert so die Neugier der Opfer, um den Adressaten zu einer bestimmten Handlung bewegen, was diese Angriffsform deutlich macht [6].

2.6.3 Tailgaiting

Tailgaiting, vergleichbar mit „Durchschlüpfen“, bezeichnet den Vorgang, wenn sich ein Unbefugter hinter einem autorisierten Mitarbeiter oder einer Person durch eine Zugangskontrolle schleicht, ohne die notwendigen Berechtigungen zu haben. Der Angreifer folgt dem Mitarbeiter oder Hausbewohner einfach direkt, indem er die Tür aufgehalten bekommt, weil er sich als Paketzusteller oder Besucher ausgibt und somit unbefugten Zutritt zum Gebäude erhält [26].

Eine nicht selten praktizierte Betrugsmasche, die vorrangig ältere Menschen betrifft, bedient sich dieser Methode. Betrüger geben beispielsweise vor, ein Handwerker, Mitarbeiter der Hausverwaltung, ein alter Bekannter oder eine Amtsperson, z. B. Gerichtsvollzieher oder Polizist zu sein, um sich Zutritt zum Haus oder zur Wohnung eines Seniors zu verschaffen. Sobald der Betrüger drinnen ist, versucht er, Wertgegenstände zu stehlen oder persönliche Informationen abzugreifen. Da viele ältere Menschen oft freundlich und hilfsbereit sein wollen, sind sie sehr anfällig für solche Arten von Betrugsmaschen.

Manchmal ist das Durchschlüpfen durch die Tür nicht einmal nötig, wenn die Hausbewohner die Kriminellen persönlich, wenn auch unbewusst, in ihre Wohnung lassen. Täter wenden heutzutage vielseitige Tricks an, um ihre Opfer schon an der Haustür auszutricksen. Die Polizeiliche Kriminalprävention der Länder und des Bundes berichtet von einem Fall, bei dem sich zwei Unbekannte Zugang zur Wohnung eines älteren Ehepaars verschafft hatten, nachdem sie nach Zettel und Stift verlangten, um angeblich einer anderen Hausbewohnerin eine Nachricht zu hinterlassen. Als die Seniorin die Utensilien holte, gingen die Unbekannten in die Wohnung. Während eine der Täterinnen das Ehepaar ablenkte, schlich sich die andere ins Schlafzimmer und suchte nach Bargeld. Die beiden Unbekannten erbeuteten so mehrere hundert Euro.

Bei einem anderen Fall erbeutete ein falscher Polizeibeamter den gesamten Inhalt eines Schmuckkastens einer 82-Jährigen, nachdem er behauptete, er müsse gestohlenen Schmuck, der wiedergefunden worden sei, vergleichen [27]. Betrüger haben das Potenzial dieser Vorgehensweise bereits vor längerer Zeit erkannt, da diese Masche der „falschen Polizisten“ immer noch funktioniert. Sie schrecken nicht davor zurück, gefälschte Dienstausweise an der Haustür vorzuzeigen, um sich so Zutritt zum Haus der Senioren zu verschaffen. Sind sie erst einmal in der Wohnung, stehlen sie Wertsachen wie Schmuck oder Bargeld ihrer ahnungslosen Opfer. Ebenso findet der Betrug im Namen der Polizei nicht nur persönlich an der Haustür, sondern auch per Mail, per Post oder am Telefon statt. Manchmal werden vermeintliche Haftbefehle verschickt, indem das Opfer gedrängt wird eine bestimmte Geldsumme zu zahlen, sonst müsse es die Haftstrafe antreten.

Diese und zahlreiche andere Abwandlungen von Betrugsmaschen finden jährlich statt und sind leider nicht selten erfolgreich.

2.6.4 Schockanruf

Besonders raffiniert ist allerdings der sogenannte „Schockanruf“. Hier wird das Opfer mit einer Geschichte beeinflusst, dass dieses aus Angst, der Polizei nicht Folge geleistet zu haben, alles tut was von ihm verlangt wird. Die Geschichten, also der Pretext der Täter, variiert stark. Mal ist es eine Einbruchserie in der Nachbarschaft, die verhindert werden müsse, indem man Wertgegenstände aushändigt, um sie zu sichern, oder die erfolgreichste Methode: ein Angehöriger habe einen schweren Unfall verursacht, bei dem jemand verstorben sei. Es müsse dringend eine hohe Kaution von beispielsweise 50.000 Euro gezahlt werden, sonst müsse der Unfallverursacher ins Gefängnis. Der Hauptkommissar der Polizeidirektion Dresden Carsten Billy beschreibt in einem Interview mit der Freien Presse den Ablauf der Anrufe wie folgt: „Das läuft immer nach dem gleichen Muster ab […] Es gibt einen Anruf, die Opfer hören am anderen Ende der Leitung jemanden weinen, schluchzen, wimmern, das dauert höchstens ein paar Sekunden.“ Dann würde das Telefon an jemand anderen übergeben, der sich als Polizist oder Staatsanwalt ausgäbe. „Die Stimmen klingen immer seriös, haben ein gewisses Alter und strahlen Autorität aus“. Der emotionale Druck, der durch die rundum seriöse Situation auf das Opfer aufgebaut wird, lässt es nicht an der Echtheit der Notlage zweifeln. In der Absicht ihrem Bekannten, Verwandten oder Freund helfen, sowie der Aufforderung eines Beamten nachkommen zu wollen, lassen sich die Opfer auf die Forderung ein.

Carsten Billy gibt an, dass allein dieses Jahr bisher (Artikel vom 10.07.2023) 20 Fälle und Schäden in Höhe von über 500.000 Euro in Dresden und Umgebung verzeichnet worden sind, die nur auf den Schockanruf zurückzuführen sind. Letztes Jahr habe es „nur“ zehn Fälle und 260.000 Euro Schaden gegeben. Die Betrugsanrufe kämen wellenartig, meint der Hauptkommissar. Immer wieder im Wochentakt oder aller paar Monate würden in den gleichen Gegenden rund um Dresden immer wieder Anrufe solcher Art verzeichnet. „Die Täter setzen auf Masse, irgendwer wird ihnen schon ins Netz gehen.“ [28] Zeit.de berichtet, in 2022 habe es allein in Sachsen 251 erfolgreiche Schockanrufe gegeben, die über 1,92 Millionen Euro Schaden angerichtet hätten [3].

Bei einer besonders ausgeklügelten Abwandlung dieser Masche werden die Opfer mithilfe eines so genannten Caller-ID Spoofing-Angriffes ausgetrickst. Dabei kann die Rufnummeranzeige so verändert werden, dass beim Empfänger auf dem Telefon eine vom Angreifer gewünschte Nummer angezeigt wird [29]. In diesem Fall wird der Anruf so geschaltet, dass auf dem Display des eingehenden Anrufes die polizeiliche Notrufnummer 110 erscheint, sodass die Senioren bereits vor dem Gesprächsbeginn manipuliert werden und die Betrüger ihre Geschichte noch glaubwürdiger vermitteln können. Am Apparat geben sie sich dann als Polizeikommissar aus, nennen falsche Namen und Dienstnummern und manchmal ein gewisses Hintergrundwissen über das Opfer. Sie behaupten sie riefen mit der Absicht an, die Opfer zu warnen, dass vermeintliche Diebe zu ihnen unterwegs seien und sie schnellstmöglich all ihre Wertsachen in einen Karton packen und ihn aus dem Fenster werfen sollen, wo ein weiterer Polizist warten und diesen in Sicherheit bringen würde. Verängstigt und verunsichert leisten die Opfer der vermeintlichen Polizei folge. Doch die Polizeibehörden warnten, dass diese nie nach Wertgegenständen fragen, geschweige denn sie in Verwahrung nehmen würden. Genau so wenig würde im Telefondisplay die 110 stehen, wenn sie jemanden anriefen. Trotzdem ist diese Art des Telefonbetrugs aufgrund seiner raffinierten Vorgehensweise sehr erfolgreich. Nicht verwunderlich, dass Täter an dieser durchtriebenen Masche weiter festhalten werden [30].

3 Grundlagen des Enkeltrick-Betrugs

3.1 Definition des „Enkeltricks“

Der Begriff „Enkeltrick“ ist die Bezeichnung für eine besonders dreiste Betrugsmasche des Social Engineerings. Ihr Name kommt daher, dass die Betrüger sich am Telefon selbst als Enkeltochter oder Enkelsohn ihrer älteren Zielgruppe, der Senioren, ausgeben. Darin liegt auch der Unterschied zum vorher beschriebenen Schockanruf. Dabei agieren Täter typischerweise am Telefon oder neuerdings auch auf dem Messenger-Dienst WhatsApp.

3.2 Analog: Ablauf des Enkeltricks

Die Täter wählen gezielt ältere Menschen als ihre Opfer aus. Sie durchsuchen Telefonbücher oder alte Telefonauskunfts-CDs nach älteren Vornamen wie z.B.: Knut, Hildegard oder Wolfgang, und deren Adressen. So können die Täter schon vor Ort feststellen, ob das potenzielle Opfer in einer sozial starken oder eher sozial schwachen Gegend wohnt. Auch können Täter anhand „altmodischer“ Dekoration wie Gardinen oder der Bepflanzung am Balkon Rückschlüsse darauf ziehen, wo ältere Menschen leben könnten [31]. Haben sie ein potenzielles Opfer ausgemacht, sprechen sie dieses direkt per Du an und nennen bewusst ihren Namen nicht. Mit Worten wie: „Hallo Oma, rate mal, wer dran ist“ beginnen sie das Telefonat, um Hinweise über eventuelle echte Enkelkinder zu bekommen. Stellt das Opfer Rückfragen wie: „Bist du das Thomas?“, wissen die Täter, dass tatsächlich Enkel vorhanden sind. Sie brauchen nun nur noch mit „Ja“ antworten und schon können sie ihren betrügerischen Plan fortsetzen. Falls das Opfer misstrauisch werden sollte und fragt, warum die gewohnte Stimme ihres Enkels plötzlich anders klingt, antwortet der Täter, er sei erkältet. Hat das Opfer bis jetzt noch nicht bemerkt, dass etwas komisch ist, wendet der Täter nun seine Social Engineering Fähigkeiten an. Er täuscht mit teilweise weinerlicher und zitternder Stimme vor, dringend Geld zu benötigen, da er sich durch Schulden oder einen Unfall in einer Notlage befände. Er appelliert an die Hilfsbereitschaft und Solidarität des Opfers mit Sätzen wie: „Bitte hilf mir!“, „Aber bitte verrate es niemandem“ und teilweise wiederholenden Anrufen übt er zusätzlichen immensen psychischen Druck auf das Opfer aus. Teilweise wird ihnen mit dem Abbruch jeglicher sozialen Beziehungen gedroht, sollte das Opfer keine absolute Verschwiegenheit bewahren. Sind diese bereit, den Betrügern das Geld auszuhändigen, haben aber die erforderliche Summe, die meist mehrere Tausend Euro beträgt, nicht zu Hause, werden sie gebeten, sofort zur Bank zu gehen und das Bargeld abzuheben. Die Täter bestellen in diesen Fällen oft sogar ein Taxi an die Haustür des Opfers, damit es die Bank schneller erreicht. Auf dem Weg dorthin und auch während des Vorgangs der Bargeldabhebung werden sie von Mittätern aus der Ferne beobachtet, um sich abzusichern, dass sie das Opfer nicht hintergeht [32]. Die Geldübergabe erfolgt dann meistens an der Haustür des Opfers. Der vermeintliche Enkel kündigt einen Freund an, der das Geld abholt, da er selbst nicht kommen könne. Sie vereinbaren ein Kennwort für die Geldübergabe, damit sich das Opfer in vermeintlicher Sicherheit wiegt, die es nicht gibt. Der Abholer steht die ganze Zeit über in engem Kontakt mit dem Anrufer. Wie beim Schockanruf, bei dem sich Fremde als Polizisten oder Staatsanwälte ausgeben, halten sie ihre Opfer manchmal über mehrere Stunden am Telefon, um sie auf dem Weg zur Bank dauerhaft zu kontrollieren. In manchen Fällen sollen sie das Handy mit dem laufenden Anruf in

die Tasche stecken, damit die Täter mithören können, was gesprochen wird. Das Opfer könnte ja die Polizei rufen oder einen Bankangestellten um Hilfe bitten. Doch sie werden dermaßen unter Druck gesetzt, indem sie sogar Anweisungen bekommen, was sie am Bankschalter sagen sollen, bzw. dass sie nicht über den Grund der hohen Bargeldabhebung sprechen dürften. Das Opfer soll gezielt daran gehindert werden, an der Echtheit des Szenarios zu zweifeln und Vorkehrungen zu treffen, sich abzusichern oder Rücksprache mit Angehörigen zu nehmen [28].

So kreieren sie eine von vorn bis hinten wasserdichte Geschichte und halten den emotionalen Druck beim Opfer aufrecht. Das Anruferhandy wird nach erfolgreicher Übergabe sofort vernichtet, um so wenig Spuren wie möglich zu hinterlassen.

3.3 Digital: Ablauf des WhatsApp-Betrugs

Da laut Statistik immer mehr ältere Menschen auch Soziale Medien und Messenger wie WhatsApp nutzen [33] um mit ihrer Familie in Kontakt zu bleiben, haben sich die Betrugsmaschen auch auf diese verlagert. Diese neue Masche wird auch als „Messenger-Betrug“, „WhatsApp-Betrug“ oder „Enkeltrick 2.0“ bezeichnet. Wobei diese Bezeichnung des „Enkels“ hier nicht ganz zutrifft. Das Opfer erhält Nachrichten von ihm unbekannte Handynummern, in denen vorgegeben wird, Sohn oder Tochter zu sein und diese eine neue Nummer hätten, aufgrund eines kaputten Handys. Hier spiegelt sich der Unterschied zum Enkeltrick am Telefon wider. Nun werden nicht nur die Großeltern angesprochen, sondern auch „Mut-

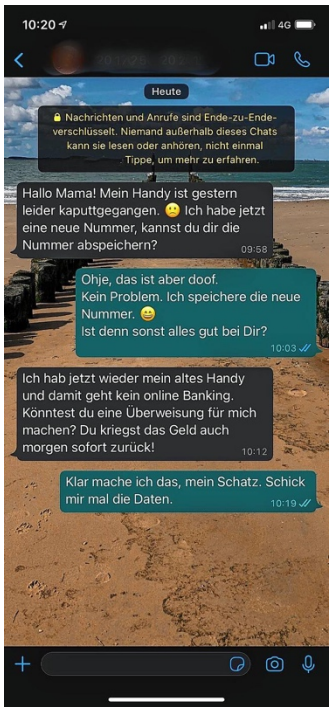


Abbildung 3: Beispiel einer WhatsApp-Nachricht des "Enkeltricks 2.0"

Quelle: Südkurier [34]

tis“ und „Vatis“. Das generelle Vorgehen ist allerdings gleich: nach der Ansprache „Hallo Mama“ oder „Hallo Papa“, folgt: „das ist meine neue Nummer, mein Handy ist kaputt. Bitte speichere die Nummer ein.“ Charakteristisches Merkmal solcher Nachrichten: die

Aufforderung die unbekannte Nummer sofort einzuspeichern, zu sehen auf Abbildung 3. Nicht selten beginnen die Chatverläufe mit kurzem Smalltalk, bei dem sich über das Wohlbefinden ausgetauscht wird. Manche Täter schreiben, es ginge ihnen nicht so gut, sie hätten Kopf- oder Bauchschmerzen, um durch Mitleid die Opfer gleich auf emotionaler Ebene auf die folgende Geldforderung vorzubereiten. Danach wird ebenfalls eine Notlage vorgetäuscht, für die dringend Geld benötigt würde. Oft wird auch als Vorwand genutzt, dass wichtige Rechnungen beglichen werden müssten, doch durch das neue Handy sei kein Zugang zum Online-Banking möglich. Das Opfer wird also gebeten diese Rechnung für das vermeintliches Kind über Überweisung zu bezahlen. Die unbekannte Nummer versichert, dass das Geld in den nächsten Tagen zurückgezahlt würde, was allerdings nicht geschieht. Hier spielt auch die Wahl der Zahlungsmethode eine Rolle. Die Täter wählen bewusst die Überweisung, da sie eine gewisse Anonymität für ihn sicherstellt. Zwar können Überweisungen nachverfolgt werden, aber diese lassen weniger Rückschlüsse auf Kontodaten der Täter zu als andere Zahlungsmethoden wie zum Beispiel PayPal (siehe Kapitel 5.1). Meist erfolgt die Überweisung auf ausländische Konten, was die Rückverfolgung erschwert. Außerdem ist es für die Opfer oft sehr schwer, bereits überwiesenes Geld zurückzufordern. Im Gegensatz dazu bieten Dienste wie PayPal bestimmte Schutzmaßnahmen, um autorisierte Zahlungen rückgängig zu machen. Zumal ist die Geldübernahme für die Betrüger viel einfacher, weil es keine weiteren Schritte verlangt, sich das Geld auszahlen zu lassen [34].

Die Verbraucherzentrale berichtet, dass seit 2022 die Masche etwas abgewandelt wurde. Nun werden Verbraucher über SMS von unbekannten Nummern gebeten, über WhatsApp zu antworten. Charakteristisch für diese Art von SMS sind die auffallenden Tippfehler in der Rechtschreibung und Zeichensetzung. Beispielsweise: „Hallo Mama, mein alte handy ist kaputt gegangen und liest meine simkarte nicht mehr. Dieser ist meine neue Nummer, diese kannst du dir abspeichern. Kannst du mir ein Nachricht schicken auf Whatsapp“ oder andere Abwandlungen wie: „Hallo, das hier ist jetzt meine neue Nummer. LG dein lieblingskind“ [35].

Empfänger solcher Nachrichten fragen sich, wie die Täter an ihre Handynummern kommen. Bisher vermutete die Polizei, dass Nummern nach Zufallsprinzip einfach ausprobiert werden. Die Täter wüssten, dass deutsche Handynummern eine gewisse Vorwahl und Länge haben. So werden verschiedene Kombinationen getestet und angeschrieben. Außerdem berichtet das Landeskriminalamt Rheinland-Pfalz, dass frei zugängliche Quellen im Internet, wie soziale Netzwerke, den Tätern ebenso in die Hände spielt [34]. Genauso wie Datenlecks bei Unternehmen, wie Telefonanbieter, bei denen sensible Kundendaten an die Öffentlichkeit gelangen, nutzen Betrüger als Informationsquelle. Beispielsweise wurden vor nicht allzu langer Zeit Daten wie E-Mail-Adressen und Handynummern von weltweit 530 Millionen Facebook-Nutzern, darunter sechs Millionen Deutsche, in einem Internet-Forum veröffentlicht. Das LKA Rheinland-Pfalz berichtet außerdem, dass Betrüger über SMS versuchten, die Mobilfunknummern zu überprüfen. Das heißt, sie senden SMS-Nachrichten mit einem Link und einer interessanten Botschaft, die das Opfer neugierig machen soll. Beim Klicken auf den Link wird es automatisch auf eine Webseite weitergeleitet, auf der das Opfer weitere persönliche Daten von sich eintragen soll. Das signalisiert den Betrügern, dass diese Nummer vergeben ist und aktiv verwendet wird. Diese Vorgehensweise wird „Smishing“ genannt, eine Wortbildung aus SMS und Phishing“.

Eine RTL-Extra-Reportage: „Jagd auf die SMS-Betrüger“ deckt neueste Erkenntnisse auf [36]. Das Reporter-Team begab sich nach monatelanger Recherche auf die Suche nach

den Tätern des SMS-Betrugs. Die Ermittlungsgruppe Oberhausen fand heraus, dass es ganze Nummernblöcke im Internet zu kaufen gibt, teilweise schon mit Informationen über das Geschlecht der Opfer und ob dieses über WhatsApp verfügt oder nicht. 1000 Nummern kosteten 150 Euro, doch die Kosten nehmen die Täter gern in Kauf, da sie damit eine hohe Ausbeute erzielten. Ein anonymer Mittäter berichtet davon, dass von 1000 Nummern durchschnittlich zehn bis zwanzig, manchmal auch bis zu 100 Leute antworten. Dies stellt ein sehr lukratives Geschäft für wenig Aufwand dar. Teilweise würden die Täter die Opfer nach getätigter Überweisung sogar weitere Geldüberweisungen verlangen. Der Kommissar gab an, dass die Masche deshalb so erfolgreich sei, da auf psychologischer Ebene beeinflusst würde. Nach dem Abspeichern der fremden Nummer unter dem Namen des vermeintlichen Kindes, höre das restliche Misstrauen auf. Da alle Nachrichten, die ab diesem Zeitpunkt folgen, nun von ihrem „Kind“ kommen. Damit sei die größte Hemmschwelle der Opfer endgültig genommen.

Eine junge Umfrage-Teilnehmerin berichtete, ihre Eltern, sowie ihr soziales Umfeld, hätten kürzlich immer wieder in sehr kurzen Zeitabständen SMS-Nachrichten erhalten, die um Beantwortung auf WhatsApp bitten. Diese Nachrichten entsprechen genau dem Schema des SMS-Betrugs. Die beiden Screenshots der Nachrichten auf Abbildung 4 stammen aus Juni bzw. November 2022.

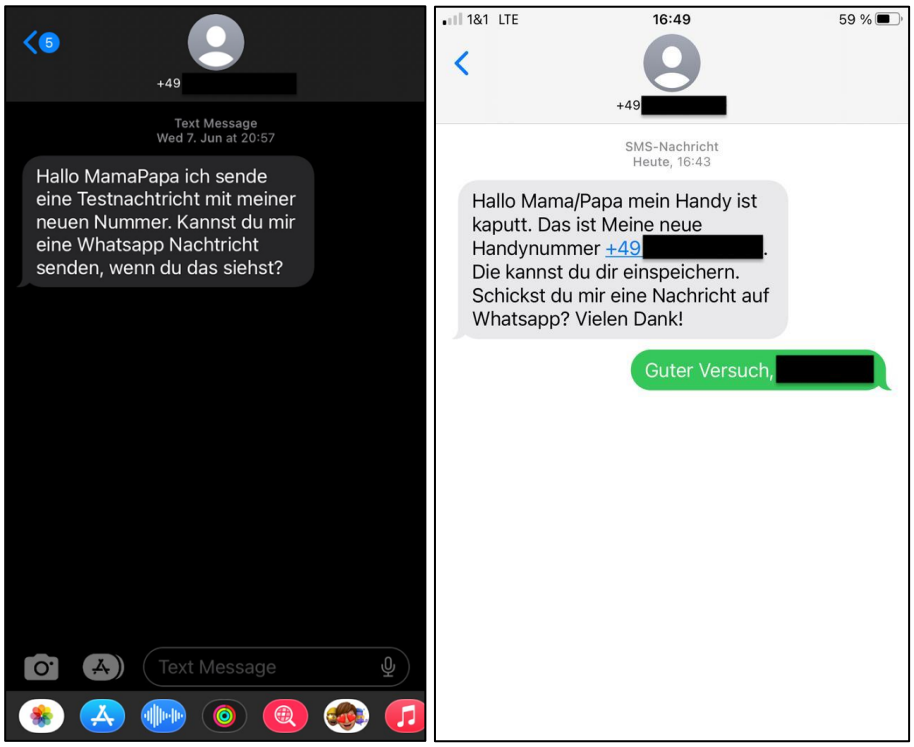


Abbildung 4: Beispiel SMS-Betrugsversuche

Quelle: Ergebnisse eigener quantitativer Umfrage

Auffällig bei diesen beiden Beispielen ist, dass die Empfänger bewusst mit „Hallo Mama/Papa“ angesprochen werden. Diese Form der Anrede würde dafürsprechen, dass die Täter nicht in jedem Fall über das Geschlecht des Opfers oder über die Verfügbarkeit von WhatsApp Bescheid wissen.

3.4 Persönlichkeit der Opfer

Eine Studie hat untersucht, ob bestimmte Persönlichkeitsfaktoren von Opfern mit Viktimisierung von Betrug in Zusammenhang gebracht werden können [37]. Die Autorin der Studie Monica T. Whitty bestätigt dabei am Beispiel des sogenannten Romance Scams (oder auch „Love Scam“), dass Opfer dieser Betrugsmasche u.a. meist kooperativer, gieriger, leichtgläubiger, leicht einschüchtbar, großzügiger und impulsiver waren als Nichtopfer. Außerdem konnte herausgefunden werden, dass der Anteil weiblicher Opfer höher war als der der männlichen. Beim Romance Scam gibt sich ein Täter mithilfe eines falschen Online-Profils als eine erfundene Person aus, getarnt durch gestohlene Bilder aus dem Internet und einer ausgedachten Biografie, die mit dem Opfer durch länger anhaltenden Kontakt eine Beziehung aufbaut, um es dann durch Vorgabe eines Notfalls um eine hohe Summe Geld zu bitten. Nach der Geldüberweisung verschwindet das Profil und die Opfer werden mit ihrem finanziellen und psychischen Schaden alleingelassen. Das Vorgehen ähnelt dem des Enkeltricks in der Form, dass der Täter, nachdem er eine starke Bindung zum Opfer aufgebaut hat, dessen erschlichenes Vertrauen ausnutzt und im Anschluss Geld fordert. Das Opfer, bereit dem liebgewonnenen Freund oder der Romanze zu helfen, führt die Überweisung aus guter Absicht heraus aus. Der Unterschied zum Enkeltrick ist hierbei, dass eine Beziehung zu einer fremden Person erst über längeren Zeitraum aufgebaut wird. Beim Enkeltrick sparen die Täter sich die Zeit und den Aufwand eine Bindung aufzubauen, denn hier nutzen sie eine vorhandene Beziehung zu Familienangehörigen aus. Aus diesem Grund könnten sich die Persönlichkeitsmerkmale auch auf den Enkeltrick anwenden lassen.

Laut dem Psychiater Professor Bielitz gäbe es viele Gründe, weshalb vor allem ältere Menschen eine beliebte Zielgruppe für Betrüger sind [38]. Ältere Menschen seien oft gesundheitlich geschwächt und könnten aufgrund nachlassender Kritikfähigkeit im Alter schwerer kritische Distanz aufbauen. Aber auch Menschen, die nicht selbstkritisch Situationen reflektieren könnten, seien besonders gefährdet Opfer von Betrügern zu werden.

Ältere Menschen sind oft großzügig und vertrauensvoll, was Betrüger dazu verleitet, sie auszunutzen. Sie glauben möglicherweise leichter den Lügen und Versprechungen der Betrüger und sind eher geneigt, persönliche Informationen oder Geld weiterzugeben, da sie meist nicht damit rechnen, dass jemand so skrupellos ist und man sie betrügen will. Alte Menschen sind oft allein und von sozialer Isolation betroffen, da zu ihrer Familie oder Bekannten teilweise nur spärlicher Kontakt herrscht. Das führt dazu, dass diese nicht von ihnen aufgeklärt oder beraten werden könnten. Betrüger nutzen diesen Umstand aus, indem sie sich dann als Enkel oder Sohn bzw. Tochter ausgeben. Das Opfer ist dann sogar froh, wenn sich das vermeintliche Kind überhaupt meldet. Dazu kommt, dass viele ältere Menschen weniger vertraut sind mit dem Internet, dem Smartphone oder anderen technologischen Entwicklungen. Sie haben meist weniger Kenntnisse über Handhabung von Computern oder Telefonen, was auch dazu führt, dass sie beispielsweise ihre Ersparnisse und Wertgegenstände lieber zu Hause aufbewahren als bei der Bank [39]. Mit dem Alter können sich auch kognitiven Fähigkeiten verschlechtern, was sie anfälliger für Täuschungen und Manipulation macht. So würde die fremde Stimme am Telefon, die sich als Enkelkind ausgibt, sie aufgrund von Schwerhörigkeit eventuell nicht unbedingt skeptisch machen. Die fehlende Interaktion mit Menschen, sowie altersbedingte Krankheiten wie Demenz oder Zerstreutheit sind weitere Faktoren, die Betrüger nutzen, um deren Hilfsbereitschaft und dem Bedürfnis nach emotionalem Austausch auszunutzen.

Das BMFSFJ nimmt an, dass Kriminelle sich außerdem eine größere Chance ausrechnen, da sie davon ausgingen, ältere Menschen würden eine Straftat eher nicht anzeigen [4]. Gründe dafür seien Scham und Angst, vor allem gegenüber der eigenen Familie, die sie verurteilen oder als „altersverwirrt“ betiteln könnte, weil sie auf den Betrug hereingefallen sind. Manchmal wird der Betrug auch gar nicht erkannt und bleibt somit auch für den Täter folgenlos. Doch selbst wenn der Betrug angezeigt wird, hofften die Täter, dass sie ungefährliche Zeugen seien, da sie sich eventuell nicht mehr an alles erinnern und den Täter nicht mehr genau beschreiben könnten.

3.5 Persönlichkeit der Täter

Es ist wichtig zu beachten, dass nicht alle Täter die gleichen Charaktereigenschaften aufweisen und individuelle Umstände und Hintergründe berücksichtigt werden müssen. Dennoch gibt es bestimmte Merkmale, die in der Regel mit Betrügern in Verbindung gebracht werden.

Das wissenschaftliche Paper „Betrügerisches Verhalten aus kriminalpsychologischer Sicht“ aus dem Jahr 2018 basiert auf einer umfangreichen Analyse von Daten aus verschiedenen Quellen wie Interviews, Gerichtsurteilen und Berichten von Strafverfolgungsbehörden [40]. Die Forscher untersuchten eine Vielzahl von demographischen Merkmalen, wie Alter, Geschlecht, Bildungsniveau und sozioökonomischer Status, sowie psychologische Eigenschaften von Betrügern. Die Ergebnisse zeigen, dass es keine eindeutigen Eigenschaften gibt, die immer alle Betrüger gemeinsam haben. Die Forscher entdeckten jedoch interessante Trends. Zum Beispiel fanden sie heraus, dass Männer häufiger als Frauen in betrügerische Aktivitäten verwickelt waren. Zudem seien jüngere Menschen tendenziell eher betrügerisch tätig, während ältere Menschen eher Betrügern zum Opfer fielen. Dies deutet darauf hin, dass das Risiko, betrügerisches Verhalten zu entwickeln, im Laufe des Lebens abnimmt. Ebenso wurde festgestellt, dass Betrüger meist einen höheren Bildungsstand aufwiesen als der Durchschnitt der Bevölkerung. Betrüger tendieren dazu, überdurchschnittliche hohe Fähigkeiten in der Manipulation von Emotionen anderer Menschen zu besitzen. Sie zeigten oft ein Muster von hohem Narzissmus und Selbstüberschätzung. Sie hätten ein übermäßiges Vertrauen in ihre eigenen Fähigkeiten und glaubten, dass sie schlauer und geschickter seien als andere. Dieses Selbstbewusstsein führt dazu, dass sie risikofreudiger sind, wenn es darum geht, verbotene Handlungen zu begehen. Eine weitere Eigenschaft ist, dass sie dazu neigen, weniger gewissenhaft und verantwortungsbewusst zu sein. Das heißt, sie sind eher bereit, Regeln und Normen zu brechen und moralische oder legale Grenzen zu überschreiten. Neben Egoismus und Narzissmus wird Personen, die zu kriminellen Handlungen neigen, fehlende Selbstkontrolle und Impulsivität zugeschrieben.

3.6 Wer sind die Täter

3.6.1 Telefonbetrug

Die Polizei und andere Strafverfolgungsbehörden arbeiten kontinuierlich daran, Trickbetrüger ausfindig zu machen, da es sich um organisierte Gruppen oder auch Einzelpersonen handeln kann. Häufig sind die Täter professionell organisierte Banden von hunderten, wenn nicht sogar tausenden Kriminellen, die in den osteuropäischen Ländern wie Polen, Tschechien, Rumänien, Bulgarien oder Ungarn sitzen und international agieren. Nicht selten handelt es sich dabei um streng hierarchisch strukturierte Roma-Banden, die aus, zu richtigen Callcentern umgebauten Wohnungen heraus, vorgehen. Die Hintermänner, also die Strippenzieher, rufen meistens die Opfer selbst an, da sie trotz direktem Kontakt, am Ende am wenigsten Risiko eingehen. Das Opfer könnte dann höchstens die Stimme oder den Akzent des Anrufers beschreiben, was aber keine verlässliche Aussage wäre. Die Hintermänner sprechen meist fließend Deutsch, trotz ihrer osteuropäischen Ansässigkeit. Die, die das größte Risiko eingehen wiedererkannt zu werden, sind die Lockvögel, auch „Läufer“ genannt. Sie sind diejenigen, die sich persönlich mit dem Opfer treffen und das Geld entgegennehmen. Die Banden wählen für diese Aufgabe oft Frauen, da sie mutmaßlich vertrauenswürdiger wirken. Sie sind die niedrig gestellten Mitglieder der Gruppierung und erhalten normalerweise eine Pauschale zwischen 500 und 1000 Euro dafür. Wenn sie in einer Region auffällig geworden sind, werden sie bandenintern schnell ausgewechselt, damit das Risiko einer Verhaftung eingedämmt wird [39] [41].

Die einzige Chance, die Ermittler haben, um die Täter ausfindig zu machen, sei laut Hauptkommissar Billy die Telekommunikationsüberwachung [28]. Das wäre aber nur machbar, wenn man den laufenden Anruf zurückverfolgen könnte oder etwas über die Geldübergaben erfährt. Da das Opfer in den meisten Fällen erst vom Betrug erfährt, wenn das Geld schon lange an die Täter übergeben wurde, ist diese Option meist unmöglich. Die Täter wechselten ständig die Telefonnummern, von denen aus sie ihre Opfer anrufen, die auf falsche Namen registriert seien. Deshalb ließen sich die Nummern schwer nachverfolgen.

Laut dem Spiegel begann alles 1999 in Hamburg. Dort versuchten die Lakatosz-Brüder diesen Trick erstmals übers Telefon, als ein älterer Mann seine Anrede nicht richtig verstand und ihn fragte, ob er sein Enkel sei [39]. Weil sich dieser Trick als zunehmend erfolgreicher herausstellte, gelten sie als die Erfinder des Enkeltricks. Nach einer Wohnungsdurchsuchung, so der Spiegel, setzten sich die Brüder nach Polen ab und agierten von dort aus, wo sie lange vor der Strafverfolgung sicher waren. Jahrelang bauten sie ihr Imperium auf und brachten deutsche Rentner um ihr lang erspartes Geld und lebten davon in Saus und Braus [42]. Mittlerweile wird die Anzahl der Enkeltrick-Mafia Mitglieder auf mehrere Tausend geschätzt, viele davon sprechen akzentfreies Deutsch, da Deutschland eines ihrer ertragsreichsten Zielgebiete sei. Die jährlichen Schäden werden auf zig Millionen Euro geschätzt. Einer der Brüder, Arkadiusz Lakatosz, genannt „Hoss“, gilt innerhalb der Gruppierung als Koryphäe, er sei „der Beste“. 2014 wurde Lakatosz in Warschau wegen gewerbsmäßigen Bandenbetrugs festgenommen, doch kam nach wenigen Monaten durch eine Kautionszahlung von 120.000 Euro wieder frei und tauchte danach wieder ab. In den folgenden Jahren wird er noch einige Male verhaftet, gelangt jedoch immer wieder auf freien Fuß. Gründe dafür seien plötzliche Einstellungen der Verfahren oder Kautionszahlungen [43].

3.6.2 WhatsApp-Betrug

Laut der vom RTL Extra Spezial Reporterteam begleiteten Ermittlungsgruppe Oberhausen, die sich speziell dem SMS-Betrug gewidmet hat, agierten die Täter ebenfalls in organisierten Gruppierungen. Bevor die Täter die Opfer anschreiben, müssten im Vorfeld die Konten organisiert werden, auf die das Opfer das Geld später überweisen soll. Der Kommissar der Ermittlungsgruppe Oberhausen sagt, Jugendliche hätten in der Regel nur Guthabenkonten, was für sie ein geringeres Risiko darstellte, ihre EC-Karte inklusive PIN-Nummer an die Hintermänner abzugeben. Junge Erwachsene hätten oft wenig Geld und nehmen Angebote, um schnell an viel Geld zu kommen, natürlich dankbar an. Sie bekämen bis zu 35% von der erbeuteten Summe, wenn sie ihre EC-Karte an sie abgeben. Deshalb werden vor allem Jugendliche für diese Betrugsmasche rekrutiert. Ein 22-jähriger Kontoinhaber, den das RTL-Team ausfindig machen konnte, berichtete, er habe dafür, dass er seine EC-Karte zur Verfügung gestellt hat, 500 Euro bekommen. Er habe sich gerade in finanzieller Not befunden und habe deshalb zugestimmt. Er behauptete nicht zu wissen, wofür die Hintermänner die Karten benutzten, doch dies ließe sich nicht bestätigen. Auf Nachfrage antworteten die Täter, dass sie eine Überweisung eines Freundes erwarteten, dieses Geld würde danach ausgezahlt und sie bekämen die Karten zurück.

Die Täter kommunizierten untereinander über die Plattform Snapchat, die es ihnen ermöglicht, Nachrichten zu verschicken, die nur für die einmalige Ansicht verfügbar sind, danach werden diese Bild- oder Videonachrichten wieder gelöscht. Die Registrierung erfordert kaum persönliche Daten, allein die E-Mail-Adresse und ein frei erfundener Benutzername reichen, um ein Konto zu erstellen. Diese Faktoren machen die Ermittlung für die Polizei schwer nachvollziehbar. Weil die Täter dies wüssten, zeigen sie sich in Videos komplett unmaskiert, posten stapelweise Bargeld und Luxus und zeigen die Namen der Opfer sogar als Trophäe im Internet. Die Kollektoren, also die, die die Karten einsammeln, leiten die Kartennummern dann an die Hintermänner, die in den Niederlanden vermutet werden, weiter. Die schreiben dann die gekauften Handynummern von bar gekauften PrePaid-Simkarten aus an. Es sei für deutsche Behörden schwieriger über Landesgrenzen hinaus zu ermitteln, deshalb agierten sie nicht im eigenen Land. Nachdem eine Geldsumme auf eines der Betrügerkonten eingegangen ist, wird genau dieser Betrag wenig später vom Konto ausgezahlt, damit das Geld bei Kontosperrung durch das Betrugsopfer nicht unerreichbar wird. Ein Karteneinsammler berichtete, dass mit einer Karte durchschnittlich ca. 10.000-12.000 Euro erbeutet werden. Dabei sind die Täter, trotz ihres jungen Alters, teilweise schon extrem gewaltbereit. Es handele sich nicht selten um bereits polizeibekannte Jugendliche, ein Großteil von ihnen mit Migrationshintergrund [36].

3.7 Gesetzlage

Strafrechtlich gesehen handelt es sich beim „Enkeltrick“ um eine besondere Form des Betrugs (§ 263 Strafgesetzbuch (StGB)). Nach § 263 Absatz 5 StGB wird er als gewerbsmäßiger Bandenbetrug eingestuft, was für den Täter eine Freiheitsstrafe von einem Jahr bis zu zehn Jahren bedeute. Liegt nur einer der Tatbestände vor, also entweder nur „bandenmäßiger“ oder nur „gewerbsmäßiger“ Betrug, drohen dem Täter „nur“ sechs Monate bis zu zehn Jahren Freiheitsstrafe (§ 263 Abs. 3 StGB). Doch beim Enkeltrick trifft in der Regel beides zu. Die Ermittlung der Betrüger ist sehr schwierig, da diese meistens aus dem

Ausland heraus agieren und irgendwo in Europa oder Westafrika leben. Ganz selten kommt es vor, dass Kontaktpersonen in Deutschland gegriffen werden [44].

4 Methodik

In diesem Kapitel soll auf die angewandten Methoden eingegangen werden. Zunächst erfolgt die Beschreibung der quantitativen Umfrage, die darauf abzielte, einen passenden Interviewpartner zu finden, um Erfahrungsberichte analysieren zu können. Darauf aufbauend folgt die Erläuterung der Vorgehensweise des Interviews mit einem Enkeltrick-Opfer.

4.1 Quantitative Umfrage

Um ein genaueres Bild davon zu bekommen, welche Auswirkungen ein Enkeltrick-Betrug auf die Opfer hat, schien ein Interview mit einem Opfer am besten geeignet. So lassen sich verlässliche Informationen aus erster Hand einholen, die die Hypothesen dieser Forschungsarbeit bestätigen oder widerlegen können. Doch aufgrund der Sensibilität des Themas ist es sehr schwierig, an jemanden zu gelangen, der sich für ein Interview zur Verfügung stellen würde. Aufgrund dieser Ausgangslage fiel die Entscheidung der Methodik auf eine quantitative Umfrage mit dem primären Ziel, Betrugsopfer für ein Interview ausfindig zu machen. Außerdem sollte damit gezeigt werden, wie präsent diese Betrugsmasche im (mittel-)sächsischen Umkreis ist, ob sich der Trend der Betrugsmasche in die jüngere Generation verlagert hat und ob mehr präventive Aufklärungsarbeit geleistet werden muss.

4.1.1 Erstellung der Umfrage

Zur Erstellung der Umfrage kam die kostenlose Online-Plattform „Survio.com“ zum Einsatz. Mit dieser Plattform war es möglich, anonyme Antworten der Teilnehmer zu generieren, die nicht auf sie zurückzuführen sind. Um einen gewissen Überblick über die sonst unbekannten Teilnehmer zu erhalten, wurden demographische Daten wie das Alter, das Geschlecht und das Bundesland, aus dem sie stammen, gewählt. Die Umfrage sollte sich größtenteils auf das Bundesland Sachsen beschränken. Außerdem war es wichtig zu betrachten, wie viele der in die Zielgruppe passenden Menschen an dieser Umfrage teilnehmen und welches Geschlecht sie haben. Da es sich hierbei um eine Betrugsmasche handelt, die es vor allem auf ältere Menschen absieht, muss nachvollziehbar sein, wie viele Daten im Nachhinein überhaupt verlässlich sind. Außerdem sollten die Fragen der Umfrage später trotzdem aussagekräftig sein, für den Fall, dass kein Interview zustande kommt. Zum einen sollte erfasst werden, wie viele Menschen entweder selbst vom klassischen Enkeltrick-Betrug am Telefon betroffen sind oder jemanden kennen, den es betrifft. Aufgrund der geringen Anzahl der tatsächlichen Opfer, die diese Umfrage eventuell erreichen wird, sollte damit sichergestellt werden, dass auch die Menschen im Umfeld dieser abgedeckt werden. Zum anderen sollte erfasst werden, wie viele Teilnehmer sich zwar nicht vom Betrug täuschen lassen, aber einen verdächtigen Anruf erhalten haben. Außerdem sollten auch diejenigen, die in Form von SMS- oder WhatsApp-Messenger Nachrichten mit dem Enkeltrick Kontakt hatten, dokumentiert werden. Nach jeder dieser Teilfragen folgte eine bedingte Frage, die die Bereitschaft der Befragten für ein Interview erfassen sollte. So sollte im Vornherein sichergestellt werden, dass sich am Ende der Umfrage nur diejenigen Teilnehmer melden, die auch wirklich bereit gewesen wären, nähere Auskunft über den Vorfall zu geben.

Um ein Bild davon zu bekommen, wie die aktuelle Aufklärungslage bezüglich dieser Betrugsmasche ist, wurden die Teilnehmer gebeten anhand ihres vorhandenen

Kenntnisstands einzuschätzen, wie sicher sie sich sind, dass sie einen versuchten Enkeltrick-Betrug, in jeglicher Form erkennen würden. Das Ergebnis dieser Fragen sollte Aufschluss über den Umfang der aktuellen Aufklärungsarbeit zu diesem Thema oder über den eventuell bestehenden Aufklärungsbedarf geben. Da es augenscheinlich noch keine ausreichende Aufklärung auf diesem Gebiet gibt, da die Täter andernfalls nicht in diesem Umfang erfolgreich wären, wurde als notwendig betrachtet, die potenziellen Opfer selbst zu fragen, wie sie informiert werden wollten, damit sie sich ausreichend schützen können. Zusätzlich sollte erfasst werden, ob es zum Zeitpunkt der Befragung Probanden gab, die präventive Schutzmaßnahmen für sich selbst oder ihr Umfeld ergriffen haben und welche das sind.

4.1.2 Umfrage-Verbreitung

Die Forschungsumfrage wurde über verschiedene Kanäle in Umlauf gebracht. Zuerst wurden Plattformen wie WhatsApp und Facebook genutzt, um auf die Umfrage aufmerksam zu machen. Wie bereits recherchiert, gibt es immer mehr Eltern und Großeltern, die Messenger Plattformen nutzen, daher die Auswahl dieser Netzwerke (siehe Kapitel 3.3). Gerade WhatsApp bietet sich dafür an, mit der Familie in Kontakt zu bleiben, wohingegen bei Facebook vermutlich mehr Menschen erreicht werden, die eher zum Bekanntenkreis gezählt werden. Zusätzlich wurde die Möglichkeit der Verbreitung über den internen Mailverteiler der Hochschule Mittweida unter den Studenten des gleichen Studiengangs „Allgemeine und Digitale Forensik“ genutzt. So sollten aktuell Studierende im Alter zwischen 19 und 22 erreicht werden. Ziel dieser Vorgehensweise war es, durch systematische Weiterverbreitung somit die Chance auf einen Interviewpartner zu erhöhen. Ausschlaggebend war hier die Annahme, dass Familienmitglieder, so auch die Enkel, die in die erreichte Zielgruppe fallen, von einem Betrugsversuch oder einem vollendeten Betrugsfall Kenntnis hätten. Um aber gleichzeitig an Eltern, die eventuelle WhatsApp- oder SMS-Nachrichten des Enkeltricks erhalten haben, zu gelangen, schien diese Methode als vorteilhaft.

4.1.3 Datenauswertung

Die Auswertung der Ergebnisse erfolgte mit dem Tabellenkalkulationsprogramm Excel. Die individuell aufgelisteten Antworten der Probanden mussten händisch in Tabellen eingetragen werden, um sie für weitere altersgruppenspezifische Untersuchungen nutzen zu können. Um betrachten zu können, wie aussagekräftig die Umfrageergebnisse sind, wurden genaue Zielgruppen für sowohl den Enkeltrick am Telefon also auch die WhatsApp-Nachrichten definiert, da sie sich offensichtlich unterscheiden.

Die Ergebnisse der quantitativ durchgeführten Umfrage werden im Zusammenhang mit den in der Einleitung aufgestellten Hypothesen in Kapitel 5 ausgewertet und anschließend diskutiert. Darauf folgt jeweils eine Kritik der durchgeführten Methodik, um die Fragen zukünftig zielorientierter beantworten zu können. Die Beantwortung der Thesen lässt auf einen inhaltlich kritisch betrachteten Ausblick zuschließen, der mit Handlungsempfehlungen für ältere Menschen und ihr Umfeld eingeleitet wird.

4.2 Betroffenen-Interview

Mit dem Interview eines Enkeltrick-Opfers sollte die Hauptfrage dieser Forschungsarbeit geklärt werden. Vorgesehen war es, anhand mehrerer Informationen Angaben zu den ethischen und moralischen Auswirkungen, die ein Betrugsfall auf das Opfer hat, zu machen. Deshalb sollte das Interview auch am meisten verwertbare Angaben hervorbringen, die man auf die Recherche beziehen kann, um gegebenenfalls aufgestellte Hypothesen zu stützen oder zu widerlegen. Anhand des Interviews sollte schließlich veranschaulicht werden, welches Kommunikationsmodell auf den Enkeltrick anwendbar ist und in welcher Form. Die Recherche brachte einen Kontakt zu einer Frau hervor, die angab, einmal auf eine fingierte WhatsApp-Nachricht ihrer tatsächlichen Tochter hereingefallen zu sein. Ihre Tochter unterzog sie 2022 einem Test, bei dem sie sie aufforderte, Geld über PayPal an eine bestimmte Adresse zu überweisen.

In der Informationsphase wurde die Befragte über den Ablauf und die Zielsetzung des Interviews sowie die vertrauliche Behandlung ihrer Daten informiert. Die Fragen, die im Interview gestellt wurden, sind überwiegend deduktiv. Hierbei liegt das Forschungssystem zugrunde, das von allgemein geltender Theorie auf einen Einzelfall schließt bzw. mit einem direkten Beispiel überprüft. Vereinzelt finden sich auch induktive Fragen wieder, mit denen Antworten auf die Forschungsfrage dieser Arbeit herausgearbeitet werden sollten [45]. Zuerst wurden Daten wie das aktuelle Alter, sowie das Alter zum Zeitpunkt des Vorfalls, als auch das heimische Bundesland in Erfahrung gebracht, um den Interviewpartner demographisch, sowie einer Zielgruppe zuordnen zu können. Zusätzlich sollte die Geschädigte kurze Angaben zu ihrer Persönlichkeit machen. Beispielsweise sollte eingeschätzt werden, ob sie sich eher als schüchterner, introvertierter, ängstlicher oder emotionaler Typ beschreiben würde. Anhand dieser Informationen sollte hervorgehen, ob die Betroffene in das Schema der Opferrolle fällt, die beschreibt, dass sich besonders zurückhaltende oder emotionale Menschen schneller manipulieren lassen. Darauf aufbauend auch die Frage nach dem Gefühlszustand zum Zeitpunkt des Erhalts der Nachricht und wenn nicht zeitgleich, auch zum Zeitpunkt der Geldüberweisung. Denn der Zeitraum zwischen diesen beiden Zeitpunkten hätte durchaus auch zu einer Änderung der Gefühlslage oder der Haltung gegenüber der Forderung führen können. Um sich ein grundlegendes Bild des Betrugsablaufs zu verschaffen, war es wichtig, einen detaillierten Ablauf des Tathergangs zu erhalten. Außerdem war es interessant zu erfahren, ob das Opfer generell Kenntnis über die Betrugsmasche hatte, sie sie nur in Form der Telefonanrufe kannte oder sie ihr komplett unbekannt war. Wichtig zu wissen war, wie der Schreibstil der Nachricht ausgesehen hat, um zu analysieren, wie der Täter vorgegangen ist und ob es stilistische Merkmale gab, die das Opfer zu einem Zeitpunkt an der Echtheit zweifeln lassen haben. Während der Durchführung des Interviews ergab sich eine weitere Frage bezüglich des geforderten Geldbetrages. Die Betroffene gab an, der Täter habe „nur“ 30 Euro gefordert, was nicht unbedingt den typischen Geldsummen entspricht, die andere Opfer beschreiben. Deshalb wurde die Betroffene gebeten einzuschätzen, ab welchem Betrag sie misstrauisch geworden wäre oder die Forderung sogar abgelehnt hätte. Je höher der geforderte Betrag, desto höher ist auch die Hemmschwelle, der Forderung wirklich nachzukommen.

Eine der Handlungsempfehlungen, die Polizei und Verbraucherschutzzentralen geben ist, dass man bevor man eine Geldüberweisung an einen unbekannten Empfänger tätigt sich erkundigen sollte, ob das (Enkel-)Kind wirklich eine neue Handynummer hat. Es gibt verschiedene Wege dies herauszufinden, beispielsweise indem man Freunde oder andere

Familienangehörige fragt, ob dies der Wahrheit entspricht oder man die Nummer einfach anruft. Doch meistens handeln die Opfer in der Absicht ihrem Kind schnell helfen zu wollen zu unbedacht und kommen dieser Empfehlung nicht nach. Deshalb war es interessant zu wissen, ob die Betroffene derartige Kontaktversuche unternommen hat. Die größte Bedeutung lag jedoch darauf zu ermitteln, wie der Gefühlszustand der Betroffenen zum Zeitpunkt war, als sie vom Betrug erfahren hat und welche emotionalen und psychischen Auswirkungen dieser Vorfall auf sie und ihr zukünftiges Verhalten hatte. Zusätzlich sollte sie angeben, wie sie die aktuelle Aufklärungslage über die Betrugsmasche „Enkeltrick“ beurteilte und welche Methoden zur Sensibilisierung der Zielgruppen sie als notwendig erachte. Zum Schluss wurde die Befragte gebeten einen Blick in die Zukunft zu wagen, wie sie die Entwicklung der Erfolgschancen derartiger Betrugsmaschen einschätzte.

Nach der Durchführung des Interviews folgte eine lautsprachliche Transkription und deren Analyse. Die Transkription orientierte sich an dem semantisch-inhaltlichen Transkriptionssystem nach Dresing & Pehl [46]. Die im Interview erhobenen Informationen wurden zusammengefasst und mit Zitaten der Befragten belegt, siehe Anlage, Teil 3. In der darauffolgenden Einordnung in ein Kommunikationsmodell wird die Manipulation der Kommunikation veranschaulicht.

5 Ergebnisse & Diskussion

Um genaue Aussagen über die für die Forschungsfrage relevanten Ergebnisse zu treffen, mussten genaue Zielgruppen definiert werden. Laut Statista sind Mütter in Deutschland bei der Geburt eines Kindes durchschnittlich 31,7 und die Väter 34,7 Jahre alt (Stand: 2022) [47]. Auf dieser Grundlage werden die Teilnehmer der Forschungsmethoden, die in die Zielgruppe des digitalen Enkeltricks in Form von SMS- oder WhatsApp-Nachrichten fallen, zwischen 31 und 51 Jahren definiert. Großeltern waren 2020/2021 laut einer Studie des Deutschen Zentrum für Altersfragen bei der Geburt ihres ersten Enkelkinds 52,8 (Großmütter) bzw. 55,7 (Großväter) Jahre alt [48]. Deshalb werden für die Zielgruppe des analogen Enkeltricks in Form des Betrugs-Anrufes Teilnehmer im Alter zwischen 52 und 80 definiert. Die Altersgrenze 80 resultiert aus dem Alter des ältesten Teilnehmers der Umfrage. In der Realität ist diese Grenze nach oben hin offen.

5.1 Interview-Analyse

In diesem Kapitel werden die Ergebnisse des Interviews mit einem SMS-Betrugsopfer ausgewertet und anhand des zugrundeliegenden Kommunikationsmodell erläutert und die Aussagen aus dem Transkript (Anlage, Teil 3) belegt.

Bei dem Betrugsopfer handelt es sich um eine 50-Jährige, zum Tatzeitpunkt 49-Jährige, Frau aus Sachsen-Anhalt. Ihre Tochter führte im Rahmen einer studentischen Arbeit einen Test an ihr durch, bei dem sie sich mit einer fremden Nummer als sie selbst ausgab und ihre Mutter um Geld bat. Diese überwies ihr das geforderte Geld und wurde später über die fingierte Situation aufgeklärt. Die Befragte sagt, sie sei in einer Arztpraxis tätig, bei der sie durchaus hin und wieder mit älteren Menschen zu tun habe. Das Alter zum Tatzeitpunkt lässt darauf schließen, dass sich der Vorfall 2022 ereignet haben muss. (Zeile 5, 10, 14, 18, 263-264) Aufgrund ihres Alters lässt sie sich der zuvor definierten Zielgruppe der typischen WhatsApp-Nachrichten-Empfänger zuordnen. Die Betroffene beschreibt sich charakterlich als: „[…] wahrscheinlich nicht […] ganz überschwänglich […]“, zwar zurückhaltend aber auch nicht schüchtern und durchaus auch sehr emotional. (Zeile 25-27) Aufgrund vorangegangener Recherche bestätigen diese Merkmale die Persönlichkeit von typischen Betrugsopfern, die aus Unerfahrenheit oder emotionaler Vertrauensseligkeit heraus eher dazu neigen, ohne ausreichende Beweise oder Unwissenheit Manipulation zum Opfer zu fallen. Gerade sehr emotionale Menschen treffen Entscheidungen meist aus dem Bauch heraus und sehr intuitiv, sodass oft keine Zeit bleibt, die Folgen der Entscheidung ausreichend zu überdenken.

Die Befragte beschreibt den Vorfall so: sie erhielt die Nachricht in einer sehr stressigen Situation, das sei ihr besonders in Erinnerung geblieben, weil sie kaum Zeit gehabt habe, über die Tat nachzudenken, da sie gedanklich schon bei ihrer nächsten Aufgabe gewesen sei. In dieser WhatsApp-Nachricht gab sich die Täterin, in dem Fall ihre richtige Tochter, als sie selbst aus, da sie aufgrund eines Vertragswechsels eine neue Nummer habe. Mit der Absicht ein Geschenk für eine Freundin besorgen zu wollen, bat sie ihre Mutter, 30 Euro an die angegebene PayPal-E-Mail-Adresse zu schicken, da sie selbst durch den Nummernwechsel keinen Zugang zu ihrem eigenen PayPal-Konto hätte. (Zeile 36-43, Abbildung 5)

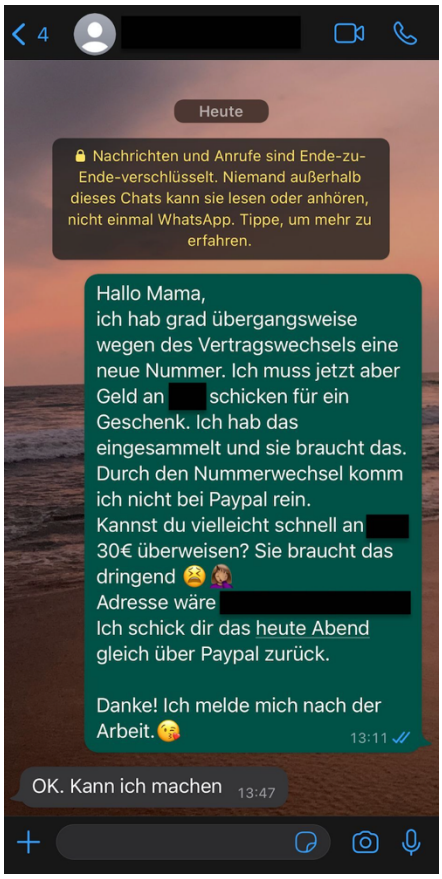


Abbildung 5: Screenshot der fingierten WhatsApp-Nachricht der Interviewpartnerin

Quelle: Interviewpartnerin

Die Funktion „Geld an Freunde senden“ des Zahlungsdienstes PayPal ermöglicht es den Nutzern, nur per Angabe der persönlichen E-Mail-Adresse einen Geldbetrag innerhalb kürzester Zeit an das PayPal-Konto des Empfängers zu senden. Die im Account verknüpften Kontodaten ermöglichen den Geldtransfer, sodass nach Erhalt des Geldes dieses auch sofort auf das richtige Bankkonto eingezahlt werden kann. Auf diese Weise besteht für den Sender kein Käuferschutz, da diese Funktion für Geldsendungen innerhalb der Familie oder Freunde vorgesehen ist. Aus diesem Grund benutzen Betrüger auf Verkaufsportalen wie beispielsweise Ebay-Kleinanzeigen gern diese Bezahlmethode, da sich die Opfer nicht über PayPal absichern können. Empfohlen wird deshalb, gerade bei hohen Geldsummen immer die Funktion „Artikel oder Dienstleistung bezahlen“ zu wählen, um im Falle eines Betruges, bei dem der Verkäufer z.B. der Warenversendung nicht nachkommt, durch den PayPal-Käuferschutz abgesichert zu sein und sein Geld zurückfordern zu können [49]. Auch Ebay-

Kleinanzeigen bietet nun eine „Sicher bezahlen“-Funktion an, um einen sicheren Handel zwischen Verkäufern und Käufern gewährleisten zu können [50].

Den Schreibstil der Nachricht beschreibt das Opfer als: „[…] für mich typisch meine Tochter, wie sie sich so ausdrückt, wie das alles so geschrieben war, deshalb bin ich auch Null stutzig geworden […]“. (Zeile 43-45) Anhand des Screenshots des Chatverlaufs kann man erkennen, dass die Tochter bewusst den ihrer Mutter bekannten Schreibstil verwendet hat. Auffällig ist, dass es kaum grammatikalische oder sprachliche Fehler gibt. Auch bei den tatsächlichen Betrugsnachrichten sind diese nicht immer anhand der Rechtschreibfehler als solche erkennbar. Zwar lassen sich schon bei zahlreichen Betrugsnachrichten anfängliche Fehlerquellen feststellen, doch auch die Betrüger entwickeln sich weiter. Sie agieren täglich zig-fach mit dem gleichen Wortlaut, sodass sie auf Standard-Antworten des Opfers wie: „Welcher meiner Söhne schreibt mir denn da?“ (siehe Abbildung 6, Beispiel Internetquelle [41]) fehlerfrei antworten können, ohne dass das Opfer anfangs schon Verdacht schöpft und sogar durch Emoticons oder spaßige Einwände („3 Mal raten Mama, wer hat immer am meisten Pech?“) die Situation glaubhafter erscheinen lassen. Doch im weiteren Verlauf des Gesprächs der Abbildung 6 lässt sich erahnen, dass Deutsch nicht die Muttersprache des Betrügers ist. Teilweise zeigen zusammenhangslose Einwürfe wie: „Seine ausstehenden Rechnungen.“, „kannst du das für mich tun überweisen?“ oder „ich höre nichts“, die keine verständliche Antwort auf die zuvor gestellt Frage darstellen, dass die Betrüger auch nur begrenzt vorbereitet sind.

Abbildung 6: Beispiel Enkeltrick über WhatsApp

Quelle: TZ [51]

Generell gehen die Betrüger immer nach dem gleichen Schema vor: die Anrede, das Handy sei kaputt, dies sei die neue Handynummer, ein Umstand, der erklärt, weshalb dringend Geld benötigt würde und ganz wichtig: die Aufforderung diese neue Nummer gleich abzuspeichern (siehe Kapitel 3.3). Dieses Merkmal ist in diesem Testszenario nicht vorhanden. Doch da die Betroffene aussagt, sie habe die Betrugsmasche mit der Bezeichnung des

Enkeltricks vorher nicht gekannt, weder am Telefon noch beim Messenger wie WhatsApp, hat das Fehlen dieses Merkmals keine Auswirkung auf den Verlauf des Szenarios gehabt. Außerdem ist in diesem Fall eher untypisch, dass dem Opfer bekannte Namen (hier geschwärzt) genannt werden, die am Szenario beteiligt seien. Zwar macht es die Forderung rundum glaubwürdiger, doch normalerweise ist es den Betrügern nicht möglich, von Namen aus dem Bekannten- oder Freundeskreis des Opfers Kenntnis zu haben, deshalb behalten sie sich auch der Nennung jeglicher Namen vor (siehe: „3 Mal raten Mama, wer hat immer am meisten Pech?“), da das das größte Risiko birgt, erwischt zu werden.

Die Befragte meinte, alle aufgezählten Faktoren, also der bekannte Schreibstil, der Name der Freundin, in deren Namen sie Geld für ein Geschenk benötigte, sowie die Angabe der E-Mail-Adresse, die den vollen Namen der Freundin beinhaltete, waren für sie so plausibel, dass sie noch weniger Verdacht geschöpft habe und gar nicht auf die Idee gekommen sei, dass hier etwas nicht stimmen könne. (Zeile 44-50)

Ebenfalls sollte die Höhe des geforderten Geldbetrags nicht außer Acht gelassen werden. Zwar gibt es keinen Betrag, der typisch für diese Art von Betrug ist, doch ist es aus Opferberichten bekannt, dass sich der Betrag zwischen mehreren hundert bzw. tausend Euro bewegt [52]. Es ist unwahrscheinlich, dass Betrüger über eine Überweisung Beträge im fünfstelligen Bereich fordern würden, die Opfer durch die klassische Vorgehensweise am Telefon schon eher bereit sind auszuhändigen. Es lässt vermuten, dass bei Forderung von sehr hohen Summen die Opfer eher zögern würden oder Rückfragen stellen, wofür das Geld gebraucht würde. Da das Opfer beim Lesen der Nachricht nicht in unmittelbarem Kontakt mit dem Betrüger steht, hat es auch die Gelegenheit gründlicher darüber nachzudenken, ob man eine Überweisung in dieser Höhe veranlasst oder nicht. Da die Betrüger, die ihre Opfer anrufen, direkten Druck auf sie ausüben können, haben diese Menschen diese Möglichkeit nicht. Deshalb lässt sich schließen, dass der Geldbetrag in einem Rahmen liegen muss, den viele Menschen als noch vertretbar ansehen würden. Jeder Mensch würde diese Grenze anders setzen, doch mit einer plausiblen und wasserdichten Hintergrundgeschichte lassen sich viele letztendlich auch auf höhere Summen ein. Die Befragte konnte jedoch keine Betragsgrenze nennen, die sie hätte zweifeln lassen. (Zeile 148-153) Dennoch wird der verhältnismäßig geringe Betrag von 30 Euro ebenfalls dazu beigetragen haben, dass sie guten Gewissens ihrer Tochter helfen wollte.

Da sie sich außerdem in einer sehr stressigen Situation befand und die Forderung dringend zu klingen schien, habe sie die Zahlung innerhalb von fünf Minuten nach Erhalt (Lesen) der Nachricht veranlasst. Dieser kurze Zeitraum ließ ihr keine Zeit für Zweifel oder darüber nachzudenken. (Zeile 178-181)

Nach der Überweisung erfolgte auch schon der Anruf der Tochter mit der Absicht, ihre Mutter über den Test aufzuklären. Die Befragte gab an, ihre Tochter habe sie erst einmal „[…] ganz eiskalt auflaufen lassen […]“, indem sie leugnete, das Geld überhaupt gefordert zu haben, nachdem sie wissen wollte, ob das Geld denn angekommen sei. Mit Sätzen wie: „Welches Geld?“ und „Was? Ich hab‘ dich nicht angeschrieben“ versetzte sie ihre Mutter in einen Schockzustand. Ihr sei in dem Moment „[…] Himmel, Angst und Bange […]“ geworden. Sie beschreibt diesen Moment als ein sehr komisches Gefühl, dass man doch relativ leicht darauf hereingefallen sei. Sie sei immer davon ausgegangen, dass das, was man in den Medien hörte oder ließ, so „[…] offensichtlich (*sei*), da kann man doch nicht drauf hereinfallen“. Sie hätte sogar sprichwörtlich ihre „[…] Hand ins Feuer gelegt, dass (*sie*) auf

sowas nicht reinfalle“. (Zeile 192-207) Diese Aussage zeigt, wie effektiv Manipulation mit den richtigen Methoden sein kann. Die allgemeine Annahme, einem selbst würde das nie passieren, da einem die Vorgehensweise bekannt ist, gilt auch nur so lange, bis man sich selbst in einer solchen Situation wiederfindet. Ob man dann immer noch der Meinung ist, man könne die Tricks durchschauen, bleibt fraglich.

Die Befragte ist der Meinung, wäre dies kein Test gewesen und sie hätte wirklich Geld an einen Betrüger geschickt, hätte sie sich wahrscheinlich ihrem Mann anvertraut. (Zeile 254-255) Doch nicht jedes Betrugsopfer hat die Möglichkeit, sich seinem Partner oder der Familie anzuvertrauen. Vor allem ältere Menschen leben oft verwitwet und sind nicht selten auf sich allein gestellt. Möglicherweise haben diese Menschen auch wenig Kontakt zu ihren Kindern oder Enkelkindern oder scheuen sich davor, es ihnen zu erzählen. Aus Angst, sie könnten von ihnen verurteilt werden, versuchen sie diesen Vorfall für sich allein zu verarbeiten. Die Interviewte könne sich das gut vorstellen, dass es für ältere Menschen schwierig sein muss, damit umzugehen und sich anderen Menschen zu öffnen. Besonders wenn sie hohe Summen ihres lebenslang angesparten Geldes, das für die Rente oder für Anschaffungen vorgesehen war, plötzlich verloren haben. (Zeile 263-273)

Die Altersarmut in Deutschland ist in den letzten Jahren gestiegen. Menschen ab 65 sind immer öfter von Armut im hohen Alter betroffen. Das wenige Geld, das sie monatlich zur Verfügung haben, reicht gerade einmal für die nötigsten Ausgaben aus. Da bleibt kein Geld für unerwartete Reparaturen oder zum Beispiel Geschenke für Familienangehörige oder Freunde. Laut der Malteser sind die Folgen, dass sich ältere Menschen immer mehr zurückziehen und vereinsamen. Die Einsamkeit verstärkt wiederum das Erkrankungsrisiko und verringert die Lebenserwartung [53]. Menschen, die ihr Leben lang ihr hart erarbeitetes Geld beiseite gelegt haben für ihre Zeit im Ruhestand wollten diese Risiken vermeiden. Wenn sie nun bereit gewesen wären, ihr Erspartes im guten Glauben ihren Enkeln aus einer Notlage zu retten, an Betrüger verlieren, ist nur zu erahnen, wie tief dieses Loch sein muss, in das die Opfer fallen müssen. So tief, dass sie sich meist nicht einmal ihren Familien anvertrauen können. Doch auch Hilfsorganisationen wie der „Weisser Ring e.V.“, ein Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten [54] sagen aus, dass sie wenige bis gar keine Erfahrungen mit Enkeltrick-Betrugsopfern gemacht hätten (siehe E-Mail-Korrespondenz Anlage, Teil 1). Dieser Umstand zeigt, dass sich Opfer selbst Experten, von denen sie nicht befürchten müssten, verurteilt zu werden, nicht anvertrauen wollen. Was das für psychologische Folgen haben kann, wenn man Probleme mit sich selbst ausmachen will, wird bei Beantwortung der These 2 in Kapitel 5.5 ausführlicher beschrieben.

Seit diesem Test, der für sie glücklicherweise glimpflich ausgegangen ist, habe die Befragte sich über die Betrugsmasche genauer informiert und den Vorfall mit ihrem Bekanntenkreis besprochen und ausgewertet. Dabei habe sie festgestellt, dass einige in ihrem Umfeld ebenfalls verdächtige Nachrichten erhalten hätten. (Zeile 228-233) Diese hohe Frequenz an Beteiligten zeigt, wie flächendeckend die Täter vorgehen und jede Möglichkeit nutzen, um eine hohe Erfolgschance zu generieren.

Die Befragte gab außerdem an, seitdem nicht besonders viel Aufklärung in diesem Bereich mitbekommen zu haben. Der Fakt, dass ihr die Betrugsmasche vor dem Test komplett unbekannt war, zeigt auch, dass es, obwohl die Vorgehensweise doch recht oft vorkommt, immer noch Menschen gibt, die die bisherigen Aufklärungskampagnen nicht erreicht. Sie

wünsche sich, dass neue Tricks, sobald sie bekannt würden, sofort in den Medien aufgegriffen werden sollten, um die Menschen zu sensibilisieren. Die Betrüger würden sich immer neue, raffiniertere und authentischere Verfahren überlegen, sodass die Menschen gerade über Kanäle, die vor allem die Zielgruppen erreichen wie Fernsehen oder Radio, vorgewarnt werden müssten. (Zeile 315-324, 329-330, 336-337)

5.2 Anwendung eines Kommunikationsmodells

Dieses Beispiel zeigt, dass sich der „Enkeltrick 2.0“ in Form des WhatsApp-Betrugs auf mehrere Kommunikationsmodelle anwenden lässt, da alle Modelle darauf abzielen, Informationsaustausch zwischen Sender und Empfänger schematisch darzustellen. Jedoch finden einige Elemente unterschiedlicher vorgestellter Kommunikationsmodelle (siehe Kapitel 2.5) bei diesem Trick in stärkerer Ausprägung Anwendung.

Die Vorgehensweise lässt sich am besten dem Vier-Seiten-Modell von Friedemann Schulz von Thun zuordnen. Anhand nur einer kurzen Textmessage werden hier die vier Ebenen einer Nachricht deutlich:

- **Sachinhalt:** mit den reinen Fakten und Informationen der Nachricht wird das Opfer um einen Gefallen gebeten. Der Sachinhalt, der Vorwand, der genutzt wird, um eine dringende Situation vorzutäuschen, ist der wichtigste Teil der Arbeit der Täter. Meist ist der Pretext so, dass das Kind eine neue Handynummer habe und aufgrund des Nummernwechsels keinen Zugang mehr zum Online-Banking habe und eine Rechnung dringend bezahlt werden müsse.
- **Beziehung:** die angebliche Beziehung zwischen Sender und Empfänger (hier: Elternteil und Kind) wird bewusst ausgenutzt, um beim Opfer Emotionen hervorzurufen, die es dazu bringen, der Forderung der Täter nachzukommen. Durch Vortäuschung einer dringenden Geldnotlage werden Mitleid und der Drang der Familie helfen zu müssen angeregt.
- **Selbstoffenbarung:** die Informationen, die der Sender über sich preisgibt, stehen in direktem Zusammenhang mit der Beziehung zum Empfänger. Er kann durch den Einsatz von Emoticons oder humorvollen Einwänden (siehe Abbildung 6) seine Gefühle und Meinungen gegenüber dem Empfänger vermitteln und somit vorgeben, vom „gleichen Stamm“ zu sein und die Bindung zum Opfer zu vergrößern oder zu erhalten.
- **Appell:** es wird meist direkt um Hilfe, die Überweisung einer dringenden Rechnung, gebeten. So wird das Opfer unter psychischen Druck gesetzt, da kein Elternteil nicht bereit wäre, ihrem Kind aus einer dringenden Notlage herauszuhelfen. Des Öfteren versichern die Täter, sie würden das Geld später zurückerhalten, um die Bereitschaft noch weiter zu erhöhen, da dies nicht nur im Kopf des Opfers hervorruft, dass sie ihrem Kind Zuneigung zeigen, indem geholfen wird, sondern auch, dass sie dadurch keinen finanziellen Schaden erleiden würden. Diese falsche Sicherheit, in der sich die Opfer zu wiegen scheinen, löst die Bereitschaft aus der Aufforderung Folge zu leisten.

Bei dieser Masche sind die Täter darauf angewiesen, ihre Forderung allein in Form von Schrift so glaubwürdig zu gestalten, dass es keiner aufwändigen Geräuschkulisse im Hintergrund (siehe Kapitel 2.6.4) oder stimmlicher Anpassung wie beispielsweise

vorgetäuschter Traurigkeit wie beim Enkeltrick-Betrug am Telefon bedarf. Hier muss der Täter über Smileys und schriftliche rhetorische Mittel eine emotionale Bindung aufbauen.

Der klassische analoge Enkeltrick am Telefon lässt sich ebenfalls problemlos auf oben genanntes Kommunikationsmodell anwenden, jedoch kommen hier weitere Techniken des Social Engineerings zum Einsatz, die sich durch das Modell nach Berlo (siehe Kapitel 2.5.1) gut beschreiben lassen. Hierbei kodiert die Quelle (der Täter) die Botschaft über einen bestimmten Kanal (das Hören am Telefon), die der Empfänger, also das Opfer wieder dekodiert. Die Täter wählen bewusst ein für die ältere Zielgruppe geeignetes Medium (das Telefon) aus. Nicht nur weil die meisten Senioren über ein Festnetztelefon verfügen, sondern auch weil die Wahrscheinlichkeit höher ist, dass sie auditiv angeschlagen sein könnten und somit die falsche Stimme am Telefon nicht wahrnehmen würden. Der Täter nutzt sowohl sprachliche als auch nonverbale Mittel, um die Nachricht so zu kodieren, dass der Empfänger sie auch mit der gewünschten Intention dekodieren kann. Der Sender möchte, dass beim Empfänger der Eindruck entsteht, er befinde sich in einer Notlage, für die er dringend Geld benötigt. Durch Ausdruck der Gefühle wie Weinen oder Hintergrundgeräusche kann das Szenario noch glaubhafter inszeniert werden. Der Empfänger weiß, dadurch dass er mit „Oma“ oder „Opa“ angesprochen wird, wie er die Nachricht zu dekodieren hat: nämlich als Hilferuf eines Verwandten. So wird vor allem die Beziehungsebene ausgenutzt, um zuerst Vertrauen zu schaffen und dieses dann zu brechen. Diese Einordnung zeigt anschaulich, wie sich Kommunikation auf verschiedenen Ebenen manipulieren lässt.

5.3 Quantitative Umfrage

Nachfolgend werden anhand der Ergebnisse der Online-Umfrage (siehe Anlage, Teil 2) die anfänglich aufgestellten Thesen dieser Forschungsarbeit durch kritische Betrachtung beantwortet. Zum Schluss werden einige Handlungsempfehlungen für gefährdete Zielgruppen des Enkeltrick- und des SMS-Betrugs vorgestellt.

Anhand einer Online-Umfrage wurde ermittelt, wie viele Menschen schon einmal Kontakt mit der Betrugsmasche „Enkeltrick“ hatten. Die Erhebung wurde anhand einer Stichprobe von 126 Teilnehmenden im sächsischen Umkreis, sowie der derzeitigen Forensik-Studenten der Hochschule Mittweida durchgeführt. Aufgrund der Anonymität der Umfrage konnten keine Rückschlüsse auf die Identität der Teilnehmer gezogen werden. Mithilfe einer Häufigkeitsverteilung wurde ermittelt, wie viele der Probanden schon entweder selbst Opfer des Enkeltricks in Form eines Anrufs oder einer Messenger-Nachricht geworden sind oder jemanden im Bekannten- oder Freundeskreis haben, dem es passiert ist. Zudem wurde die Bereitschaft abgefragt, als Betrugsopfer genauer über den Vorfall zu sprechen oder Chatverläufe zu veröffentlichen.

Die Umfrage stand für 3 Wochen zur Antwort-Erhebung zur Verfügung. Die Beantwortung der insgesamt 15 Fragen dauerte die Teilnehmer durchschnittlich 5 Minuten. Nach Ende des Umfragezeitraumes lagen 126 abgeschlossene Datensätze vor.

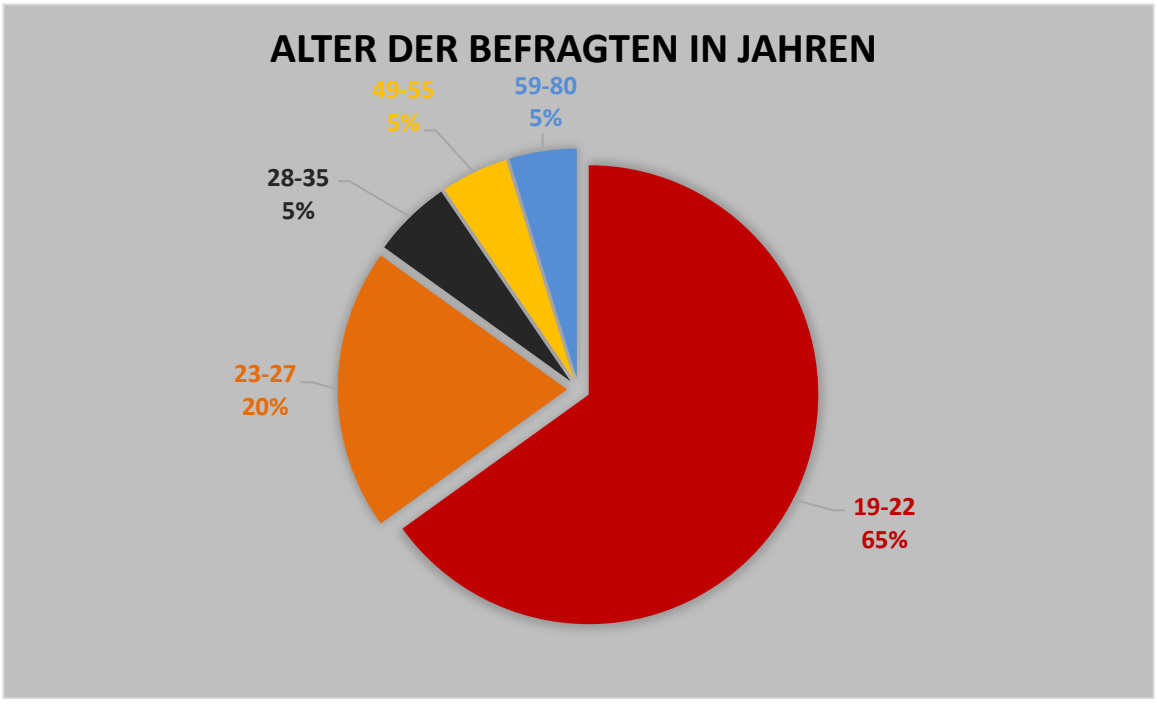


Abbildung 7: Alter der Umfrage-Teilnehmer in Jahren

Quelle: Eigene Darstellung

Abbildung 7 zeigt, dass die Mehrheit der Teilnehmer zwischen 19 und 22 Jahre alt waren, gefolgt von den 23-27-Jährigen. Nur 15% der Befragten fallen in die Zielgruppe des Enkeltrick-Betrugsschemas, die im Alter zwischen Anfang 30 und ca. 80 Jahren liegt.

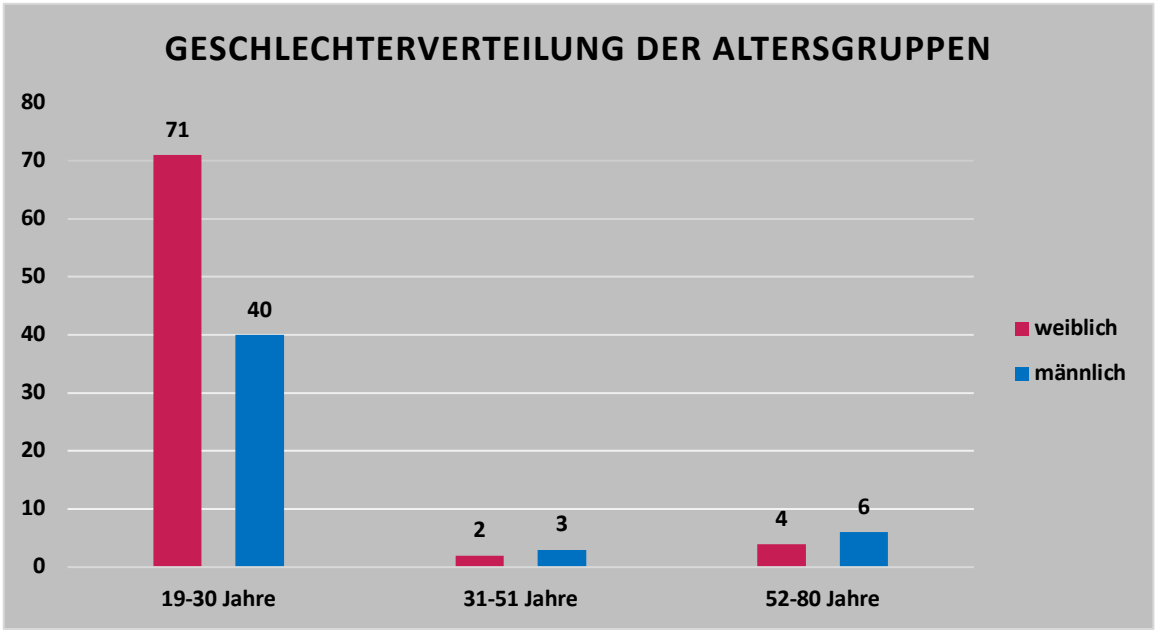


Abbildung 8: Geschlechterverteilung der Altersgruppen

Quelle: Eigene Darstellung

In Abbildung 8 ist zu sehen, dass circa 60% (77) der Befragten weibliche Teilnehmer waren, 40% (49) waren männlich. Die Aufteilung zeigt, dass nur insgesamt 15 Datensätze der Enkeltrick-Zielgruppe relevant sind. In dieser Alterspanne zeichnet sich ein höherer Männer-Anteil ab. Die Mehrheit der Teilnehmer kommt aus Sachsen. Nur 23 der insgesamt 126 Teilnehmer kamen aus anderen Bundesländern.

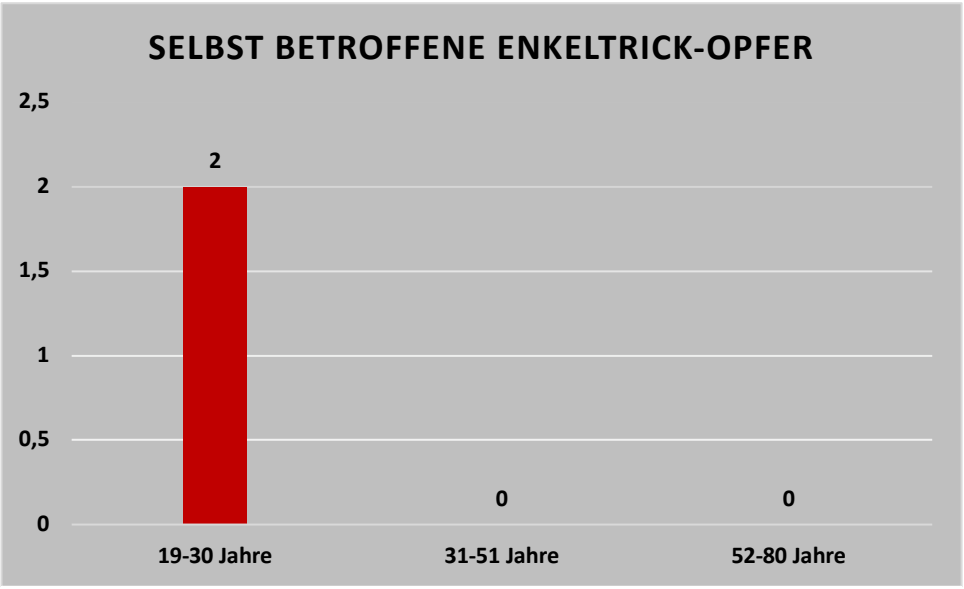


Abbildung 9: Anzahl der Enkeltrick-Betrugsopfer

Quelle: Eigene Darstellung

Entgegen der Erwartung mit dieser Umfrage ältere Betrugsopfer zu erreichen, stellte sich heraus, dass von 126 Teilnehmern lediglich zwei 20-jährige Frauen angaben, betroffen gewesen zu sein, zu sehen auf Abbildung 9. Diese beiden fallen nicht in die typische Zielgruppe des Enkeltricks. Beide wären auch nicht bereit gewesen, nähere Auskunft über den Vorfall zu geben. Diese beiden Frauen geben in einer folgenden Frage an, auch schon einmal selbst eine verdächtige WhatsApp-Nachricht erhalten zu haben. Aus diesem Grund ist davon auszugehen, dass die Frage 4 „Sind Sie oder jemand, den Sie kennen jemals Opfer des Enkeltricks geworden?“ von den Teilnehmerinnen als Oberbegriff verstanden worden ist. Außerdem verneinten ebenfalls beide die Frage 6, ob sie kürzlich einen verdächtigen Anruf erhalten hätten. Demzufolge lässt sich vermuten, dass die beiden nicht wirklich Betrugsopfer sind, die Geld an osteuropäische Betrüger verloren haben, sondern den Erhalt einer WhatsApp-Betrugsnachricht als „Opfer des Enkeltrick-Betrugs – Sein“ eingeordnet haben. Außerdem kann die Schädigung der beiden Frauen ausgeschlossen werden, da sie aufgrund ihres Alters keine Enkelkinder haben können. Demzufolge ist das Ergebnis dieser Frage als ungültig zu betrachten bzw. brachte diese Frage kein echtes Betrugsopfer hervor.

5.3.1 These 1

„Enkeltrick-Betrugsopfer haben Langzeitfolgen in Form von Depressionen, Angstzuständen und Vereinsamung.“

Aufgrund fehlender Ergebnisse zu diesem Thema lässt sich diese Hypothese weder bestätigen, noch widerlegen. Da es leider nicht gelungen ist, einen passenden Interviewpartner zu finden, um die psychologischen Auswirkungen auf Betrugsopfer zu untersuchen, lässt sich keine zufriedenstellende Aussage treffen.

Es lässt sich jedoch anhand einleitend genannter Erfahrungsberichte vermuten, dass Menschen, die aufgrund sozialer Isolierung oder gesundheitlicher Einschränkung von vornherein zur Zielgruppe der Betrüger gehören, nur noch stärker von diesen Faktoren betroffen sind. Durch den Vertrauensbruch, der das ausschlaggebende Instrument dieser Social Engineering Attacke ist, dürfte es den Opfern schwerfallen, (fremden) Menschen gegenüber überhaupt Vertrauen wieder aufzubauen. Die Süddeutsche berichtete 2020 von zwei älteren Frauen, die dem Enkeltrick zum Opfer gefallen waren. Eins der beiden Opfer, eine 86-Jährige, habe sich wochenlang nicht in ihrer eigenen Wohnung aufhalten können, nachdem eine 25-Jährige mit dem Vorwand Geld für den Schwiegersohn zu benötigen, weil dieser einen Unfall gehabt haben soll, sämtlichen Schmuck in ihrer Wohnung einsammelte. Sie habe unter Schlaflosigkeit gelitten und sich einer Therapie unterziehen müssen. Eine andere Frau gab an, seitdem in Angst zu leben und sich nach Einbruch der Dunkelheit nicht mehr aus dem Haus zu trauen und nur noch bei Kerzenlicht in der Wohnung zu sitzen. Außerdem zucke sie zusammen, wenn sie von Fremden angesprochen würde [55].

Auch das SMS-Betrugsopfer aus der RTL-Reportage gibt an, sie sei unmittelbar nach der Tat durch die Hölle gegangen. Sie habe unter Schlaflosigkeit und Konzentrationsproblemen gelitten, da sie das Geschehene gedanklich immer wieder durchgespielt habe. Auch habe sie einen nicht unerheblichen finanziellen Einbruch erlitten, da ihr die knapp 3000 Euro, die sie an die Betrüger verloren hat, in alltäglichen Situationen fehlten. Sie fühle sich hilflos, da ihr weder die Behörden noch die Bank helfen konnten. Sie habe alles allein durchstehen müssen [36].

Leider ließen sich solche Angaben nicht durch diese Forschungsarbeit bestätigen oder erweitern. Weiterhin lässt sich nur vermuten, dass Opfer psychische Folgen wie Depressionen, Angstzustände oder soziale Abkapselung entwickeln. Auch das Interview ergab diesbezüglich keine verlässlichen Angaben, da die Voraussetzung der Echtheit des Vorfalls für die Befragung nicht gegeben war. Da es sich in diesem Fall um ein Testszenario handelte, können nur Aussagen zum zukünftigen Verhalten der Testperson getroffen werden. Die Befragte sei jetzt vorsichtiger und würde solchen Nachrichten zukünftig keine Beachtung schenken. (Zeile 223)

Mithilfe der Umfrage konnten keine Ergebnisse zu dieser These gesammelt werden, da diese primär dazu diente, einen Probanden für ein Interview ausfindig zu machen. Die psychischen Folgen sollten noch einmal Gegenstand einer zukünftigen Forschungsarbeit sein. Dafür wird empfohlen ausgeprägte Kontaktierungsarten zu wählen, die genügend Probanden zur Verfügung stellen können. Aufgrund der Verbreitung der Umfrage innerhalb des Hochschulverteilers und des kleinen persönlichen Umfelds, liegen diesbezüglich wenig

bzw. zu den psychischen Folgen keine aussagekräftigen Daten vor. Diese Frage bleibt somit unbeantwortet.

5.3.2 These 2

„Betroffene scheuen sich davor, sich anderen Menschen anzuvertrauen."

Die der Umfrage vorangegangene Recherchearbeit bestätigt, dass sich Betrugsopfer gehemmt fühlen, sich selbst an Hilfsorganisationen zu wenden. Die Ansätze waren, bei Zeitungsverlagen, Nachrichtenportalen und einer Hilfsorganisation für Kriminalitätsopfer anzufragen, ob sie einen Kontakt zu einem Betrugsopfer vermitteln könnten. Bei der Sächsischen Zeitung, dem Mitteldeutschen Rundfunk (MDR) sowie bei der Freien Presse wurde angegeben, dass sie selbst aus datenschutzrechtlichen Gründen keine Daten der Opfer bekämen, sondern die Informationen für ihre Beiträge bei den zuständigen Polizeidienststellen bezogen (siehe Anlage, Teil 1).

Nach Kontaktaufnahme mit mehreren sächsischen Zweigstellen des Vereins „WEISSER RING – Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten e. V.", wurde die Anfrage auf weitere Bundesländer ausgeweitet. In Sachsen zeichnete sich ein eindeutiges Bild ab: keine der kontaktierten Zweigstellen habe bisher mit Enkeltrick-Opfern zu tun gehabt (Anlage, Teil 1). Dies zeigt, dass sich Betroffene sogar davor scheuen, sich an Experten zu wenden, die ihnen professionell bei der psychologischen Verarbeitung des Vorfalls helfen könnten. Eine andere Vermutung ist, dass es in Sachsen zahlenmäßig weniger Opfer vom Enkeltrick-Betrug gibt und es aufgrund dessen keine bekannten Fälle beim Weissen Ring e.V. vorliegen. Aufgrund fehlender Statistik ist diese Vermutung jedoch nicht nachweisbar. Auch in den anderen Bundesländern zeigte sich eine ähnliche Situation. Lediglich zwei Bundesländer gaben an, Enkeltrick-Opfer zu betreuen, allerdings sei man sich sehr sicher, dass diese sich nicht für ein Interview bereitstellen würden. Das Führen von Interviews mit Opfern sei eher schwierig, da nicht einzuschätzen sei, inwieweit die Betroffenen dadurch erneut mit der durchlebten Situation belastet würden. Dieser Umstand zeigt, dass die Folgen eines solchen Betrugsfalls verheerend sind.

Die Umfrageergebnisse haben ebenfalls ergeben, dass die Bereitschaft sich einer fremden Person über einen Betrugsfall anzuvertrauen, sehr gering ausgefallen ist.

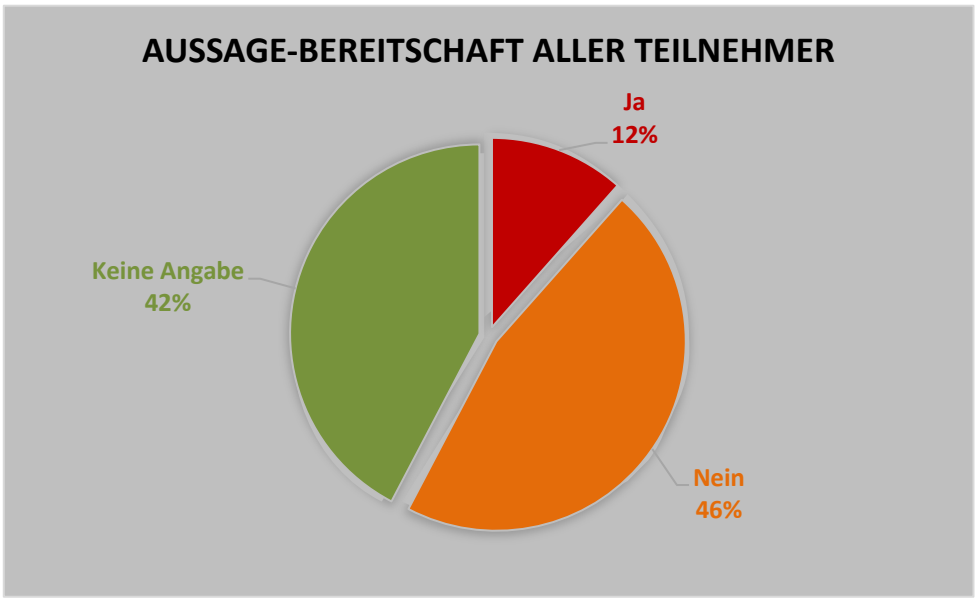


Abbildung 10: Aussage-Bereitschaft aller Umfrage-Teilnehmer
Quelle: Eigene Darstellung

Wie auf Abbildung 10 zu sehen, hätten nur 12% der Teilnehmer, die selbst Kontakt zum Enkeltrick hatten, einer fremden Person Informationen preisgegeben. Ein ebenfalls sehr großer Anteil enthielt sich der Aussage. Dieses Ergebnis ist jedoch aus vielerlei Hinsicht nicht aussagekräftig und wird nachfolgend kritisch betrachtet. Hierbei ließe sich die Auswahl „Keine Angabe“ eher dem „Nein“ als dem „Ja“ zuordnen, jedoch lässt dies keine genaue Beurteilung der Bereitschaft zu.

Es stellte sich heraus, dass bei den bedingten Fragen, ob der Teilnehmer selbst oder im Falle einer Bekanntschaft diese bereit wäre, zum Vorfall auszusagen, falsche Ergebnisse erzielt wurden. Es sind Datensätze vorhanden, bei denen Teilnehmer vorher angaben, nicht betroffen zu sein und dennoch bereit wären, Informationen preiszugeben. Dieser Widerspruch taucht bei 5 Teilnehmern auf, deshalb wurden für das Diagramm und zur Beantwortung dieser Frage nur richtige Datensätze verwendet.

Dennoch zeigen diese „falschen“ Ergebnisse, dass 5 Teilnehmer, falls sie in die Situation kämen, einem Enkeltrick-Betrug zum Opfer zu fallen, bereit für ein Interview wären. Vier dieser fünf Personen lassen sich sogar in die Zielgruppe des Enkeltricks einordnen. Nur eine jüngere Person wäre ebenfalls bereit. Jedoch lässt sich vermuten, dass aufgrund der schweren psychischen Belastung, die ein Betrug verursachen kann, dies als keine verbindliche Einschätzung zu werten ist.

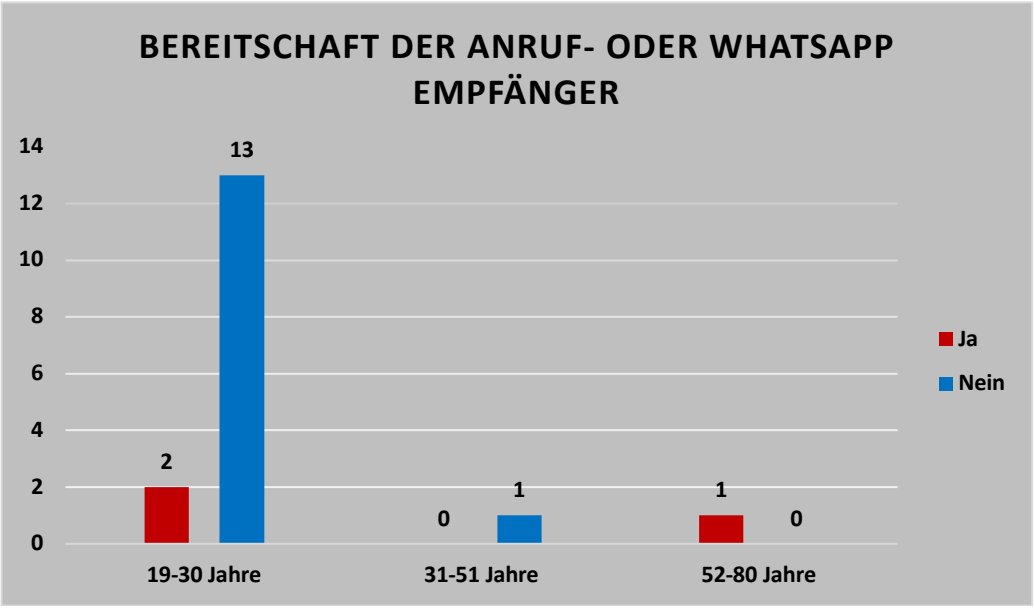


Abbildung 11: Bereitschaft der Teilnehmer, die einen verdächtigen Anruf oder eine WhatsApp-Nachricht erhalten haben

Quelle: Eigene Darstellung

Abbildung 11 zeigt, dass die 12% aus Abbildung 10 nur 3 Personen ausmachen. Beide 19-30-Jährigen haben sich stellvertretend für ihre Familienangehörigen gemeldet und von verdächtigen Text-Nachrichten berichtet, auf die aber nicht geantwortet wurde. Der 79-jährige Mann gab zwar an, sowohl einen verdächtigen Anruf als auch eine WhatsApp-Nachricht erhalten zu haben, jedoch erfolgte seinerseits keine Kontaktaufnahme. Dies würde dafürsprechen, dass es trotz Bereitschaft eine Hürde ist, selbst den Aufwand zu wagen, eine fremde Person zu kontaktieren.

Es gilt zu hinterfragen, aus welchen Gründen sich Betrugsopfer oft niemandem anvertrauen und warum sich die geringe Bereitschaft in der Umfrage widerspiegelt. Zum einen spielt Scham eine große Rolle, selbst innerhalb der Familie. Ältere Menschen haben Angst, ihre Angehörigen oder fremde Menschen könnten sie verurteilen oder verstoßen, da sie sich auf einen Betrüger eingelassen haben. Zudem ist die Hemmschwelle sich einer fremden Person anzuvertrauen vermutlich noch größer, da zu ihr erst einmal Vertrauen aufgebaut werden müsste, damit sich die Betroffenen sicher genug fühlen, sie in diese sensiblen Daten einzuweihen. Laut der RTL-Reportage erstatteten viele Betrugsopfer aus Scham nicht einmal Anzeige bei der Polizei [36]. Wahrscheinlich befürchteten die Opfer, die Polizei könne sowieso nichts für sie tun oder sie würden ebenfalls von ihnen verurteilt.

Dabei ist es wichtig, psychische Probleme nicht nur mit sich selbst ausmachen zu wollen. Eine Studie untersuchte, ob professionelle psychische Hilfe und Unterstützung von

Angehörigen das Leben von kranken Teilnehmern verlängern könne [56]. Die Untersuchung kam zu dem Ergebnis, dass Einzelkämpfer ein um elf Prozent höheres Risiko hätten, 20 Jahre früher zu sterben als diejenigen Teilnehmer, die sich professionelle Hilfe suchten. Die Forscher begründen dies mit der Selbstreflektion der Hilfesuchenden. Sie könnten ihre Situation realistisch analysieren und erkannten, dass sie auf die Expertise von Profis angewiesen seien. Dies führt dazu, dass oft verhindert werden kann, dass sich die Krankheiten verschlechtern. Dies zeigt, wie ausschlaggebend sich professionelle Hilfe und Unterstützung von Angehörigen auf die Psyche von Menschen auswirken kann. Aus diesem Grund ist es immer ratsam, diese Hilfe auch zu beanspruchen.

Kritisch zu beurteilen ist hier wieder die Durchführung der Umfrage selbst. Da es mithilfe des kostenlosen Programms leider nicht möglich war, bedingte Fragestellungen zu generieren, kam es zu einigen unzufriedenstellenden Ergebnissen. Vorgesehen war, dass die Teilnehmer zuerst angeben, ob sie selbst oder jemand, den sie kennen schon einmal Opfer des Enkeltricks geworden sind bzw. schon einmal einen verdächtigen Anruf oder eine WhatsApp-Nachricht erhalten haben. Falls dies der Fall ist, wurde in der nächsten Frage abgefragt, ob sie oder der/die Bekannte auch bereit wäre über den Vorfall zu sprechen, da dies die vorrangige Zielstellung dieser Umfrage war. Allerdings wurden nun diejenigen Teilnehmer, die weder selbst noch einen Bekannten hatten, der betroffen war, auch auf diese Frage weitergeleitet. Für diejenigen war die Antwortmöglichkeit „Keine Angabe“ vorgesehen. Doch wie es sich herausgestellt hat, haben Teilnehmer, die betroffen waren, ebenfalls keine Angabe gemacht. Dies führt dazu, dass nun der größte Ergebnisteil dieser Frage nicht zuordbar ist. Weiterführenden Forschungsarbeiten wird also dringend empfohlen, andere Umfrageprogramme zu nutzen, die über eine Funktion der bedingten Fragestellung verfügen, um diese Fehlerquellen auszuschließen. Rückblickend hätten die Fragen zusätzlich eindeutiger formuliert werden müssen, um dieser Entwicklung vorzubeugen. Ebenso kann auch das Interview mit der Betroffenen keine deutlichen Ergebnisse liefern, da aufgrund der zugrundeliegenden Testsituation, die Voraussetzungen nicht gegeben waren. Es kann vermutet werden, dass sie nur bereit war für ein Interview, da sie keinen wirklichen Schaden erlitten hat.

5.3.3 These 3

„Frauen sind häufiger Enkeltrick-Betrugsopfer als Männer.“

Ausschlaggebend für die Aufstellung dieser These war die Aussage, dass 99% der Enkeltrick-Opfer Frauen seien [31]. Dieser Behauptung sollte mit der Umfrage nachgegangen werden. Wie eingehend erwähnt, liegen anhand der Umfrage keine Ergebnisse für diese These vor. Allerdings lässt sich auf Abbildung 12 erkennen, dass Frauen egal welchen Alters, häufiger von Betrugsversuchen betroffen sind als Männer.

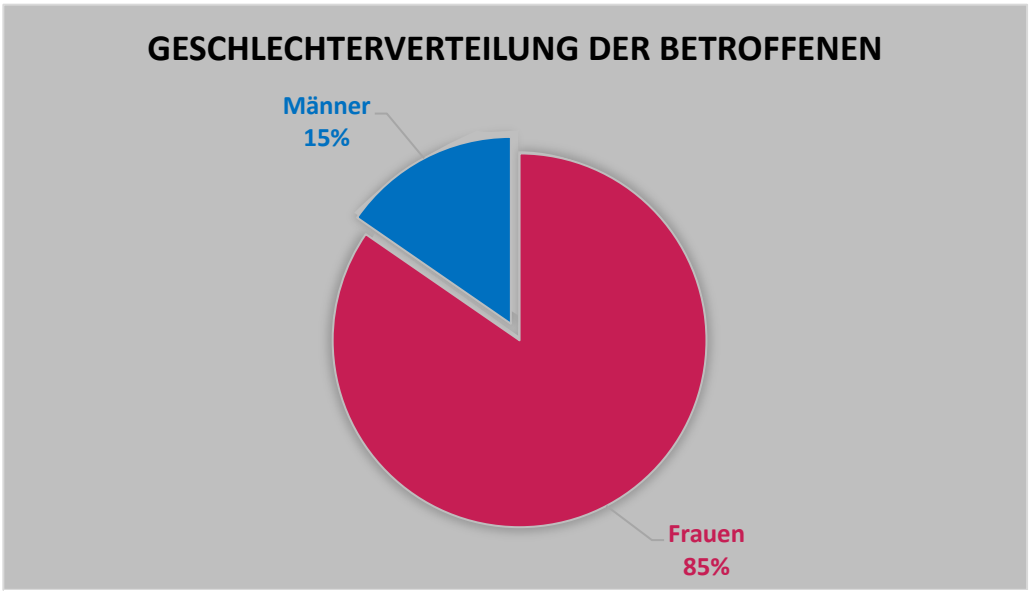


Abbildung 12: Geschlechterverteilung der Anruf- oder WhatsApp-Empfänger

Quelle: Eigene Darstellung

Unter den 25 insgesamt von verdächtigen Anrufen oder Nachrichten betroffenen Teilnehmern befinden sich 21 Frauen und 4 Männer. Speziell für die WhatsApp-Empfänger lässt sich ein deutliches Bild zeichnen:

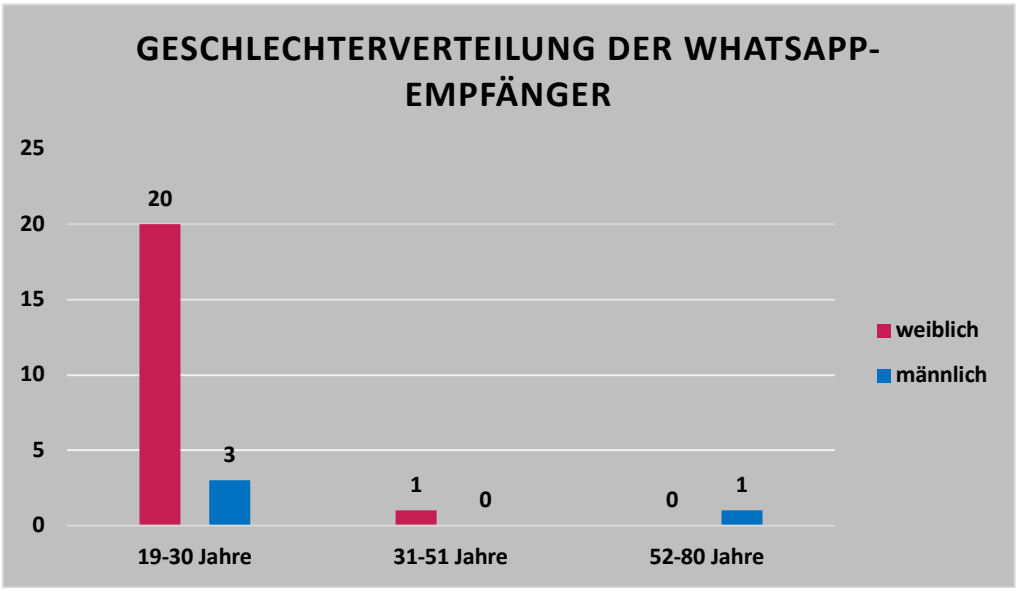


Abbildung 13: Geschlechterverteilung der WhatsApp-Empfänger

Quelle: Eigene Darstellung

Abbildung 13 macht deutlich, dass besonders junge Frauen, obwohl sie eigentlich nach anfänglicher Definition aufgrund ihres Alters nicht in die Zielgruppe einzuordnen sind, am meisten von den WhatsApp-Nachrichten betroffen sind. 20 von 71 jungen Frauen und nur 3 von 40 jungen Männern gaben an, eine betrügerische Nachricht erhalten zu haben. Also knapp 30% der Frauen und nur 7,5% der Männer sind davon betroffen.

Wie in der Studie von Monica T. Whitty aus 2018 beschrieben, bestätigen die Umfrageergebnisse die These, dass Frauen häufiger von betrügerischen Vorhaben betroffen sind als Männer [37]. Laut einem Bericht über Geschlechterforschung seien Persönlichkeitsmerkmale wie Rücksichtnahme, Empathie oder emotionaler Labilität und Verletzlichkeit bei Frauen deutlicher ausgeprägt als bei Männern [57].

Demzufolge werden die Täter gezielt mehr Frauen ins Visier ihrer Betrugsaktivitäten nehmen, da es wahrscheinlicher ist, dass eine Frau auf eine Masche hereinfällt als ein Mann. Es lässt sich schlussfolgern, dass Frauen eine größere Ausprägung der genannten Persönlichkeitsmerkmale zugeschrieben werden kann als Männern.

5.3.4 These 4

„Es erfolgt eine Trendentwicklung des Enkeltrick-Betrugs zur jüngeren Generation.“

Abbildung 13 zeigt nicht nur, dass Frauen vermehrt unter das Opferschema der Betrüger fallen, sondern auch generell die jüngere Generation. Offensichtlich liegen verhältnismäßig weniger Daten der beiden Zielgruppen ab 31 Jahren vor, jedoch ist es nicht zu ignorieren, dass immer mehr junge Menschen mit dem Messenger-Betrug in Kontakt kommen.

Anhand der vorliegenden Forschungsdaten ist zu erkennen, dass sich der Trend des klassischen Enkeltrick-Betrugs auf die jüngere Generation und die Messenger-Plattform WhatsApp zu verschieben scheint. Die Umfrage ergab, dass 25 Teilnehmer bereits eine Nachricht erhalten haben, wobei nur 2 Teilnehmer angaben, von Betrügern angerufen worden zu sein. Zwar befand sich unter den 25 Betroffenen nur eine Teilnehmerin, die in diese Zielgruppe einzuordnen ist, doch aufgrund der hohen Anzahl der 19-30-jährigen Umfrage-Teilnehmer, liegen zu wenig zielgruppenspezifische Daten vor. Doch auch das Interview stützt diese These, da die Befragte aufgrund ihres Alters ebenfalls zur typischen Zielgruppe der WhatsApp-Nachrichten-Empfänger zuzuordnen sind. 92 % der WhatsApp-Empfänger sind die 19-30-Jährigen.

Grund für diese Ergebnislage könnte sein, dass aufgrund gezielter Aufklärung mehr Menschen bezüglich dieser Betrugsmasche sensibilisiert sind und somit ihre Erfolgschance gesunken ist. Dies zwingt die Betrüger ihre Vorgehensweise anzupassen und es auf neue Opfer abzuzielen. Kritisch zu sehen ist, dass die jungen Personen unter 30 Jahren theoretisch gesehen ebenfalls nicht zur optimalen Zielgruppe gehören können, da sie aufgrund ihres jungen Alters mit hoher Wahrscheinlichkeit keine Kinder haben, die sie per SMS- oder WhatsApp-Nachricht um Geld bitten können.

Dadurch, dass laut jüngster Rechercheergebnisse Betrüger ganze Nummernblöcke online kaufen können und diese einfach beliebig anschreiben, können sicherlich auch viele Empfänger dabei sein, die nicht in die Zielgruppen passen. Diese Betrugsmasche zielt vor allem auf die Masse ab. Die RTL-Reportage ergab, dass vor allem Jugendliche hinter der neuen SMS-Betrugsmasche stecken und sich an der Vorgehensweise des klassischen Enkeltricks orientiert haben [36]. Der Zustand der Trendverschiebung kann außerdem auf die technologische Entwicklung zurückzuführen sein. Immer mehr ältere Menschen passen sich der Digitalisierung an und nutzen Smartphones oder Computer. Deshalb nutzen auch immer

mehr Eltern und Großeltern den WhatsApp-Messenger, um mit ihrer Familie und Freunden in Kontakt zu bleiben. WhatsApp ist als Plattform für diese Betrugsmasche aus mehreren Gründen für die Betrüger vorteilhaft: es bietet zum einen eine große Nutzerbasis, da WhatsApp weltweit mehr als 2 Milliarden aktive Nutzer hat und somit eine der beliebtesten Messenger darstellt [58]. Außerdem ermöglicht die App den Betrügern anonym zu bleiben und ihre echte Identität zu verbergen, da man bei der Anmeldung keinen Identitätsnachweis erbringen muss. Betrüger können sich mit Telefonnummern von PrePaid-Sim-Karten anmelden, die bei Barzahlung auf keine Person zurückzuführen ist, was die strafrechtliche Verfolgung der Täter erheblich erschwert.

Möglicherweise kann eine rückläufige Erfolgschance des Enkeltricks am Telefon der Grund dafür sein, dass die Betrüger auf Plattformen wie WhatsApp und eine jüngere Zielgruppe umsteigen. Möglicherweise sind ältere Menschen aufgrund zahlreicher Aufklärungskampagnen in den Medien sensibilisierter und besser informiert als noch vor einigen Jahren, sodass sie seltener auf den klassischen Trick hereinfallen. Sie könnten gelernt haben, bei unbekannten oder verdächtigen Anrufen aufzulegen oder diese gar nicht erst anzunehmen. Eventuell haben die Täter gemerkt, dass die Bekanntheit der Vorgehensweise in den letzten Jahren deutlich gestiegen ist und die ursprüngliche Zielgruppe nicht mehr so leicht zu manipulieren ist. Dadurch, dass diese Betrugsmasche in der Form schon seit Ende der 1990er Jahre existiert, könnte die SMS-Masche großes Potenzial haben erfolgreich zu sein, weil sie einfach „neu“ ist. Diese Gründe können dazu geführt haben, dass die Zielgruppe sich auf die Altersgruppe der „Eltern“ verschoben hat. Jedoch sind diese Schlussfolgerungen kritisch und nur als Tendenz zu betrachten, da aufgrund fehlender Rücksprache mit richtigen Enkeltrickopfern keine bestätigten Daten vorliegen.

5.3.5 These 5

„Es muss mehr Aufklärungsarbeit geleistet werden.“

Interessant zu sehen ist, dass 95 % der 126 Probanden sich sicher bzw. sehr sicher sind, dass sie einen versuchten Enkeltrick erkennen würden, wie Abbildung 14 zeigt. Nur zwei Teilnehmer schätzen sich als unsicher ein. Es stellte sich heraus, dass diese beiden, ein 51-Jähriger und ein 80-jähriger Mann, sogar in die Enkeltrick-Zielgruppe fallen und potenzielle Opfer darstellen.

Ein Proband, der sich nicht der Zielgruppe dieser Umfrage zuordnen ließ, gab später in den Anmerkungen an, dass er aufgrund der schnellen technischen Entwicklung, insbesondere im Hinblick auf die Künstliche Intelligenz (KI) und der einhergehenden Möglichkeiten der Manipulation, diese Frage mit „neutral“ beantwortet hat. Dadurch sei es zukünftig noch schwieriger für potenzielle Opfer zu erkennen, was der Wahrheit entspricht oder doch Betrug sein könnte. Deshalb würde er nicht behaupten, dass er einen Betrugsversuch zu jeder Zeit erkennen würde.

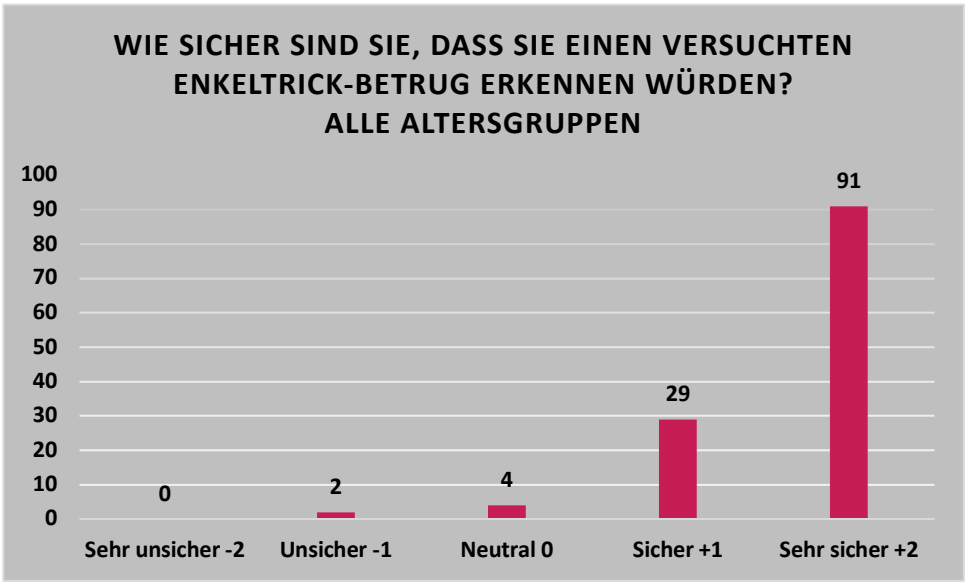


Abbildung 14: Selbsteinschätzung der Teilnehmer

Quelle: Eigene Darstellung

Noch drei weitere 19-21-Jährige schätzen ihre Bewertung eher neutral ein. Erstaunlicherweise sind sich alle 15 Zielgruppen-Teilnehmer („Eltern“ bzw. „Großeltern“) sicher bis sogar sehr sicher, dass sie nicht auf einen Enkeltrick hereinfallen würden.

Frage 11 sollte Aufschluss darüber geben, ob Betroffene oder Nicht-Betroffene Teilnehmer in letzter Zeit Schutzmaßnahmen gegenüber sich selbst oder ihren Bekannten bzw. Verwandten ergriffen haben. Abbildung 15 zeigt, dass fünf der zu den Zielgruppen zugehörigen Teilnehmer kürzlich Schutzmaßnahmen gegen den Enkeltrick ergriffen haben. Diese geben an, mit ihren Angehörigen präventive Vorsichtsmaßnahmen besprochen oder Meldungen über den Enkeltrick im Fernsehen oder in der Presse gesehen zu haben, in denen Aufklärungsarbeit geleistet wurde.

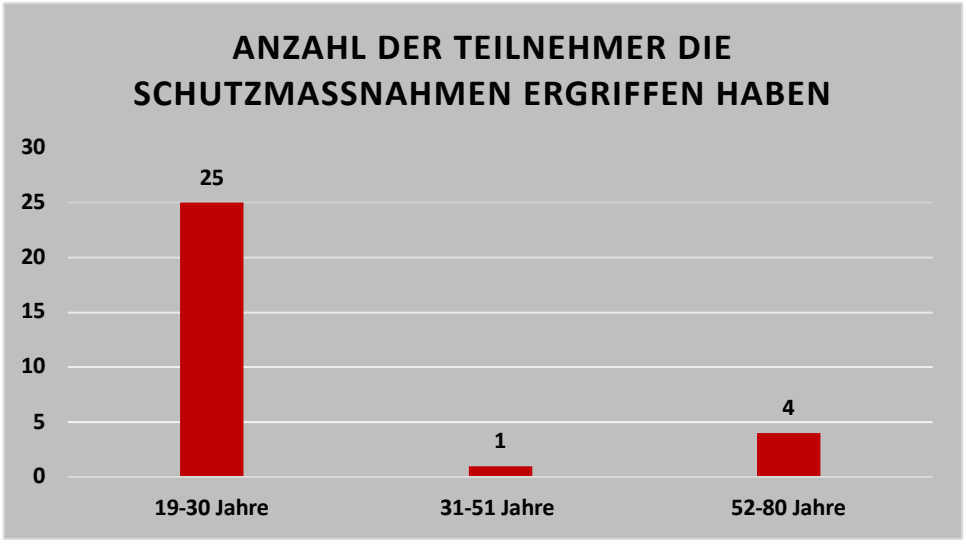


Abbildung 15: Teilnehmer, die Schutzmaßnahmen ergriffen haben

Quelle: Eigene Darstellung

Die meisten 19-30-Jährigen gaben an, ihre Eltern und Großeltern über die Betrugsmasche informiert und Vorgehensweisen besprochen zu haben, um sie vor dem Enkeltrick zu schützen. Einige hätten mit ihren Großeltern Absprachen getätigt, wie sie sich verhalten sollen, falls sie aufgefordert würden Geld zu überweisen oder an Fremde auszuhändigen. Beispielsweise wurde vereinbart, dass sie ein bestimmtes Codewort nennen oder Fragen zum Geburtstag oder -ort stellen sollen, um sicherzustellen, dass es sich auch wirklich um den richtigen Angehörigen handelt. Andere erklärten ihren Großeltern, es sei wichtig, bei der Kontaktaufnahme durch eine fremde Nummer, über andere Familienmitglieder zu erfahren, ob das Kind oder das Enkelkind wirklich eine neue Handynummer besitze. Auch sei abgesprochen worden, dass sich die Anrufer gleich zu Beginn mit ihrem Namen melden, damit der Angerufene gar nicht erst erraten muss, wer am Telefon ist und so schon anfänglich sichergestellt ist, dass es sich nicht um Betrüger handeln kann.

Außerdem wurde genannt, dass jemand einen Eintrag aus dem Online-Telefonbuch entfernen lassen hat, sowie, dass ein Vorfall sogar bei der Polizei gemeldet worden ist. Rund ein Viertel der Teilnehmer haben kürzlich etwas getan, um sich oder ihre Angehörigen gegen den Enkeltrick zu schützen. Aufgrund der vielen Handlungsmöglichkeiten, die genannt wurden, lässt sich eine gewisse Grundkenntnis der Teilnehmer feststellen. Ihnen ist nicht nur die Betrugsmasche an sich bekannt, sondern auch Schutzmaßnahmen.

Abschließend wurden die Probanden gebeten einzuschätzen, ob ihrer Meinung nach genügend Aufklärungsarbeit geleistet wird. Wie auf Abbildung 16 zu sehen, schätzt die Mehrheit der Befragten (75) die bisherige Aufklärungsarbeit zum Enkeltrick als zu gering ein. Nur insgesamt 23 sind der Meinung, es würde genug darüber informiert. 28 Teilnehmer geben an, sich bisher noch nicht intensiv genug mit dem Thema auseinandergesetzt zu haben, um die Lage einschätzen zu können. Innerhalb der Enkeltrick Zielgruppen ist das Verhältnis diesbezüglich ausgeglichen, sechs sind der Meinung es wird genügend informiert, sieben finden, es sollte deutlich mehr Aufklärungsarbeit geleistet werden.

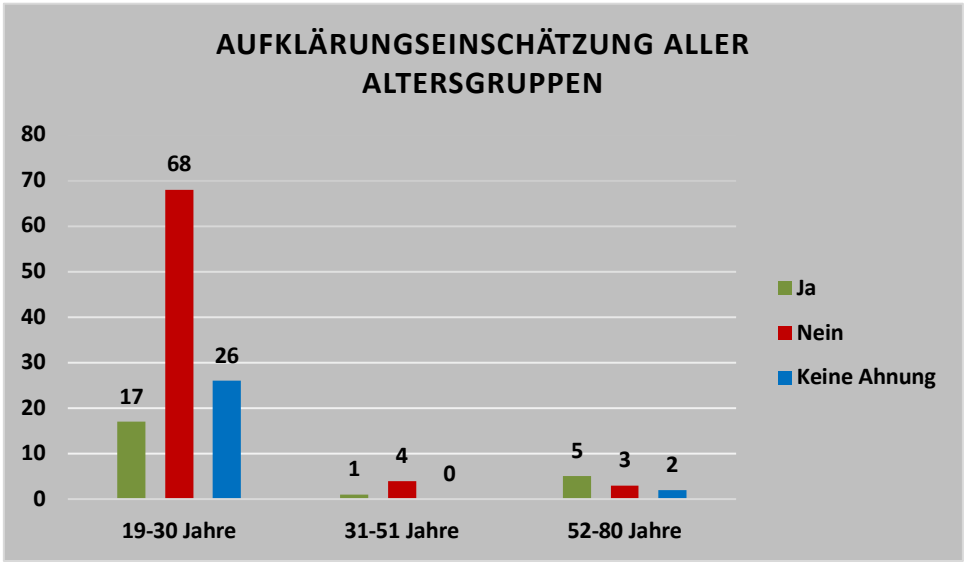


Abbildung 16: Einschätzung der Teilnehmer über Aufklärungslage

Quelle: Eigene Darstellung

Möglicherweise können gerade junge Menschen nicht beurteilen, ob und in welcher Menge aufklärende TV- oder Radiospots existieren, da Jugendliche viel weniger klassisches Fernsehen schauen als früher. In Zeiten von Streaming und Video-On-Demand, die es ermöglichen, Serien und Filme jederzeit abrufen zu können, ist man nicht mehr gezwungen, das zu sehen, was das TV-Programm vorgibt. Demzufolge schauen weniger junge Menschen Nachrichten und vor allem gibt es keine Werbepausen, in denen Platz für Warnhinweise wäre [59].

Um die Situation seriös einschätzen zu können, muss geklärt werden, wie viele Aufklärungsangebote es derzeit gibt und wie viele davon auch genutzt werden. Es lässt sich feststellen, dass es auf Abruf im Internet sehr viele Verhaltensvorgaben gibt, die auf den Schutz gefährdeter Menschen abzielen. Doch die erhält man in der Regel erst, wenn man sich bewusst mit der Thematik auseinandersetzt und speziell danach sucht. Die meisten älteren Menschen kommen aber erst damit in Kontakt, wenn sie sich mit dem Thema befassen wollen oder es aufgrund eines bereits geschehenen Betrugsversuchs müssen. Es gibt einige Organisationen, wie zum Beispiel Verbraucherschutzverbände, Polizei oder Seniorenorganisationen, die Aufklärungskampagnen über den Enkeltrick und andere Betrugsmaschen durchführen und dafür verschiedene Medien wie Flyer, Plakate, Fernsehspots, Radiobeiträge oder Informationsveranstaltungen nutzen. Beispielsweise will die saarländische Landesregierung mithilfe der neuen Kampagne „Enkeltrick und Co – nicht mit uns!“ für Sensibilisierung und Aufklärung sorgen [2]. Außerdem gibt es zahlreiche Internetseiten und Broschüren, speziell für die ältere Zielgruppe. Dort finden sich Informationen zu den gängigsten Betrugsmaschen, sowie Tipps wie man sich schützen kann und auch Fallbeispiele von Betroffenen. Zudem gibt es spezielle Beratungs- und Aufklärungshotlines, an die sich ältere Menschen oder Angehörige wenden können, um sich zu informieren oder verdächtige Anrufe zu melden. Aber auch in den Printmedien wie Zeitungen wird regelmäßig von Fällen berichtet und anschließend Verhaltensregeln vorgeschlagen, die anderen älteren Menschen helfen sollen, sich vor Telefonbetrug zu schützen.

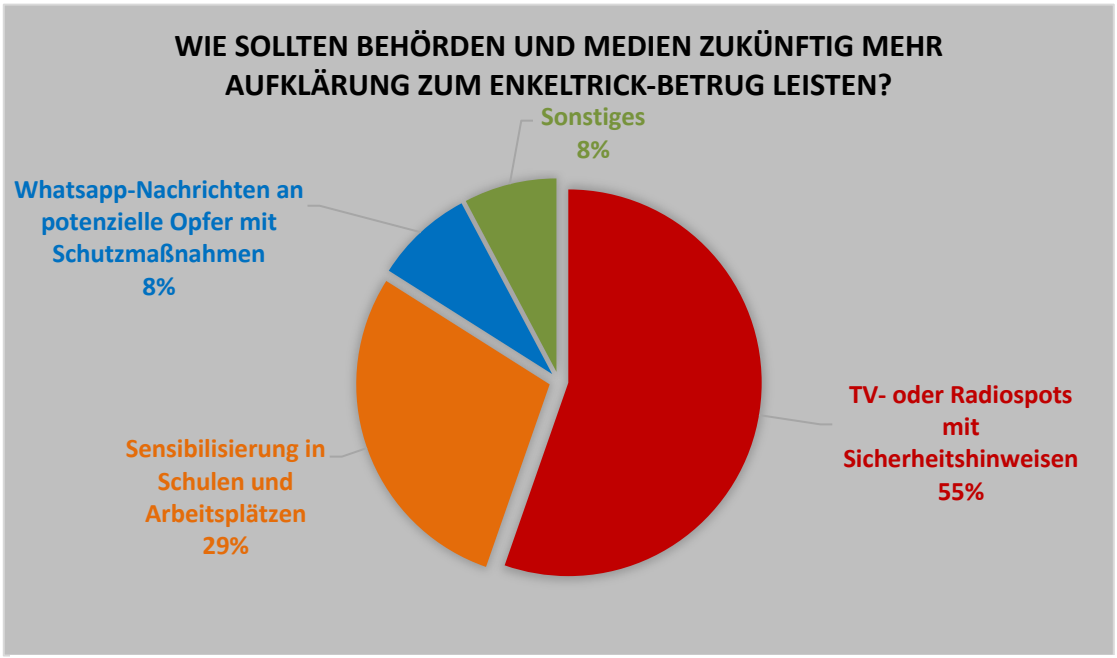


Abbildung 17: Ergebnisse der Aufklärungsvorschläge

Quelle: Eigene Darstellung

Allerdings zeigt das Interviewbeispiel, dass es immer noch Menschen gibt, denen die Betrugsmasche noch komplett unbekannt ist. Das spricht dafür, dass dennoch zu wenig Aufklärung betrieben wird. Die Interviewpartnerin kannte weder den klassischen Enkeltrick-Anruf noch die neuere SMS-Betrugsmasche. Erst nach ihrem Vorfall begann sie, sich mit der Thematik auseinanderzusetzen. Die verfügbaren Angebote haben ihr einen umfangreichen Überblick über das Thema gegeben. Das zeigt, dass die Informationen zwar verfügbar sind, aber eben erst auf Abruf.

Auf Abbildung 17 ist zu sehen, dass die Mehrheit der Befragten Medien wie Fernsehen oder Radio als die geeignetsten Aufklärungskanäle einschätzen. 55% der Teilnehmer sind der Meinung, Behörden sollten künftig mehr Aufklärungsspots zur Sensibilisierung älterer Menschen schalten. Nur knapp ein Drittel der Befragten sehen es als notwendig, Schulen und Firmen in die Aufklärung miteinzubeziehen. Die Idee, WhatsApp-Nachrichten an potenzielle Opfer mit Schutzmaßnahmen zu versenden, erhält dagegen nur wenig Zustimmung. Es lässt sich vermuten, dass Opfer diese Schutznachrichten ebenfalls als neue Betrugsmasche wahrnehmen könnten und die Hinweise eher nicht befolgen. Als sonstige Vorschläge wurde beispielsweise angegeben, dass mehr Aufklärungsarbeit von Pflegediensten oder Bankmitarbeitern erfolgen sollte.

Schlussendlich lässt sich sagen, dass durchaus viel Aufklärung von Behörden und Verbraucherschutzzentralen betrieben wird. Die Ergebnisse der Umfrage zeigen, dass sich die Mehrheit, aufgrund vorhandener Kenntnisse, als sehr sicher einschätzt, ausreichend über die Betrugsmasche des Enkeltricks Bescheid zu wissen. Dennoch gibt es Menschen, denen die Vorgehensweise unbekannt ist und es gilt zukünftig, diese Menschen über alle möglichen Kanäle zu erreichen. Viele der jungen Umfrageteilnehmer wünschen sich mehr Aufklärungskampagnen, die vor allem die Zielgruppen sensibilisieren müssen. Wichtig ist hierbei Kommunikationskanäle wie Fernsehen oder Radio zu wählen, die gerade ältere Menschen erreichen. Genauso ist es weiterhin erforderlich, dass das Umfeld älterer Menschen aufmerksam ist und ebenfalls zur Aufklärung beiträgt. Gerade Menschen, die mit Senioren arbeiten, zum Beispiel in Pflegeheimen oder Bankmitarbeiter sollten informiert sein, um potenzielle Opfer zu schützen und in verdächtigen Momenten richtig zu reagieren. Einige Fälle berichten, dass viele Betrugsfälle bereits verhindert werden konnten, weil Bankmitarbeiter oder Altenpfleger ausreichend sensibilisiert waren [60]. Es bleibt weiterhin Aufgabe der Polizei, bei Bekanntwerden neuer betrügerischen Vorgehensweisen, potenzielle Opfer sofort zu informieren. Doch leider fordert dies meist mindestens ein Opfer.

5.4 Handlungsempfehlungen

Um sicherzustellen, dass zukünftig die Zahl der Opfer der dieser Arbeit zugrundeliegenden Betrugsmasche vermindert werden kann, folgen in diesem Kapitel Handlungsempfehlungen für potenziell gefährdete Menschen und deren Umfeld. Es wird hierbei auf Handlungsempfehlungen bezüglich des klassischen Anrufes und der Messenger Nachrichten eingegangen.

5.4.1 Enkeltrick-Anruf

Folgend werden Handlungen aufgezählt, die empfohlen werden, um sich vor dem Enkeltrick am Telefon zu schützen:

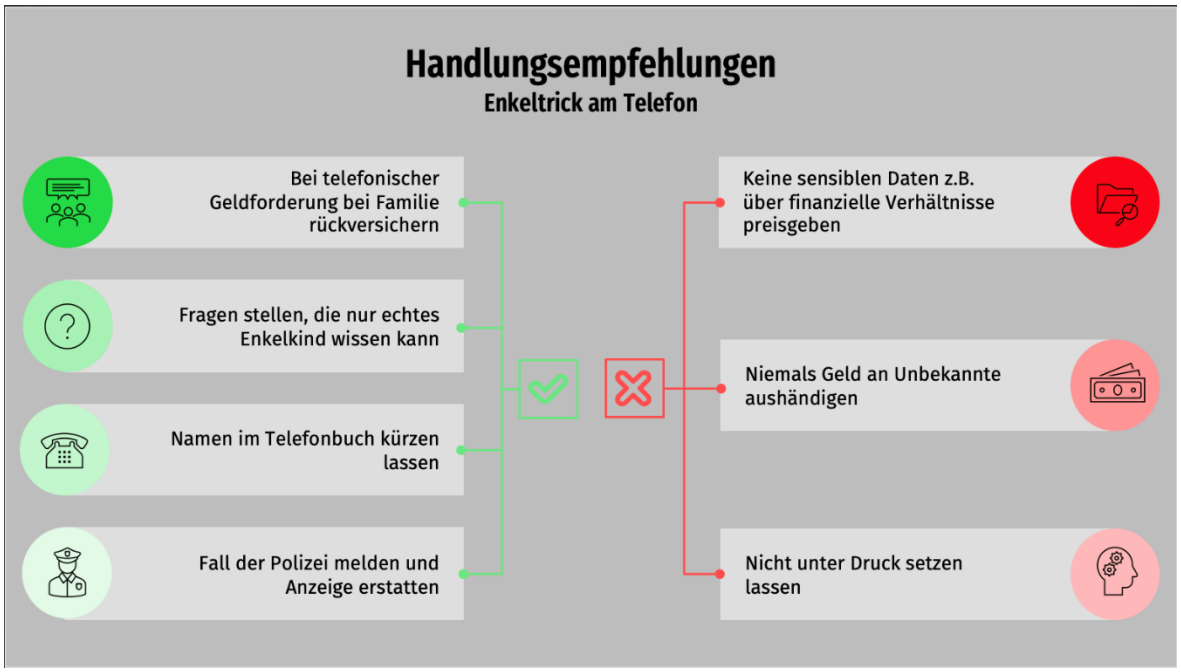


Abbildung 18: Handlungsempfehlungen für den Enkeltrick am Telefon

Quelle: Eigene Darstellung, Vorlage: Slidesgo [61]

Ältere Menschen sollten zuerst skeptisch sein, wenn sich ein unbekannter Anrufer am Telefon meldet und seinen Namen nicht sagen will, bzw. der Angerufene ihn erraten soll. Gegebenenfalls einfach den Anruf beenden. Bei telefonischer Geldforderung eines vermeintlichen Enkels in Notlage sollten sie stutzig werden und Rücksprache mit anderen Familienangehörigen halten, ob die Situation der Wahrheit entspricht (Abbildung 18). Senioren sollten dem Anrufer gezielte Fragen stellen, die nur der richtige Enkel wissen kann, um die Echtheit zu überprüfen. Sie sollten außerdem keine Details über Kontodaten oder familiäre und finanzielle Verhältnisse preisgeben, die den Betrügern in die Hände spielen könnten. Niemals sollte Geld an unbekannte Personen übergeben werden. Bei wahrheitsgemäßer Geldnot würde ein Bekannter oder Angehöriger einer persönlichen Geldübergabe zustimmen. Außerdem sollten Senioren ihren Namen im Telefonbuch kürzen lassen, damit sie Betrüger auf diese Art nicht als Opfer in Betracht ziehen kann. Sofort sollte die Polizei über einen verdächtigen Anruf informiert werden. Auch wenn jemand bereits Opfer geworden ist, sollte unbedingt Anzeige bei der Polizei erstattet werden.

Bei Betrug der „falschen Polizei“: Menschen sollten sich niemals von vertrauenserweckenden Absendernummern im Telefondisplay täuschen lassen. Wenn die Polizei anruft, würde niemals die „110“ im Display stehen. Gibt sich eine Person als Polizist aus, sollte nach Vorlage des Dienstausweises verlangt werden. Polizisten würden niemals die Opfer an der Haustür um Aushändigung von Wertsachen bitten. Auch hier: den Vorfall sofort der richtigen Polizei melden [32] [62].

5.4.2 WhatsApp-Betrug

Zum Schutz vor dem SMS-Betrug über WhatsApp werden folgende Empfehlungen ausgesprochen:

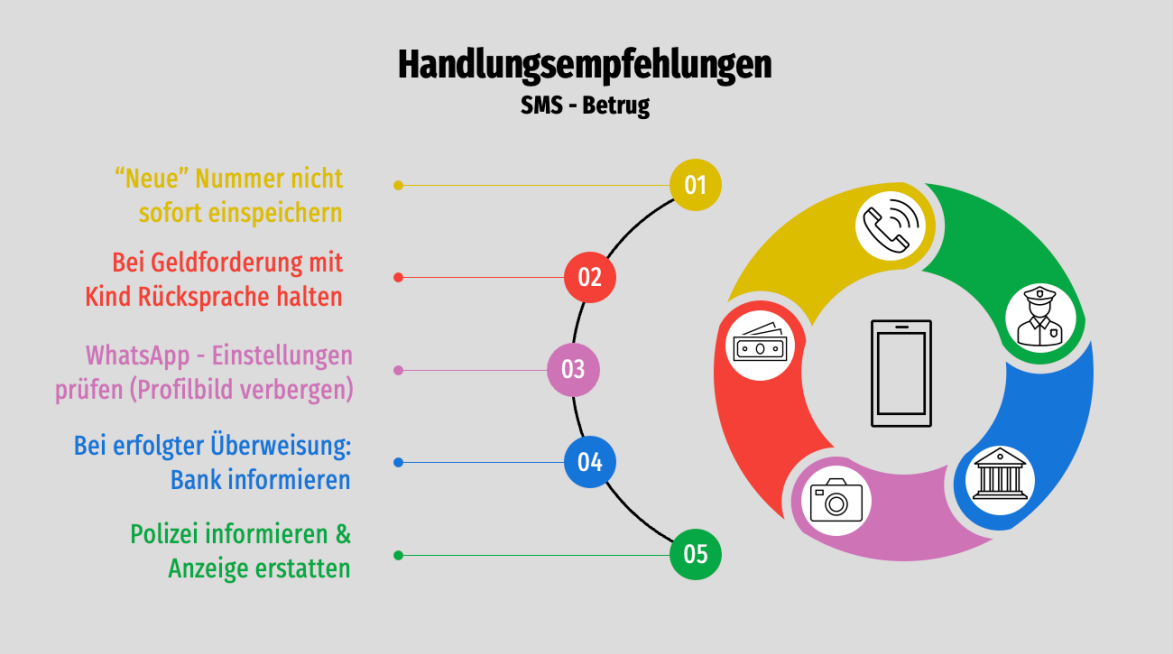


Abbildung 19: Handlungsempfehlungen für Enkeltrick bei WhatsApp

Quelle: Eigene Darstellung, Vorlage: Slidesgo [63]

Wie Abbildung 19 zeigt, gilt hier: Betroffene sollten die „neue“ Telefonnummer des angeblichen Kindes nicht sofort einspeichern, da es sonst keine Möglichkeit mehr gibt, das richtige Kind zu erreichen, falls nur die Handynummer vorliegen sollte. Außerdem wird so unterbewusst die Hemmschwelle verringert, bei Geldforderungen skeptisch zu werden. Man sollte nicht auf die Geldforderung eingehen, ohne vorher mit dem Kind Rücksprache gehalten zu haben. Es empfiehlt sich für jeden WhatsApp-Nutzer seine Einstellungen zu prüfen. Es besteht die Möglichkeit, sein Profilbild nur für eingespeicherte Kontakte sichtbar zu machen. Betrüger könnten über das Bild schon vorher Rückschlüsse auf das Alter oder andere Verhältnisse über das potenzielle Opfer ziehen. So wissen sie im Voraus, ob sie das Opfer mit „Mama“ oder „Oma“ ansprechen müssen.

Bei erfolgter Geldüberweisung: sofort Polizei und die Bank informieren. Je schneller nach einer Überweisung reagiert, desto höher ist die Wahrscheinlichkeit, dass das Geld

zurückgebucht werden kann. Außerdem kann das Betrügerkonto unter Umständen rechtzeitig eingefroren werden, bevor der Täter den Geldbetrag abheben kann [34].

Wichtig zu betonen ist hierbei, dass es sich egal unter welchen Umständen empfiehlt, bei jeglichen verdächtigen Aktionen die Polizei zu informieren. Jede kleine Information kann den Ermittlern helfen, Kenntnisse über die Täter und deren Vorgehen zu sammeln, um so die Wahrscheinlichkeit zu erhöhen, dass Betrüger zukünftig keinen Erfolg mehr haben. Ebenfalls gilt für Familienangehörige, dass sie jederzeit das Gespräch mit ihrer älteren Verwandtschaft suchen, damit auch auf diesem Weg sichergestellt werden kann, dass die ältere Generation über dieses Thema informiert und geschützt werden kann.

Darüber hinaus wäre es erforderlich, dass Kommunikationsdienste wie WhatsApp oder Snapchat ihre Registrierungsverfahren überdenken. Beispielsweise könnte eine verstärkte Identitätsprüfung helfen, betrügerischen Missbrauch ihrer Plattformen zu verhindern. Betroffene sollten sich in jedem Fall Menschen, denen sie vertrauen, öffnen, um das Geschehene nicht allein verarbeiten zu müssen. Es gibt in ganz Deutschland verschiedene Anlaufstellen, wie den „Weisser Ring e.V.“, der sich professionell um Betrugsopfer kümmern kann.

6 Zusammenfassung und Ausblick

6.1 Zusammenfassung

Anhand einer quantitativen Umfrage wurde die Präsenz des Enkeltrick-Betrugs in analoger und digitaler Form analysiert und mithilfe eines Interviews mit einer Betroffenen Erfahrungen bezüglich des Themas Enkeltrick aufgezeigt. Da es sich dabei jedoch nur um ein Testszenario handelte, konnten nur teilweise verlässliche Aussagen zu den aufgestellten Forschungsfragen getroffen werden.

Zusammenfassend lässt sich sagen, dass mit dieser Forschungsarbeit leider keine Enkeltrick-Betrugsopfer ausfindig gemacht werden konnten und somit auch keine Aussagen über die psychischen Langzeitfolgen der Opfer getätigt werden können. Allerdings kommt man zu der Erkenntnis, dass die Folgen so verheerend sein müssen, dass sich viele Betroffene nicht einmal trauen, sich ihren Verwandten oder Bekannten anzuvertrauen, geschweige denn fremden Personen oder öffentlichen Einrichtungen wie der Polizei oder Hilfsorganisationen. Weiterhin konnten vorhandene Kenntnisse über Persönlichkeitsmerkmale der Zielpersonen von Betrüger bestätigt werden. Es lässt sich sagen, dass Frauen eher dazu neigen charakteristische Merkmale aufzuweisen, die in Verbindung mit dem Opfer-Sein gebracht werden und somit eher ins Visier der Betrüger geraten. Insgesamt muss trotz enormer Informationsvielfalt noch mehr Aufklärung in den für die Zielgruppen relevanten Medien geleistet werden, um weitere Opfer des Enkeltricks und auch des WhatsApp-Betrugs zu verhindern. Der Trend scheint sich auf die jüngere Generation zu verschieben, da vor allem die WhatsApp-Betrugsmasche immer mehr Beachtung erfährt. Die Vorgehensweise orientiert sich am klassischen Enkeltrick, bei dem sich fremde Anrufer als die Enkelkinder älterer Menschen ausgeben und wegen eines dringenden finanziellen Notfalls Geld von ihnen benötigen. Der SMS-Betrug geht nach dem gleichen Schema vor, lediglich nicht mit persönlichem Kontakt über das Telefongespräch, sondern hier werden Menschen im Eltern-Alter über eine digitale SMS- oder WhatsApp-Nachricht nach Geld gebeten. Es bleibt abzuwarten, wie sich betrügerische Vorgehensweisen weiterhin entwickeln.

6.2 Ausblick

In einer Welt, in der Technologie und Kommunikation immer vernetzter werden, wird das Social Engineering zweifellos weiterhin eine Rolle spielen. Es ist davon auszugehen, dass sich die Betrüger sämtlicher Betrugsmaschen weiterentwickeln und sich dabei fortschreitender technologischer Entwicklung bedienen werden. Schon jetzt ist eine Zunahme von verschiedenen Betrugsmaschen, die über digitale Kommunikationsmittel wie E-Mails oder soziale Medien zu verzeichnen. Bei der Vorgehensweise des Enkeltricks sind keine opferspezifischen Informationen, außer das Alter und eventuell das Geschlecht von Nöten. Es ist verblüffend zu sehen, wie erfolgreich diese Masche trotz wenig persönlicher Informationen ist und wie universell anwendbar sie auf so viele Menschen ist.

Romance Scams als weiteres Beispiel des Social Engineerings zeigt, dass Betrug, der auf der Ausnutzung von Vertrauen auf Beziehungsebene basiert, wahrscheinlich immer

funktionieren wird. Wenn Betrüger die Mühe und den Zeitaufwand in Kauf nehmen, tage- oder wochenlang eine Beziehung zu einer Person aufzubauen, dann kann das Opfer sich gar nicht wirksam davor schützen. Wie soll Wahrheit von Betrug unterschieden werden? Liebe macht bekanntlich blind und Betrüger werden immer mehr Aufwand in ihre Vorgehensweisen stecken, um letztendlich erfolgreich zu sein. So auch bei sämtlichen Trickbetrugsmaschen.

Soziale Medien bieten die Möglichkeit, vor allem für junge Menschen, viele persönliche Daten über sich preiszugeben. Je jünger die Social-Media-Nutzer werden, desto geringer ist die Hemmschwelle, viele Informationen über sich für alle zugänglich zu machen. Das macht es Betrügern besonders leicht, ohne viel Aufwand Daten über ein potenzielles Opfer zu sammeln, die er für illegale Handlungen wie zum Beispiel Identitätsdiebstahl ausnutzen kann. Deshalb sollten Jugendliche und junge Erwachsene über ein gesundes Einschätzungsvermögen verfügen, welche Informationen sie über sich im Internet teilen.

Nicht außer Acht zu lassen ist die Entwicklung KI. Bereits jetzt ist es über Deep Fakes möglich, Bilder oder Videos so glaubwürdig zu manipulieren, dass sie sich kaum noch als solche identifizieren lassen. Mit Entwicklung der KI ist davon auszugehen, dass Manipulation durch Sprachassistenzprogramme oder automatisierte Chatbots perfektioniert wird und Opfer gar keine Chance mehr haben werden, Betrug von Wahrheit unterscheiden zu können. Beispielsweise könnten diese KI-basierten Programme Verhaltensweisen und Stimmen von Bekannten analysieren und imitieren, um noch authentischer zu sein und die Menschen zu täuschen. Diese Technik kann außerdem auch auf politischer Ebene instrumentalisiert werden, um große Menschenmassen zu manipulieren.

Aufgrund dieses Ausblicks ist es notwendig eine gewisse Skepsis zu bewahren. Die technologische Entwicklung kann das alltägliche Leben erleichtern, gleichzeitig birgt sie auch weiterhin Gefahren, die immer von irgendjemandem ausgenutzt werden können.

Es ist weiterhin erforderlich alle Generationen hinsichtlich neu bekanntwerdender Betrugsmaschen aufzuklären und zu sensibilisieren. Dafür sollten alle verfügbaren Kanäle genutzt werden. Insgesamt ist es wichtig, dass sich die Gesellschaft gegen Enkeltrick und ähnliche Betrugsmaschen stellen. Nur die Kombination aus Aufklärung, technologischer Weiterentwicklung und konsequenter Strafverfolgung kann die Erfolgschance verringern und (ältere) Menschen vor finanziellen Schäden schützen, ohne dass erst jemand aus dem Schaden klug werden muss.

Zukünftige Forschungsarbeiten sollten das Thema der ethischen und moralischen Auswirkungen auf die Enkeltrickopfer erneut aufgreifen und tiefgründiger erforschen. Dabei ist es wichtig, geeignetere Forschungsmethoden und eindeutigere Formulierungen von Umfragen oder Experteninterviews zu wählen. Es empfiehlt sich, die Forschung über einen längeren Zeitraum durchzuführen, damit genügend verlässliche Quellen gefunden werden können, um empirische Aussagen zu treffen. Ansätze für die Findung geeigneter Zielgruppen könnten Aushänge in Alters- oder Pflegeheimen sein, sowie Anfragen bei Polizeidienststellen oder in sozialen Medien wie Instagram, Facebook. Diese Arbeit kann als Grundlage weiterführender Forschungsarbeiten dienen.

Literatur

[1] Polizei Sachsen: Immer wieder hohe finanzielle Schäden durch Schockanrufer. URL: https://www.polizei.sachsen.de/de/98446.htm (verfügbar am 09.08.2023)

[2] Saarländischer Rundfunk: Neue Kampagne soll Senioren vor Enkeltrick schützen. URL: https://www.sr.de/sr/home/nachrichten/politik_wirtschaft/enkeltrick_und_co_nicht_mit_uns_kampagne_gegen_telefonbetrug_100.html (verfügbar am 09.08.2023)

[3] ZEIT ONLINE: 2022 weniger Schockanrufe im Land, Schadensumme gestiegen. URL: https://www.zeit.de/news/2023-02/03/2022-weniger-schockanrufe-im-land-schadenssumme-gestiegen (verfügbar am: 09.08.2023)

[4] Bundesamt für Familie, Senioren, Frauen und Jugend: „Rate mal, wer dran ist!“ URL: https://www.bmfsfj.de/resource/blob/95226/de8770bf7aa5c5d82fa3f95a69b0c898/rate-mal-wer-dran-ist-data.pdf (verfügbar am: 09.08.2023)

[5] Vodafone: Social Engineering – Angriffe auf die Schwachstelle Mensch. URL: https://www.vodafone.de/business/featured/digitales-business/digitale-geschaeftsprozesse/social-engineering-angriffe-auf-die-schwachstelle-mensch/ (verfügbar am: 09.08.2023)

[6] Hadnagy, Christopher; Ekman, Paul: Social Engineering enttarnt: Sicherheitsrisiko Mensch. 1. Auflage Heidelberg: mitp Verlags GmbH & Co. KG, 2014

[7] Mitnick, Kevin; Simon, William L.: Die Kunst der Täuschung: Risikofaktor Mensch. 1. Auflage Heidelberg: mitp Verlags GmbH & Co. KG, 2011

[8] Stirnimann, Sonja: Der Mensch als Risikofaktor bei Wirtschaftskriminalität: Handlungsfähig bei Non-Compliance und

Cyberkriminalität, 2. Auflage Wiesbaden: SpringerGabler, 2021 (e-Book) URL: https://link.springer.com/content/pdf/10.1007/978-3-658-34631-7.pdf (verfügbar am: 21.06.2023)

[9] Uven, Patrick; Carl von Ossietzky Universität Oldenburg: Sicherheitslücken im Internet: Social Engineering. URL: http://www.informatik.uni-oldenburg.de/~iug10/sli/index7c87.html?q=node/31 (verfügbar am: 21.06.2023)

[10] Frankfurter Rundschau: Putins Troll-Fabrik. URL: https://www.fr.de/politik/putins-troll-fabrik-11164748.html (verfügbar am: 25.07.2023)

[11] Kaspersky: Was ist Social Engineering? URL: https://www.kaspersky.de/resource-center/definitions/social-engineering (verfügbar am: 15.06.2023)

[12] Digital Guide, Ionos: Shoulder Surfing – eine unterschätzte Gefahr? URL: https://www.ionos.de/digitalguide/server/sicherheit/shoulder-surfing/ (verfügbar am: 15.06.2023)

[13] Hadnagy, Christopher: Die Kunst des Human Hacking: Social Engineering – Deutsche Ausgabe. 2. Auflage Heidelberg: mitp Verlags GmbH & Co. KG, 2011

[14] Schumacher, Stefan: Die psychologischen Grundlagen des Social Engineerings. Magdeburg, 2013 URL: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiwhfr798qAAxVSta-QKHcJ0Dg4QFnoECA4QAQ&url=https%3A%2F%2Fwww.degruyter.com%2Fdocument%2Fdoi%2F10.1515%2Fiwp-2014-0039%2Fpdf&usg=AOvVaw1ZHNDq6H_XOSyfvSecU-fd&opi=89978449 (verfügbar am: 01.07.2023)

[15] Cialdini, Robert B.: Die Psychologie des Überzeugens: Wie Sie sich selbst und Ihren Mitmenschen auf die Schliche kommen. 8. Auflage Bern (Schweiz): Verlag Hans Huber, 2007 URL: https://books.google.de/books?hl=de&lr=&id=yI2rEAAAQBAJ&oi=f

nd&pg=PA4&dq=Cialdini,+R.+B.+(2007).+Die+Psychologie+des+Überzeugens&ots=dMjyzeAcDv&sig=fA5vPoYYYklfqv8rnvvCBkIbBqo#v=onepage&q=Cialdini%2C%20R.%20B.%20(2007).%20Die%20Psychologie%20des%20Überzeugens&f=false (verfügbar am: 01.07.2023)

[16] Kahneman, Daniel: Schnelles Denken, langsames Denken. München: 19. Auflage Siedler Verlag, 2012

[17] Lerner, Jennifer S.; Keltner, Dacher: Fear, Anger, and Risk. 2001 URL: https://d1wqtxts1xzle7.cloudfront.net/30821181/10271368_Lernerlibre.pdf?1363295190=&response-content-disposition=inline%3B+filename%3DIIIIIIIIIIIIIII.pdf&Expires=1691430306&Signature=PJRFFIP4hkM2ZE9fn4EgraoyAkmoNb2RjK-DsNJXVUhIYtv0VKvUlQ8c0ZjZDEMOq3mXkKc38R9thcf4tDRSBKjvEFORcajkQDO6VGTOOeHSjayN1j90H-j6~IFKKQlRsRvecbUZTQrk5cxrxqTGXBunrrncEbdrHI3poXGROpKboLojqJIUgcoHU9WleKfl~pvczBGu~lrQ-WKi6zbPTWapv55-xrT6yNrle87t2KX6DHeYtfaCPgv9ArcMASJfcImI8knpPNMDLuUpRnpqvr0MVOx9G1zqlmBMyW0jnqfmM9JwVg29XeluzeSL4YAZBHXxjVE1H-cPne6Gg5vlg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (verfügbar am: 12.07.2023)

[18] Allhoff, Dieter-W.; Allhoff, Waltraud: Rhetorik & Kommunikation: Ein Lehr- und Übungsbuch. 16. Auflage München: Ernst Reinhardt Verlag, 2014

[19] Praxis Framework: Berlo. URL: https://www.praxisframework.org/de/library/berlo (verfügbar am: 20.06.2023)

[20] Schulz von Thun Institut für Kommunikation: Das Kommunikationsquadrat. URL: https://www.schulz-von-thun.de/die-modelle/das-kommunikationsquadrat (verfügbar am: 02.07.2023)

[21] Watzlawick, P., Beavin, Janet H.; Jackson, Don D.: Menschliche Kommunikation. Formen, Störungen, Paradoxien. URL: https://www.ciando.com/img/books/extract/345675745X_lp.pdf (verfügbar am: 02.07.2023)

[22] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2022. S. 27 URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6 (verfügbar am: 24.07.2023)

[23] Bundesamt für Sicherheit in der Informationstechnik: Phishing-E-Mails erkennen. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html (verfügbar am: 24.07.2023)

[24] Verbraucherzentrale NRW e.V.: Phishing-Radar: Archiv. URL: https://www.verbraucherzentrale.de/geld-versicherungen/phishingradar-archiv-71872 (verfügbar am: 24.07.2023)

[25] Bundesamt für Sicherheit in der Informationstechnik: Social Engineering – der Mensch als Schwachstelle. URL: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html (verfügbar am: 24.07.2023)

[26] Mailfence: Social Engineering: Was ist Tailgaiting (Durchschlüpfen). URL: https://blog.mailfence.com/de/social-engineering-was-ist-tailgating/ (verfügbar am: 24.07.2023)

[27] Polizeiliche Kriminalprävention der Länder und des Bundes: Gut beraten im hohen Alter. URL: https://polizei.nrw/sites/default/files/2020-04/229-BR-Gut-beraten-im-hohen-Alter%20%28002%29.pdf (verfügbar am: 21.07.2023)

[28] Wolf, Tobias: Jagd auf die Schockanrufer. In: Freie Presse: Zeitgeschehen, 10. Juli 2023, S. 3

[29] Bundesnetzagentur: Manipulation von Rufnummern. URL: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html (verfügbar am: 03.07.2023)

[30] Polizei Nordrhein-Westfalen Landeskriminalamt: Präventionshinweis für Bürgerinnen und Bürger. URL: https://polizei.nrw/sites/default/files/2021-01/LKA%20Dokument%20Präventionshinweis%20Falsche%20Amtsträger.pdf (verfügbar am: 09.08.2023)

[31] Pfiffige Senioren: Enkeltrick am Telefon: Statistik & Polizei Tipps. URL: https://www.pfiffige-senioren.de/enkeltrick-telefon.htm (verfügbar am: 03.08.2023)

[32] Polizei Beratung: Informationsblatt für Mitarbeiter von Banken und Geldinstituten: Enkeltrick. URL: https://polizei.nrw/sites/default/files/2018-07/093_IB_Enkeltrick_2015-06.pdf (verfügbar am: 09.08.2023)

[33] Statista: Umfrage zur Häufigkeit des Kommunizierens über Soziale Medien bei Personen ab 60 Jahren in Deutschland in den Jahren 2019 und 2020. URL: https://de.statista.com/statistik/daten/studie/1101100/umfrage/nutzungshaeufigkeit-von-sozialen-medien-bei-senioren/#:~:text=Laut%20der%20Verbraucher%2D%20und%20Medienanalyse,in%20Deutschland%20ab%2060%20Jahren (verfügbar am: 09.08.2023)

[34] Südkurier: Vorsicht bei Herausgabe der eigenen Handynummer: So schützen Sie sich vor dem neuen Enkeltrick per WhatsApp. URL: https://www.suedkurier.de/ueberregional/wissenschaft/vorsicht-bei-herausgabe-der-eigenen-handynummer-so-schuetzen-sie-sich-vor-dem-neuen-enkeltrick-per-whatsapp;art1350069,10919706 (verfügbar am: 04.08.2023)

[35] Verbraucherzentrale NRW e.V.: „Hallo Mama“, „Hallo Papa“ – Betrugsversuche über WhatsApp und SMS. URL: https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-

festnetz/hallo-mama-hallo-papa-betrugsversuche-ueber-whatsapp-und-sms-72910 (verfügbar am: 07.07.2023)

[36] RTL News GmbH: RTL Extra Spezial: Jagd auf die SMS-Betrüger. [Film] 2023, TV-Ausstrahlung am 31.07.2023

[37] Whitty, Monica T.: Do You Love Me? Psychological Characteristics of Romance Scam Victims. 2018 URL: https://www.liebert-pub.com/doi/10.1089/cyber.2016.0729 (verfügbar am: 07.07.2023)

[38] Südkurier: Ein Psychiater erklärt: Darum sind Betrüger so erfolgreich. URL: https://www.suedkurier.de/region/hochrhein/kreis-waldshut/Ein-Psychiater-erklaert-Darum-sind-Betrueger-so-erfolgreich;art372586,10179595 (verfügbar am: 01.07.2023)

[39] Handelsblatt: So funktioniert der Enkeltrick. URL: https://www.handelsblatt.com/arts_und_style/aus-aller-welt/kriminalitaet-so-funktioniert-der-enkeltrick/11462534.html (verfügbar am: 28.06.2023)

[40] Allwinn, Mirko; Hoffmann, Jens; Tultschinetski, Sina; Streich, Katrin: Betrügerisches Verhalten aus kriminalpsychologischer Sicht: Literaturübersicht und Vorstellung eines integrativen Modells zur Psychologie von Betrügern. Ausgabe 2/2018

[41] Fachanwalt.de: Was ist der Enkeltrick? URL: https://www.fachanwalt.de/magazin/strafrecht/enkeltrick (verfügbar am: 20.06.2023)

[42] Spiegel Panorama: Polizei nimmt Erfinder des Enkel-Tricks fest: Ermittlungen in Polen. 30.05.2014 URL: https://www.spiegel.de/panorama/justiz/betrug-durch-enkel-trick-polizei-nimmt-bande-in-polen-fest-a-972412.html (verfügbar am: 27.06.2023)

[43] Spiegel Panorama: Champagner für Boss „Hoss“: Enkeltrick-Pate wieder frei. 21.03.2020 URL: https://www.spiegel.de/panorama/justiz/enkeltrick-erfinder-arkadiusz-hoss-lakatosz-wieder-auf-

freiem-fuss-a-0245fe78-9c8e-4a87-9e46-f980f34cf932 (verfügbar am: 27.06.2023)

[44] StGB (idF v. 06.04.2021) § 263 und online: Fachanwalt.de: Was ist der Enkeltrick? URL: https://www.fachanwalt.de/magazin/strafrecht/enkeltrick (verfügbar am: 03.07.2023)

[45] Empirio: Deduktive und induktive Forschung. URL: https://www.empirio.de/empiriowissen/deduktive-und-induktive-forschung (verfügbar am: 28.07.2023)

[46] Dresing, Thorsten; Pehl, Thorsten: Praxisbuch Interview, Transkription & Analyse: Anleitungen und Regelsysteme für qualitativ Forschende. 8. Auflage Marburg: Eigenverlag, 2018 URL: https://www.audiotranskription.de/wp-content/uploads/2020/11/Praxisbuch_08_01_web.pdf (verfügbar am: 27.07.2023)

[47] Statista: Durchschnittliches Alter der Mütter und Väter bei der Geburt eines Kindes in Deutschland von 1991 bis 2022. URL: https://de.statista.com/statistik/daten/studie/1180171/umfrage/durchschnittliches-alter-der-muetter-und-vaeter-bei-der-geburt-in-deutschland/ (verfügbar am: 27.07.2023)

[48] Bünning, Mareike; Deutsches Zentrum für Altersfragen: Großeltern in Deutschland: Befunde des Deutschen Alterssurveys (DEAS) 2008-2020/21. 25.08.2022 URL: https://www.dza.de/fileadmin/dza/Dokumente/Fact_Sheets/DZA_Fact_Sheet_Großeltern_in_Deutschland_Befunde_des_Deutschen_Alterssurveys_2008-2020_21.pdf (verfügbar am: 27.07.2023)

[49] PayPal: Was ist der Unterschied zwischen Zahlungen an Freunde und Familie und Zahlungen für Waren und Dienstleistungen? URL: https://www.paypal.com/de/cshelp/article/was-ist-der-unterschied-zwischen-zahlungen-an-freunde-und-familie-und-zahlungen-für-waren-und-dienstleistungen-help277 (verfügbar am: 28.07.2023)

[50] Kleinanzeigen: Sicher Bezahlen – mit gutem Gefühl handeln. URL: https://themen.kleinanzeigen.de/sicher-bezahlen/ (verfügbar am: 28.07.2023)

[51] TZ: Betrüger geben sich als Sohn oder Tochter aus – So funktioniert der Enkeltrick über WhatsApp. 03.11.2022 URL: https://www.tz.de/welt/enkeltrick-whatsapp-betrueger-ueberweisung-polizei-name-handy-sohn-tochter-masche-91889899.html (verfügbar am: 15.07.2023)

[52] NDR: Enkeltrick über WhatsApp: So schützen Sie sich vor Betrug. URL: https://www.ndr.de/ratgeber/verbraucher/Betrugsmasche-ueber-WhatsApp-So-koennen-Sie-sich-schuetzen,trickbetrug222.html (verfügbar am 11.08.2023)

[53] Malteser: Altersarmut in Deutschland: Die Zahl der Betroffenen wächst. URL: https://www.malteser.de/dabei/information-tipps/altersarmut-in-deutschland-ein-ueberblick.html (verfügbar am: 17.07.2023)

[54] WEISSER RING e.V.: Impressum. URL: https://weisser-ring.de (verfügbar 29.07.2023)

[55] Süddeutsche Zeitung: „Da hilft auch kein Weinen in der Verhandlung“. 24.02.2020 URL: https://www.sueddeutsche.de/muenchen/prozess-enkeltrick-betrug-urteil-1.4816822 (verfügbar am: 26.07.2023)

[56] Delaney, Rebecca K.; Turiano, Nicholas A.; Strough, JoNell: Living longer with help from others: Seeking advice lowers mortality risk. 12.10.2018. URL: https://journals.sagepub.com/doi/epub/10.1177/1359105316664133 (verfügbar am: 26.07.2023)

[57] GEO: Wie sich Frau und Mann unterscheiden: Verblüffende Erkenntnisse der Forschung. URL: https://www.geo.de/wissen/forschung-und-technik/geschlechterforschung-wie-sich-frau-und-

mann-unterscheiden-verblueffende-30179942.html (verfügbar am: 26.07.2023)

[58] WhatsApp: Über WhatsApp. URL: https://www.whatsapp.com/about (verfügbar am: 25.07.2023)

[59] Süddeutsche Zeitung: Das warme Lagerfeuer. 14.11.2021 URL: https://www.sueddeutsche.de/wirtschaft/fernsehen-streaming-ard-rtl-prosieben-sat-1-1.5462466 (verfügbar am: 05.08.2023)

[60] Volksfreund: Enkeltrick-Betrüger wollen 87-Jährige über den Tisch ziehen – Bankmitarbeiter werden hellhörig. 15.03.2023 URL: https://www.volksfreund.de/blaulicht/schweich-bankmitarbeiter-verhindern-enkeltrick-betrug_aid-86728969 (verfügbar am: 05.08.2023)

[61] Slidesgo.com: Pros and Cons Infographics. URL: https://slidesgo.com/search?q=pro+contra#rs=search (verfügbar am: 08.08.2023)

[62] Fachanwalt.de: Betrug im Namen der Polizei: Tricks der falschen Polizisten am Telefon und vor der Tür erkennen. URL: https://www.fachanwalt.de/magazin/strafrecht/betrug-im-namen-der-polizei (verfügbar am 09.08.2023)

[63] Slidesgo.com: Infographics for tips. URL: https://slidesgo.com/theme/infographics-for-tips#search-infographics+for+tips&position-10&results-16&rs=search (verfügbar am: 08.08.2023)

Anlagen

Anlage, Teil 1: E-Mail-Korrespondenz

Von: [redacted] | WEISSER RING e. V.
An: "Marie Köhler" [redacted]
Cc:
Betreff: AW: Interview-Anfrage für Bachelorarbeit
Datum: 02.06.2023, 09:44
Anhänge:

Hallo Frau Köhler,

vielen Dank für Ihre Anfrage. Leider (oder zum Glück) mußten wir in unserer Außenstelle noch kein Opfer eines "Enkeltricks" betreuen. Erfahrungsgemäß tritt dieser gehäuft eher in Großstädten auf. Treten Sie doch am Besten einmal an unsere Außenstellen in Dresden, Leipzig oder Chemnitz heran.

Alles gute & viel Erfolg für Ihre Arbeit!

[redacted]
Außenstellenleiter

Außenstelle Döbeln
Tel: 0151/55164680
E-Mail: [redacted]

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
Internet: https://doebeln-sachsen.weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

Von: [redacted] | WEISSER RING e. V.
An: "Marie Köhler" [redacted]
Cc:
Betreff: AW: Interview-Anfrage für Bachelorarbeit
Datum: 02.06.2023, 08:15
Anhänge:
powered by zertificon

Sehr geehrte Frau Köhler, leider kann ich Ihnen hier nicht weiterhelfen.

Zu uns, in die Aussenstelle Riesa/ Großenhain, ist noch niemand gekommen, der von dem Enkeltrick betroffen war.

Das heißt aber nicht, dass es das hier in der Region nicht gibt.
Die Polizeistatistik gibt sicher darüber Auskunft.

Aus Angst, Scham und mit dem Wissen, dass die Täter nicht gefasst werden und das Geld auch nicht wieder kommt, scheuen sicher die Betroffenen den Weg zu uns.

Ich könnte mir allerdings vorstellen, dass Sie in den Großstädten, wie Dresden, Leipzig, Chemnitz, mehr Glück haben werden. Dort sind die Opferzahlen ganz anders, als hier im ländlichen Gebiet.

Für Ihre Arbeit wünsche ich Ihnen alles Gute und bin überzeugt, dass Sie noch Ansprechpartner finden.

Mit freundlichen Grüßen

[redacted]
Außenstellenleiterin

Außenstelle Riesa-Großenhain
Tel: 0151/55164731
E-Mail: [redacted]

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
Internet: https://riesa-grossenhain-sachsen.weisser-ring.de

Von: [redacted] | WEISSER RING e. V.
An: "Marie Köhler" [redacted]
Cc:
Betreff: AW: Interview-Anfrage für Bachelorarbeit
Datum: 02.06.2023, 13:48
Anhänge:
powered by zertificon

Sehr geehrte Frau Köhler,

Ihr gewähltes Thema ist sehr interessant und Aufklärung in diesem Themengebiet ist sehr wichtig.
Es gibt beim Weissen Ring e. V. sicher Außenstellen, die Ihnen weiterhelfen können.
Für die Bereiche Annaberg und Marienberg muss ich Ihnen jedoch mitteilen, dass wir bisher mit Opfern des Enkeltrickbetruges noch keinen Kontakt hatten und Ihnen somit leider nicht helfen können.

Ich drücke Ihnen die Daumen, Hilfe für Ihr Ansinnen zu finden, wünsche Ihnen ein schönes Wochenende und verbleibe mit freundlichen Grüßen

[redacted]
Außenstellenleiter
Außenstellen Annaberg und Marienberg
Tel: 0175/6528064
E-Mail: [redacted]

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
Internet: https://annaberg-sachsen.weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

AW: Interview-Anfrage für Bachelorarbeit

Von: "Weisser Ring e.V., Landesbüro Thüringen" <Thueringen@weisser-ring.de>
An: "'Marie Köhler'" [redacted]
Datum: 23.06.2023 09:12:33

Sehr geehrte Frau Köhler,

zu der von Ihnen angesprochenen Thematik, speziell ethische und moralische Auswirkungen auf Opfer des Enkeltricks, liegt uns keine Expertise vor.

Das Führen von Interviews mit Opfern ist eher schwierig, da wir nicht einschätzen können, inwieweit die Betroffenen dadurch erneut mit der durchlebten Situation belastet werden.

Deshalb bedauern wir, Sie bei Ihrer wissenschaftlichen Arbeit nicht Ihren Wünschen entsprechend unterstützen zu können.

Alles Gute für Ihre berufliche Zukunft!

Mit freundlichen Grüßen

[redacted]

Landesbüro Thüringen
Michaelisstraße 24
99084 Erfurt

Tel: +49 361 3464646
Fax: +49 361 3464647
Thueringen@weisser-ring.de

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
https://weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

AW: Interview-Anfrage für Bachelorarbeit

Von: "Weisser Ring e.V., Landesbüro Sachsen" <Sachsen@weisser-ring.de>
An: "'Marie Köhler'" [redacted]
Datum: 24.05.2023 09:24:23

Sehr geehrte Frau Köhler,

vielen Dank für Ihre Anfrage. Wir bewegen uns in diesem Thema sehr tief in der Thematik der Prävention. Allerding sind bislang wenige Opfer des Enkeltricks bei uns vorstellig geworden.

Aufgrund dessen können wir Ihnen leider im Moment leider nicht weiterhelfen.

Liebe Grüße

[redacted]

Landesbüro Sachsen
Burckhardtstraße 1
01307 Dresden

Tel: +49 351 85074496
Fax: +49 351 85074498
Sachsen@weisser-ring.de

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
https://weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

AW: Interview-Anfrage für Bachelorarbeit

Von: "Weisser Ring e.V., Landesbüro Mecklenburg-Vorpommern" <mecklenburg-vorpommern@weisser-ring.de>
An: "'Marie Köhler'" [redacted]
Datum: 23.06.2023 08:50:50

Sehr geehrte Frau Köhler,

ich freue mich darüber das Sie dem Thema „Enkeltrick" Aufmerksamkeit schenken möchten.

Sie schrieben das Sie an der Hochschule Mittweida studieren.

Ich würde Ihnen gerne Vorschlagen das Sie Ihre Anfrage nochmal an das Landesbüro in Sachsen richten.

Da wir hier in Mecklenburg-Vorpommern zwar Fälle von Enkeltrick haben aber ich Ihnen sagen kann das keiner von den Betroffenen sich für ein Interview zur Verfügung stellen wird.

Ich gebe Ihnen gerne die Kontaktdaten:

Telefon: 0351/85074496

E-Mail: Sachsen@weisser-ring.de

Ich wünsche Ihnen viel Erfolg!

Mit freundlichen Grüßen

[redacted]

Landesbüro Mecklenburg-Vorpommern
Magdeburger Straße 10a
19063 Schwerin

Tel: +49 385 5007660
Fax: +49 385 5007661
mecklenburg-vorpommern@weisser-ring.de

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
https://weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

AW: Interview-Anfrage für Bachelorarbeit

Von: [redacted] | WEISSER RING e. V." [redacted]@mail.weisser-ring.de>
An: "Marie Köhler" [redacted]
Datum: 22.05.2023 07:28:31

Guten Morgen Frau Köhler,

vielen Dank für Ihre Anfrage.

In unserer Außenstelle hatten wir in den letzten 24 Monaten zwar anrufe zu diesem Thema, aber keine Betroffenen die sich an uns gewandt haben. Somit kann ich Ihnen leider nicht weiterhelfen.

Gern können wir einmal telefonieren.

Sollten Sie noch Fragen haben, stehe ich Ihnen gern zur Verfügung.

Mit freundlichen Grüßen
[redacted]
Außenstellenleiter
Außenstelle Chemnitz (Stadt)
[redacted]
E-Mail: [redacted]
Internet: https://chemnitz-stadt-sachsen.weisser-ring.de

WEISSER RING e. V.
Bundesgeschäftsstelle
Weberstraße 16
55130 Mainz
https://weisser-ring.de

Eingetragen unter VR 1648 beim Amtsgericht Mainz
Bundesvorsitzender: Dr. Patrick Liesching

AW: Anfrage für Bachelorarbeit

Von: [redacted]
An: "Marie Köhler" [redacted]
Datum: 04.07.2023 17:43:42

Sehr geehrte Frau Köhler,

entschuldigen Sie, dass die Antwort so lange gedauert hat. Wir beziehen die meisten unserer Beiträge von der Polizei, sodass die Personen auch bei uns nicht mit Klarnamen auftauchen oder identifizierbar sind. Vielleicht würde ein Aufruf über soziale Netzwerke weiterhelfen, um mit Opfern in Kontakt zu treten?

Mit freundlichen Grüßen

[redacted]

Redakteurin

Stadtredaktion Dresden

DDV Sachsen GmbH

Sächsische Zeitung

Stadtredaktion Dresden

Ihre Nachricht an den MDR_ Anfrage für Bachelorarbeit

Von: "Publikumsservice" <Publikumsservice@mdr.de>
An: [redacted]
Datum: 30.06.2023 14:17:54

Sehr geehrte Frau Köhler,

vielen Dank für Ihre Nachricht und das damit verbundene Interesse am Mitteldeutschen Rundfunk.

Auf Nachfrage antwortete uns die Redaktion, dass Sie die Informationen von der Polizei erhalten. Die Identitäten werden uns aus datenschutzrechtlichen Gründen nicht bekannt gegeben.

Wir bedauern Ihnen hier nicht weiterhelfen zu können und wünschen Ihnen alles Gute.

Freundliche Grüße

[redacted]

Ihr Team des MDR Publikumsservice

[redacted]

mdr

Mitteldeutscher Rundfunk

Intendanz

Hauptabteilung Kommunikation

Abteilung Marketing

Tel.: (0341) 3 00 96 96

Fax: (0341) 3 00 29 65 37

E-Mail: Publikumsservice@mdr.de

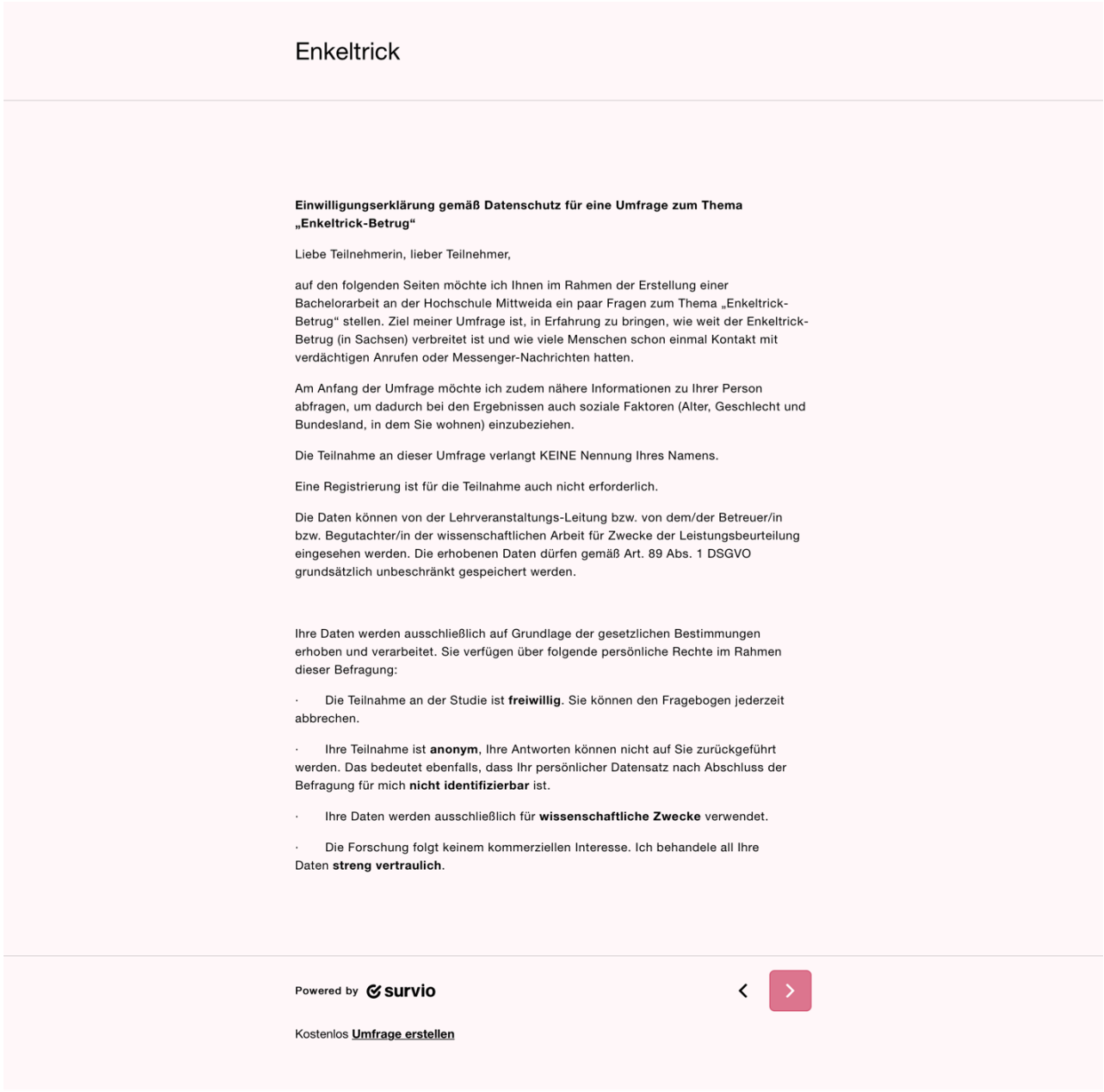
Kantstraße 71-73, 04275 Leipzig

Postanschrift: 04360 Leipzig

www.mdr.de

Datenschutzinformationen: www.mdr.de/datenschutzhinweise

Anlage, Teil 2: Umfrage-Fragebogen



Enkeltrick

Einwilligungserklärung gemäß Datenschutz für eine Umfrage zum Thema „Enkeltrick-Betrug“

Liebe Teilnehmerin, lieber Teilnehmer,

auf den folgenden Seiten möchte ich Ihnen im Rahmen der Erstellung einer Bachelorarbeit an der Hochschule Mittweida ein paar Fragen zum Thema „Enkeltrick-Betrug“ stellen. Ziel meiner Umfrage ist, in Erfahrung zu bringen, wie weit der Enkeltrick-Betrug (in Sachsen) verbreitet ist und wie viele Menschen schon einmal Kontakt mit verdächtigen Anrufen oder Messenger-Nachrichten hatten.

Am Anfang der Umfrage möchte ich zudem nähere Informationen zu Ihrer Person abfragen, um dadurch bei den Ergebnissen auch soziale Faktoren (Alter, Geschlecht und Bundesland, in dem Sie wohnen) einzubeziehen.

Die Teilnahme an dieser Umfrage verlangt KEINE Nennung Ihres Namens.

Eine Registrierung ist für die Teilnahme auch nicht erforderlich.

Die Daten können von der Lehrveranstaltungs-Leitung bzw. von dem/der Betreuer/in bzw. Begutachter/in der wissenschaftlichen Arbeit für Zwecke der Leistungsbeurteilung eingesehen werden. Die erhobenen Daten dürfen gemäß Art. 89 Abs. 1 DSGVO grundsätzlich unbeschränkt gespeichert werden.

Ihre Daten werden ausschließlich auf Grundlage der gesetzlichen Bestimmungen erhoben und verarbeitet. Sie verfügen über folgende persönliche Rechte im Rahmen dieser Befragung:

· Die Teilnahme an der Studie ist **freiwillig**. Sie können den Fragebogen jederzeit abbrechen.

· Ihre Teilnahme ist **anonym**, Ihre Antworten können nicht auf Sie zurückgeführt werden. Das bedeutet ebenfalls, dass Ihr persönlicher Datensatz nach Abschluss der Befragung für mich **nicht identifizierbar** ist.

· Ihre Daten werden ausschließlich für **wissenschaftliche Zwecke** verwendet.

· Die Forschung folgt keinem kommerziellen Interesse. Ich behandele all Ihre Daten **streng vertraulich**.

Powered by survio

Kostenlos **Umfrage erstellen**

Enkeltrick

1. Bitte wählen Sie Ihr Geschlecht:*

Wählen Sie eine Antwort

- Weiblich
- Männlich
- Divers

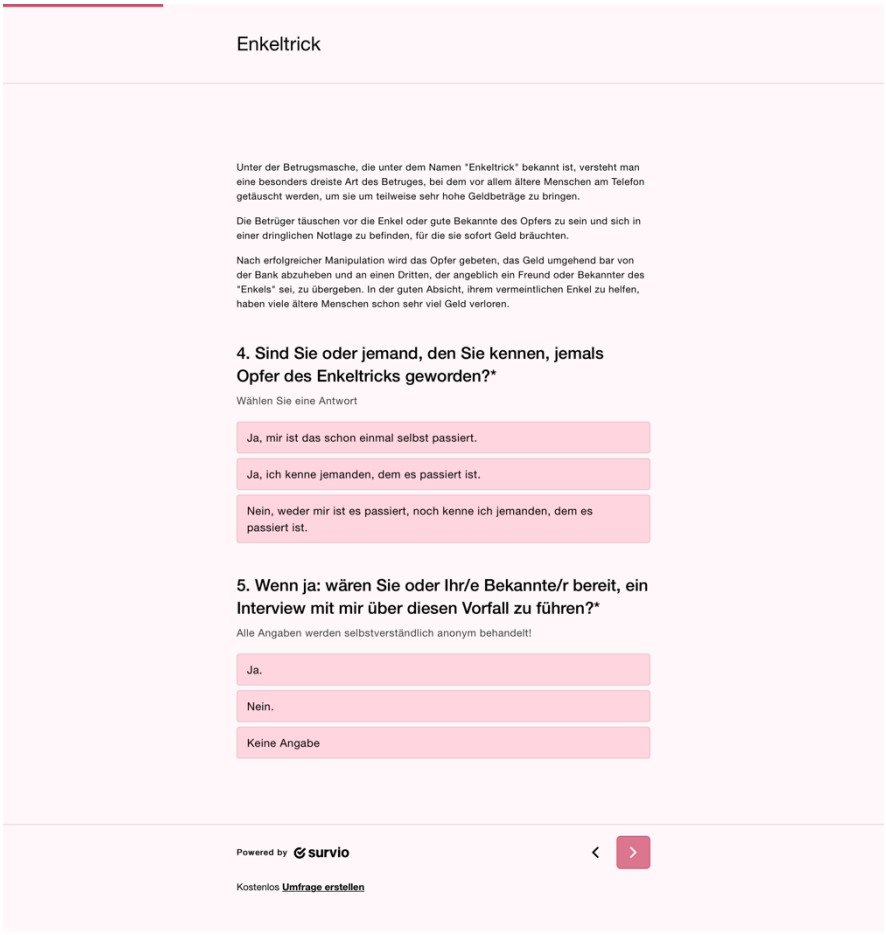
2. Bitte nennen Sie mir Ihr Alter:*

Geben Sie eine Zahl ein...

3. In welchem Bundesland wohnen Sie?*

Wählen Sie eine Antwort

- Baden-Württemberg
- Bayern
- Berlin
- Brandenburg
- Bremen
- Hamburg
- Hessen
- Mecklenburg-Vorpommern
- Niedersachsen
- Nordrhein-Westfalen
- Rheinland-Pfalz
- Sachsen
- Sachsen-Anhalt
- Saarland
- Schleswig-Holstein
- Thüringen



Enkeltrick

Unter der Betrugsmasche, die unter dem Namen "Enkeltrick" bekannt ist, versteht man eine besonders dreiste Art des Betruges, bei dem vor allem ältere Menschen am Telefon getäuscht werden, um sie um teilweise sehr hohe Geldbeträge zu bringen.

Die Betrüger täuschen vor die Enkel oder gute Bekannte des Opfers zu sein und sich in einer dringlichen Notlage zu befinden, für die sie sofort Geld bräuchten.

Nach erfolgreicher Manipulation wird das Opfer gebeten, das Geld umgehend bar von der Bank abzuheben und an einen Dritten, der angeblich ein Freund oder Bekannter des "Enkels" sei, zu übergeben. In der guten Absicht, ihrem vermeintlichen Enkel zu helfen, haben viele ältere Menschen schon sehr viel Geld verloren.

4. Sind Sie oder jemand, den Sie kennen, jemals Opfer des Enkeltricks geworden?*

Wählen Sie eine Antwort

- Ja, mir ist das schon einmal selbst passiert.
- Ja, ich kenne jemanden, dem es passiert ist.
- Nein, weder mir ist es passiert, noch kenne ich jemanden, dem es passiert ist.

5. Wenn ja: wären Sie oder Ihr/e Bekannte/r bereit, ein Interview mit mir über diesen Vorfall zu führen?*

Alle Angaben werden selbstverständlich anonym behandelt!

- Ja.
- Nein.
- Keine Angabe

Powered by survio

Kostenlos **Umfrage erstellen**

Enkeltrick

Mit Sätzen wie: "Rate mal, wer hier ist" oder "Hallo, hier ist dein Enkel" beginnen die betrügerischen Telefonate. Anschließend rät das Opfer, wenn es wirklich Enkel hat, welches sich gerade bei ihm/ihr meldet.

Jetzt wird ihnen eine Notlage, wie zum Beispiel die Verwicklung in einen Autounfall, vorgegaukelt, wofür dringend Bargeld benötigt würde. Sie werden gebeten, den Betrügern zu helfen und es niemandem zu erzählen. Somit werden die Opfer unter psychischen Druck gesetzt.

6. Haben Sie oder jemand, den Sie kennen, in letzter Zeit einen verdächtigen Anruf von Personen erhalten, die behaupteten Enkel oder Verwandte zu sein?*

Wählen Sie eine Antwort

- Ja, ich habe so einen Anruf erhalten.
- Ja, ich kenne jemanden, der so einen Anruf erhalten hat.
- Nein, weder ich, noch jemand, den ich kenne, hat so einen Anruf erhalten.

7. Wenn ja: wären Sie oder Ihr/e Bekannte/r bereit, mir zu erzählen, wie das Gespräch abgelaufen ist?*

Alle Angaben werden selbstverständlich anonym behandelt!

- Ja.
- Nein.
- Keine Angabe

Powered by survio

Kostenlos **Umfrage erstellen**

Enkeltrick

Zunehmend verlagern Betrüger Ihre Betrugsmasche auch auf Messenger-Dienste und richten sich nicht mehr nur an "Großmütter" und "Großväter", mittlerweile werden gezielt auch "Mütter" und "Väter" angesprochen.

Unbekannte Nummern schicken Nachrichten mit den Anfangsworten: "Hallo Mama, ich habe eine neue Telefonnummer. Bitte speichere sie ein." und geben vor Tochter oder Sohn zu sein, deren Handy kaputt sei und sie deshalb eine neue Nummer hätten. Auch hier täuschen sie eine Notlage vor und bitten um Überweisung einer wichtigen Rechnung, da zum Beispiel durch das kaputte Handy kein Zugang zum Online-Banking möglich sei. Erst bei Kontakt zu den echten Kindern werden Opfer auf den Betrug aufmerksam.

8. Haben Sie oder jemand, den Sie kennen, in letzter Zeit eine verdächtige Whatsapp-Nachricht von Personen erhalten, die behaupteten Enkel oder Verwandte zu sein?*

Wählen Sie eine Antwort

- Ja, ich habe so eine Whatsapp-Nachricht selbst erhalten.
- Ja, ich kenne jemanden, der so eine Whatsapp-Nachricht erhalten hat.
- Nein, weder ich, noch jemand, den ich kenne, hat so eine Whatsapp-Nachricht erhalten.

9. Wenn ja: wären Sie oder Ihr/e Bekannte/r bereit, mir zu erzählen, wie diese Nachricht ausgesehen hat und wie der Chatverlauf war?*

Alle Angaben werden selbstverständlich anonym behandelt!

- Ja.
- Nein.
- Keine Angabe

Powered by survio

Kostenlos **Umfrage erstellen**

Enkeltrick

10. Wie sicher sind Sie, dass Sie einen versuchten Enkeltrick-Betrug erkennen würden?

-2 -1 0 1 2

Sehr unsicher Sehr sicher

Die Betrüger durchsuchen Telefonbücher gezielt nach altmodischen Vornamen wie Klara, Hedwig oder Josef und täuschen beim Telefonat mit diesen Personen eine vermeintliche Verwandtschaft vor.

Beim Messenger-Betrug werden beispielsweise Telefonnummern genutzt, die bei Datenlecks von Unternehmen veröffentlicht werden. Um zu überprüfen, ob Nummern überhaupt vergeben sind, werden SMS mit einer Botschaft geschickt, die Interesse wecken soll. Mit einem Link, der beim Anklicken auf eine Webseite weiterleitet, wird den Betrügern bestätigt, dass diese Nummer aktiv verwendet wird.

Teilweise werden Nummern aber auch einfach ausprobiert. Das Profilbild lässt außerdem auch Rückschlüsse auf das Alter der Zielperson ziehen.

Maßnahmen, um sich gegen diese Betrugsmasche zu schützen:

- Name im Telefonbuch kürzen lassen
- Misstrauisch werden, wenn der Anrufer seinen Namen nicht sagen will und man ihn erraten soll und Sie außerdem um Geld bittet
- Codewort mit Angehörigen vereinbaren um sicherzustellen, dass man mit den echten Kindern oder Enkeln spricht/schreibt
- Unbekannte Nummern nicht sofort einspeichern
- In Messenger-Einstellungen lässt sich die Anzeige des Profilbildes auf die eingespeicherten Kontakte beschränken
- Sich durch einen Anruf versichern, dass man wirklich mit der Tochter/ dem Sohn spricht
- Nach veranlasster Überweisung sofort die Bank kontaktieren und eine Rücküberweisung veranlassen
- Chatverläufe nicht löschen, sind wichtig für die Kriminalpolizei
- Bei der Polizei Anzeige erstatten

11. Haben Sie oder jemand, den Sie kennen, in letzter Zeit etwas getan, um sich gegen den Enkeltrick-Betrug zu schützen?*

Wählen Sie eine Antwort

- Ja.
- Nein.

12. Wenn ja: welche Maßnahmen wurden ergriffen?

Schreiben Sie einen kurzen Text...

500

13. Sind Sie der Meinung, es wird genügend getan, die Öffentlichkeit über den Enkeltrick-Betrug aufzuklären und zu warnen?*

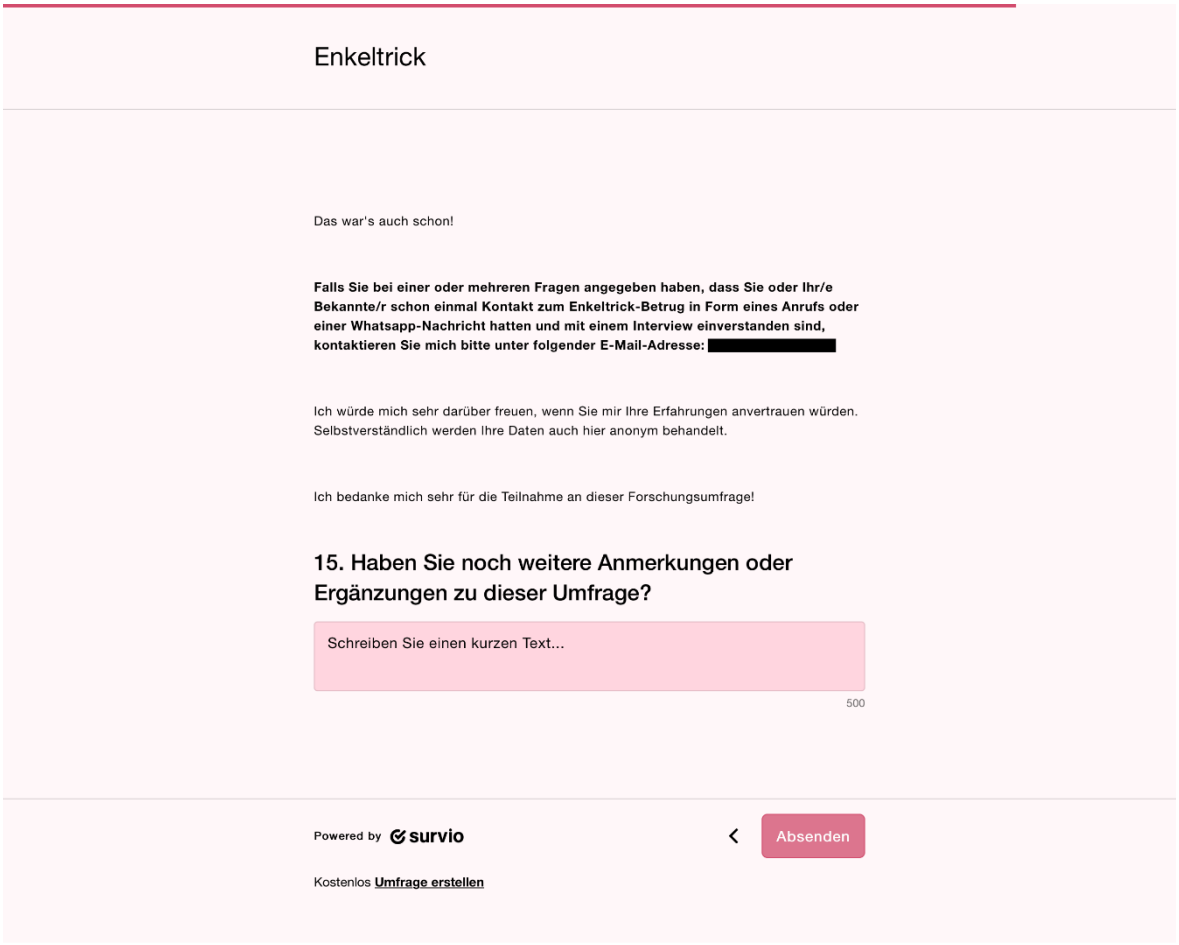
Wählen Sie eine Antwort

- Ja, finde ich schon.
- Nein, ich finde, es sollte deutlich mehr thematisiert werden.
- Keine Ahnung, ich habe mich mit diesem Thema noch nie genauer auseinandergesetzt.

14. Wie sollten Behörden und Medien zukünftig mehr Aufklärung zum Enkeltrick-Betrug leisten?*

Wählen Sie eine oder mehr Antworten

- Sensibilisierung in Schulen und Arbeitsplätzen
- TV- oder Radiospots mit Sicherheitshinweisen
- Whatsapp-Nachrichten an potenzielle Opfer mit Schutzmaßnahmen
- Sonstiges:



Enkeltrick

Das war's auch schon!

Falls Sie bei einer oder mehreren Fragen angegeben haben, dass Sie oder Ihr/e Bekannte/r schon einmal Kontakt zum Enkeltrick-Betrug in Form eines Anrufs oder einer Whatsapp-Nachricht hatten und mit einem Interview einverstanden sind, kontaktieren Sie mich bitte unter folgender E-Mail-Adresse: [redacted]

Ich würde mich sehr darüber freuen, wenn Sie mir Ihre Erfahrungen anvertrauen würden. Selbstverständlich werden Ihre Daten auch hier anonym behandelt.

Ich bedanke mich sehr für die Teilnahme an dieser Forschungsumfrage!

15. Haben Sie noch weitere Anmerkungen oder Ergänzungen zu dieser Umfrage?

Schreiben Sie einen kurzen Text...

500

Powered by survio

Absenden

Kostenlos **Umfrage erstellen**

Anlage, Teil 3: Interview-Fragebogen

1. Wie alt sind Sie? Wie alt waren Sie zum Zeitpunkt des Vorfalls? Kommen Sie aus Sachsen?

2. Wie würden Sie Ihren Charakter beschreiben? Würden Sie behaupten Sie sind eher ein schüchterner, introvertierter, ängstlich, emotionaler Typ?

3. Wie hat der Vorfall genau ausgesehen? Können Sie den Chatverlauf beschreiben? Gibt's einen Screenshot?

4. War Ihnen der klassische Enkeltrick bisher nur in Form des typischen Anrufes bekannt oder kannten Sie diese Vorgehensweise über WhatsApp auch schon?

5. Sind Sie an irgendeiner Stelle misstrauisch geworden? Kam Ihnen irgendetwas am Schreibstil komisch vor?

6. Wie war der Schreibstil der Nachricht?

7. Wie hätten Sie reagiert, wenn der Geldbetrag, der gefordert wurde um ein vielfaches höher gewesen wäre? Ab welchem Betrag hätten Sie gesagt, hier kann etwas nicht stimmen?

8. Was war das ausschlaggebende Merkmal, das Sie dazu gebracht hat, das Geld zu überweisen? (Bsp. Smileys oder einen Ausdruck, den nur Sie verwenden)

9. Wie viel Zeit lag zwischen Erhalt der Nachricht und der Überweisung? Haben Sie sofort überwiesen oder lagen dazwischen noch ein paar Stunden, in denen Sie Zeit zum darüber nachdenken hatten?

10. Wie war Ihre Gefühlslage zum Zeitpunkt der Nachricht/Überweisung? Falls Sie sich erinnern, waren Sie gestresst, traurig oder entspannt und glücklich?

11. Wann haben Sie von dem „Betrug" erfahren?

12. Wie haben Sie sich gefühlt, als Sie davon erfahren haben?

13. Was hat die Tat für emotionale und psychische Auswirkungen auf Sie?

14. Wie würden Sie heute reagieren, wenn Sie wieder so eine Nachricht bekämen?

15. Wie wirkt sich dieser Vorfall auf ihr weiteres Verhalten aus? Sind Sie vorsichtiger, wenn Ihnen fremde Nummern schreiben?

16. Wem hätten Sie sich anvertraut, wenn das kein Test und der Geldbetrag viel höher gewesen wäre?

17. Welche Langzeitfolgen glauben Sie, haben ältere Menschen, die auf diesen Trick reinfallen und teilweise ihre gesamten Ersparnisse verlieren?

18. Hätten Sie die Tat bei der Polizei angezeigt, wenn Ihnen nicht danach gesagt worden wäre, dass das ein Test war?

19. Warum hätten Sie die Tat angezeigt bzw. warum nicht?

20. Sind Sie der Meinung es wird genug Aufklärung geleistet?

21. Wie sollte mehr Aufklärung geleistet werden? Z.B.: TV- und Radiospots, Sensibilisierung in Schule und am Arbeitsplatz, etc.

Anlage, Teil 4: Interview-Transkript

Telefonisches Interview vom 26.07.2023

I: So. Also vielen Dank nochmal, dass Sie sich die Zeit genommen haben und auch äh sich bereit erklärt haben dieses Interview mit mir zu führen. Ähm zu Beginn, würden Sie mir bitte verraten, wie alt Sie sind? #00:14#

B: Fünfzig. #00:15#

I: Fünfzig, ok. Ähm und zum Alter des Zeitpunkts des Vorfalls also wie lange ist das schon her, wie alt waren Sie da? #00:22#

B: Äh da war ich noch 49 würd ich sagen (lacht) #00:26#

I: Also letztes Jahr war das, ok. #00:28#

B: Ja ja, das war letztes Jahr. #00:30#

I: Ok. Und Sie kommen auch aus Sachsen oder? #00:32#

B: Aus Sachsen-Anhalt. #00:33#

I: Aus Sachsen-Anhalt, alles klar. (…) Ok. Dann fangen wir schon an mit dieser Charaktereinschätzung, wie würden Sie sich denn beschreiben, würden Sie eher sagen Sie sind eher schüchtern oder introvertiert oder ängstlich, emotional oder eher das komplette Gegenteil? #00:54#

B: (…) Also (…) also wahrscheinlich nicht so nicht ganz überschwänglich, aber jetzt so schüchtern vielleicht auch nicht (…) ja, vielleicht schon eher zurückhaltender aber in manchen Situationen sicherlich auch sehr emotional, ja. #01:11#

I: Ok. (…) Ähm wie hat denn der Vorfall genau ausgesehen, also können Sie den Chatverlauf nochmal beschreiben oder gibt's sogar noch einen Screenshot davon? #01:21#

B: Ähm (…) da müsste ich tatsächlich gucken ob es einen Screenshot davon gibt, das kann durchaus sein. Ähm (…) dass ich das noch habe (…) ähm es war, also ich weiß, dass es eine stressige Situation war ich bin nämlich gerade zu Hause rein (…) hatte auch nicht viel Zeit, also es war wirklich Stress. Ähm und in dem Moment kriegte ich dann also von ja meiner vermeintlichen Tochter, (was ja in meinem Fall Gott sei Dank meine Tochter war) diese Anfrage mit diesem „Kannst du mal –„ wie man das so kennt, „Kannst du mal ganz schnell ähm das und das überweisen, ich hab ein neues Handy und rufe oder/ hab noch kein Vertrag oder/ rufe jetzt über ein Handy von einer Freundin an und ähm (…) praktisch dann per PayPal die Summe X (…) überweisen. Aber eben so (…) ja für mich ähm typisch meine Tochter, wie sie sich so ausdrückt, wie das alles so geschrieben war, deshalb bin ich auch so Null stutzig geworden ja, aber ich hatte auch keine Zeit darüber nachzudenken (lacht), weil ich schon gefühlt bei dem war, was ich als nächstes machen musste (…) und diese Sache so dringend klang. Und ich hab auch keinen Verdacht geschöpft, weil ich den Namen tatsächlich von der Freundin, die sie mir schrieb, den kannte ich. Und insofern hab ich also noch weniger Verdacht geschöpft. Ja (…) #02:51#

I: Das hätt ich Sie nämlich auch alles jetzt noch gefragt (lacht) #02:54#

B: Ah okay/ (lacht) #02:54#

55:I: (lacht) Also grade auch ähm wie Ihre Gefühlslage war, gerade, dass Sie Stress
56:hatten und so das passt alles. Okay. (lacht) Können Sie sich denn noch erinnern,
57:wie viel Bet/ also wie viel Euro Sie überweisen mussten, waren das //jetzt (..)
58:fünfzig Euro oder/ #03:10#
59:
60:B: Das// war nicht viel, das waren 35 Euro #03:11#
61:
62:I: 35 ok. #03:12#
63:
64:B: 35 (lacht) #03:13#
65:
66:I: Ok. (.) Ähm (..) und Sie sagen auch über PayPal #03:17#
67:
68:B: Genau, das war über PayPal ja. #03:19#
69:
70:I: Hm, weil das ist ja auch eigentlich relativ un(.)normal also viele Betrüger wollen
71:ja eher über Überweisung da/ da das schlechter zurückverfolgbar ist und auch
72:zurück äh // buchbar ist. Ok #03:32#
73:
74:B: Ja// #03:34#
75:
76:I: Ähm, genau das wollte ich Sie nämlich auch fragen (lacht), äh sind Sie an
77:irgendeiner Stelle misstrauisch geworden, kam Ihnen der Schreibstil irgendwie
78:komisch vor, aber Sie sagen, das war genau so wie sie sie kennen #03:44#
79:
80:B: (lacht) genau, genau der Schreibstil, den ich halt gewohnt war, ja das war also
81:alles so vertraut, deshalb bin ich so Null äh misstrauisch geworden, ja #03:54#
82:
83:I: Hat sie auch äh bestimmte Smileys benutzt oder irgendwelche/ #03:58#
84:
85:B: (atmet schwer) das, das könnt ich jetzt tatsächlich so äh spontan nicht sagen,
86:also ähm das müsste ich mir dann nochmal raussuchen (.) ähm nochmal gucken,
87:das das kann ich ja dann aber eventuell als Screenshot auch nochmal schicken 88:#04:11#
89:
90:I: Das wäre #04:13#
91:
92:B: Wenn ich (..) //wenn ich das finde, ja #04:14#
93:
94:I: das wär wirklich perfekt// wenn ich den Screenshot hätte. Ok. #04:15#
95:
96:I: Ähm (…) (sucht in Aufzeichnungen) Achso, kannten Sie denn den typischen
97:Enkeltrick vorher schon also nur jetzt / #04:25#
98:
99:B: Nein #04:26#
100:
101:I: Ne, also nur über Anruf oder auch jetzt die die WhatsApp-Vorgehensweise 102:nicht / #04:32#
103:
104:B: Überhaupt nicht #04:33#
105:
106:I: Überhaupt nicht, ok. #04:34#
107:
108:B: Gar nicht. Und ich habe, ich hab tatsächlich im Nachhinein das hab ich aber
109:letztens erst festgestellt, vor vielleicht 2 Monaten, ähm dass ich in meinem ähm
110:E-Mail äh Verkehr im Spam-Ordner ein oder zweimal solche E-Mails bekomme
111:habe. Mit genau so einem Wortlaut (..) das hab ich aber nicht mitgekriegt, weil
112:ich da eigentlich so nicht reingucke, ja. Ich hab bloß mal äh was gesucht, wollte
113:deshalb dort gucken ob das dort ist und ähm habe dann nur so auf die Schnelle
114:gesehen, dass da ein oder zweimal so eine Mail gekommen ist. #05:05#
115:
116:I: Ok (fragend) #05:06#

117:
118:B: Hm (bejahend) #05:08#
119:
120:I: Ähm, also Sie haben auch vorher überhaupt noch nichts von dem, von der
121:Bezeichnung „Enkeltrick“ gehört? #05:16#
122:
123:B: Nein //gar nicht #05:17#
124:
125:I: Ok // #05:17#
126:
127:B: Ähm ich hatte das dann auch ähm (.) wir hatten das auf Arbeit dann praktisch
128:ausgewertet und ich hab sozusagen meine Kollegen vorgewarnt und äh kurze
129:Zeit später ähm (..) war dann meine eine Kollegin auch die hat auch ne äh Anfr/
130:irgendwie sowas gekriegt #05:32#
131:
132:I: Ah ok #05:33#
133:
134:B: (…) Würd ich sagen die hat das nämlich auch erzählt also das kam dann
135:kurze Zeit später, eine Woche oder zwei Wochen später oder (.) so da hat sie
136:gesagt ähm Mensch hier ich hab hier auch sowas gekriegt. #05:45#
137:
138:I: (lacht) verrückt, also wie das zum gleichen Zeitpunkt dann kommen kann. 139:#05:51#
140:
141:B: Ja #05:51#
142:
143:I: Ähm (..) Wenn das jetzt ein höherer Geldbetrag gewesen wäre, hätten Sie an
144:irgendeiner Stelle gesagt, ok ab dem und dem Betrag wär ich misstrauisch
145:geworden oder hätt ich gesagt ‚Nein, also den Betrag den überweise ich dir so
146:jetzt nicht‘? #06:10#
147:
148:B: Hm (überlegt) das ka/ das kann ich nicht äh nicht wirklich sagen. Ich könnte
149:nicht sagen, ob ich ob ich misstrauisch gewesen wäre (..) ähm ich hätte
150:wahrscheinlich aber ich kann auch nicht sagen ab welchem Betrag dass ich
151:dann gesagt hätte jetzt muss ich aber erstmal wissen was sie damit vor hat
152:oderso, ja, aber ähm könnt ich nicht hundert Prozentig sagen. Ich könnte jetzt
153:auch nich/ nicht sagen ab welchem Betrag. #06:33#
154:
155:I: Hm (zustimmend), weil gerade 35 Euro sind eben auch, also da ist die
156:Hemmschwelle geringer da eher nein zu sagen #06:42#
157:
158:B: Ja #06:43#
159:
160:I: Ähm, hat ihre Tochter denn oder ist das normal oder was heißt normal also (..)
161:hat sie Sie schon öfter mal so über WhatsApp ähm nach Geld gefragt oder also
162:ist das (..) machen Sie das öfter so / #06:57#
163:
164:B: Nein/ #06:58#
165:
166:I: Weil es kann ja auch sein / nein? Ok #06:59#
167:
168:B: Hm hm (verneinend) Nein eigentlich nicht. Ähm (.) kam eigentlich noch nie
169:vor, wir hatten in letzter Zeit einmal so eine Situation, wo äh sie weil sie grad
170:umgezogen ist halt äh sie auf eine Dienstreise sollte ähm und dann da da hat sie
171:mich aber tatsächlich angerufen und hat mit mir gesprochen, ja aber da ging das
172:dann, also haben wir bis jetzt, bis dahin auch noch nie gehabt so. #07:24#
173:
174:I: Hm ok (zustimmend). (…) Ähm (…) wie viel Zeit lag denn zwischen dieser
175:Nachricht und auch der Überweisung also Sie haben ja gesagt sie waren im
176:Stress also haben sie es relativ zeitnah dann gemacht oder #07:37#
177:

178:B: Ich hab das würd ich sagen innerhalb von fünf Minuten gemacht, ja. (..) Weil
179:wie gesagt ich war im Stress (lacht) ich weiß nicht mehr was ich hinterher gleich
180:machen musste, aber ähm da hatte sie mich wirklich in so einer Situation
181:erwischt wo ich äh (.) wo ich echt im Stress war #07:55#
182:
183:I: Vielleicht wusste sie das ja sogar (lacht) und hat das gleich mit ausgenutzt 184:#07:57#
185:
186:B: Weiß ich nicht (..) das ist möglich (lacht) #07:59#
187:
188:I: Ok. (..) Ähm (…) Ja gut, die Frage hatten wir jetzt schon beantwortet, ob Sie
189:gestresst waren ähm (…) wie haben Sie sich denn gefühlt, als Ihre Tochter dann
190:erzählt hat, dass es bloß ein Test war? #08:16#
191:
192:B: Naja erstmal hat sie mich ja hinterher angerufen und äh dann hab ich sie
193:gefragt ob das Geld angekommen ist und dann hat sie natürlich äh mich erstmal
194:so ganz ganz eiskalt auflaufen lassen mit ‚Welches Geld', ‚Was? Ich hab dich
195:nicht angeschrieben" da ist mir in dem Moment äh Himmel, Angst und Bange
196:geworden, irgendwas stimmt hier nicht, ja. Da ist mir schon komisch geworden
197:ähm (..) das war eine blöde Sit/ sie hats dann relativ schnell aufgeklärt aber
198:man/ ich muss sagen ähm (.) das war ein komisches Gefühl, dass man da so
199:doch relativ leicht drauf reingefallen ist. Weil ich immer gesagt hätte bei dem was
200:man so hört und liest im Fernsehen oder in Medien oder den Zeitungen, das ist
201:ja so offensichtlich, da kann man doch nicht drauf reinfallen, ja #09:10#
202:
203:I: Ja, man denkt immer man selber würde nie drauf reinfallen #09:13#
204:
205:B: Genau, genau. Ja also wenn man das so erzählt bekommt sagt man ‚Das ist
206:doch aber so plausibel, so offensichtlich' ja, und ich hätte meine Hand dafür ins
207:Feuer gelegt, dass ich auf sowas nicht reinfalle, ja. (..) Und das ist dann schon
208:eine komische Situation und man fühlt sich wirklich nicht gut danach ja also. (..)
209:Bei mir waren es nur 35 Euro aber hätte man über eine andere Summe geredet,
210:wär das ja wahrscheinlich nochmal was anderes gewesen ja #09:37#
211:
212:I: Hm wie/ #09:40#
213:
214:B: Aber ich habs ja auch wieder gekriegt ja also/ (lacht) #09:41#
215:
216:I: Achso ok (lacht) das ist schon mal gut #09:45#
217:
218:B: Ja sie hat mir das zurücküberwiesen (lacht) #09:46#
219:
220:I: Wie würden Sie denn heute reagieren, wenn Sie wieder so eine Nachricht
221:bekommen würden von einer fremden Nummer? #09:54#
222:
223:B: Ähm ich glaub ich würd sie einfach ignorieren (.) ja #09:58#
224:
225:I: Also Sie haben sich quasi direkt danach erstmal mit der Masche richtig
226:auseinandergesetzt, sich informiert/ #10:05#
227:
228:B: Ja, ja und man hat auch, also was ich vorher auch überhaupt nicht registriert
229:hab, dadurch dass man äh sich tatsächlich über diese Aktion mit einigen
230:unterhalten hat ja, hat man erstmal mitbekommen ähm dass einigen tatsächlich
231:das auch schon passiert ist ja, also das war jetzt gar nicht so unbekannt. Für
232:mich war es total unbekannt, aber ich hab dann hinterher festgestellt, dass das
233:äh doch schon eine ganze Weile gelaufen sein muss, ja #10:34#
234:
235:I: Genau, also ich hab das auch immer bloß im Bekanntenkreis mitbekommen,
236:hier und da hat mal jemand so eine WhatsApp Nachricht bekommen und da man
237:das aber irgendwo bekannt war, dass die immer gleich vorgehen hat halt auch
238:niemand mal drauf reagiert sondern/ also da waren schon Leute bekannt, die so

eine Nachricht bekommen haben aber nie jemand der wirklich Geld verloren hat, ne, das ist mir eben auch aufgefallen. (.)
Also Sie haben dann auch wirklich mit Bekannten, äh Kollegen und so darüber gesprochen und da haben Sie festgestellt, dass das schon vielen Leuten auch passiert ist. #11:14#

B: Ja (... unverständlich durch Verbindungsabbruch) #11:18# Kollegin ja auch (unverständlich) #11:19# das ist ja auch schon irre ja, dass nun ausgerechnet der Zufall das so wollte. Hm ja. #11:25#

I: Ähm, wem hätten Sie sich denn anvertraut, vielleicht können Sie sich darein versetzen, wenn ihre Tochter das nicht aufgelöst hätte, wem hätten sie sich anvertraut? Weil gerade viele ältere Leute, die schämen sich da innerhalb selbst der Familie sich an Enkel oder Kinder zu/ #11:42#

B: Ne also ich denke ich hätte mich an meinen Mann gewa/ also mit meinem Mann hätte ich das erstmal besprochen ja #11:47#

I: Hm (zustimmend) (…) Ok. Ähm, ich weiß ja nicht in welcher Branche/ also es kann ja sein, dass Sie zum Beispiel in der Pflege oder im Altersheim arbeiten und mit älteren Leuten zu tun haben, denen das auch passiert sein könnte, aber was denken sie denn welche Langzeitfolgen das auf ältere Menschen haben kann? Gerade wenn sie eben auch ihre ganzen Ersparnisse verlieren? #12:15#

B: Naja ich denke schon also ähm ich hab schon mit älteren Leuten zu tun, ich bin jetzt nicht in der Pflege ich bin in einer Arztpraxis, wo wir auch ältere haben, und ich denke mal dass die ähm dass das wahrscheinlich für die dann sehr schwierig ist damit dann umzugehen ja, weil ähm die haben ja äh doch sich das ihr Leben lang alles bitter zusammengespart und vielleicht so ein paar Euros zusammengespart für die Rente oder damit sie sich mal was leisten können ja und wenn das das alles weg ist und man nix wiederkriegt und man kriegt ja in den meisten Fällen nix wieder, das ist schon bitter, ich kann mir schon vorstellen, dass da viele wirklich lange dran zu knabbern haben ja (..) und kann mir auch vorstellen, dass gerade wenn man noch älter ist 70, 80 dass man vielleicht auch Angst hat sich überhaupt wem anzuvertrauen #13:01#

I: Ja (zustimmend) Das zeigt eben auch dass gerade auch diese Hilfsorganisationen, an die ich mich gewandt habe die haben alle kein Kontakt bisher mit Enkeltrickopfern gehabt, WEIL sich eben viele oder fast alle davor scheuen sich auch zu öffnen jemanden, gerade auch Experten eigentlich, was ja eigentlich verrückt ist, weil dafür sind die ja da, und trotzdem haben die Scheu sich da an so jemanden zu wenden also es ist schon krass. #13:29#

B: Das stimmt schon, ja ja ja das denk ich auch, dass ist sicherlich schwierig ja (..) wobei ich denke wenn es bei mir wenn es wirklich so gewesen wäre und wir eine größere Summe verloren hätten, dann hätt ich mich schon sicherlich auch an die Polizei gewandt ja, dass man dann versucht da irgendwie äh Anzeige zu erstatten, was wieder zu bekommen wie auch immer man hat ja jetzt auch keine Erfahrung wie ähm wie das so läuft, man hörts meistens dann nur in den Medien, dass man eben kaum eine Chance hat irgendwas wiederzubekommen ja aber ich denke schon, dass ich mich dann an die Polizei gewandt hätte #14:00#

I: Hm (zustimmend) Das wäre jetzt meine nächste Frage gewesen (lacht), ob Sie die Tat angezeigt hätten //ähm und/ #14:07#

B: Ja das glaub ich, also doch// #14:09#

I: Also auch obwohl Sie wussten oder ge/ jetzt wüssten, dass da die Erfolgschance eh gering ist hätten sie es trotzdem angezeigt? #14:17#

299:
300:B: Ja, ja, weil ich auch immer denke, je mehr sowas angezeigt wird, desto eher
301:hat man da eine Chance da überhaupt wem auf die Schliche zu kommen ja und
302:äh je weniger das bekannt wird, ich meine/ irgendwann denkt man machen sie ja
303:alle mal Fehler oder die Technik geht weiter oder man erwischt da doch mal
304:irgendwen ja, also ich denke schon dass ich das gemacht hätte, auf alle Fälle,
305:doch #14:38#
306:
307:I: Ok. (…) #14:43#
308:
309:I: #15:02# Und ähm was denken Sie denn also dadurch dass sie ja davor noch
310:nichts gehört haben davon finden sie, dass da mehr aufgeklärt werden sollte?
311:Also ich denke mal man kann nie genug aufklären aber wenn sie tatsächlich
312:davor noch nichts davon gehört haben ähm muss ja auf jeden Fall mehr
313:aufgeklärt werden oder? #15:23#
314:
315:B: Ja, also ich wie gesagt im Nachhinein hab ich dann schon ab und an mal was
316:mitbekommen äh dann hab ich jetzt auch mal irgendwo gelesen oder in den
317:Med/ aber das kam alles wirklich erst später, es kam auch nicht dann zeitgleich,
318:kurz danach oder so, aber irgendwann später hab ich schon mal was da drüber
319:auch ähm so aus den Medien gehört, aber so richtig viel (…) nicht. Also ich
320:denke schon dass man über diese ganzen Tricks immer mal so Sendungen oder
321:Berichte oder sowas bringen sollte, einfach um die Leute wieder zu
322:sensibilisieren, denn man lässt sich ja immer was neues einfallen, es ist immer
323:ausgewiefter irgendwo ja immer irgendwie authentischer auch so, weil die sind ja
324:manchmal auch nicht auf den Kopf gefallen und äh lassen sich da ja schon keine
325:schlechten Sachen einfallen #16:13#
326:
327:I: Ja, gerade auch mit dem/ #16:14#
328:
329:B: Schon sobald sowas bekannt wird müsste man eigentlich wirklich über die
330:Medien gehen und die Leute sensibilisieren. #16:21#
331:
332:I: Ja (zustimmend) Ok also sie sagen gerade über die Medien sollte mehr
333:passieren, gerade Fernsehen, Radio, alles auch was vor allem ältere Leute auch
334:erreicht, also es nützt nix/ #16:32#
335:
336:B: Genau, Fernsehen, Radio, das ist ja das was so bei den doch äh der ganz
337:alten Generation äh noch am meisten ankommt. #16:43#
338:
339:I: Hm (zustimmend), (.) ok aber es ist ja eigentlich auch wichtig ähm gerade so
340:über ähm zum Beispiel in der Schule schon oder aufm Arbeitsplatz/ #16:54#
341:
342:B: Ja/ #16:54#
343:
344:I: Gerade auch die jüngere Generation zu sensibilisieren, dass auch (…) die mit
345:ihren Familien darüber sprechen und die da darüber nochmal aufklären, falls/ es
346:kann ja trotzdem Leute geben, die weder Fernsehen gucken, noch Radio hören
347:äh dass die abgesichert sind dass die innerhalb der Familie dann aufgeklärt
348:werden. #17:14#
349:
350:B: Ja das stimmt wobei ich denke, dass ja einfach ähm das Format Schule äh
351:irgendwie da nicht erreichen ja, ähm ich habe immer den Eindruck in den
352:Schulen also das war früher alles ein bisschen anders, früher wars noch ein
353:bisschen persönlicher, da hat man auch über andere Sachen noch geredet, nicht
354:nur über den Lernstoff so ähm (.) es bleibt vieles auf der Strecke in den Schulen
355:und da ist nicht mehr viel Zeit für (.) für solche Sachen habe ich immer so den
356:Eindruck #17:45#
357:
358:I: Ja, ja also kann ich aus Erfahrung sprechen, ja #17:48#

359:
360:B: Ja also diese alltäglichen Sachen eigentlich was vielleicht eben wirklich auch
361:mal wichtig wäre. Ich finde, dass wenn die Kinder heute aus den Schulen
362:kommen, ähm sie nicht wirklich auf das Leben vorbereitet sind, auf das
363:Alltagsleben ja (lacht). Vollgestopft mit Wissen, aber vom Alltag her ist man da
364:ganz weit von entfernt. Das hab ich zumindest ähm bei meiner großen (Tochter)
365:auch gesehen, ähm die dann auch gesagt hat, ich hab gar keine Ahnung wie ist
366:das was bräu/ Versicherung wie geht das jetzt hier überhaupt alles'. Man hat
367:keine Ahnung davon ja, darum sag ich, egal ob das solche Sachen sind, die
368:Sensibilisierung für solche Themen oder Alltagsthemen, das hat in den Schulen
369:überhaupt keinen Platz mehr, das ist ein bisschen schade ja #18:33#
370:
371:I: Hm (zustimmend) das stimmt auf jeden Fall. (…) Ok, dann sind wir sogar
372:schon am Ende der Umfrage (lacht) //oder des Interviews eher #18:44#
373:
374:B: Okay (lacht) #18:43#
375:
376:
377:I: Dann bedanke ich mich recht herzlich! #18:48#

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 14.08.2023

Marie Köhler