Betrug-sprävention

Toolbox

Reihe Nr 13

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

eu2018bg.bg
Българско председателство на Съвета на Европейския съюз

“

Individual fraud is
a type of fraud in which individual citizens are being targeted by criminals and are persuaded into a cooperative mindset. The essential tactic to nudge the victim into this compliant relationship is called social engineering. This allows the offender to obtain the confidence from the victim that is crucial to the success of the scam.

“

DANKSAGUNGEN

Diese Toolbox wurde in enger Zusammenarbeit zwischen dem EUCPN-Sekretariat und der bulgarischen Präsidentschaft entwickelt. Wir möchten ihnen für ihre Bemühungen während ihrer Präsidentschaft und die Organisation eines Seminars über Telefonbetrug danken.

Darüber hinaus möchten wir allen nationalen Vertretern, Stellvertretern und akademischen Kontaktstellen des EUCPN für ihre kontinuierliche Unterstützung unserer Arbeit, für den Austausch ihres Fachwissens und die Bereitstellung von Informationen für diese Toolbox danken.

Unser besonderer Dank gilt den Experten, die bereit waren, an dem Workshop teilzunehmen, den wir im Zusammenhang mit dieser Toolbox organisiert haben:

- Mark Button, University of Portsmouth, Vereinigtes Königreich
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Abteilung Betrug in der Generaldirektion der nationalen Polizei, Bulgarien
- Charlotta Mauritzson, Nationales Betrugszentrum, Schweden
- Andries Bomans, Zentrum für Cybersicherheit, Belgien
- Constantin Lica, Abteilung Betrugsbekämpfung, Rumänien
- Aurelian Bocan, Generaldirektion der Polizei Bukarest, Rumänien
- Romana Mazalová, Projekt „Nedáme se“, Tschechien

Zitat
EUCPN (2018). EUCPN Toolbox Serie Nr. 13 Prävention von Einzelbetrug. Brüssel

Rechtlicher Hinweis
Der Inhalt dieser Veröffentlichung spiegelt nicht unbedingt die offizielle Meinung eines EU-Mitgliedstaates oder einer Behörde oder Institution der Europäischen Union oder der Europäischen Gemeinschaft wider.

Autoren/Redakteure
Jorne Vanhee, Research Officer, EUCPN-Sekretariat, Brüssel, Belgien
Febe Liagre, Strategy and Policy Officer, EUCPN-Sekretariat, Brüssel, Belgien

Im Rahmen des Projekts „The further implementation of the MAS of the EUCPN and the Informal Network on the Administrative Approach“ - EUCPN-Sekretariat, November 2018, Brüssel

Mit finanzieller Unterstützung des Programms der Europäischen Union zur Prävention und Bekämpfung von Kriminalität
Europäische Kommission - Generaldirektion Innere Angelegenheiten

INHALTSVERZEICHNIS

Danksagungen 3

Vorwort 6

Zusammenfassung 8

01

Einführung 14

Informationsbild 18

1. Einführung ... 18
2. Die Kunst der Überredung ... 22
3. Suchen Sie sich Ihren Betrug aus ... 32
4. Die Zahlen ... 42
5. Schlussfolgerungen ... 48

02

Bewährte Praktiken 50

1. Einführung ... 51
2. Wenn es zu schön erscheint, um wahr zu sein, dann ist es das wahrscheinlich ... 56
3. Verhindern von Telefonbetrug: Wie kann ich Ihnen helfen? ... 63
4. Schlussfolgerungen ... 68

03

Beispiele aus der Praxis 70

„Enkeltrick - schon mal davon gehört?“ (AT) 70
Hallo Oma, ich brauch Geld (DE) 71
Silver Surfer (LU) 73
Versuch nicht, mich für dumm zu verkaufen (SE) 74
Österreich: Watchlist Internet 75
Abteilung Betrug in der Generaldirektion der nationalen Polizei (BG) 76
Betrugsbekämpfungs mechanismus First Investment Bank Bulgaria (BG) 77
#CyberScams (EC3, Europol) 77
Wie phishing-sicher sind Sie? (BE) 78
Nedáme se (Das lassen wir uns nicht gefallen) (CZ) 79
Der Preis der Freundschaft (RO) 79
Sicherheitsleitfaden für Senioren (FI) 80
„Tricks gegen Überredungstricks“ (NL) 81
Action Fraud (UK) 81

Endnotes 82

Referenzen 83

VORWORT

Die 13. Toolbox in der vom EUCPN-Sekretariat veröffentlichten Reihe konzentriert sich auf das Hauptthema der bulgarischen Präsidentschaft: Betrug mit besonderem Fokus auf Telefonbetrug. Da Betrug ein breites Themenspektrum abdeckt, haben wir beschlossen, uns auf Einzelbetrug zu konzentrieren. Dabei handelt es sich um Betrugsfälle, die von Einzelpersonen oder kriminellen Organisationen an Einzelpersonen begangen werden. Zunehmend ist diese Art von Betrug zu einer profitablen und grenzüberschreitenden Aktivität geworden, einige Wissenschaftler bezeichnen diese Straftäter sogar als „Scampreneurs“ (Scam-Unternehmer). Daher verdient diese Art von Kriminalität einen EU-weiten Ansatz. Dies wird auch in dem Strategiepapier deutlich, das parallel zu dieser Toolbox verfasst wird.

Diese Toolbox besteht aus drei Teilen. Im ersten wird versucht, das aktuelle Aufklärungsbild über individuelle Betrugsfälle darzustellen. Im zweiten Teil diskutieren wir interessante bewährte Praktiken und geben auch einige Empfehlungen, wie man Telefonbetrug verhindern kann. Diese bewährten Verfahren werden im dritten Teil aufgeführt. Eine Zusammenfassung wird dem Leser ebenfalls zur Verfügung gestellt.

ZUSAMMENFASSUNG

Die 13. Toolbox in der vom EUCPN-Sekretariat veröffentlichten Reihe konzentriert sich auf die Prävention von *Einzelbetrug.* Die bulgarische Präsidentschaft (erstes Halbjahr 2018) beschloss, sich auf Folgendes zu konzentrieren:

> „[...] *Betrugsfälle, insbesondere Telefonbetrug. Diese Art von Kriminalität ist in den letzten Jahren zu einer profitablen kriminellen Aktivität geworden, die sich sowohl auf nationaler als auch auf grenzüberschreitender Ebene entwickelt. Kriminelle Gruppen, die sich auf diese Tätigkeit spezialisiert haben, entwickeln sich dynamisch und treffen ein breiteres Spektrum von Opfern. Angesichts der aktiven Beteiligung der Opfer und ihrer Einbeziehung in kriminelle Szenarien und der traumatisierenden Wirkung auf die Opfer müssen ernsthafte Präventivmaßnahmen ergriffen werden, wobei die Besonderheiten auf lokaler, nationaler und grenzüberschreitender Ebene zu berücksichtigen sind*".

Beim Einzelbetrug werden einzelne Bürger von Kriminellen ins Visier genommen. Die Opfer werden zu einer kooperativen Einstellung überredet und anschließend betrogen. Unser heutiges Verständnis dieser Art von Betrug hängt hauptsächlich mit ihren zeitgenössischen Formen zusammen, wobei Phishing das wahrscheinlichste Beispiel ist. Es ist jedoch wichtig zu erkennen, dass es Einzelbetrug seit langem gibt. Die technologischen Entwicklungen der letzten Jahrzehnte haben es nur ermöglicht, diese Betrügereien in einem Umfang zu industrialisieren, den man nie für möglich gehalten hätte. Wer hat in seinem Leben noch keine Phishing-E-Mail erhalten?

Wie aus der *Grundüberlegung* der bulgarischen Präsidentschaft hervorgeht, sind die Opfer aktiv an ihrer Viktimisierung beteiligt. Der Täter hat das Geld des Opfers im Visier, aber er kann nur dann Zugang zu ihm erhalten, wenn er das Opfer überzeugt. Die wesentliche Taktik, das Opfer in diese konforme Beziehung zu drängen, nennt man **Social Engineering**. Dies ermöglicht es dem Täter, das Vertrauen des Opfers zu gewinnen, was für den Erfolg des Betrugs entscheidend ist. Die Sozialpsychologie bietet uns ein besseres Verständnis dieses Phänomens. Indem sie an alltägliche soziale Prinzipien appellieren und diese „menschlichen Schwächen" ausnutzen, sind Täter in der Lage, den sogenannten zweiten Weg der Überzeugung zu aktivieren. Der erste Weg erfordert viel Überlegung und

kognitive Anstrengung. Der zweite erfordert jedoch keinen wirklichen Aufwand und reagiert fast unbewusst. Indem sie sich beispielsweise als Autoritätsperson, etwa als Polizist ausgeben, können die Täter bei ihren Opfern leicht ein gewisses Maß an Gehorsam erreichen. Diese sozialen und kognitiven Faustregeln haben ihren alltäglichen Nutzen, erlauben es aber den Tätern, sie zu ihrem eigenen Vorteil zu nutzen.

Diese irreführenden Taktiken werden bei einer **Vielzahl von Betrügereien** eingesetzt. *419 Scams, Enkeltricks, Romance Scams, CEO Fraud usw.,* die Möglichkeiten sind so vielfältig wie die Kreativität der Betrüger. Das Spektrum der Täuschungen ermöglicht es Betrügern, eine sehr große Öffentlichkeit gleichzeitig anzuvisieren oder einen stärker individualisierten Ansatz zu verfolgen. In zunehmendem Maße scheint Letzteres der Fall zu sein. Betrüger haben erkannt, dass durch die geschickte Fokussierung auf ihre Opfer ihre „Investitionsrendite“ höher ist. Phishing-E-Mails werden immer ausgefeilter und richten sich an ein(e) ausgewählte(s) Ziel(Gruppe). Der überraschende letzte Schritt in dieser Entwicklung ist die Kombination aus neuer und älterer Technologie: die Benutzung des Telefons. Vishing oder Voice Phishing bietet die Möglichkeit, die Vorteile von Internet und Telefon zu kombinieren. Ein Online-Telefonat ist fast kostenlos, ist schwieriger zu verfolgen und kann automatisiert werden. Die Nutzung des Telefons hat zusätzliche Vorteile: Die Menschen vertrauen ihm mehr und aufgrund der intimeren Umgebung werden die Opfer effizienter überzeugt. Zur Veranschaulichung des wachsenden Niveaus der Raffinesse: Täter werben sogar Muttersprachler an, damit die Telefonate möglichst echt wirken.

Unser derzeitiges Verständnis von individuellem Betrug ist jedoch begrenzt. Die **Dunkelziffer** bei dieser Art von Kriminalität ist enorm, da so viele Fälle nicht gemeldet werden. Die Opfer wissen nicht, dass sie Opfer geworden sind, sie empfinden es nicht als schwerwiegend genug, sie glauben nicht, dass eine Anzeige etwas bringen wird, oder sie wissen einfach nicht, wo sie überhaupt Anzeige erstatten sollen. Darüber hinaus halten Gefühle der Selbstbeschuldigung und des Schams die Opfer aufgrund der aktiven Rolle, die das Opfer bei seiner eigenen Viktimisierung spielt, davon ab, ihre Geschichte zu erzählen. Einige Betrügereien haben sogar „eingebaute“ Mechanismen zur Verhinderung einer Anzeige, da die Opfer im Rahmen des Betruges illegale Handlungen vornehmen müssen und sich dabei selbst belasten. Den Betrug zu melden, würde sich so anfühlen, als würde man sich selbst anzeigen.

Diese Dunkelziffer führte auch zum dem **Mythos**, dass ältere Menschen die Hauptopfer dieses Verbrechens sind, da sie leichte Beute sind. Einige Studien haben diesen Mythos widerlegt, obwohl wir aufgrund der begrenzten verfügbaren Erkenntnisse vorsichtig bleiben sollten. Dennoch wird berichtet, dass die jüngere Bevölkerung und die Gruppe mittleren Alters anfälliger für Betrug sind. Ein weiterer Mythos ist, dass Opfer typischerweise als ungebildet oder in Finanzdingen uninformiert dargestellt werden, aber das Gegenteil scheint der Fall zu sein. Eine mögliche Erklärung ist die so genannte Kluft zwischen Wissen und Handeln, bei der es gelingt, die Signale eines Betrugs zu erkennen, dieses Wissen aber nicht auf die eigene Situation angewandt wird.

Leider ist die Existenz so genannter „**Sucker Lists**“ (Trottel-Listen) kein Mythos. Telefonbetrüger können ihre Opfer zufällig kontaktieren oder aus öffentlichen Verzeichnissen wählen, aber sie geben auch Listen bereits betrogener Opfer untereinander weiter. Die Verwendung solcher Listen ist ein Hinweis auf das hohe Maß an wiederholter Viktimisierung. Zum Beispiel versuchen einige Betrüger, Ihnen zu „helfen“, Ihr verlorenes Vermögen wiederzuerlangen...

Da die polizeiliche Überwachung dieser Kriminalität äußerst schwierig ist, ist der Präventionsbedarf hoch. Es wurden jedoch nur wenige akademische und evaluative Untersuchungen über individuellen Betrug durchgeführt. Dennoch können wir einige allgemeine Ergebnisse vermelden. Die verbreitetste Präventionstaktik ist die Aufklärung der Öffentlichkeit. Dies kann in einer allgemeinen Sensibilisierungskampagne geschehen, aber vor allem, wenn sie in einer Art Trainingsformat durchgeführt wird, sind einige positive Effekte zu verzeichnen. Im Wesentlichen wird mit diesen Schulungen versucht, die bereits erwähnte Kluft zwischen Wissen und Handeln zu schließen. Eine weitere wichtige Taktik ist die Arbeit mit den Opfern. Aufgrund ihrer aktiven Rolle und der bestehenden Gefahr, mehrfach Opfer zu werden, sollten die Opfer unterstützt und auf ihre besondere Position aufmerksam gemacht werden.

Während der bulgarischen Präsidentschaft hat das Sekretariat eine Reihe von **bewährten Praktiken** zu diesem Thema gesammelt. Diese können nach ihrer Zielgruppe kategorisiert werden. Eine erste Kategorie konzentriert sich auf die gesamte Bevölkerung. Dabei handelt es sich um Sensibilisierungskampagnen, wie die Beispiele aus Bulgarien, Schweden, Belgien oder von Europol. Dazu gehören Radiospots, Poster, Flyer, Gadgets usw., die der Öffentlichkeit nützliche Informationen liefern und zeigen, wie man sich vor Schaden schützen kann. Eine zweite Reihe von Aktivitäten richtet sich an ältere Menschen. Hier werden mehr

interaktive Methoden eingesetzt, wie dies in der Tschechischen Republik der Fall ist. Ältere Menschen nehmen an einem interaktiven lehrreichen Theaterstück teil, in dem sie die gängigsten Täuschungsmodelle kennenlernen und darauf reagieren können. Diese „gelebte Erfahrung“ soll es ihnen ermöglichen, in realen Szenarien angemessen zu reagieren. Die Bewertung dieses Projekts bewies die Richtigkeit dieser Annahme, da die Gruppe vorgetäuschte Deals zweieinhalb Mal häufiger ablehnte als eine Kontrollgruppe, die das Stück nicht sah. Die letzte Kategorie der Präventionsmaßnahmen konzentrierte sich auf die Opfer. Beispiele aus Australien, Großbritannien und Kanada zeigten, dass diese Art der Prävention notwendig ist. Es gibt jedoch - auch weltweit - nur wenig Unterstützung für Opfer von Einzelbetrug.

Zu guter Letzt organisierte das EUCPN-Sekretariat einen Workshop mit verschiedenen Experten, um einige **Empfehlungen** zur Prävention von Telefonbetrug zu entwickeln. Diese sind nach den fünf Strategien der situativen Kriminalprävention gegliedert. Die erste mögliche Strategie ist, den Aufwand zu erhöhen, den ein Täter auf sich nehmen muss, damit der Betrug erfolgreich ist. Dies kann bereits durch die Beschränkung der Veröffentlichung und des Zugangs zu Telefonnummern erreicht werden. Eine andere Technik könnte darin bestehen, die Anzahl der Telefonnummern zu begrenzen, die eine Person haben darf, oder diese zumindest mit einem Bankkonto oder einer ID-Nummer zu verbinden.

Eine zweite Strategie ist die Erhöhung der Risiken. Dabei ist der Informationsaustausch von zentraler Bedeutung. Dieser Austausch sollte nicht an den Grenzen des öffentlichen oder privaten Sektors oder auf nationaler Ebene enden. Jeder Partner hat ein wichtiges Teil zum Füllen des Informations-Puzzles. Zu wissen, womit man es zu tun hat, erhöht die Chancen, dass es überhaupt nicht passiert. Es versteht sich von selbst, dass die Erstattung einer Anzeige einfacher und zugänglicher gestaltet werden sollte. Informationen müssen gesammelt werden, bevor sie weitergegeben werden können. Weitere Empfehlungen wurden ausgesprochen, die Anonymität des Anrufers zu verringern, indem es ihm nahezu unmöglich gemacht wird, seinen Standort zu verschleiern. Spracherkennungssoftware könnte hier ebenfalls von Interesse sein.

Die Reduzierung des Lohns, der sich durch die Begehung dieses Verbrechens erzielen lässt, ist eine dritte Strategie zur Verhinderung von Telefonbetrug. Die Beschlagnahme der illegal erworbenen Vermögenswerte ist hier die wichtigste Empfehlung. Um dies zu erreichen, ist die Überwachung des Geldflusses entscheidend, um verdächtige Transaktionen zu erkennen. Eine EU-weite Initiative

mit dem Bankensektor zur Unterstützung wurde von unseren Experten empfohlen.

Eine weitere Strategie besteht in der Reduzierung von Provokationen. In diesem Zusammenhang ist es wichtig, nicht zu viele Informationen darüber weiterzugeben, wie der Betrug tatsächlich ausgeführt wurde, da dies Nachahmungen verhindert. Es könnte auch dazu beitragen, einige Formen der wiederholten Viktimisierung zu verhindern.

Die letzte Strategie bestand in der Beseitigung der Rechtfertigungen. Dabei geht es vor allem darum, das Bewusstsein für Telefonbetrug und Selbstschutz zu schärfen. Frühere sinnvolle Praktiken werden hier als wichtige Beispiele angeführt. Sensibilisierungskampagnen sollten die gleiche Botschaft verbreiten. Daher müssen öffentlich-private Partnerschaften und internationale Zusammenarbeit so kohärent wie möglich gestaltet werden: *Sag einfach nein.*

EINFÜHRUNG

Es mangelt nicht an Beispielen betrügerischer Machenschaften von Kriminellen, die versuchen, an hart verdientes Geld und/oder persönliche Informationen zu kommen, und auch nicht an Menschen, die auf sie hereinfallen (Crosman, 2017). Wer fand noch nie das „einmalige Angebot“ in seinem E-Mail-Posteingang oder hat nicht von dem Microsoft-Support-Betrug gehört, bei dem Sie angerufen werden, um Ihren Computer reparieren zu können, der eben noch problemlos funktioniert hat?

Entgegen der landläufigen Meinung sind diese Arten von Betrügereien alles andere als neu. Gaunereien und Betrug gibt es schon seit Jahrhunderten (Murphy & Murphy, 2007). Das heutige Verständnis von persönlichem Betrug ist untrennbar mit neuen Technologien wie dem Internet verbunden, aber Betrug gibt es, seit der Menschen sprechen kann und Vermögen besitzt (Button & Cross, 2017). Tatsächlich hat das Internet einen neuen Raum für Kriminelle geschaffen, um eine viel größere Zahl von Opfern zu betrügen, als je für möglich gehalten wurde (Whitty, 2013). Neue und ältere Technologien wie das Telefon werden kombiniert, um Angriffe gezielt durchzuführen und den Gewinn zu maximieren. Umfang und Effektivität haben zugenommen, die Kosten sind gesunken, aber die Kerntechniken sind die gleichen (Crosman, 2017; Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Diese neuen Entwicklungen, kombiniert mit den negativen Auswirkungen - finanziell, emotional, relational,... – diese Arten von

„Im Kontext der Prävention wird sich der bulgarische Vorsitz auf betrugsbezogene Fragen, insbesondere auf Telefonbetrug, konzentrieren. Diese Art von Kriminalität ist in den letzten Jahren zu einer profitablen kriminellen Aktivität geworden, die sich sowohl auf nationaler als auch auf grenzüberschreitender Ebene entwickelt. Kriminelle Gruppen, die sich auf diese Tätigkeit spezialisiert haben, entwickeln sich dynamisch und treffen ein breiteres Spektrum von Opfern. Angesichts der aktiven Beteiligung der Opfer und ihrer Beteiligung an kriminellen Szenarien und der traumatisierenden Wirkung auf die Opfer müssen ernsthafte Präventivmaßnahmen ergriffen werden, wobei die Besonderheiten auf lokaler, nationaler und grenzüberschreitender Ebene zu berücksichtigen sind.“

Kriminalität haben (Button, Lewis, & Tapley, 2009; 2014) die Notwendigkeit der Prävention deutlich gemacht, und Bulgarien hat dies während seiner EUCPN-Präsidentschaft in der ersten Jahreshälfte 2018 als Schwerpunkt gewählt:

Diese Toolbox bietet nützliche Erkenntnisse über diese Art von Betrug und Gaunereien und deren Prävention. Der erste Teil dieser Bemühungen wird sich auf die vorhandene Literatur stützen, um Licht in dieses Thema zu bringen, das zunehmend von Wissenschaftlern untersucht wird. Bis vor kurzem haben (kriminologische) Studien den Betrug zugunsten anderer Massenkriminalität vernachlässigt, aber das hat sich geändert (Button & Cross, 2017; Button, Lewis, & Tapley, 2009; Button, Lewis, & Tapley, 2014; Titus & Gover, 2001; Levi, 2008; Button, Tapley, & Lewis, 2012).

Im zweiten Teil werden wir einige bewährte Praktiken im Zusammenhang mit dieser Kriminalität aufzeigen und einige Empfehlungen und Tipps für vorbeugende Maßnahmen, insbesondere gegen Telefonbetrug, geben. Diese Empfehlungen basieren auf einem Workshop, der mit einer Vielzahl von Experten aus der gesamten Europäischen Union durchgeführt wurde. Schließlich wird ein dritter Teil einige bewährte Verfahren auflisten, die bei der Produktion dieser Toolbox gesammelt wurden.

01 TEIL I: INFORMATIONSBILD

1. Einführung

In diesem ersten Teil der Toolbox wird die aktuelle Literatur zum Thema Gaunereien und Betrug in Augenschein genommen. Genauer gesagt werden wir uns in dieser Toolbox auf Betrug auf individueller Ebene konzentrieren, der hauptsächlich (aber nicht ausschließlich) unter Einsatz von IKT begangen wird (Button, Tapley, & Lewis, 2012). Betrug ist ein sehr vielfältiges Delikt und umfasst ein breites Spektrum von Verhaltensweisen (Button, Lewis, & Tapley, 2014). Levi und Burrows (2008) definieren ihn so:

> *„Betrug ist die Erlangung eines finanziellen Vorteils oder die Verursachung von Verlusten durch implizite oder explizite Täuschung; er ist der Mechanismus, durch den der Betrüger einen rechtswidrigen Vorteil erlangt oder rechtswidrige Verluste verursacht“* (Levi & Burrows, 2008, S. 7)

Generell können wir feststellen, dass alle Arten von Betrug eine Art von Täuschung oder List beinhalten, mit der Absicht, eine Art von Gewinn zu erzielen (Button, Lewis, & Tapley, 2009; Murphy & Murphy, 2007; Button &

Victim sector	Victim sub-sector	Examples of fraud
Private	Financial services	- Cheque fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Data-compromise fraud - Embezzlement - Insider dealing/market abuse - Insurance fraud - Lending fraud - Payment card fraud - Procurement fraud
	Non-financial services	- Cheque fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Data-compromise fraud - Embezzlement - Gaming fraud - Lending fraud - Payment card fraud - Procurement fraud
	Individuals	- Charity fraud - Consumer fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Investment fraud - Pension-type fraud
Public	National bodies	- Benefit fraud - Embezzlement - Procurement fraud - Tax fraud
	Local bodies	- Embezzlement - Frauds on Council taxes - Procurement fraud
	International (but affecting public)	- Procurement fraud (by national against other – mainly but not always foreign – companies to obtain foreign contracts) - EU funds fraud

Cross, 2017). Levi (2008) kategorisierte Betrugsfälle nach der Art des Opfers und entwickelte folgende Typologie:

Wenn wir uns auf den Bereich der privaten Opfer und insbesondere auf den Teilsektor der Einzelpersonen als Opfer konzentrieren, gibt es immer noch viele verschiedene Möglichkeiten, betrogen zu werden, wie die gleiche Grafik verdeutlicht. Innerhalb dieser Toolbox werden wir uns jedoch auf den Verbraucherbetrug konzentrieren, den Levi und Burrows (2008) wie folgt definieren:

„eine breite Kategorie, die Lotterie-/Preisbetrug, „Rogue Dialling“ und andere kommunikationsbasierte Betrügereien umfasst, „unehrliche“ Falschbeschreibungen von Produkten und Dienstleistungen (darunter „alternative Gesundheitsprodukte“ oder Sexualhilfsmittel); Spielbetrug (z.B. abgesprochene Rennen und Spiele, auf die Wetten (einschließlich Spreadbetting) abgeschlossen wurden), Käufe von Waren und Dienstleistungen, die nicht vom Anbieter versandt werden“ (Levi & Burrows, 2008, S. 7).

Andere Begriffe, die in der Literatur zirkulieren, sind „individueller Betrug“ (Button, Tapley, & Lewis, 2012) und Massenmarketing-Betrug (Button, Lewis, & Tapley, 2009; Whitty, 2018; 2015; Wood, Liu, Hanoch, Xi, & Klapatch, 2018), obwohl Letzterer sich eher auf Massenkommunikationstechniken bezieht, die genutzt werden (Button & Cross, 2017). Aus Gründen der Einheitlichkeit innerhalb dieser Toolbox werden wir im Folgenden den Begriff „individueller Betrug“ verwenden, da dieser unseren Fokus am stärksten widerspiegelt. Die derzeitigen Vorstellungen von dieser Art von Betrug sind zwar stark mit diesen neuen Technologien verbunden, doch ist es wichtig, zu erkennen, dass es individuellen Betrug schon so lange gibt, wie wir sprechen können und Privatbesitz haben. Die Entwicklung der Technologie hat die Mittel zur Durchführung dieser Art von Kriminalität lediglich verändert und ihr ermöglicht, sich in größerem Umfang zu industrialisieren (Button & Cross, 2017; Leukfeldt & Stol, 2011; Crosman, 2017). Daher können wir diese neueren Formen als „cyber-fähige Verbrechen“ einstufen, d.h. traditionelle Verbrechen, deren Umfang durch den Einsatz von IKT in ihrem Ausmaß und ihrer Reichweite vergrößert werden kann. Phishing ist wahrscheinlich das bekannteste Beispiel für diese Entwicklung und nimmt massive Ausmaße an (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018).

Ohne alle Arten von individuellem Betrug als Cyber-Betrug zu kategorisieren, wird der Fokus dieser Toolbox auf diesen zeitgenössischen Betrugsformen und ihren aktuellen gemischten On-/Offline-Merkmalen liegen. In den folgenden Kapiteln

werden wir uns zunächst intensiver mit den angewandten Überzeugungstaktiken und insbesondere mit dem Social Engineering befassen, das den meisten dieser Betrugsformen zugrunde liegt (Button, McNaughton, Kerr, & Owen, 2014; Europol, 2017). Da sich die bulgarische Präsidentschaft entschlossen hat, sich auf Betrügereien zu konzentrieren, an denen das Opfer tatsächlich aktiv beteiligt ist, ist es unerlässlich zu untersuchen, wie Täter Menschen zu dieser kooperativen Einstellung drängen (Button & Cross, 2017). Anschließend wird ein Überblick über die verschiedenen Arten von individuellem Betrug gegeben. Zuletzt werden wir uns auch mit den Profilen der Opfer und Täter befassen.

https://cyberessentialsdotblog.wordpress.com/2017/02/25/phishing-evolved/

2. Die Kunst der Überredung

Unabhängig von der Art des Betrugs ist der Aufbau einer Beziehung zum Opfer unerlässlich. Der Täter muss das Vertrauen seiner Opfer durch Vertrauen, Mitgefühl und Überzeugungskraft erlangen, damit der Betrug funktioniert (Crosman, 2017). Die Mittel, die heute eingesetzt werden, mögen andere sein; die Technik ist im Wesentlichen immer noch die gleiche (Maggi, 2010). **Social Engineering** ist die entscheidende Taktik, um dieses Vertrauen zu erlangen, und beinhaltet die Täuschung einer Person, um sie davon zu überzeugen, entweder unwissentlich sensible Informationen preiszugeben oder Handlungen vorzunehmen, zu denen sie normalerweise nicht bereit wäre (Europol, 2017; Atkins & Huang, 2013; Europol, 2016). Konkret werden wir uns auf Täuschung konzentrieren, die auf menschlicher Interaktion basiert: Social Engineering, das den natürlichen Wunsch des Opfers nutzt, gemocht zu werden. Darüber hinaus gibt es jedoch eine zweite Kategorie des Social Engineering, die computerbasierte Täuschung beinhaltet, z.B. unter Verwendung von Malware, die in der E-Mail installiert ist, von Key Loggern oder gefälschten Popups (Atkins & Huang, 2013; Singh & Imphal, 2018).

Das zweifelhafte Verhältnis zwischen Opfer und Täter ist im Rahmen des individuellen Betrugs von zentraler Bedeutung. Der Täter ist im Wesentlichen abhängig von der Fähigkeit, eine Vertrauensbeziehung zu seinem Opfer aufzubauen, um mit seiner bösartigen Absicht erfolgreich zu sein (Atkins & Huang, 2013). Tatsächlich muss der Täter die Opfer dazu bringen, Handlungen vorzunehmen, die sie nicht beabsichtigten und die sogar für sie selbst schädlich sein können (Yeboah-Boateng & Amanor, 2014; Ollmann, 2007). Die meiste Literatur zu diesem Thema ist in Studien im breiteren Rahmen der Sozialpsychologie anzusiedeln (Rusch, 1999). Laut dieser Arbeit:

> *„Social Engineers versuchen oft, potenzielle Opfer mit Appellen an starke Emotionen wie Aufregung oder Angst zu überzeugen, während andere Wege nutzen, zwischenmenschliche Beziehungen aufzubauen oder ein Gefühl von Vertrauen und Engagement zu erzeugen“* (Workman, 2008, S. 1).

Darüber hinaus fügen Atkins und Huang (2013) hinzu, dass „Social Engineers auf kognitive Vorurteile oder soziale Fehler im mentalen Prozess setzen, um ihre

Angriffe zu initiieren und auszuführen und automatische emotionale Reaktionen bei ihren Opfern zu erzeugen“ (Atkins & Huang, 2013, S. 24). Diese automatischen emotionalen Reaktionen deuten auf den so genannten peripheren Weg innerhalb des Elaboration Likelihood Model hin. Dieses Modell scheint in der Literatur über Betrug und warum Menschen ihm zum Opfer fallen, eine eher hegemoniale Position zu haben. Im Kern geht sie davon aus, dass es zwei Wege der Überzeugung gibt. Der eine ist der zentrale Weg, die viel Überlegung und daher hohen Aufwand erfordert. Die zweite, der periphere Weg, erfordert keinen wirklichen Aufwand, da das Individuum sich auf emotionale Auslöser wie Attraktivität oder empfundene Glaubwürdigkeit konzentriert (Petty & Cacioppo, 2012; Petty & Cacioppo, 1986; Rusch, 1999; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Whitty, 2013). Betrüger drängen ihre Opfer auf diesen zweiten Weg und appellieren traditionell an negative Emotionen wie Gier, Einsamkeit oder Angst, und seit kurzem werden auch alltägliche und legitime Geschäftsanfragen (z.B. CEO-Betrug) einbezogen (Workman, 2008; Jakobsson, 2016). Um das Opfer auf diesen zweiten Weg zu lenken, definiert die Literatur einige Prinzipien, die von den Tätern gebraucht/missbraucht werden (Jakobsson, 2016). Es ist jedoch sehr wichtig zu beachten, dass diese Prinzipien - diese kognitiven „Faustregeln“ - alle ihren alltäglichen Nutzen haben. Der Schlüssel dazu ist, dass die Betrüger einen Rahmen schaffen, in dem sie diese „Überzeugungswaffen“, meist kombiniert, zu ihrem eigenen Vorteil einsetzen können. Wir werden nun die drei einflussreichsten Autoren diskutieren, die in der Literatur in diesem Zusammenhang identifiziert wurden (Ferreira, Coventry, & Lenzini, 2015).

Unter diesen drei werden Cialdini und seine „sechs Prinzipien der Einflussnahme“ am häufigsten genannt (Rusch, 1999; Workman, 2008; Ferreira, Coventry, & Lenzini, 2015; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Cialdini, 2001).

1. Autorität:

Dieses Prinzip beschreibt die Neigung der Menschen, der Aufforderung von maßgeblichen Persönlichkeiten nachzukommen. In der richtigen Situation ist es sehr wahrscheinlich, dass Menschen auf Autoritätsbehauptungen reagieren. Dies gilt auch für Autoritätssymbole, z.B. Uniformen, Abzeichen und Titel oder in Telefongesprächen, bei denen Autorität leicht vorgegeben werden kann.

Beispiel: Dieses Prinzip wird bei Betrügereien mit falschen Polizisten deutlich. Wir glauben und gehorchen Beamten ganz natürlich aufgrund ihrer Uniform, ihrer Titel

usw. Stellen Sie sich vor, Sie werden von einem Mann angerufen, der behauptet, Polizist zu sein und Ihren PIN-Code so schnell wie möglich zu benötigen, um Ihr von Straftätern gekapertes Konto zu sperren. Gesperrt wird jedoch nur Ihre Möglichkeit, künftig noch auf das Geld auf Ihrem Konto zuzugreifen.

2. Verknappung:

Menschen schätzen den Wert von Gegenständen, die als knapp wahrgenommen werden, höher ein. Dieser spezielle Artikel oder dieses Angebot gilt als knapp oder nur für einen begrenzten Zeitraum verfügbar. Infolgedessen wird er als attraktiver und begehrenswerter wahrgenommen.

Beispiel: Viele Phishing-E-Mails weisen in ihrem Betreff darauf hin, dass das Angebot „begrenzt“ ist, „nur noch 50 übrig“, „einzigartig“ usw.

3. Sympathie:

Menschen neigen dazu, andere zu mögen, die ähnliche Interessen, Einstellungen und Überzeugungen haben. Die Neigung, Menschen zu mögen, die wie wir sind, ist zutiefst menschlich. Wenn wir eine Person mit identischen oder ähnlichen Merkmalen wie unseren eigenen identifizieren, ist dies für uns auch ein starker Anreiz, eine mentale Abkürzung im Umgang mit dieser Person zu nehmen.

Beispiel: Dieses Prinzip ist bei Social Media Influencern sehr deutlich zu erkennen. Ihres Erfolgs beruht zum Teil darauf, dass sie als „Junge oder Mädchen von nebenan“ auftreten. Natürlich möchte man das gleiche Outfit haben. Ähnlich möchten Sie auch das gleiche Shirt kaufen, das Ihr Lieblings-Fußballer trägt. Betrüger nutzen dies leicht aus, indem sie bei ihren Betrügereien auf bekannte Personen verweisen.

4. Gegenseitigkeit:

Dies ist eine bekannte soziale Regel, die uns verpflichtet, anderen zurückzugeben, was wir von ihnen erhalten haben. Im Allgemeinen wird dies als „Wenn du mir den Rücken kratzt, kratze ich deinen“ bezeichnet. Selbst wenn der Gefallen, den jemand anbietet, von der anderen Person nicht verlangt wurde, kann sich die Person, die

die Gefälligkeit erhalten hat, stark verpflichtet fühlen, die Regel der Gegenseitigkeit einzuhalten, indem sie sich zur Gefälligkeit bereit erklärt, die der ursprüngliche Anbieter im Gegenzug verlangt. Auch wenn dieser Gefallen deutlich kostspieliger ist als das ursprüngliche Angebot.

Beispiel: Wenn etwas von einem gewissen Wert angeboten wird, z.B. eine kostenlose Probe, fühlt man sich verpflichtet, diesen Gefallen durch den Kauf des Vollprodukts oder der Dienstleistung zu erwidern. Auch wenn diese kostenlose Probe noch nicht eingetroffen ist oder gar nicht existiert.

5. Verpflichtung und Konsistenz:

Eine weitere soziale Regel ist die Konsistenz des Verhaltens und die Verpflichtung dazu. Wenn wir etwas versprechen, werden wir unser Versprechen höchstwahrscheinlich halten, weil wir sonst unzuverlässig oder unerwünscht wirken. Konsistenz wird aktiviert, indem kleineren, anfänglichen Verpflichtungen verlangt werden, die leichter zu erfüllen sind.

Beispiel: Beim klassischen Betrug mit dem nigerianischen Prinzen (siehe unten), auch bekannt 419 Scam, wird in der Regel zuerst ein kleinerer Gefallen verlangt, zu dem das Opfer leichter Ja sagen kann. Als nächstes wird ein größerer Gefallen verlangt, den das Opfer nur schwer ignorieren oder ablehnen kann, da dies nicht dem früheren Verhalten des Opfers entspräche...

6. Sozialer Beweis/Konformität:

Dieses letzte Prinzip zeigt sich auch in vielen sozialen Situationen. Bei der Entscheidung, welche Handlungsweise die angemessenste ist, orientieren wir uns an anderen Menschen (Peer Groups, Vorbilder usw.). Dies kann sogar zu Handlungen führen, die nicht in unserem Interesse sind, es aber ermöglichen, innerhalb der Gruppe akzeptiert zu werden.

Beispiel: Auf Facebook sehen wir anhand der Anzahl der Likes, ob eine Seite oder ein Produkt als beliebt angesehen wird. Betrüger können eine neue Seite so einfach wie jeder andere erstellen und mit der Verwendung von gefälschten Likes kann dieses Prinzip des sozialen Beweises angeregt werden, um das Opfer von ihrer Echtheit und Popularität zu überzeugen.

Die Prinzipien von Cialdini wurden ursprünglich auf der Grundlage von Marketing-Erkenntnissen entwickelt, haben sich aber in der Social-Engineering-Literatur ebenso bewährt wie bei Betrügern, die diese Prinzipien zu ihrem Vorteil missbrauchen. Einige Autoren haben jedoch unterschiedliche, aber ähnliche Prinzipien mit einem stärkeren Fokus auf Betrug entwickelt (40). Einer davon ist Gragg mit seinen „sieben psychologischen Triggern“ (40,49):

1. Starker Affekt

Dieser Trigger nutzt einen erhöhten emotionalen Zustand, damit der Täter mehr bekommen kann, als in einer normalen Situation rational möglich wäre. Wenn man das Opfer zum Beispiel überrascht oder wütend macht, wird es daran gehindert, rational zu denken.

Beispiel: Dem potenziellen Opfer einen Preis in Millionenhöhe zu versprechen, wird höchstwahrscheinlich starke Emotionen wecken und als mächtige Barriere gegen die logische und rationale Bewertung des Angebots wirken.

2. Überlastung

Hat das Opfer zu viele Informationen auf einmal zu verarbeiten, wirkt sich dies negativ auf die Bewertung der Informationen aus, was zu Entscheidungen führt, die normalerweise nicht getroffen worden wären.

Überlastung kann auch durch Argumente aus einer unerwarteten Perspektive ausgelöst werden. Es braucht Zeit, einen neuen Gesichtspunkt zu verarbeiten, aber wenn diese nicht verfügbar ist, könnte dies zu einer verminderten Fähigkeit führen, die Informationen zu verarbeiten und damit zu falschen Entscheidungen.

Beispiel: Um die DSGVO (Datenschutzgrundverordnung) einzuhalten, versandten Unternehmen auf der ganzen Welt eine große Anzahl von E-Mails, um ihre Kunden zu fragen, ob sie mit ihrer erneuerten Datenschutzerklärung einverstanden sind. Es dauerte jedoch nicht lange, bis Betrüger diese Überlastung ausnutzten und begannen, ähnliche Nachrichten zu versenden, jedoch mit anderen Absichten als dem Schutz der Privatsphäre der Bevölkerung.

3. Gegenseitigkeit:

Ähnlich wie beim Prinzip von Cialdini sollte man sich revanchieren, wenn man etwas bekommt oder einem etwas versprochen wird.

Beispiel: Beim 419 Scam werden den Opfern große Belohnungen versprochen. Sie fühlen sich natürlich geneigt, die Gunst durch Überweisung des Geldes zu erwidern.

4. Trügerische Beziehungen

Hier baut der Betrüger eine Beziehung auf falschen Prämissen auf, mit dem Ziel, die andere Person auszunutzen.

Beispiel: Beim Enkeltrick wird das Verhältnis des älteren Menschen zu seinen Enkeln geschickt ausgenutzt. Unter falschen Prämissen erschleichen sie sich den Weg in diese intime und vertrauensvolle Beziehung und nutzen sie zu ihrem Vorteil.

5. Diffusion von Verantwortungsgefühl und moralischer Verpflichtung

Nach diesem Trigger fühlt sich das Opfer nur teilweise für die von ihm begangenen Handlungen verantwortlich. Die folgenden Handlungen werden weniger schwierig zu begehen sein, und dies ist vor allem dann der Fall, wenn das Opfer sich „moralisch verpflichtet“ fühlt.

Beispiel: Beim CEO Fraud lässt man das Opfer glauben, es sei für das Nichtzustandekommen eines Großauftrags verantwortlich, wenn es keine Vorauszahlung leistet.

6. Autorität:

Ähnlich wie bei Cialdini sind die Menschen in der modernen Gesellschaft konditioniert, auf Autorität zu reagieren, was von den Tätern leicht ausgenutzt werden kann.

Beispiel: Um beim selben Beispiel wie oben zu bleiben, wer sind Sie, „Nein“ zu sagen, wenn der Auftrag scheinbar vom CEO selbst kommt?

Integrität und Konsistenz

Dieser letzte Trigger ähnelt ebenfalls „Verpflichtung und Konsistenz“ nach Cialdini. Menschen neigen dazu, eingegangene Verpflichtungen einzuhalten, auch wenn diese für sie selbst potenziell schädlich sind.

Beispiel: Dies kann genutzt werden, damit ein Betrug weiterhin funktioniert, kann aber auch den Betrug auslösen, indem man an Handlungsweisen appelliert, zu denen eine Person normalerweise neigen würde, oder indem man ein Szenario nachahmt, in dem das Opfer sich bereits zu etwas verpflichtet zu haben scheint.

Stajano (2011) ist ein weiterer einflussreicher Autor, der sich „sieben Prinzipien des Betrugs“ hat einfallen lassen, die von den Tätern genutzt werden:

1. Ablenkungsprinzip

Während das Opfer durch das, was sein Interesse erregt, abgelenkt wird, kann der Betrüger die eigentliche „Tat“ begehen und das Opfer wird sie höchstwahrscheinlich nicht bemerken.

Beispiel: Beim sogenannten Hütchenspiel, bei dem das Opfer die Kugel verfolgen muss, die unter einem Hütchen versteckt ist, sprechen die Täter oft über den Preis, den das Opfer gewinnen kann, und zeigen ihm ein Beispiel für den Preis. Währenddessen werden die Hütchen gemischt und das Opfer ist abgelenkt.

2. Social-Compliance-Prinzip

Ähnlich wie bei der „Autorität“ bei Cialdini und Gragg argumentiert Stajano, dass Betrüger diese „Aufhebung des Misstrauens“ ausnutzen, um Sie dazu zu bringen, ihren Wünschen nachzukommen.

Beispiel: Täter können so auftreten, als seien sie legitimierte Arbeiter und betreten unter dieser Prämisse das Haus des Opfers. Wenn sie einmal drinnen sind, können sie das Haus leicht ausrauben.

3. Herdenprinzip

In Übereinstimmung mit dem „sozialen Beweis“ von Cialdini erlaubt dieses soziale Prinzip auch misstrauischen Opfern, ihre Wachsamkeit aufzugeben, wenn sie wahrnehmen, dass andere Personen in der gleichen Situation sich ebenso verhalten.

Beispiel: In einigen Phishing-E-Mails wird ein wirksames Mittel gegen Haarausfall angepriesen. Oft wird darin ein Zitat eines glücklichen „Kunden“ verwendet, als Beweis, dass es funktioniert. Das Opfer wird möglicherweise weniger misstrauisch, da offensichtlich auch andere das Produkt gekauft haben.

4. Unehrlichkeitsprinzip

Bis zu einem gewissen Grad unter Nachahmung der „Diffusion von Verantwortung und moralischer Pflicht“ nach Gragg, sorgt dieses Prinzip dafür, dass es Ihnen schwerer fällt, Hilfe zu finden. Sobald Sie erkannt haben, dass Sie betrogen wurden, sind Sie selbst in eine kriminelle Machenschaft verwickelt, was weniger wahrscheinlich macht, dass Sie zur Polizei gehen. Dies kann auch durch Erregung des Schamgefühls des Opfers erreicht werden.

Beispiel: Bei vielen Betrügereien schämt sich das Opfer, in die Falle gegangen zu sein. Dies wird es davon abhalten, das Verbrechen anzuzeigen. Betrüger gestalten solche Betrügereien gezielt so, dass das Opfer beschämt wird (siehe auch unten).

5. Täuschungsprinzip

Betrüger wissen, wie man manipuliert und lassen das Opfer glauben, dass Dinge und Menschen real sind, auch wenn dies nicht der Fall ist.

Beispiel: Tatsächlich nutzen fast alle Betrügereien dieses Prinzip. Dinge und Menschen sind nie das, was sie bei Betrügereien zu sein scheinen. Wenn es zu schön erscheint, um wahr zu sein, dann ist es das wahrscheinlich.

6. Bedürfnis- und Gierprinzip

Ebenfalls verwandt mit der „Verknappung“ nach Cialdini bedeutet dieses Prinzip, dass die Täter Ihre Bedürfnisse und Wünsche manipulieren, um zu bekommen, was sie wollen.

Beispiel: Wenn Sie sich in einem Land mit einer anderen Währung aufhalten, müssen Sie Geld wechseln. Dieser Bedarf kann von Betrügern leicht ausgenutzt werden, um die Wechselkurse zu senken.

7. Zeitprinzip

Wenn dem Opfer ein Gefühl der Dringlichkeit und des Zeitdrucks vermittelt wird, wird es höchstwahrscheinlich den Entscheidungsprozess beschleunigen. Dies erlaubt weniger Überlegung, was dem Täter einen Vorteil verschafft, da hierdurch das Opfer anfälliger wird.

Beispiel: Bei vielen E-Mail-Betrügereien wird das Opfer davon überzeugt, dass es schnell handeln muss, um diese „einmalige Chance“ nicht zu verpassen.

Ferreira, Coventry und Lenzini (2015, S. 3) entwickelten folgende Grafik, um diese drei wichtigen Gruppen von Prinzipien zu vergleichen, die von Betrügern verwendet und missbraucht werden:

	C	G	S
1	Authority	Authority	Social Compliance
2	Social Proof	Diffusion Responsibility	Herd
3	Linking & Similarity	Deceptive Relationship	Deception
4	Commitment & Consistency	Integrity & Consistency	Dishonesty
5	Scarcity	Overloading	Time
6	Reciprocation	Reciprocation	Need & Greed
7	-	Strong Affect	Distraction

Nun, da wir einige der wichtigsten Techniken und Prinzipien verstehen, die Betrüger verwenden und missbrauchen, werden wir einen Blick auf die Vielfalt der Betrugsfälle werfen.

3. Suchen Sie sich Ihren Betrug aus

Wie bereits an anderer Stelle erwähnt, mögen die Taktiken, die von den Betrügern angewandt werden, immer noch die gleichen sein, die Mittel, mit denen sie verfolgt werden, sind heute andere. In diesem Abschnitt bieten wir einen nicht erschöpfenden Überblick über die Vielfalt der Betrugsfälle, die es heute gibt. Zunächst werden einige Beispiele für Betrug auf der Grundlage ihres Inhalts gegeben. Anschließend wird eine Klassifizierung nach der Art der Durchführung vorgenommen.

Obwohl sich die kriminologische Forschung erst seit kurzem für diese Art von Verbrechen interessiert, hat der *419 Scam*, besser bekannt als Vorschussbetrug, bei dem ein *nigerianischer Prinz* eine Rolle spielt, deutlich mehr Aufmerksamkeit durch Wissenschaftler erfahren (Whitty, 2015; Whitty, 2018; Mba, Onaolapo, Stringhini, & Cavallaro, 2017). Zwar hat Nigeria keinen Prinzen, die Ursprünge dieses Betrugs sind jedoch typischerweise in Nigeria zu finden. Dies erschwert die Strafverfolgung der Täter (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). Im klassischen Szenario wird dem Opfer ein Prozentsatz einer großen Geldsumme angeboten, aber nur, wenn das Opfer hilft, das Geld außer Landes zu bekommen. Das Opfer wird überredet, die zusätzlichen Gebühren zu zahlen, um das Geld zu überweisen. Unnötig zu sagen, dass das Geld und der Prinz nie existierten (Murphy & Murphy, 2007).

Diese Art von individuellem Betrug bezeichnet man als „Vorschussbetrug“. Ein geringerer Betrag muss gezahlt werden, um von einem höheren Betrag zu profitieren (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). *Romance Scams* können ebenfalls unter diese Kategorie fallen (Whitty, 2018), umfassen aber mehr als nur finanzielle Verluste. Tatsächlich hat diese Art von Betrug auch in emotionaler Hinsicht verheerende Auswirkungen, aufgrund der intimen Beziehung, die aufgebaut werden muss, damit dieser Betrug funktioniert.

> *„Kriminelle geben vor, eine Beziehung einzugehen, mit der Absicht, ihre Opfer um große Geldbeträge zu betrügen. Betrüger erstellen gefälschte Profile auf Dating-Websites und Social-Networking-Websites mit gestohlenen Fotos (z.B. attraktive Modelle, Armeeoffiziere) und einer erfundenen Identität. Sie entwickeln eine Online-Beziehung mit dem Opfer außerhalb der Website, „pflegen“ das Opfer*

https://blog.eset.ie/2017/09/18/email-phishing-is-old-but-not-dead/

> *(entwickeln eine hyperpersönliche Beziehung mit dem Opfer), bis sie das Gefühl haben, dass das Opfer bereit ist, sich von seinem Geld zu trennen. Es wurde festgestellt, dass dieser Betrug einen „doppelten Schlag" verursacht - einen finanziellen Verlust und den Verlust einer Beziehung"* (Whitty, 2018, S. 105)

Ebenso auf einer falschen Beziehung aufgebaut, wenn auch auf eine andere Weise, ist der *Enkeltrick*. Wie in früheren EUCPN-Studien erläutert (EUCPN, 2017), wird älteren Menschen der Eindruck vermittelt, dass sie mit einem Verwandten sprechen. Ein seit langem verschollenes Enkelkind befindet sich angeblich im Krankenhaus und benötigt sofort die Überweisung einer Geldsumme, um die Behandlung bezahlen zu können (Jakobsson, 2016). Sie haben lange nichts von ihm gehört und werden wahrscheinlich auch nie wieder von ihm hören...

Ein weiterer „berühmter“ Betrug mit den gleichen Merkmalen ist der *Technical Support Scam* (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). Meistens kommt dieser technische Support von Microsoft und informiert das Opfer telefonisch oder per E-Mail über ein latentes Computerproblem. *„Sie haben es vielleicht noch nicht bemerkt, aber es befindet sich ein Virus auf Ihrem Computer“.* Gegen Überweisung einer geringen Geldsumme ist der Mitarbeiter in der Lage, Ihr Problem aus der Ferne zu beheben (Harley, Grooten, Burn, & Johnston, 2012; Bullée J.-W., Montoya, Junger, & Hartel, 2016). Da viele Menschen von diesem Betrug gehört haben, haben die Täter in jüngster Zeit ausgefeiltere gefälschte Support-Webseiten entwickelt, die das Opfer dazu bringen, das Support-Center selbst anzurufen, höchstwahrscheinlich unter einer Mehrwertdienstnummer (Rauti & Leppänen, 2017).

Die 13 Mitgliedstaaten, die unseren Fragebogen beantworteten, gaben die folgenden Telefonbetrügereien als die häufigsten an: Enkeltrick, falscher Polizist, Lotteriebetrug, Rechtsgeschäftsbetrug, Betrug, bei dem es um den angeblichen Unfall eines Verwandten geht.

Weitere Beispiele sind *Lotteriebetrug, Glücksspielbetrug, Geschäftschancenbetrug, Kettenbriefbetrug, Telemarketing-Betrug usw.* (Button, Lewis, & Tapley, 2014; Button & Cross, 2017; Button, Lewis, & Tapley, 2009; Jakobsson, 2016; Stajano & Wilson, 2011). Button (2017) bietet uns eine Klassifizierung basierend auf acht Kategorien der häufigsten Betrugsfälle.

1. Verbraucheranlagebetrug

Hier werden den Opfern als hochprofitabel dargestellte Aktien oder Anteile verkauft. In Wirklichkeit sind diese wertlos oder nicht vorhanden.

2. Betrug bei Konsumgütern und Dienstleistungen

Dieser Betrug beinhaltet den Verkauf von nicht existierenden Produkten und Dienstleistungen oder den Verkauf von Produkten und Dienstleistungen, die bei der Lieferung deutlich anders aussehen.

3. Beschäftigungsbetrug

Dem Opfer wird ein gefälschter oder unzureichender Dienst zur Sicherung der

Beschäftigung oder Ausbildung angeboten, der so dargestellt wird, dass er zu einer Beschäftigung führt.

4. Preis- und Zuschussbetrug

Entweder wird dem Opfer vorgegaukelt, dass es an einer echten Lotterie teilnimmt und eine Teilnahmegebühr zahlen muss, oder ihm wird mitgeteilt, dass es bereits gewonnen hat und zunächst eine Gebühr zahlen muss, um diesen Preis in Empfang nehmen zu können.

5. Phantom-Inkasso-Betrug

Oftmals durch die Nachahmung vertrauenswürdiger Akteure oder Organisationen wird das Opfer getäuscht oder dazu gedrängt, Schulden zu bezahlen, die gar nicht existieren.

6. Wohltätigkeitsbetrug

Hier tritt der Betrüger als legitime Wohltätigkeitsorganisation auf, um Spenden von Einzelpersonen zu erhalten.

7. Beziehungs- und Vertrauensbetrug

Romance Scam, Enkeltrick, Unfallbetrug usw. sind klassische Beispiele für Betrug, der die Intimität einer persönlichen Beziehung missbraucht.

8. Identitätsbetrug

Dies beinhaltet die Verwendung personenbezogener Daten eines Opfers, um andere Betrügereien oder kriminelle Aktivitäten zu begehen. Wir berücksichtigen diese Art von Betrug nicht in dieser Toolbox, da sie keine aktive Beteiligung des Opfers an der Transaktion erfordert.

Die Liste ist so beeindruckend wie die Kreativität der Betrüger und kann alle Bevölkerungsgruppen erreichen. Betrüger können aber auch einen gezielteren Ansatz verfolgen. Dies ist der Fall bei *Business Email Compromise (BEC) Scams* (Jakobsson, 2016). Dabei wird das Opfer ausgewählt, da es für ein bestimmtes Unternehmen arbeitet oder eine bestimmte Rolle in diesem Unternehmen hat. Der Täter tritt meist, nachdem er gewisse Erkundigungen eingeholt hat, als Chef des Opfers (CEO Fraud) oder als eine andere vertrauenswürdige Drittpartei („Mandate Fraud“) auf und fordert eine scheinbar normale Zahlung (Europol, 2017). Zum Beispiel fordert Ihr Chef Sie per E-Mail auf, eine Überweisung an das Unternehmen X vorzunehmen. Die Angelegenheit ist dringend, daher verwendet er seine „persönliche“ E-Mail-Adresse und bittet Sie, dies zu tun. Weder ist das

Unternehmen echt, noch stimmt die E-Mail-Adresse, Sie befolgen jedoch die Anweisungen (Jakobsson, 2016). Laut dem jüngsten *Internet Organised Crime Threat Assessment* (Europol, 2018) meldeten 65% aller Mitgliedstaaten Fälle von CEO Fraud und über die Hälfte von ihnen nannten steigende Zahlen.

Eine weitere Möglichkeit, diese Betrügereien zu klassifizieren, besteht darin, sie nach der Art und Weise zu unterteilen, wie sie beim Opfer ausgeführt werden. Logischerweise kann es sich dabei entweder um eine persönliche, reale Interaktion handeln oder das Opfer kann aus der Ferne mit Kommunikationsmethoden

https://www.europol.europa.eu/socta/2017/fraud.html

wie E-Mail oder Telefon kontaktiert werden. Es ist jedoch unerlässlich, sich nicht blenden zu lassen, indem man sich auf eine einzige Art der Durchführung konzentriert, damit ein Betrug funktioniert. Täter können problemlos zwischen E-Mail, Telefon, Website usw. wechseln. So können sie ihren Angriff optimal anpassen (Button & Cross, 2017).

Ein klassisches Beispiel für den **persönlichen Betrug** ist das Auftreten als falsche Polizisten, um das Opfer dazu zu bringen, eine angebliche Geldstrafe zu zahlen oder sensible Informationen preiszugeben. Ein ähnlicher Fall sind Täter, die sich als Handwerker ausgeben, die einige Arbeiten im Haus erledigen möchten. Um es dem ahnungslosen Opfer angenehmer zu machen, bieten sie an, ihre Pflichten zu erfüllen, während das Opfer bei der Arbeit oder im Urlaub ist... Andere gängige Beispiele sind gefälschte Geldrollen oder typische Fallen wie das „Hütchenspiel“ oder der Verkauf von gefälschten Gadgets (Stajano & Wilson, 2011).

Falschgeldrolle: z.B. Umtausch von Fremdwährung in Falschgeld

„Hütchenspiel“: das klassische Spiel, bei dem eine Kugel unter einem Becher versteckt wird, der dann mit zwei anderen Bechern vertauscht wird. Das Opfer muss erraten, wo sich die Kugel befindet, was unmöglich ist, weil sich unter keinem Becher eine Kugel befindet.

In den meisten Social-Engineering-Fällen verzichten die Täter jedoch auf physischen Kontakt, da dies ihnen mehr Schutz bietet. Darüber hinaus ist die Nutzung von E-Mail oder Telefon der ideale Rahmen, um Opfer auf den peripheren Weg zu lenken (Workman, 2008). Anderson (2016) beschreibt diese Entwicklung aus amerikanischer Sicht:

> *„Noch in den 1980er-Jahren war die Betrugsproblematik weitgehend ein lokales Phänomen oder eines, das die Post betraf. Täter lokalisierten ihre Opfer, indem sie von Tür zu Tür gingen, Mechaniker stellten die Notwendigkeit von Reparaturen in der örtlichen Autowerkstatt falsch dar, und Hausierer verkauften ihre gefälschten Waren auf dem*

> *Jahrmarkt oder verschickten ihre gefälschten Versprechungen per Post. Heute begehen Betrüger Massenmarkt-Betrügereien auf einem landesweiten oder gar internationalen Markt, auf dem sie potenzielle Opfer über Telemarketing, Infomercials im Spätfernsehen oder das Internet ansprechen. Betrüger in Indien erzählen Verbrauchern, die sich im Internet an den technischen Support gewandt haben, dass ihre Computer 133 Probleme haben, die sie aus der Ferne beheben können, wenn Sie nur ihre Gebühren bezahlen. Statt sich darauf zu beschränken, von Tür zu Tür zu gehen oder die US-Post zu benutzen, können die Anbieter einer Vielzahl von gefälschten Produkten Werbesendungen im Spätnachtfernsehen laufen lassen, ihre Waren im Internet bewerben oder computergenerierte Telemarketinganrufe an Millionen von Verbrauchern innerhalb weniger Minuten platzieren.* (Anderson, 2016, S. 4)

Die Revolution in der Kommunikationstechnologie hat es den Tätern ermöglicht, herkömmlichen Betrug zu niedrigen Kosten zu industrialisieren und neue Arten von Betrug zu entwickeln (Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Damit ist dies eine so genannte *cyber-fähige Kriminalität*, d.h. eine traditionelle Kriminalität, die sich durch den Einsatz von IKT weiterentwickelt hat (Whitty, 2018; Button & Cross, 2017). Die digitale Umgebung hat eine Atmosphäre der Anonymität erzeugt, die den Betrügern willkommen ist (Agustina, 2015). Neben dieser (wahrgenommenen) Anonymität und den niedrigen Kosten hat sich die Anzahl der erreichbaren Ziele so weit vervielfacht, dass die ganze Welt in Schach zum potentiellen Opfer wird (Leukfeldt & Stol, 2011). Noch schlimmer ist, dass diese Globalisierung des Betrugs die Strafverfolgungsbehörden daran hindert, die Täter zuzuordnen und/oder festzunehmen. Einige sind sogar zu „Scampreneurs“ geworden, indem sie das volle Potenzial der technologischen Veränderungen ausgeschöpft haben (Button & Cross, 2017).

Die häufigste dieser „Betrügereien im industriellen Maßstab“ ist Phishing (Europol, 2017; Europol, 2016). Es werden die gleichen Ziele wie bei Betrügereien „im wirklichen Leben“ verfolgt, höchstwahrscheinlich aber tritt der Betrüger als vertrauenswürdiges oder legitimes Subjekt auf, wenn das Opfer getäuscht wird, um persönliche und/oder finanzielle Informationen preiszugeben (Singh & Imphal, 2018; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Moreno-Fernández,

Blanco, Garaizar, & Matute, 2017). Dies ist die einfachste Methode, um eine große Anzahl potenzieller Opfer zu erreichen. Es wird berichtet, dass Täter ihre Opfer in 95% der Fälle per E-Mail kontaktieren. 40% der Mitgliedstaaten hoben Untersuchungen zum Phishing hervor, und es handelt sich um ein Phänomen, das von Jahr zu Jahr zunimmt. Von 2015 bis 2016 nahm die Zahl der Phishing-Angriffe deutlich um 65 Prozent zu (Europol, 2017). Aufgrund von Problemen bei der Anzeigeerstattung (siehe unten) müssen wir mit diesen Zahlen vorsichtig sein, dennoch sind sie alarmierend.

Phishing ist ein sehr verbreitetes Phänomen. Mehr als 30% der erwachsenen Bevölkerung haben schon mindestens eine Phishing-E-Mail erhalten. In der Studentenpopulation steigt diese Zahl sogar auf mehr als 50%. Darüber hinaus öffnet jedes 14. Ziel tatsächlich einen Link oder einen Anhang, was zu einer möglichen Viktimisierung führt (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018).

Bei geringem Risiko für den Täter können die Verluste für das Opfer erheblich sein: finanzielle Verluste, Reputationsschäden, Identitätsdiebstahl,... (Ollmann, 2007).

Hier ist die Rede von irreführendem Phishing, was den Einsatz von Social-Engineering-Taktiken impliziert. Der Vollständigkeit halber sei erwähnt, dass es auch eine Form des Phishing gibt, die auf Malware oder computerbasierter Täuschung basiert, mit Hilfe von Key Loggern, Hacking, Trojanern usw., um die Ziele des Täters zu erreichen, wie bereits oben und in früheren Veröffentlichungen erwähnt wurde (EUCPN, 2017).

Bis vor kurzem waren E-Mail-Betrügereien noch recht leicht zu erkennen. Sie fielen durch schlechte Grammatik und Rechtschreibfehler auf und enthielten eher abwegige Geschichten. Betrüger haben jedoch erkannt, dass sie durch geschickte Fokussierung auf ihre Opfer ihre „Investitionsrendite“ steigern können. Die Gezieltheit des Angriffs erhöht die Chance, dass die E-Mail gelesen wird, um das Zwanzigfache (Jakobsson, 2016). Diese Entwicklung ebnete den Weg für eine neue und größere Vielfalt von Phishing-Formen und professionellere und glaubwürdigere Modi operandi (Europol, 2017; Jakobsson, 2016; Ollmann, 2007). Phishing wird immer gezielter eingesetzt. Während die Täter früher so viele E-Mails wie möglich verschickten, recherchieren Betrüger heute und nutzen dieses

https://www.pinterest.co.uk/pin/760897299514084725/

Wissen, um natürlicher und plausibler zu erscheinen; der CEO Fraud ist dafür das perfekte Beispiel (Jakobsson, 2016). Spear Phishing ist ein weiterer Begriff, der die Fokussierung auf eine bestimmte Gruppe bezeichnet. Whale Phishing hingegen richtet sich an *hochrangige* Personen (Singh & Imphal, 2018). Es gibt auch andere Varianten wie Pharming, bei dem eine gefälschte Website gehostet wird, um das Opfer zu täuschen (Europol, 2014) oder Smishing, eine Form des Phishing, bei der SMS oder Online-Textnachrichten verwendet werden (Europol, 2018).

Da Phishing immer raffinierter wird, ist der überraschende letzte Schritt das erneute Interesse an einer älteren Technologie: dem Telefon (Maggi, 2010). Diese Telefonbetrügereien werden zunehmend als Vishing bezeichnet, da sie ebenfalls das Potenzial des Internets nutzen (Europol, 2017). Vishing, eigentlich „Voice Phishing“ nutzt das Medium Telefon, um seine Opfer zu täuschen (Maggi, 2010). Allerdings hat das Medium Telefon auch einige Änderungen erfahren. Das Voice Over Internet Protocol (VOIP) hat es ermöglicht, Anrufe über das Internet zu tätigen (Singh & Imphal, 2018). Das bringt einige Vorteile mit sich. Die Verwendung dieses Protokolls senkt die Kosten für Anrufe erheblich, die Täter sind schwerer zu verfolgen und sie sind in der Lage, ihre Anruferinformationen zu manipulieren (Ollmann, 2007). Spoofing ist die Verfälschung der Informationen, die vom Anrufer übermittelt werden. Nicht nur das, die Betrüger haben auch die Möglichkeit, ihre

Opfer per „Robodialling“ anzurufen. Dabei wird ein computergesteuerter Autodialer verwendet, der eine zuvor aufgezeichnete Nachricht übermittelt (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). Heutzutage sind Menschen es gewohnt, Fremden oder gar Maschinen Informationen zu geben, da Call Center in der modernen Gesellschaft allgegenwärtig sind (Maggi, 2010). Betrüger nutzen diese Entwicklung nur allzu gerne.

Telefonbetrügereien haben einen viel höheren Wirkungsgrad und der Ertrag ist genauso hoch wie beim normalen Phishing (Yeboah-Boateng & Amanor, 2014). Dieser Erfolg beruht auf der Tatsache, dass Vishing das Beste aus beiden Welten, persönlich und über Kommunikationstechnologie, kombiniert. Die Stärke des Telefons über das Internet liegt darin, dass es dem Täter die Möglichkeit bietet, viel schneller eine glaubwürdige Rolle zu erschaffen. Darüber hinaus kann die Person am anderen Ende immer noch diejenige sein, die sie sein will und die Anonymität genießen. Auf diese Weise verbindet es auch diese intime Umgebung mit der Unmöglichkeit, den Betrug im wirklichen Leben durch visuelle Hinweise zu erkennen. Tatsächlich kann man seinen Angriff bis ins letzte Detail gezielt ausführen, indem man ein Echtzeit-Gespräch führt und den Zeitpunkt der Übermittlung der Nachricht kontrolliert (Ollmann, 2007). Organisierte kriminelle Gruppen haben sogar begonnen, Muttersprachler anzuwerben, um so glaubwürdig und professionell wie möglich zu sein (Europol, 2016).

Zusätzlich zu diesen Vorteilen setzen Menschen traditionell auch mehr Vertrauen in das Telefon als in das Internet. Laut der jüngsten Eurobarometer-Umfrage über Kommunikationstechnologien in der EU (European Commission, 2018) halten 60% der Befragten das Telefon für zuverlässiger und glauben, es biete ihnen mehr Schutz als das Internet. Darüber hinaus ist der Telefonzugang fast universell, da 97% daheim Zugang dazu haben, während 70% zu Hause Zugang zum Internet haben. Außerdem ist das Telefonat nach wie vor die am häufigsten verwendete Kommunikationsform, wobei 92% der Befragten häufig telefonieren, verglichen mit 72%, die E-Mails versenden (European Commission, 2018). Dieses tief verwurzelte Vertrauen wird natürlich von Betrügern leicht ausgenutzt, außerdem stehen, während E-Mail-Spam zu einer Multi-Milliarden-Anti-Spam-Industrie geführt hat, Telefonbetrügereien und Betrügereien nicht so sehr im Mittelpunkt des Interesses (Gadhave & Sirsat, 2015).

4. Die Zahlen

Generell gibt es in diesem Bereich eine große Dunkelziffer (Button, McNaughton, Kerr, & Owen, 2014). Die größte Schwierigkeit dabei, eine genaue Vorstellung von diesen Arten von Verbrechen zu erhalten, besteht darin, dass ein großer Teil nicht angezeigt wird (van de Weijer, Leukfeldt, & Bernasco, 2018; Crosman, 2017). Sogar die Daten, die wir haben, vermitteln uns ein verzerrtes Bild, da sie aufgrund dieser nicht erfolgten Anzeigen wahrscheinlich eine Unterschätzung des Problems darstellen (Bidgoli & Grossklags, 2017). Die Gründe für dieses Problem sind jedoch bekannt. Einer davon ist, dass die Opfer oft nicht einmal wissen, dass sie von einem Betrüger kontaktiert wurden (Bidgoli & Grossklags, 2017; Button & Cross, 2017). In einer Umfrage unter 745 Opfern, die von Button, Tapley and Lewis (2012), durchgeführt wurde, wussten 40% der Befragten nicht, dass sie Opfer waren, bis sie von einem Dritten informiert wurden. Ein weiterer Grund dafür, dass die Taten nicht zur Anzeige gebracht werden, ist die Wahrnehmung der Schwere des Verbrechens durch das Opfer. Während beispielsweise ein Massen-Phishing-Angriff zu einem hohen Gesamtbetrag führt, sind die Verluste im Einzelfall eher gering. Opfer glauben oft, dass die Erstattung einer Anzeige die Mühe nicht lohnt und es außerdem unwahrscheinlich ist, dass die Täter jemals gefasst werden (Bidgoli & Grossklags, 2017; Button & Cross, 2017). Darüber hinaus liegt eine Anzeige bei der Polizei nicht unbedingt auf der Hand. Es gibt mehrere Akteure, denen der Betrug gemeldet werden kann, außerdem betrachtet die Polizei diesen Bereich nicht unbedingt als Priorität (Button & Cross, 2017). Laut der Eurobarometer-Umfrage zum Thema Cyber-Sicherheit (Europäische Kommission, 2017) würde nur die Hälfte der Befragten zur Polizei gehen, wenn sie eine(n) betrügerische(n) E-Mail oder einen Telefonanruf erhalten. 18 Prozent von ihnen würden es überhaupt nicht melden, vier Prozent wissen nicht einmal, an wen sie sich wenden sollten. Dies wurde auch durch andere Studien bestätigt (Button & Cross, 2017; Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014).

Die vielleicht größten positiven Nebenwirkungen für den Täter, wenn er sein Opfer durch Social Engineering zur Mitwirkung bewegt, sind die Gefühle der Selbstbeschuldigung und Scham, die das Opfer danach hat. Umgekehrt ist dies ein weiterer Grund, warum so selten Anzeige erstattet wird (Cross, Richards, & Smith, 2016; Titus & Gover, 2001). So befürchten Opfer beispielsweise bei CEO Fraud eine Rufschädigung im Unternehmen oder gar den Verlust ihres Arbeitsplatzes (Europol, 2016). Die Opfer geben sich oft selbst die Schuld, da sie aktiv an der Begehung des Verbrechens beteiligt waren und sich schämen, dass sie darauf hereinfielen (Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014). Sie betrachten sich

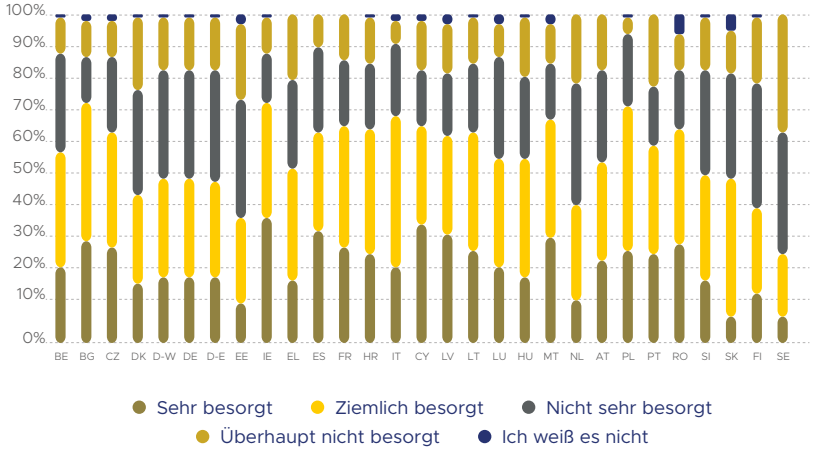
als wesentlicher Bestandteil des Verbrechens und schämen sich für ihr Handeln, sie fürchten, dass die Polizei ihnen nicht glaubt oder sie nicht ernst nimmt (Button, Tapley, & Lewis, 2012). Diese aktive Beteiligung des Opfers am Verbrechen verdeckt also nicht nur unsere Sicht auf das Problem, sondern kann sogar zu einer sekundären Viktimisierung führen (Button & Cross, 2017). Einige Betrügereien, wie der 419 Scam, verfügen über diesen eingebauten Anti-Anzeige-Mechanismus, da das Opfer in einigen Fällen auch illegale Handlungen durch Überweisungen von illegalem Geld vornimmt (Button, Lewis, & Tapley, 2009) (siehe oben) und Betrüger bewusst beschämende Szenarien schaffen, um Anzeigen zu vermeiden (Button, McNaughton, Kerr, & Owen, 2014).

Wenn die Betrügereien an die offiziellen Institutionen gemeldet werden, werden sie höchstwahrscheinlich unter dem breiteren Begriff „Betrug“ zusammengefasst, was es sehr schwierig macht, einzelnen Betrug zu isolieren (Button & Cross, 2017). In einem Fragebogen, der den Mitgliedstaaten zur Vorbereitung dieser Toolbox zugesandt wurde, fanden wir ähnliche Beobachtungen. In elf der 13 Mitgliedstaaten, die geantwortet haben, werden Telefonbetrügereien unter „Betrug“ vermeldet.

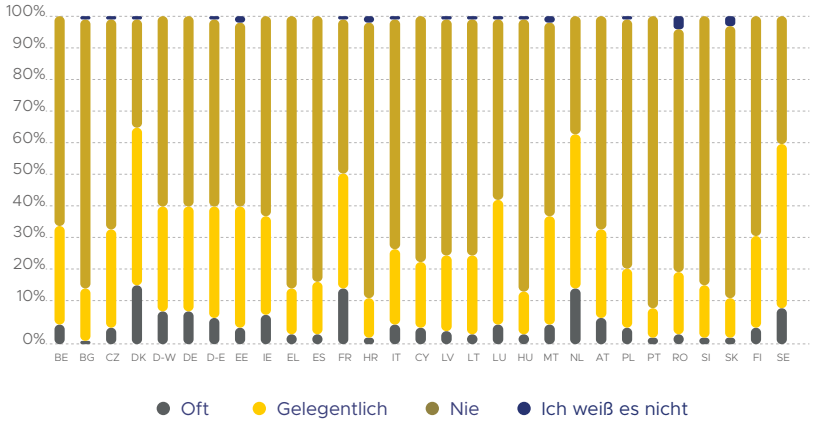
Eine Lösung für dieses Problem der Dunkelziffer bei amtlichen Statistiken ist der Einsatz von Viktimisierungserhebungen. Die gleichen Probleme werden jedoch von den Wissenschaftlern wieder aufgeworfen. Viele dieser Studien unterscheiden nicht zwischen Betrug, der online oder mit Methoden der „alten Schule“ begangen wird, oder decken Einzelbetrugsfälle überhaupt nicht ab. Und auch hier wird immer noch gezögert, Anzeige zu erstatten, es gibt immer noch Opfer, die nicht wissen, dass sie Opfer sind oder die glauben, dass ihr besonderer Fall eine Anzeige nicht lohnt (Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Ungeachtet dieser kritischen Fragen wurden in der Eurobarometer-Sonderumfrage zur Cyber-Sicherheit (Europäische Kommission, 2017) fast 30.000 EU-Bürger zu Hause gezielt zum Thema Betrugs-E-Mails oder -Telefonate befragt. Levi (2017) beschreibt diese Umfrage als „einzige länderübergreifende vergleichende Datenerhebung über Betrugsviktimisierung in der EU“ (Levi, 2017, S. 4).

In allen bis auf fünf Mitgliedstaaten äußerte mindestens die Hälfte der Teilnehmer der Eurobarometer-Umfrage eine gewisse Besorgnis darüber, Opfer von betrügerischen E-Mails oder Telefonaten zu werden, wobei Irland und Bulgarien die höchsten Zahlen (73%) aufwiesen. Dänemark (45%), die Niederlande (42%), Finnland (41%), Estland (38%) und Schweden (27%) sind die Ausnahmen von diesen allgemeinen Ergebnissen. Interessant ist jedoch, dass drei dieser Länder zu den Ländern mit den höchsten selbst gemeldeten Viktimisierungszahlen gehören. In Dänemark (66%),

Wie besorgt sind Sie persönlich darüber, Opfer folgender Situationen zu werden: Erhalt von betrügerischen E-Mails oder Anrufen, in denen nach Ihren persönlichen Daten gefragt wird (einschließlich Zugang zu Ihrem Computer, Logins, Bank- oder Zahlungsinform



Wie oft haben Sie persönlich folgende Situationen erlebt oder sind ihnen zum Opfer gefallen: Erhalt von betrügerischen E-Mails oder Anrufen, in denen nach Ihren persönlichen Daten gefragt wird (einschließlich Zugang zu Ihrem Computer, Logins, Bank- oder Z



den Niederlanden (64%), Schweden (61%) hat mehr als die Hälfte der Befragten betrügerische E-Mails oder Telefonate erhalten. Die Slowakei (14%), Kroatien (14%) und Portugal (11%) weisen die niedrigsten Prozentsätze auf.

Von der enormen Dunkelziffer einmal abgesehen herrscht auch ein Mangel an Forschung über die Viktimologie dieses Verbrechens (Whitty, 2018; Button, Lewis, & Tapley, 2014). Die meisten Studien zu Opferprofilen konzentrieren sich außerdem auf Online-Betrügereien, sodass die folgenden Aussagen hauptsächlich auf diesen Ergebnissen basieren. Wie jedoch im Abschnitt über die verschiedenen Arten von Betrügereien gezeigt wurde, gibt es eine Vielzahl von Betrügereien, was die Grundlage dafür bildet, dass fast jeder in der Gesellschaft zum potenziellen Opfer wird. Dies erschwert allgemeine Aussagen über eine Typologie der Opfer. Dennoch haben Studien gezeigt, dass bestimmte Gruppen besonders anfällig für bestimmte Betrugsfälle sind. Betrügereien bei Verbraucherinvestitionen kommen beispielsweise bei älteren Menschen und der Erwerbsbevölkerung häufiger vor, da sie über die tatsächlichen Investitionsmöglichkeiten verfügen (Button & Cross, 2017).

Die vielleicht wichtigste Ergänzung der Viktimologie-Studien zu diesem Thema ist die Überwindung des Mythos, der hinsichtlich der Prävalenz zwischen verschiedenen Altersgruppen existiert. Insbesondere in den Medien ist die Auffassung verbreitet, dass vor allem ältere Menschen Opfer dieses Verbrechens sind (Button, Lewis, & Tapley, 2009). Entgegen dieser landläufigen Meinung haben Umfragen jedoch gezeigt, dass jüngere Erwachsene die vorherrschende Opfergruppe sind (Button, Lewis, & Tapley, 2009; Ross, Grossmann, & Schryer, 2014). Diese verbreitete Vorstellung leitet sich aus dem Stereotyp ab, dass ältere Menschen keine Finanzkenntnisse haben, vertrauensseliger sind, langsamere kognitive Funktionen haben usw. Diese Ergebnisse sind natürlich bis zu einem gewissen Grad zutreffend, aber es ist wichtig zu verstehen, *warum* ältere Menschen überhaupt ins Visier genommen werden. Wenn wir uns auf die Attraktivität des Ziels konzentrieren, haben ältere Menschen problemlosen Zugang zu Ersparnissen, haben eher Privatbesitz, mehr zusätzliche Kreditlinien (Barnes, 2017). Dies ist laut Button und Cross (2017) der Hauptgrund, warum sie in hohem Maße Ziel von Betrugsfällen sind. Die jüngere Bevölkerung und die Gruppe mittleren Alters sind jedoch Berichten zufolge anfälliger für diese Betrügereien (Button & Cross, 2017; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Whitty, 2018). Die meisten Studien gelangen tatsächlich zu dem Schluss, dass ältere Verbraucher ein geringeres Risiko haben, Opfer von individuellem Betrug

zu werden. Andererseits ist Betrug für die ältere Bevölkerung das Verbrechen, mit dem sie am wahrscheinlichsten konfrontiert werden (Button & Cross, 2017). Dies bleibt jedoch ein ambivalentes Thema, das näher untersucht werden muss, da spezifische Betrugsformen wie Anlagebetrug oder Lotteriebetrug eine höhere Prävalenz bei älteren Menschen aufweisen (Anderson, 2016).

In diesem Zusammenhang werden vor allem junge Menschen (15-25 Jahre) als gefährdet eingestuft (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Dies könnte auf ein niedrigeres Bildungsniveau, weniger online verbrachte Jahre, weniger Verfügbarkeit von Aufklärungsmaterial und geringere Risikoaversion zurückzuführen sein (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Dieser letzte Punkt wird auch von Button, Lewis und Tapley (2009) angesprochen, da Menschen mit einer positiveren Einstellung zum Eingehen finanzieller Risiken und Personen mit geringer Selbstkontrolle als anfälliger angesehen werden. In Untersuchungen von De Kimpe, Walrave, Hardyns, Pauwels und Ponnet (2018) wird behauptet, dass ein hohes Maß an Vertrauen oder „Compliance“ zu einer höheren Anfälligkeit führt, die ein positiver Indikator für die Reaktion auf Phishing-Mails ist. Ein hohes Maß an Pflichtbewusstsein soll auch positiv mit der Viktimisierung verbunden sein. In akademischen Studien wird jedoch diskutiert, ob mehr Interneterfahrung und technologisches Wissen zu einer geringeren Anfälligkeit für Phishing führt oder genau umgekehrt, denn technisch kompetent zu sein bedeutet auch eine höhere Gefährdung (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018). Außerdem stellt Button (2017) fest, dass in Studien darauf hingewiesen wurde, dass Betrugsopfer zwar typischerweise als ungebildet und in Finanzdingen unkundig dargestellt werden, das Gegenteil jedoch der Fall zu sein scheint. Sie bieten drei mögliche Erklärungen für dieses Phänomen. Die erste ist die „Kluft zwischen Wissen und Handeln“, womit gemeint ist, dass Menschen oft die Signale eines Betrugs erkennen, dieses Wissen aber nicht auf ihre Situation anwenden. Eine zweite Erklärung wird als „Expertenfalle“ bezeichnet und bezieht sich auf die Falle, in die finanziell versierte Menschen geraten, da sie zu vertrauensselig sind und die Gefahren ignorieren. Eine letzte Erklärung könnte sein, dass die Opfer zwar über ausreichende finanzielle Kenntnisse verfügen könnten, ihnen jedoch das Gespür für Überzeugungs- und Social-Engineering-Taktiken fehlt (Button & Cross, 2017).

Bei der Untersuchung, wie einzelne Opfer tatsächlich kontaktiert werden, hat die Literatur auch einige Auswahltechniken identifiziert, die von Betrügern verwendet

werden. Zum Beispiel wählen einige Betrüger bei bestimmten Telefonbetrügereien einfach zufällig Nummern aus Telefonbüchern oder Registern von öffentlichen Unternehmen. Andere hingegen verwenden so genannte „Sucker Lists“ (Trottellisten). Diese Listen sind Verzeichnisse bereits betrogener Opfer, die unter Betrügern gehandelt werden (Wood, Liu, Hanoch, Xi, & Klapatch, 2018). Levi (2008) beschreibt dies wie folgt:

> *„Sobald jemand per Internet, Post oder Telefon an einer Lotterie teilgenommen oder ein anderes Produkt erworben hat, erhält er bald ähnliche betrügerische „Angebote“ von anderen Betrügern“* (Levi, 2008, S. 404)

Die Verwendung solcher Listen lässt auch auf ein hohes Maß wiederholter Viktimisierung schließen (Button, Lewis, & Tapley, 2009). Auch scheint eine relativ kleine Anzahl von Tätern für die Mehrheit der Telefonbetrügereien verantwortlich zu sein. In einer Studie von Marzuoli, Kingravi, Dewey und Pindrop (2016) wurde ein Honeypot-System zur Analyse des Betrugsökosystems verwendet. Von 8.000.000 erhaltenen Anrufen analysierten die Forscher 40.000. Nur 1,8% der anrufenden Quellen waren für 66% der Beschwerden verantwortlich. Diese Ergebnisse weisen in die Richtung der so genannten „Scampreneurs“, was sich auf den Unternehmergeist einiger Betrüger bezieht, die ihr Betrugsangebot diversifizieren und versuchen, ihre Effektivität zu maximieren (Button, Lewis, & Tapley, 2009; Button, McNaughton, Kerr, & Owen, 2014).

Dennoch sind nicht alle Betrüger gleichermaßen professionell und organisiert. Im Telefonbetrugsgeschäft arbeiten einige Betrüger auf Ad-hoc-Basis und ändern ihre Vorgehensweise, sobald die Strafverfolgungsbehörden sie zu bemerken scheinen. Andere Netzwerke sind größer und haben eher „formale“ Proportionen, sie haben eine Art Hierarchie, Arbeitsteilung und gestaffelte Bezahlung. Solche Betrüger können auch in die traditionelle organisierte Kriminalität verwickelt sein (z.B. die Drogenszene) oder sich ausschließlich auf Betrug konzentrieren (Levi, 2008; Barnes, 2017; Button, Lewis, & Tapley, 2009).

Was die Herkunft der Betrüger betrifft, so sind Nigerianer fast per Definition schon in den Betrug mit dem nigerianischen Prinzen verwickelt, aber im Allgemeinen sind Täter aus westafrikanischen Ländern in allen Arten von Betrügereien aktiv (Button, Lewis, & Tapley, 2009; Levi, 2008; Button & Cross, 2017). Im Bereich des

internetbasierten Betrugs haben osteuropäische kriminelle Gruppen (Russland, Rumänien, Litauen usw.) eine besondere Kompetenz und Reputation entwickelt (Button, Lewis, & Tapley, 2009; Levi, 2008). Grenzüberschreitende Betrügereien sind besonders häufig, was es für die Strafverfolgung und die nationale Politik sehr schwierig macht, diese Probleme anzugehen (Button & Cross, 2017). Umso mehr Gründe, dieses Verbrechen von vornherein zu verhindern.

5. Schlussfolgerungen

Im ersten Teil dieser Toolbox haben wir eine Zusammenfassung des aktuellen **Erkenntnisstandes** zum Thema individueller Betrug gegeben. Da Betrug ein sehr vielfältiges Verbrechen ist, das ein breites Spektrum von Aktivitäten umfasst, haben wir unseren Fokus auf individuellen Betrug verengt und gleichzeitig die aktuellen gemischten Online- und Offline-Merkmale dieser Art von Verbrechen hervorgehoben.

Den meisten Fällen von individuellem Betrug liegt eine Technik zugrunde, die als Social Engineering bezeichnet wird. Diese Technik ist die wesentliche Taktik, um das Vertrauen der Opfer zu gewinnen zu überzeugen, auf den Betrug einzugehen. Das Opfer spielt daher eine sehr aktive Rolle bei der Ausführung des Verbrechens, was zu Scham und Schuldgefühlen führt. Wir haben **Social Engineering** in Studien im Bereich der Sozialpsychologie angesiedelt und einige der Grundprinzipien gezeigt, die an der Überzeugungskunst beteiligt sind.

Es gibt jedoch viele verschiedene **Formen und Typen** von Betrug. Wir haben diese Typen entweder nach ihrem Inhalt oder nach der Art der Durchführung (persönlich oder unter Einsatz von IKT) kategorisiert. Zusätzlich zu dieser großen Vielfalt scheinen sie an Raffinesse und Komplexität zuzunehmen. Außerdem kratzen wir höchstwahrscheinlich nur an der Oberfläche, da in diesem Bereich die **Dunkelziffer** immens ist. Die Opfer zeigen dieses Verbrechen aus verschiedenen Gründen nicht an: Schamgefühle, empfundene Schwere ihrer Verluste, Unwissen, dass sie Opfer wurden, Unwissen, wo sie Anzeige erstatten sollen,...

Opferbefragungen, wie die Eurobarometer-Umfrage, bieten jedoch eine Lösung für diesen Mangel an Anzeigeerstattung bei offiziellen Stellen. Dennoch sind weitere Untersuchungen über die Schwere dieses Verbrechens und das Profil der Opfer

unerlässlich. So können Präventionsmaßnahmen gezielter und effizienter gestaltet werden. Wir werden nun einen Blick auf die derzeitigen bewährten Verfahren in diesem Bereich werfen.

02 TEIL II: BEWÄHRTE PRAKTIKEN

1. Einführung

Im zweiten Teil dieser Toolbox werden wir gründlicher darauf eingehen, wie wir verhindern können, dass es zu individuellem Betrug kommt. Wie bereits im vorherigen Teil erläutert, ist die Bewältigung dieses Problems für die Polizei äußerst schwierig. Button (2017) macht geltend, dass die Polizei nicht über die notwendigen Mittel verfügt, um die Mehrheit dieser Betrugsformen zu untersuchen, was die Prävention umso wichtiger macht (Europol, 2016). Zu dieser Gefahr kommt hinzu, dass die Betrugsprävention in der Regel wenig wissenschaftliche Aufmerksamkeit erlangt hat. Dies erschwert Aussagen über die Wirksamkeit, obwohl es in diesem Bereich zahlreiche Aktivitäten gibt (Button & Cross, 2017). In diesem Teil der Toolbox werden wir eine Bestandsaufnahme einiger der akademischen Erkenntnisse zur Prävention von individuellem Betrug vornehmen, aber auch einige bewährte Praktiken aufzeigen. Zuletzt werden wir einige Empfehlungen geben, wobei wir uns besonders auf die Prävention von Telefonbetrug konzentrieren werden.

Die am meisten verbreitete Taktik zur Prävention von individuellem Betrug ist die Aufklärung der Öffentlichkeit. Technische Maßnahmen wie Spamfilter, Rechtschreibprüfung, Überwachung gefälschter Website-Domains usw. haben alle ihre eigenen Vorzüge. Sie bleiben jedoch reaktiv, da sie letztlich als Reaktion auf bestimmte Methoden konzipiert sind (Jakobsson, 2016; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Die Täter können sich auf diese Maßnahmen einstellen, was sich an ihrem ständig wachsenden Entwicklungsstand zeigt. Darüber hinaus sind diese technischen und verfahrenstechnischen Maßnahmen nicht zu 100% sicher, da es immer wieder Schwächen bei diesen Systemen und Personen geben wird. Dennoch bringt uns jede Sicherheitsmaßnahme zu einer sichereren Grundlinie und ist wichtig, um dieses komplexe Verbrechen zu bekämpfen.

Das Schließen dieses „Sicherheitslecks“ ist der wahrscheinlichste Grund, warum viele präventive Maßnahmen zur Aufklärung der Öffentlichkeit und zur Sensibilisierung ergriffen werden (Workman, 2008). Wie bereits erwähnt, bleibt ein großer Teil dieser Bemühungen unbewertet (Mears, Reisig, Scaggs, & Holtfreter, 2016), aber es gibt einige allgemeine Erkenntnisse. Online-Trainings, kontextbezogenes Lernen1, eingebettetes Training2 und interaktive Spiele3 haben sich alle als effektiv erwiesen, um die Sicherheit der Benutzer zu verbessern (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Die Menschen werden beispielsweise darin geschult, bestimmte sprachliche Merkmale zu erkennen

(Tabron, 2016) oder instinktive Unterscheidungstaktiken anzuwenden (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Diesen Schulungen sind wichtig, um die bereits erwähnte Kluft zwischen Wissen und Handeln zu schließen. Die Sensibilisierung führt zu einem besseren Verständnis des Phänomens, aber nicht unbedingt zu einer verstärkten Anwendung dieses Wissens auf die eigene Situation (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Eine Kombination aus Sensibilisierung und Training scheint den größten Nutzen zu haben (Cross, Richards, & Smith, 2016; Europol, 2016; Bullée J.-W. , Montoya, Junger, & Hartel, 2016). In einer Studie von Sheng, Holbrook, Kumaragur, Cranor und Downs (2010) wurden diese Schulungen gemischt und sie zeigte eine 40%ige Verbesserung nach der Einführung von Trainingsmaterial im Vergleich zu einer Kontrollgruppe (Online-, Kontext- und Embedded-Training und interaktive Spiele kombiniert).

Charakteristisch für diese Art von Kriminalität ist die aktive Beteiligung des Opfers und das hohe Maß an wiederholter Viktimisierung (Button, Lewis, & Tapley, 2009; Cross, Richards, & Smith, 2016). Aufgrund dieser aktiven Rolle wird das Opfer oft beschuldigt und beschämt. Sensibilisierungskampagnen sollten sich auch auf diesen Aspekt konzentrieren, damit die Opfer und ihre Umgebung erkennen können, dass dies nicht ihre Schuld ist, sondern das Ergebnis einer böswilligen Handlung des Täters (Burgard & Schlembach, 2013). In dieser Hinsicht können viele emotionale Schäden vermieden werden. Darüber hinaus sollte das Opfer auch auf die Gefahr aufmerksam gemacht werden, ein zweites Mal zum Opfer zu

„Situative Verbrechensprävention kann dadurch charakterisiert werden, dass sie Maßnahmen (1) umfasst, die auf hochspezifische Kriminalitätsformen (2) ausgerichtet sind, die das Management, die Gestaltung oder die Manipulation der unmittelbaren Umgebung in einer möglichst systematischen und dauerhaften Weise beinhalten (3), um die Chancen für Kriminalität zu verringern und die von einer Reihe von Straftätern wahrgenommenen Risiken zu erhöhen“ (Lab, 2010, S. 192). Im Wesentlichen geht es darum, Kriminalität zu verhindern, indem man die Merkmale von Situationen reduziert, die Straftaten erleichtern. Spezifische situative Merkmale werden manipuliert, um Gelegenheiten für Verbrechen zu blockieren (Jacques & Bonomo, 2017).

werden, z.B. aufgrund der Existenz von „Sucker Lists“ (Cross, Richards, & Smith, 2016).

Es gibt eine besonders interessante wissenschaftliche Publikation zu diesem Thema. Vor kurzem veröffentlichten Mark Button und Cassandra Cross ein Buch mit dem Titel *Cyber Frauds, Scams and their Victims* (2017). Neben zahlreichen Einblicken in diese Art von Kriminalität ist ein ganzes Kapitel der Prävention von Cyber-Betrug und Scams gewidmet. Die Autoren bauten dieses Kapitel auf dem Rahmen der situativen Verbrechensprävention auf. Nach der Arbeit von Clarke haben sie die 25 Techniken der situativen Verbrechensprävention (Cornish & Clarke, 2003) an den Kontext von Cyber-Betrug und Scams angepasst.

Diese 25 Techniken lassen sich in fünf umfassende Strategien einteilen (was in der Verbrechensprävention funktioniert):

1. Erhöhung des mit der Begehung einer Straftat verbundenen Aufwandes
2. Erhöhung des mit der Begehung einer Straftat verbundenen Risikos
3. Reduzierung des Nutzens der Straftat
4. Reduzierung der Provokationen, die ansonsten zu Verbrechen führen könnten.
5. Beseitigung der Vorwände, die Täter sonst verwenden könnten, um kriminelle Handlungen zu rechtfertigen.

Button and Cross (2017, S. 203) fassten ihre Arbeit in der folgenden Grafik zusammen. Wir empfehlen allen interessierten Lesers dieses Buch, da es einen sehr umfassenden Überblick über Cyber-Betrügereien und Scams bietet und viele Forschungsergebnisse bündelt.

	Erhöhung des Aufwands	Erhöhung der Risiken
Individuum	> Schutz von Konten mit komplexen Passwörtern, Antivirenschutz > Schutzregistrierungen > Maßnahmen ergreifen, um Dritten die Auffindbarkeit persönlicher Kontaktinformationen zu erschweren.	> Regelmäßige Bereinigung von Computern von Viren und Spyware > Überprüfung von Websites, E-Mail-Adressen und Anrufern
Organisation	> Geeignete Kontrollen zum Schutz der personenbezogenen Daten von Kunden > Hintergrundüberprüfungen: Überprüfung, ob Kunden die sind, für die sie sich ausgeben.	> Informationsaustausch: Datamatching und Datamining > Überprüfen von Stimme und Standort der Kunden
Polizeibehörden	> Störung der Aktivitäten von Betrügern > Scambaiting > Erwirken von Urteilen und Beschränkungen gegen Betrüger unter Anwendung des Zivil-, Regulierungs- oder Strafrechts.	> Informationsaustausch: Datamatching und Datamining > Zentrale Berichterstattung > Veröffentlichung von Informationen über vermutete Betrugsfälle, verdächtige Websites > Gefälschte Scams, um potenzielle Opfer zu alarmieren

Reduzierung des Lohns	Reduzierung von Provokationen	Beseitigung von Vorwänden
Wenn Betrüger bekannt sind und über Vermögenswerte verfügen, Zivilklagen erheben, um Schadenersatz zu erhalten oder Wiedergutmachung durch ein Strafverfahren zu erreichen.		
Wenn Betrüger bekannt sind und über Vermögenswerte verfügen, Zivilklagen erheben, um Schadenersatz zu erhalten oder Wiedergutmachung durch ein Strafverfahren zu erreichen.		Kommunikation mit den Kunden, um sie über die Risiken und bewährten Verfahren zur Risikominderung zu informieren
> Wenn Betrüger bekannt sind und über Vermögenswerte verfügen, Zivilklagen erheben, um Schadenersatz zu erhalten oder Wiedergutmachung durch ein Strafverfahren zu erreichen. > Überwachung von Finanztransfers an Hochrisikodrittländer, um mögliche Opfer zu identifizieren und sie vor einer möglichen Viktimisierung zu warnen.	> Einschränkung der Informationen darüber, wie bestimmte Betrugsfälle durchgeführt wurden > Regulierung von Werbeaktivitäten	> Kommunikation mit der Öffentlichkeit und den Risikogruppen, um die Risiken und bewährten Verfahren hervorzuheben. > Werbekampagnen: Fernsehen, Radio, Zeitungen, Fachpresse, online > Pressemitteilungen zur Sicherung des Medieninteresses > Websites von Spezialisten > Mailshots > Social-Media-E-Mails, Texte, Tweets usw. > Gemeinschafts- und Interessengruppenaktivitäten > Handlungsstränge im Schauspiel

2. Wenn es zu schön erscheint, um wahr zu sein, dann ist es das wahrscheinlich

In diesem Abschnitt werden wir einen Überblick über einige der bewährten Praktiken geben, die wir während der bulgarischen Präsidentschaft kennengelernt haben. Die Projekte und Kampagnen werden in verschiedenen Kategorien diskutiert, die jeweils die Zielgruppe repräsentieren: universelle, ausgewählte oder indizierte Prävention bzw. die gesamte Bevölkerung, eine bestimmte Risikogruppe oder bereits geschädigte Personen. Alle diese Kampagnen und Projekte finden Sie auch im dritten Teil dieser Toolbox.

Universelle Prävention

Die bulgarische Präsidentschaft begann damit, sich auf Betrug und Scams zu konzentrieren, und diese Dringlichkeit spiegelt sich in der Politik der nationalen Polizei wider. Eine komplette „Betrugsabteilung“ innerhalb der nationalen Generaldirektion der Polizei widmet sich diesem Thema, insbesondere dem Telefonbetrug. Sie arbeiten reaktiv, aber auch die Prävention ist bei der Bekämpfung dieses Verbrechens eine grundlegende Aufgabe. Im Rahmen ihrer Arbeit werden das Wissen und die Sensibilisierung der Bevölkerung für dieses Verbrechen durch Informationskampagnen gefördert. So werden beispielsweise Informationsbroschüren verbreitet, aber auch Ratschläge in einer nationalen Radiosendung gegeben. Ein weiteres Beispiel aus Bulgarien sind Aufkleber, die verteilt werden. Diese Aufkleber tragen präventive Botschaften und die Menschen werden gebeten, sie auf ihr Telefon zu kleben. Die Idee ist, dass, wenn sie angerufen werden, sie an die präventive Botschaft erinnert werden, weil sie den Aufkleber sehen, während sie den Hörer abnehmen.

In Schweden gibt es eine ähnliche Einrichtung zur Betrugsbekämpfung: die Schwedische nationale Betrugszentrale. Im Mittelpunkt ihrer Präventionsarbeit steht die Sensibilisierung durch traditionelle Medien und Social-Media-Kanäle, aber auch der Aufbau externer Partnerschaften

mit Behörden und Unternehmen. Einige Kampagnen dienen einem doppelten Zweck. Neben der Sensibilisierung für die Gefahren von Betrug durch Medienkampagnen nutzten sie die Medien auch, um Druck bezüglich einer bestimmten App mit schwerwiegenden Sicherheitsproblemen auszuüben, die von Betrügern ausgenutzt wurden. Diese Medienpräsenz veranlasste die App-Designer, ihre Sicherheit zu verbessern.

Auf europäischer Ebene findet jedes Jahr im Oktober der European Cyber Security Month (ECSM)4 statt. Diese EU-weite Kampagne soll die Cyber-Sicherheit bei Bürgern und Organisationen fördern und zeigt einfache Schritte auf, die unternommen werden können, um dies zu erreichen. Die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), die Europäische Kommission, Europol und insbesondere das Europäische Zentrum für Cyber-Kriminalität (EC3) sowie eine Vielzahl öffentlicher und privater Partner aus den Mitgliedstaaten arbeiten zusammen, um dieses Ziel zu erreichen und während des Monats zahlreiche Veranstaltungen und Kampagnen zu organisieren. In der dritten Woche der Kampagne 2018 lag der Schwerpunkt auf Cyber-Betrug. Ziel war es, die Öffentlichkeit darüber aufzuklären, wie man betrügerische Inhalte erkennt, um online sowohl für die eigene Sicherheit als auch die ihrer Finanzen zu sorgen. EC3, der Europäische Bankenverband (EBF) und andere Partner schlossen sich zusammen, um eine Sensibilisierungskampagne zu diesem Thema durchzuführen. Einige Beispiele aus dem Material finden Sie unten.

Eine weitere Sensibilisierungskampagne ist die Anti-Phishing-Kampagne, die vom belgischen Zentrum für Cyber-Sicherheit (CCB) durchgeführt wurde. Diese klassische Kampagne informierte darüber, wie man betrügerische E-Mails erkennt. Die Kampagne wurde durch Videos, E-Mail-Signaturen, Banner, Poster, aber auch auf einer Webseite verbreitet. Neben Informationen und Präventionstipps bot die Website auch einen Test für die Öffentlichkeit, um zu sehen, wie „phishing-sicher“ sie ist. Nach dem Test werden präventive Materialien dazu gezeigt, welche Schritte

ROMANCE SCAM

Scammers target victims on online dating websites, but can also use social media or email to make contact.

WHAT ARE THE SIGNS?

Someone you have recently met online professes strong feelings for you, asking to chat privately.

Their messages are often poorly written and vague.

Their online profile is not consistent with what they tell you.

They may ask you to send intimate pictures or videos of yourself.

First they gain your trust. Then they ask you for money, gifts or your bank account/credit card details.

If you don't send the money, they may try to blackmail you. If you do send it, they will ask for more.

ARE YOU A VICTIM?

Don't feel embarrassed!
Stop all contact immediately.
If possible, keep all communication, such as the chat messages.
File a complaint with the police.
Report it to the site where the scammer first approached you.
If you have provided your account details, contact your bank.

WHAT CAN YOU DO?

- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used elsewhere.
- **Be alert** to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working.
- **Don't share** any compromising material that could be used to blackmail you.
- If you agree to meet in person, **tell family and friends** where you are going.
- **Beware of money requests.** Never send money or give credit card details, online account details, or copies of personal documents.
- **Avoid sending them upfront payments.**
- **Don't transfer money** for someone else: money laundering is a criminal offence.

EUROPOL EC3 | European Cybercrime Centre

EBF

EUCPN

#CyberScams

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.

WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**

EUROPOL EC3 European Cybercrime Centre

EBF

EUCPN

#CyberScams

und Maßnahmen zur weiteren Verbesserung der Sicherheit unternommen werden können. Darüber hinaus kann man auch E-Mails, die als verdächtig empfunden werden, an eine E-Mail-Adresse des CCB senden. Das CCB prüft dann diese E-Mails und Links zu betrügerischen Websites und setzt diese auf die schwarze Liste der vier wichtigsten Browser (Internet Explorer, Mozilla Firefox, Google Chrome und Safari). Dies geschieht im Rahmen der Partnerschaft der EU-Phishing-Initiative. Sobald diese Websites auf der schwarzen Liste stehen, werden sie für andere Benutzer gesperrt. Dieser CCB-Mechanismus ist in der Lage, jeden Tag fünf Websites auf die Liste zu setzen, was einen sehr interessanten, gruppenfinanzierten Präventionsmechanismus darstellt.

Die EU-Anti-Phishing-Initiative ist ein von der Europäischen Kommission finanziertes Projekt, das in erster Linie die Störung betrügerischer Websites zum Ziel hat. Ziel ist es, Phishing-Scams operativ daran zu hindern, Opfer zu täuschen, indem die zu diesem Zweck verwendeten Websites blockiert werden. Sie basiert auf einer öffentlich-privaten Partnerschaft zur Bekämpfung von Phishing.

Weitere Informationen: https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2013_ISEC_AG_INT_4000005246_en

Selektiv

Wie bereits in den vorangegangenen Abschnitten erwähnt, gilt älteren Menschen bei dieser Art von Verbrechen besondere Aufmerksamkeit. Dies wurde bereits in der Toolbox zu Verbrechen gegen ältere Menschen deutlich, die unter slowakischer Präsidentschaft erstellt wurde. Eine Reihe von Projekten, die in diesem Jahr am Wettbewerb des European Crime Prevention Award teilnahmen, befassten sich mit dieser Art von Kriminalität gegen ältere Menschen. So konzentrierte sich beispielsweise das deutsche Projekt „Hallo Oma, ich brauch Geld“, das an zweiter Stelle stand, auf Telefonbetrug mit dem Enkeltrick. Mit einem interaktiven Bühnenstück werden ältere Menschen über dieses Kriminalitätsphänomen informiert, während gleichzeitig das Ziel verfolgt wird, subjektive Unsicherheitsgefühle zu reduzieren.

Ähnlich ist das tschechische Programm „Nedáme se“ (oder „Das lassen wir uns nicht gefallen“) ein interaktives Aufklärungsstück, bei dem vier Arten von gängigen betrügerischen manipulativen Täuschungen älterer Menschen auf der Bühne dargestellt werden. Dies sind Verkaufskampagnen, der Verkauf von Parfums auf der Straße, Telemarketing und Verkauf im Seniorenheim. Neben den Schauspielern traten ein Polizist und auch die Autorin des Stücks, die Psychologin Ph. Dr. Romana Mazalová auf. Sie kommen auf die Bühne, interagieren mit dem Publikum und vermitteln ihm so neue Strategien der Verteidigung. So macht das Stück nicht nur Spaß, sondern wird auch zu einer neuen Form der Aufklärung gegen sogenannte „Šmejdi“ oder Betrüger. Insgesamt nahmen tausend ältere Menschen an dem Projekt teil. Die pädagogische Wirkung dieses Theaterstücks auf das Publikum wurde experimentell untersucht. Die Ergebnisse bestätigten, dass die Senioren, die das Stück gesehen hatten, sich als erfolgreicher bei der Verteidigung gegen betrügerische Verkäufer erwiesen. Im Experiment wurden 130 Senioren, die das Bühnenstück sahen, mit einer Kontrollgruppe verglichen. Ein halbes Jahr nach dem Anschauen des Bühnenstücks lehnte die Versuchsgruppe ein betrügerisches Geschäft 2,5 mal öfter ab als die Gruppe, die das Stück nicht sah.

Ein weiteres Projekt, das sich auf die Arbeit mit älteren Menschen konzentriert, ist das Projekt „Der Preis der Freundschaft“ aus Rumänien. Ziel des Projekts war es, das Risiko für ältere Menschen, Betrügern zum Opfer zu fallen, zu verringern, indem es folgende Ziele verfolgte: Kenntnis der Zielgruppe aus Einstellungs- und Verhaltenssicht, Erhöhung des Niveaus des präventiven Wissens der älteren Menschen und Steigerung der Fähigkeit zur Selbstverteidigung. Die Zielgruppe bestand aus Personen über 60 Jahren, die Mitglieder lokaler Seniorenclubs sind. Im Jahr 2017 wurden insgesamt 34 präventive Informationsmaßnahmen durch die Polizei durchgeführt. Die Informationen wiesen auf die Risiken hin, die mit dem Alter verbunden sind, aber auch auf die Vermeidung der Viktimisierung bei Täuschungen, wie beispielsweise gefälschten

Telefonkampagnen. Außerdem wurden für ältere Menschen Online-Trainingskurse angeboten. Darüber hinaus wurde ein „Senioren-Sicherheits-Ball“ veranstaltet, um eine öffentliche Informationskampagne zu starten.

Neben der Sensibilisierung dieser Zielgruppe wird in Bulgarien ein interessanter Mechanismus umgesetzt. Die bulgarische Betrugsabteilung unterhält mehrere enge Partnerschaften mit privaten Akteuren, wie beispielsweise dem Bankensektor. Dieser eher situative Präventionsmechanismus führt ein Kontrollsystem ein, wenn eine Person über 50 Jahre einen Betrag von mehr als 3000 Euro abhebt. In diesem Fall erhält der Bankmitarbeiter eine Warnung, worauf er einige Fragen stellen kann, um zu prüfen, ob der ältere Kunde eventuell Opfer einer manipulativen Täuschung wird.

Angezeigt

Eine weitere Reihe von Präventionsmaßnahmen konzentriert sich auf Personen, die bereits Opfer geworden sind. Spezifische Maßnahmen zielen darauf ab, eine fortgesetzte Viktimisierung zu verhindern und zu vermeiden, dass Personen mehrfach Opfer verschiedener Betrugsfälle werden. So konzentriert sich beispielsweise das Projekt Sunbird in Australien auf Finanztransaktionen zwischen Westaustralien und einigen westafrikanischen Ländern. Die Polizei überprüft diese Transaktionen und listet die illegal erscheinenden Transaktionen auf. Die Opfer werden dann kontaktiert und ihnen wird erklärt, warum die Polizei glaubt, dass sie einem Betrug zum Opfer gefallen sein könnten. Nach Auswertung hörten 73 Prozent der kontaktierten Personen auf, Geld in diese Länder zu schicken (Button & Cross, 2017).

Im Vereinigten Königreich berichtet Action Fraud, die nationale Meldestelle für Betrug und Cyber-Kriminalität, regelmäßig über die neuesten Betrugsfälle und Scams (Button & Cross, 2017). Sie leitet die Opfer auch an bestimmte Unterstützungsgruppen weiter, um den von der Straftat Betroffenen zu helfen oder ihnen mitzuteilen, an wen sie sich wenden müssen5. Dies kann dazu beitragen, den emotionalen Schaden zu verringern, aber auch den Opfern bei der Wiedererlangung verlorener Gelder zu helfen oder Ratschläge zu geben, wie sie sich in Zukunft verhalten sollten, wenn sie erneut kontaktiert werden. Aufgrund der Existenz von „Sucker Lists“ (siehe oben) ist dies eine echte Bedrohung.

Wie bereits erwähnt, leiden die Opfer aufgrund ihrer Viktimisierung unter einer Vielzahl von negativen Auswirkungen. Unter anderem äußerten die Opfer das

dringende Bedürfnis, einfach angehört und als Opfer anerkannt zu werden. Allerdings gibt es - auch weltweit - nur wenige Unterstützungsleistungen für diese Opfer. Ein seltenes Beispiel für ein solches Unterstützungsprogramm findet sich in Kanada: die Senior Support Unit. Über einen Telefondienst, der mit älteren Freiwilligen und ebenfalls Betroffenen besetzt ist, unterstützt sie Betrugsopfer. Sie geben Ratschläge und Warnungen, hören zu und beruhigen (Cross, 2016). Eine solche Initiative bietet nicht nur Unterstützung für einzelne Opfer, sondern trägt auch dazu bei, den Grad der Anzeigeerstattung zu erhöhen, was wiederum zu einer besser informierten Polizeiarbeit und Prävention führt.

3. Verhindern von Telefonbetrug: Wie kann ich Ihnen helfen?

Das EUCPN-Sekretariat veranstaltete einen Workshop zum Thema individueller Betrug. Eine Reihe von Experten kamen zusammen und diskutierten ihre Ideen und ihre präventive Arbeit auf diesem Gebiet. Der Workshop bestand aus drei Teilen. Zunächst wurde der Aufklärungsstand des individuellen Betrugs diskutiert. Dies spiegelt den ersten Teil dieser Toolbox wider. Zweitens wurden verschiedene Projekte vorgestellt und mit der Gruppe diskutiert, was sich im obigen Abschnitt widerspiegelt. Zuletzt wurde eine Weltcafé-Methode organisiert, um Empfehlungen zur Prävention von Telefonbetrug zu erarbeiten. So diskutierten die Experten ihre Empfehlungen in kleineren Gruppen. Dies waren die Experten, die am Workshop teilnahmen:

- Mark Button, University of Portsmouth, Vereinigtes Königreich
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Abteilung Betrug in der Generaldirektion der nationalen Polizei, Bulgarien
- Charlotta Mauritzson, Nationales Betrugszentrum, Schweden
- Andries Bomans, Zentrum für Cybersicherheit, Belgien
- Constantin Lica, Abteilung Betrugsbekämpfung, Rumänien
- Aurelian Bocan, Generaldirektion der Polizei Bukarest, Rumänien
- Romana Mazalová, Projekt „Nedáme se“, Tschechien

Wir haben die Empfehlungen nach dem früheren Beispiel von Button (2017) zusammengefasst und die fünf umfassenden Strategien von Clarke als Orientierungsrahmen verwendet. Es versteht sich von selbst, dass diese einander

nicht ausschließen, sondern in verschiedenen Projekten kombiniert werden können. Wie bereits erwähnt, sind dies:

1. Erhöhung des Aufwands
2. Erhöhung der Risiken
3. Reduzierung des Lohns
4. Reduzierung von Provokationen
5. Beseitigung von Vorwänden

Erhöhung des Aufwands

Die erste mögliche Strategie besteht darin, den Aufwand zu erhöhen, den ein Täter auf sich nehmen muss, damit das Verbrechen erfolgreich ist. Die Idee dabei ist, dass, wenn der Aufwand zu hoch ist, der Täter von der Tat absieht. Wie im ersten Teil dieser Toolbox deutlich wurde, können Täter ihre potenziellen Opfer auf legitimen Listen finden. Hier veröffentlichen Organisationen die Kontaktdaten von Personen, ebenso teilen aber auch Personen ihre Telefonnummern frei- und bereitwillig. Beispielsweise kann man Telefonnummern auf Facebook-Profilen, LinkedIn-Seiten usw. sehen. Die Einschränkung der Veröffentlichung von Telefonnummern auf diesen Listen und Social-Media-Profilen könnte es einem Täter bereits erschweren, seine Opfer zu kontaktieren.

Eine weitere Möglichkeit, den Aufwand zu erhöhen, besteht darin, den Zugang zur Nutzung von Telefonnummern zu beschränken. Der Erwerb einer Prepaid-Karte oder einer neuen Telefonnummer ist denkbar einfach. Dies ermöglicht es den Tätern, die Telefonnummer ständig zu wechseln, was die Strafverfolgung erschwert. Eine Idee aus dem Workshop war es, die Anzahl der Telefonnummern pro Person zu begrenzen, indem sie mit ihrem Bankkonto oder ihrer ID-Nummer verknüpft werden. Eine intensive Zusammenarbeit mit Mobilfunkunternehmen wäre hier ratsam. Dies erhöht nicht nur den Aufwand für den Täter, sondern verringert auch die Anonymität und erhöht das Risiko, gefasst zu werden.

Dank des Aufkommens der Internet-Telefonie ist es nach wie vor recht einfach, potenzielle Opfer zu kontaktieren und den eignen Standort zu fälschen, um ihn legitim erscheinen zu lassen. Die zunehmende Verwendung von Passwörtern, Verschlüsselung und die fast vollständige Verhinderung von Standortverfälschungen dürften auch den Aufwand erhöhen, den der Täter betreiben muss, um die Opfer zu kontaktieren und zu betrügen.

Scambaiting wurde ebenfalls als mögliche Taktik genannt, obwohl dies an sich nicht ausreichend ist. Die Idee ist, dass Polizeibehörden oder andere Organisationen versuchen könnten, die Betrüger zu betrügen, indem sie sie auf falsche Fährten locken, sodass sie ihre Zeit verschwenden. Während sie damit beschäftigt sind, diesen Spuren nachzugehen, können sie unschuldige Opfer nicht betrügen.

Erhöhung der Risiken

Ein wichtiger Aspekt bei der Betrugsprävention, ist es, zu wissen, womit man es zu tun hat. Der Informationsaustausch ist dabei von entscheidender Bedeutung. Da Betrügereien bei einer Vielzahl von Akteuren, wie z.B. der Polizei, aber auch bei privaten Akteuren angezeigt werden können, ist der Informationsaustausch zwischen dem öffentlichen und dem privaten Sektor unerlässlich. Dies würde eine schnellere Reaktion und besser informierte Präventivmaßnahmen ermöglichen und damit das Risiko erhöhen. Daher müssen auch andere Interessengruppen als die Strafverfolgungsbehörden einbezogen werden. Mobilfunkbetreiber, Banken, Non-Profit-Organisationen usw. haben alle ihre Rolle zu spielen und stellen wichtige Teile für das Informationspuzzle bereit. Auch sollte diese Zusammenarbeit nicht an den Landesgrenzen enden. Europol spielt dabei eine entscheidende Rolle als Vermittler für den Informationsaustausch und grenzüberschreitende Aktivitäten. Da diese Art von Kriminalität zunehmend international ist, sollten auch Drittländer zum Informationsaustausch herangezogen werden. Diese Informationen könnten auch an die breite Öffentlichkeit weitergegeben werden. Wenn bekannt ist, welche Unternehmen Straftäter zu repräsentieren vorgeben, kann sie bereits gewarnt werden.

Natürlich müssen diese Informationen zuerst gesammelt werden, und die Opfer sollten besser über die Möglichkeiten der Anzeigeerstattung informiert werden. Beispielsweise könnten sich Sensibilisierungskampagnen auch darauf konzentrieren, zu zeigen, dass die Anzeige der Straftat zu einer erfolgreichen Ermittlung und angemessenen Lösungen führt. Ein zentrales Meldesystem für Opfer mit Zugang zu allen Akteuren in diesem Bereich würde auch den Prozess der Anzeigeerstattung erheblich erleichtern und die Schwelle senken, an der die Opfer tatsächlich den Schritt zur Anzeige wagen können.

Eine weitere Strategie zur Erhöhung der Risiken besteht darin, die Anonymität zu verringern. Wie unter der Rubrik „Erhöhung des Aufwands“ erwähnt, haben es die Entwicklungen im Bereich IKT ermöglicht, den Standort, von dem aus man anruft,

zu manipulieren. Auf diese Weise könnte man dem Opfer vorgaukeln, dass es mit jemandem aus seinem Land spricht, während es jedoch mit jemandem im Ausland spricht. Die Erschwerung der Manipulation des Standorts führt zu einer erhöhten Exposition und dem Risiko, erwischt zu werden. Dies könnte z.B. ein Mechanismus für Banken sein. Sie könnten über Spracherkennungssoftware und Ortungsdienste verfügen, um zu überprüfen, ob diese Daten mit den normalen Daten des Kunden übereinstimmen oder nicht. Der Vergleich dieser „normalen" Merkmale ist auch etwas, das im Beispiel bestimmter Banken in Bulgarien angewandt wird (siehe oben), wo der Bankmitarbeiter benachrichtigt wird, wenn eine Person über 50 Jahren einen größeren als den üblichen Geldbetrag abheben möchte.

Nach Ansicht der Experten im Workshop sollten Sensibilisierungskampagnen auch die Risiken und Sanktionen für die Täter aufzeigen, um sie abzuschrecken. Diese Sanktionen sollten auch verschärft werden, um dem wahrgenommenen Nutzen für die Täter entgegenzuwirken. Insbesondere Geldstrafen werden in diesem Zusammenhang als geeignet erachtet. Zusammen mit einer stärker spezialisierten Ausbildung und Ressourcen für die Strafverfolgung sollte diese Kriminalität als eine Art organisierte Kriminalität behandelt und entsprechend bestraft werden.

Reduzierung des Lohns

Diese dritte Reihe von Maßnahmen zur Verhinderung von Telefonbetrug beinhaltet die Reduzierung des Lohns, der mit der Begehung dieses Verbrechens erzielt werden könnte. Die wichtigste Empfehlung lautet hier, die Vermögenswerte, die durch Telefonbetrug erschlichen werden, zu beschlagnahmen. Ein wichtiger Schritt ist die Überwachung des Geldflusses. Das oben erwähnte australische Beispiel zeigt uns genau, worum es hier geht und wie effektiv die Erkennung verdächtiger Transaktionen sein kann. Die Experten betonten, dass eine EU-weite Initiative mit den Banken erforderlich ist, um dies an die europäische Situation anzupassen. Eine weitere Empfehlung ist die Beschlagnahmung der Ausrüstung und Ressourcen, die für die Begehung der Straftat erforderlich waren.

Reduzierung von Provokationen

Während des Workshops wurden keine spezifischen Empfehlungen formuliert, um Provokationen zu reduzieren. Nach Button (2017) konnten wir jedoch feststellen, dass es in einigen Fällen wichtig ist, nicht zu viele Informationen darüber preiszugeben, wie

der Betrug durchgeführt wurde, um Nachahmungen zu verhindern. Darüber hinaus ist auch bekannt, dass Betrüger die Opfer mit einem Angebot kontaktieren, das es beispielsweise ermöglichen würde, ihre Verluste wettzumachen. Die Absicht ist jedoch natürlich, einen zweiten Betrug durchzuführen. Die Sensibilisierung für dieses Thema ist von entscheidender Bedeutung.

Beseitigung von Vorwänden

Die letzte Reihe von Empfehlungen konzentriert sich hauptsächlich auf die Sensibilisierung für Telefonbetrug und wie man sich am besten vor Schaden schützen kann. Dabei handelt es sich um die klassische Informationskampagne über eine Vielzahl von Kanälen wie Radio, Fernsehen, Flyer usw. Die Informationen, die weitergegeben werden müssen, können die Vorgehensweise bei bestimmten Betrügereien erklären, aber auch, wie man sich schützen kann. Dies wurde bereits an den Beispielen aus Rumänien oder der Tschechischen Republik deutlich. Ein Bühnenstück ist zum Beispiel eine interessante Methode, um zu vermitteln, wie man Abwehrstrategien auf die eigene Situation anwenden kann. Öffentlich-private Partnerschaften sind hier ebenso wichtig, um eine präventive Botschaft zu verbreiten, wie der Informationsaustausch zur Zuordnung von Straftätern. Dies ist eine gemeinsame Aufgabe, die auch innerhalb von Gemeinschaftsgruppen oder Peergroups erfolgen kann.

Natürlich müssen Kampagnen ausgewertet werden, um die Effektivität zu gewährleisten. Ein wichtiger Aspekt dabei ist die Verbreitung derselben Botschaft in den verschiedenen Organisationen, aber auch in verschiedenen Ländern. Das Beispiel von Europol (siehe oben) ist dafür exemplarisch. Darüber hinaus könnte es sinnvoll sein, Informationen über die Vielfalt der vorhandenen Betrügereien auszutauschen und ihre Vorgehensweise zu erklären. Die Botschaft, wie man sich selbst schützen kann, sollte jedoch konstant sein, um so klar und einfach wie möglich zu sein. *Sag einfach nein*.

Die Sensibilisierung sollte sich auch an diejenigen richten, die bereits Opfer waren. Sie sollten nicht nur auf die Gefahr aufmerksam gemacht werden, ein zweites Mal Opfer zu werden, sondern es besteht auch ein eindeutiger Bedarf an Unterstützung für diese Opfer. Bemerkenswert sind hier unterstützende Netzwerke, in denen die Opfer Informationen untereinander austauschen und sich gegenseitig bei ihren Verlusten (finanziell und emotional) unterstützen. Auch eine Hotline, um den Opfern die richtigen Informationen und Ratschläge zu geben, wurde von den Experten erwähnt.

4. Schlussfolgerungen

In diesem zweiten Teil der Toolbox haben wir uns mit der Prävention von individuellem Betrug befasst. Zunächst wurden einige allgemeine Bemerkungen auf der Grundlage wissenschaftlicher Forschung gemacht. Trotz des Mangels an wissenschaftlichen Studien zur Verhinderung von individuellem Betrug haben wir festgestellt, dass die häufigste Präventionstaktik in der **Aufklärung der Öffentlichkeit** darüber besteht, wie man Betrug erkennt und wie man darauf reagieren kann. Eine Studie zeigte eine 40%ige Verbesserung nach der Auswertung von Schulungsmaterialien, die an eine Versuchsgruppe verteilt wurden. Solche Auswertungen sind jedoch selten und wir können nur empfehlen, mehr Forschung und Bewertungen zu diesem Thema durchzuführen.

Studien brachten auch die Notwendigkeit zum Ausdruck, sich auf Menschen zu konzentrieren, die bereits Opfer geworden sind. Dies ist auf ein hohes Maß an wiederholter Viktimisierung zurückzuführen, aber auch auf die Gefahren der sekundären Viktimisierung durch Personen in der gleichen Situation, Familienangehörige, Behörden usw. Die **Opfer** sollten hinsichtlich ihrer Verluste unterstützt und auf die Gefahren, ein zweites Mal zum Opfer zu werden, aufmerksam gemacht werden.

Zweitens haben wir einen Überblick über einige **bewährte Praktiken** in den Mitgliedstaaten gegeben. Diese wurden nach ihrer Zielgruppe kategorisiert: universelle, selektive und indizierte Präventionsmaßnahmen. Im dritten Teil dieser Toolbox findet der Leser auch alle diese Projekte.

Zuletzt formulierten wir, auf der Grundlage eines Workshops mit einer Vielzahl von europäischen Experten, **Empfehlungen**, wie man Telefonbetrug verhindern kann. Im Mittelpunkt standen die fünf umfassenden Strategien der situativen Verbrechensprävention: Erhöhung des Aufwandes, Erhöhung des Risikos, Verringerung des Lohns, Verringerung der Provokationen und Beseitigung von Vorwänden.

Factsheet

PREVENTING PHONE SCAMS

HOW CAN I HELP YOU?

SOCIAL ENGINEERING

Underlying most individual frauds is a technique called social engineering. This is the essential tactic to obtain the trust from victims and to convince them to follow the scam. As such, the victim has a very active part in the fulfilment of the crime, leading to feelings of shame and guilt.

DARK NUMBER

THESE ARE THE STEPS

01 Increase the effort

> Restrict publication of phone numbers
> Stronger password protection and encryption
> Scambaiting

02 Increase the risk

> Share information between all involved partners
> Promote reporting
> Reduce anonymity of the caller

03 Reduce the rewards

> Seize criminal assets
> Monitor money flow

04 Reduce the provocations

> Prevent copycats
> Raise awareness on retrieval scams

05 Remove the excuses

> Raise awareness
> Evaluate campaigns
> Support victims

Want to learn more?
Visit www.eucpn.org

03 TEIL III: BEISPIELE AUS DER PRAXIS

„ENKELTRICK - SCHON MAL DAVON GEHÖRT?“ (AT)

Kurzbeschreibung:
Das Telefon klingelt beim Opfer („Oma“). Ahnungslos geht das Opfer davon aus, dass der Anrufer ein Freund oder Verwandter ist. Das Opfer fängt an zu raten, wer anruft, nennt verschiedene Namen von Familienmitgliedern (in den meisten Fällen die Namen von Enkeln oder Neffen), der Betrüger wählt einen aus und behauptet, diese Person zu sein. Später beschreibt der Anrufer seine finanzielle Notfallsituation und bittet das Opfer um Bargeld. Nicht selten verlieren Opfer in solchen Fällen alle ihre Ersparnisse; oft führt dieser Verlust zu schweren emotionalen Problemen, sogar zu körperlichen Beschwerden.
Die Verbrechensprävention erweist sich als schwierig; potenzielle Opfer sind oft nicht für Vorträge oder Kampagnen zugänglich. Da die Bankmitarbeiter eine entscheidende Rolle bei der Prävention spielen, konzentriert sich diese Kampagne in Zusammenarbeit mit der Österreichischen Nationalbank und der Handelskammer auf die Information und Motivation der Öffentlichkeit und insbesondere des Bankenpersonals und beinhaltet einen Informationsfilm mit dem Titel „Der Enkeltrick“.

Beginn/Dauer:
Datum des Projektbeginns: 01.04.2015
Öffentliche Mitteilung (Pressekonferenz): 18.02.2016
Laufend: Sensibilisierung mit Printkampagne, basierend auf dem produzierten Videoclip.

Hintergrundrecherche:
Die Unterabteilung Verbrechensprävention und Opferbetreuung hat zusammen mit der Unterabteilung Wirtschaftskriminalität, der Unterabteilung Betrug, Fälschung und Wirtschaftskriminalität sowie der Abteilung Kriminalanalyse des österreichischen Bundeskriminalamts eine Bewertung und eine Bestandsaufnahme der Auswirkungen, der Funktionsweise und des Ausmaßes dieser Art von Betrug vorgenommen.

Budget:
Am kostspieligsten waren der vom österreichischen Bundeskriminalamt finanzierte Clip (7.000 Euro) und die Kosten für die Printkampagne (1.000 Euro); daneben wurde die Pressekonferenz von der Nationalbank finanziert; die Verteilung der Inhalte wurde gemeinsam von allen drei Beteiligten finanziert.

Art der Auswertung:
Einer der Projektpartner - die Österreichische Nationalbank - organisierte eine Roadshow, die im Laufe des Sommers 2016 in allen Bundesländern und Bezirken Österreichs Station machte. Nach der Tour nahmen sich die Mitarbeiter die Zeit und befragten in jeder Bank in jeder Stadt, in der sie mit der Roadshow Station gemacht hatten, die Bankmitarbeiter, ob sie vom Enkeltrick gehört hatten, ob sie den Clip gesehen hatten und ob sie wussten, wie sie richtig reagieren sollten, falls sie auf einen Verdächtigen treffen.

91% der Mitarbeiter war der Enkeltrick bekannt und sie wussten auch, wie sie bei Verdacht reagieren sollten. Der Clip war nur durchschnittlich 19% bekannt, weshalb beschlossen wurde, eine weitere Kampagne mit Informationsblättern durchzuführen, um den Modus und den Clip erneut zu bewerben.

Akteur, der die Auswertung/das Timing durchführt:
Extern: die Österreichische Nationalbank

Art der Datenerfassungsmethode:
Wirkungsbewertung der Österreichischen Nationalbank bei 158 Banken in ganz Österreich.

Weitere Informationen
http://eucpn.org/document/granny-scam

HALLO OMA, ICH BRAUCH GELD (DE)

Kurzbeschreibung:
Ältere Menschen sind für Betrüger attraktiv. Eine unter Kriminellen populär gewordene Methode ist der „Enkeltrick-Betrug“, bei dem sich Betrüger als Verwandte des Opfers ausgeben und vorgeben, sich in einer verzweifelten

Situation zu befinden und dringend Geld zu brauchen.

Das Projekt „Hallo Oma, ich brauch Geld“ bietet ein innovatives Konzept zur Verbrechensprävention gegen Betrug. Es handelt sich dabei um ein interaktives Bühnenstück, das einen Überblick über gängige Techniken bietet und Maßnahmen aufzeigt, um sich davor zu schützen, ein potenzielles Opfer zu werden. Es mindert auch die subjektive Angst vor Schwindlern und ermutigt zu mehr Selbstvertrauen.

Das Publikum wird aktiv in die Aufführung einbezogen. Zufällig ausgewählte Zuschauer nehmen aktiv an der Aufführung teil, während die Schauspieler improvisieren und spontan auf Anregungen aus dem Publikum reagieren. Der Hintergrund realistischer Fälle hilft, die Dringlichkeit zu vermitteln und der unterhaltsame Faktor gewährleistet einen bleibenden Eindruck.

Beginn/Dauer:
Das Projekt startete am 28.03.2012 und läuft noch.

Hintergrundrecherche:
Es gab laut PKS (polizeiliche Kriminalstatistik) eine Zunahme der Fälle von „Enkeltrick-Betrug“. Auffällig waren die Anzahl der Fälle und die daraus resultierenden Schäden.
Die Zahl der Fälle im Land Baden-Württemberg stieg von 95 (2007), 64 (2008), 143 (2009) auf 311 im Jahr 2010.
Die finanziellen Verluste in Baden-Württemberg stiegen von 234.890 Euro (2007), 45.870 Euro (2008), 557.900 Euro (2009) auf 1.108.131 Euro in 2010.

Budget:
Das Stück wurde in ehrenamtlicher Tätigkeit von Allan Mathiasch verfasst und entwickelt, der dabei von seinem Theaterensemble und den Kooperationspartnern (Polizei und Stadt) unterstützt wurde. Die Kosten einer Vorstellung - einschließlich zweier Schauspieler und Ausrüstung - belaufen sich auf 790-890 €, zuzüglich Reisekosten.

Art der Auswertung:
Prozess- und Wirkungsanalyse.

Akteur, der die Auswertung/das Timing durchführt:
Extern: Theresa Siegler, Studentin an der Hochschule Kehl.

Art der Datenerfassungsmethode:
Fragebogenbasierte Umfrage.

Weitere Informationen
https://eucpn.f2w.fedict.be/document/hello-granny-i-need-money

SILVER SURFER (LU)

Kurzbeschreibung:
Das Projekt „Silver Surfer“ ist ein Projekt von Senioren für Senioren. Freiwillige Senioren werden gezielt geschult, um ein Bewusstsein für die sichere Nutzung des Internets zu schaffen. Sie vermitteln ihr Wissen an andere Senioren durch Konferenzen, z.B. bei Seniorenveranstaltungen, in Seniorenclubs oder in Seniorenverbänden. „Silver Surfer“ fungieren als Multiplikatoren.
Das Projekt wurde 2014 auf Initiative von BEE SECURE ins Leben gerufen und basiert auf der Zusammenarbeit zwischen dem Ministerium für Familie, Integration und der Großregion Luxemburg, SECURITYMADEIN.LU, dem RBS-Center fir Altersfroen und dem SenioreSécherheetsBeroder.

Beginn/Dauer:
Das Projekt startete 2014 und läuft noch.

Hintergrundrecherche:
Im Jahr 2013 startete der Partner SECURITYMADEIN.LU während einer Seniorenmesse eine Umfrage. Das Ergebnis zeigte, dass die befragten Senioren den PC nur zum Austausch von E-Mails (94%) oder zum Skypen (32%) mit Familienmitgliedern nutzten. Kaum die Hälfte von ihnen wusste von Internetbetrug. 32% von ihnen waren bereits Opfer von Phishing-Angriffen und 12% Opfer eines Ransomware-Betrugs. Die gleiche Umfrage wurde 2014 auf der gleichen Messe wiederholt. Die Ergebnisse waren vergleichbar und zeigten, dass ältere Menschen das Internet häufiger nutzen (5% mehr als 2013).

Weitere Informationen
https://eucpn.org/document/silver-surfer

VERSUCH NICHT, MICH FÜR DUMM ZU VERKAUFEN (SE)

Kurzbeschreibung:
Das Projekt „Versuch nicht, mich für dumm zu verkaufen“ wurde ins Leben gerufen, um Betrugsdelikte an älteren Menschen durch Sensibilisierung für diese Verbrechen zu verhindern und es möglichen Opfern zu erleichtern, Betrugsversuche zu erkennen und sich dagegen zu schützen.

Die Methode, die für das Projekt gewählt wurde, war die Erstellung eines Informationspakets und einer Struktur für die Verwendung des Materials in aktiven Meetings, in denen die teilnehmenden Teilnehmer für verschiedene Situationen trainieren können, in denen sie Opfer von Betrug werden könnten und wie sie handeln können, um zu verhindern, einem Betrug zum Opfer zu fallen.

Das Material soll bei drei verschiedenen Treffen verwendet werden und beinhaltet einen Führer für den Meeting-Leiter, drei verschiedene Kurzfilme und drei verschiedene Lernanleitungen. Jeder Anlass beinhaltet die Arbeit mit einem Film und einer Lernanleitung. Beim Material handelt es sich um Selbstlernmaterial, das auf verschiedenen Fällen basiert, die für Diskussionen und praktische Übungen verwendet werden können.

Beginn/Dauer:
Das Projekt startete offiziell am 16.09.2015 und läuft noch.

Hintergrundrecherche:
Das nationale Zentrum für Betrugsbekämpfung bei der schwedischen Polizeibehörde analysierte die Entwicklung des Betrugs in Schweden und stellte einen starken Anstieg des Betrugs an älteren Menschen fest. Die eingehende Analyse zeigte, welche Vorgehensweise bei diesen Verbrechen angewendet wurde und an welcher Stelle die Betrüger zuschlugen. Diese Analyse wurde verwendet, um das Material und die Fallstudien im Projektmaterial zu erstellen. Die Analyse basierte hauptsächlich auf Daten von Verbrechen, die bei der schwedischen Polizei angezeigt wurden.

Budget:
Die Kosten für das Projekt wurden nicht angegeben. Da das Projekt Priorität erhielt, wurden alle Mittel aus dem normalen Finanzrahmen entnommen und daher nicht spezifiziert. Die Polizei und die Organisationen produzierten die Filme und sonstigen Materialien selbst, dadurch wurden die Kosten relativ niedrig gehalten.

Art der Auswertung:
Eine Prozessauswertung ist noch nicht abgeschlossen, aber die Methode wird durch Messung der Anzahl der durchgeführten Meetings und eine Umfrage bei den Teilnehmern über ihre Ansicht zum Projekt und die daraus resultierenden Veränderungen in Bezug auf ihr Bewusstsein für Betrug und was zu tun ist, um zu verhindern, dass sie ihm zum Opfer fallen, bewertet. Die Wirkungsbewertung wurde noch nicht durchgeführt, aber es wird eine Analyse durchgeführt, und die Arbeit hat mit der Analyse von Veränderungen bei angezeigten Straftaten dieser Art und Unterschieden in Bezug auf erfolgreiche und versuchte Straftaten begonnen.

Weitere Informationen
https://eucpn.f2w.fedict.be/document/do-not-try-fool-me

ÖSTERREICH: WATCHLIST INTERNET

Kurzbeschreibung
Watchlist Internet ist ein Projekt zur Prävention und Bekämpfung von Online-Kriminalität in Form von Betrug und anderen Online-Fallen. Seit 2013 untersucht das Projektteam gefälschte Websites und Online-Betrugsfälle mit dem Ziel, die breite Öffentlichkeit mit Nachrichtenartikeln auf seiner Website seriös zu informieren. Die Alleinstellungsmerkmale sind Kontinuität und effektive Suchmaschinenoptimierung. Das Projekt trägt auch durch die Vernetzung von E-Commerce-Plattformen, Privatbanken, staatlichen Stellen und Strafverfolgungsbehörden in Österreich zur Bekämpfung der Online-Kriminalität im Allgemeinen bei. Entscheidend für den Projekterfolg ist auch die enge Zusammenarbeit mit der Online-Schlichtungsstelle „Internet-Ombudsmann“ und mit den Interessengruppen und Nutzern der Website, die zur Meldung von Fällen beitragen.

Beginn/Dauer
Das Projekt startete am 3. Juli 2013 und läuft noch.

Hintergrundrecherche
Es gab eine Kontextanalyse durch das Team von Internet Ombudsmann. Die beobachtete Zunahme der Fälle von Internetbetrug verdeutlichte die Notwendigkeit, die Anstrengungen zur Sensibilisierung zu verstärken. Die Zahl der Fälle nahm 2012 gegenüber dem Vorjahr um 18 Prozent zu. Basierend auf diesen Daten wurde Watchlist Internet vom Österreichischen Institut

für Angewandte Telekommunikation gegründet.

Budget
Watchlist Internet wird vom Bundesministerium für Arbeit, Soziales und Konsumentenschutz, der Arbeiterkammer Österreich, dem größten österreichischen Online-Marktplatz willhaben.at und der Bank Austria finanziert. Die jährlichen Kosten des Projekts belaufen sich auf ca. 65.000 Euro.

Art der Auswertung
Im August 2014 fand eine interne Prozessbewertung in Form einer Online-Umfrage unter den Lesern der Watchlist-Internet-Website statt. Basierend auf diesen Erkenntnissen wurde das Projekt weiter gestaltet, zum Beispiel mit einer leichter verständlichen Sprache im Hinblick auf das ältere Publikum. Es wurden keine externen Ergebnis- oder Wirkungsbewertungen durchgeführt, eine interne Wirkungsbewertung wird jedoch jährlich durchgeführt.

Akteur, der die Auswertung/das Timing durchführt:
Intern: durch das Projektteam und einen Beirat mit öffentlichen und privaten Interessengruppen

Art der Datenerfassungsmethode
Die jährliche Auswertung basiert auf Google Analytics, z.B. Nutzerstatistiken, Website-Besucher, Besuchsdauer usw., dem Feedback von Nutzern und Finanzierungspartnern sowie ständig durch Überprüfung, ob Nachrichten über Internetbetrug zum Verschwinden einer gefälschten Website führen.

Links zu weiteren Informationen
http://eucpn.org/document/watchlist-internet

ABTEILUNG BETRUG IN DER GENERALDIREKTION DER NATIONALEN POLIZEI (BG)

Kurzbeschreibung:
In Bulgarien befasst sich eine komplette „Betrugsabteilung“ innerhalb der nationalen Generaldirektion der Polizei mit dem Thema Telefonbetrug. Neben ihrer reaktiven Polizeiarbeit hat sie auch die grundlegende Aufgabe der Prävention. Im Rahmen ihrer Arbeit werden das Wissen und die Sensibilisierung der

Bevölkerung für dieses Verbrechen durch Informationskampagnen gefördert. So werden beispielsweise Informationsbroschüren verbreitet, aber auch Ratschläge in einer nationalen Radiosendung gegeben. Ein weiteres Beispiel aus Bulgarien sind Aufkleber, die verteilt werden. Diese Aufkleber tragen präventive Botschaften und die Menschen werden gebeten, sie auf ihr Telefon zu kleben. Die Idee ist, dass, wenn sie angerufen werden, sie an die präventive Botschaft erinnert werden, weil sie den Aufkleber sehen, während sie den Hörer abnehmen.

BETRUGSBE-KÄMPFUNGS MECHANISMUS FIRST INVESTMENT BANK BULGARIA (BG)

Kurzbeschreibung:
Diese Bank in Bulgarien verfügt über einen Mechanismus zur Aufdeckung und Prävention von Telefonbetrug. Wenn große Beträge abgehoben werden, die nicht einer festgelegten Liste von Kriterien der Bank entsprechen, wird der Sachbearbeiter alarmiert und aufgefordert, mit dem Kunden zu klären, ob er möglicherweise unter Druck gesetzt wird. Ein Algorithmus übermittelt einen Bericht an den Sachbearbeiter, wenn diese Kriterien auf einen möglichen Telefonbetrugsfall hinweisen. Der Sachbearbeiter kann sich dann mit dem Kunden gemäß einer „Telefonbetrugs-Checkliste“ in Verbindung setzen und Fragen stellen, z.B. zum Zweck der Abhebung oder durch Beobachtung der Handlungen des Kunden.

#CYBERSCAMS (EC3, EUROPOL)

Kurzbeschreibung:
Jedes Jahr findet im Oktober der European Cyber Security Month (ECSM) statt. Dies ist eine Sensibilisierungskampagne der EU, die

die Cyber-Sicherheit bei Bürgern und Organisationen fördert und einfache Maßnahmen zum Schutz ihrer persönlichen, finanziellen und beruflichen Daten hervorhebt. Das Hauptziel besteht darin, das Bewusstsein zu schärfen, das Verhalten zu verändern und Ressourcen dazu bereitzustellen, wie man sich online schützen kann. Jede Woche gibt es ein spezifisches Thema und in der dritten Woche der Ausgabe 2018 haben sich das European Cybercrime Centre (EC3), der Europäische Bankenverband (EBF) und Partner aus dem öffentlichen und privaten Sektor zusammengetan, um Cyber-Betrügereien zu thematisieren. 7 gängige Online-Finanzbetrügereien werden auf Factsheets gezeigt und es wird erklärt, wie man sie vermeidet. Diese Materialien wurden in der gesamten EU im Rahmen einer Social-Media-Kampagne verbreitet. Nach dem Start wurde jede Betrugsform einen Tag lang näher beleuchtet.

Beginn/Dauer:
Der offizielle Start der Kampagne erfolgte am 17. Oktober 2018. Die Materialien bleiben online verfügbar.

Weitere Informationen
https://www.europol.europa.eu/cyberscams

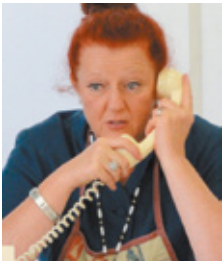
WIE PHISHING-SICHER SIND SIE? (BE)

Kurzbeschreibung:
Diese Kampagne wurde vom Belgischen Zentrum für Cybersicherheit (CCB) während des European Cyber Security Month (ECSM) 2017 eingeleitet. Ziel der Kampagne war es, die Öffentlichkeit über Phishing-E-Mails und ihrer Erkennung zu informieren. Durch Verbreitung von Flyern, Postern, aber auch eine umfangreiche (soziale) Medienkampagne soll das Projekt von rund 2 Millionen Internetnutzern in Belgien aufgegriffen worden sein. Neben dieser Informationskampagne wurde die Öffentlichkeit auch aufgefordert, verdächtige E-Mails an das CCB weiterzuleiten. Durch Scannen dieser E-Mails und deren Überprüfung mit komplexer Software werden täglich 5 verdächtige Links blockiert.

Beginn/Dauer:
Der offizielle Start der Kampagne erfolgte am 2. Oktober 2017. Die Materialien sind noch online verfügbar und der Weiterleitungsmechanismus ist noch aktiv.

Weitere Informationen:
www.safeonweb.be

NEDÁME SE (DAS LASSEN WIR UNS NICHT GEFALLEN) (CZ)



Kurzbeschreibung:
Das Programm „Nedáme se“ ist ein interaktives Aufklärungstheaterstück, in dem vier Arten von betrügerischen Manipulationstechniken, die gegen ältere Menschen eingesetzt werden, auf der Bühne präsentiert werden. Dies sind Verkaufskampagnen, der Verkauf von Parfums auf der Straße, Telemarketing und Verkauf im Seniorenheim. Neben den Schauspielern traten ein Polizist und auch die Autorin des Stücks, die Psychologin Ph. Dr. Romana Mazalová auf. Sie kommen auf die Bühne, interagieren mit dem Publikum und vermitteln ihm so neue Strategien der Verteidigung. So macht das Spiel nicht nur Spaß, sondern wird auch zu einer neuen Form der Aufklärung gegen sogenannte „Šmejdi“ (Gauner). Die pädagogische Wirkung auf das Publikum wurde experimentell untersucht. Die Ergebnisse bestätigten, dass die Senioren, die das Stück gesehen hatten, sich als erfolgreicher bei der Verteidigung gegen betrügerische Verkäufer erwiesen.

Beginn/Dauer:
2015

Weitere Informationen:
https://eucpn.org/document/czech-elderly-dont-swallow-bait

DER PREIS DER FREUNDSCHAFT (RO)

Kurzbeschreibung:
Ziel des Projekts war es, das Risiko für ältere Menschen, Betrügern zum Opfer zu fallen, zu verringern, indem es folgende Ziele verfolgte: Kenntnis der Zielgruppe aus Einstellungs- und Verhaltenssicht, Erhöhung des Niveaus des präventiven Wissens der älteren Menschen und Steigerung der Fähigkeit zur Selbstverteidigung. Die Zielgruppe bestand aus Personen über 60 Jahren, die Mitglieder lokaler Seniorenclubs sind. Im Jahr 2017 wurden insgesamt 34 präventive Informationsmaßnahmen durch die Polizei durchgeführt. Die Informationen wiesen auf die Risiken hin, die mit dem Alter verbunden sind, aber auch auf die Vermeidung der Viktimisierung bei Täuschungen, wie beispielsweise gefälschten Telefonkampagnen. Außerdem wurden für ältere Menschen Online-Trainingskurse angeboten. Darüber hinaus wurde ein „Senioren-Sicherheits-Ball“ veranstaltet, um eine öffentliche Informationskampagne zu starten.

Beginn/Dauer:
Januar 2017

Weitere Informationen:
https://eucpn.org/document/price-friendship-project

SICHERHEITS-LEITFADEN FÜR SENIOREN (FI)

Kurzbeschreibung:
In Finnland entsendet der Finnische Verband für das Wohlergehen älterer Menschen regionale Fachleuchte für Hausrenovierungen, die ältere Menschen kostenlos beraten. Sie helfen unter anderem in Situationen, in denen ältere Menschen überredet werden, eine teure Hausrenovierung in Auftrag zu geben.
Ältere Menschen können sich in folgenden Situationen mit ihnen in Verbindung setzen:

- Betrügerische Verkäufer (Telefon, Hausbesuche).
- Renovierungs- und Reparaturbetrügereien (überteuert, unnötig usw.)
- Ratschläge, **wie man sich verhält**, wenn der Verkäufer auf den Verkauf drängt.
- Beratung zu **Verträgen und Kündigung** innerhalb von 2 Wochen usw.

„TRICKS GEGEN ÜBERREDUNGS-TRICKS“ (NL)

Kurzbeschreibung:
Eine Seniorenorganisation in den Niederlanden entwickelte eine Anwendung für ältere Menschen, die sie über die Gefahren von Betrug informiert. Die App simuliert „Betrugssituationen“, sodass ältere Menschen ihre neu erworbenen Fähigkeiten sofort testen können. So wird beispielsweise eine Simulation eines Lotteriebetrugs gezeigt. Der ältere Mensch kann dann im wirklichen Leben antworten, woraufhin die App den Grad der Durchsetzungsfähigkeit seiner Antwort bewertet.

ACTION FRAUD (UK)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Kurzbeschreibung:
Action Fraud ist die nationale Meldestelle für Betrug und Cyber-Kriminalität im Vereinigten Königreich, wo man Anzeige erstatten sollte, wenn man in England, Wales und Nordirland betrogen oder Opfer von Cyber-Kriminalität wurde. Die Opfer werden auch an bestimmte Unterstützungsgruppen verwiesen, um den von der Straftat Betroffenen zu helfen oder ihnen mitzuteilen, wo sie Anzeige erstatten müssen.

Weitere Informationen:
https://www.actionfraud.police.uk/

ENDNOTES

1 Benutzer erhalten beispielsweise simulierte Phishing-E-Mails, um ihre Anfälligkeit zu testen, am Ende des Tests erhalten sie zusätzliche Informationen, wie sie dies in Zukunft verhindern können (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

2 Hier erhalten Nutzer sofort zusätzliche Informationen, wenn sie auf einen falschen Link klicken (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

3 Anti-Phishing Phill ist ein gutes Beispiel für ein Online-Spiel, das den Nutzern sinnvolle Gewohnheiten beibringt, um Phishing-Angriffe zu vermeiden. Am Ende des Trainings erkannten die Benutzer betrügerische Websites besser als die Kontrollgruppe und waren besser über Strategien informiert, um zu verhindern, dass sie Opfer werden (Sheng, et al., 2007).

4 https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

5 https://www.actionfraud.police.uk/support-and-prevention/ive-been-a-victim-of-fraud

REFERENZEN

Agustina, J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. International Journal of Cyber Criminology, 9(1), 35-54.

Anderson, K. (2016). Mass-market consumer fraud: who is most susceptible to becoming a victim? Washington D.C.: FTC Bureau of Economics.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. Open Journal of Social Sciences, 1(3), 23-32.

Barnes, P. (2017). Stock market scams, shell companies, penny shares, boiler rooms and cold calling: the UK experience. International Journal of Law, Crime and Justice, 48, 50-64.

Bidgoli, M., & Grossklags, J. (2017). „Hello. this is the IRS calling“: a case study on scams, extortion, impersonation, and phone spoofing. 2017 APWG Symposium on Electronic Crime Research (eCrime) (S. 57-69). Scottsdale: AZ.

Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. Singapore Cyber-Security Conference, (pp. 107-114). Singapur.

Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: a literature-based dissection of successful attacks. J Investig Psychol offender Profil, 15, 20-45.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: a qualitative analysis of the structure and process of victimization on the internet. International journal of Cyber Criminology, 7(2), 112-124.

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. London: Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: literature review. National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36-54.

Button, M., McNaughton, N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408.

Button, M., Tapley, J., & Lewis, C. (2012). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. Criminology and Criminal Justice, 13(1), 37-61.

Cialdini, R. (2001). Influence: Sciende and practice. Boston : Allyn & Bacon.

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. Crime prevention Studies, 16, 41-96.

Crosman, K. (2017). Phone and Television Scams in the Age of the Internet. Lewis & Clark L.Rev., 21, 791.

Cross, C. (2016). 'I'm anonymous, I'm a voice at the end of the phone': a Canadian case study into the benefits of providing telephone support to fraud victims. Crime Prevention and Community Safety, 18, 228-243.

Cross, C., Richards, K., & Smith, R. (2016). The reporting experiences and support needs of victims of online fraud. Trends & issues in crime and criminal justice, 518, 1-14.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. Telematics and Informatics, 35(5), 1277-1287.

EUCPN. (2017). Cyber Safety: A theoretical insight. In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

EUCPN. (2017). Organised Crime Targeting Elderly People: a theoretical overview. In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

European Commission. (2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Brussels: European Commission.

European Commission. (2018). Special Eurobarometer 462: E-Communications and Digital

Single Market. Brussels: European Commission.

Europol. (2014). Internet organised Crime Threat Assessment. The Hague: Europol.

Europol. (2016). Internet Organised Crime Threat Assessment. The Hague: Europol.

Europol. (2017). Internet Organised Crime Threat Assessment . The Hague: Europol.

Europol. (2018). Internet Organised Crime Threat Assessment. The Hague: Europol.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. International Conference on Human Aspects of Information Security, Privacy, and Trust (S. 36-47). Cham: Springer.

Gadhave, U., & Sirsat, S. (2015). Review of Cyber-crimes and their impacts over the society. international Journal of Electronics, Communication & Soft Computing Science and Engineering, 357-359.

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Conference, (pp. 1-8).

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' perspective on crime prevention. In B. Leclerc, & E. Savona, Crime Prevention in the 21st Century: insightful approaches for crime prevention initiatives (S. 9-18). Springer.

Jakobsson, M. (2016). Understanding Social Engineering based scams. New York: Springer.

Lab, S. (2010). Crime prevention: approaches, practices and evaluations. LexisNexis Group.

Leukfeldt, E., & Stol, W. (2011). De marktplaats-fraudeur ontmaskerd: Internetfraudeurs vergeleken met klassieke fraudeurs. Secondant, 25(6), 26-31.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. Criminology & Criminal Justice, 8(4), 389-419.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, law and social change, 67, 3-20.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK. British Journal of Criminology, 48, 293-318.

Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. 10th IEEE International Conference on Computer and Information Technology, (pp. 824-831).

Marzuoli, A., Kingravi, H., Dewey, D., & Pindrop, R. (2016). Uncovering the landscap of fraud and spam in the thelephony channel. 15th IEEE international Conference on Machine Learning and Applications, (pp. 853-858).

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: targeting the weak and the vulnerable. International World Wide Web Conference, (pp. 1301-1310). Perth.

Mears, D., Reisig, M., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimization among the elderly: the effect of information access on program awareness and contact. Crime & Delinquency, 62(9), 1235-1259.

Moreno-Fernández, M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior, 69, 421-436.

Murphy, D. R., & Murphy, R. H. (2007). Phishing, Pharming, and Vishing: Fraud in the Internet Age. In T. Fowler, & J. Leigh, The Telecommunications Review (pp. 37-45). VA: Noblis.

Ollmann, G. (2007). The vishing guide. IBM Global Technology Services.

Petty, R., & Cacioppo, J. (1986). The elaboration likelihood model of persuasion. Communication and persuasion, 1-24.

Petty, R., & Cacioppo, J. (2012). Communication and persuasion: Central and peripheral routes to attitude change. Springer Science & Business Media.

Rauti, S., & Leppänen, V. (2017). "You have a potential hacker's infection": a study on technical support scams. IEEE International Conference

on Computer and Information Technology, (pp. 197-203).

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspectives on psychological science, 9(4), 427-442.

Rusch, J. (1999). The "social engineering" of internet fraud. Internet Society Annual Conference. Retrieved from http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm.

Sheng, S., Holbrook, M., Kumaragur, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Privacy Behaviors, 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that teaches people not to fall for phish. Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.

Singh, L., & Imphal, N. (2018). A survey on phishing and anti-phishing techniques. International Journal of Computer Science Trends and Technology, 6(2), 62-68.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

Tabron, J. (2016). Linguistic features of phone scams: a qualitative survey. 11th Annual symposium on information assurance, (pp. 52-58).

Titus, R., & Gover, A. (2001). Personal Fraud: The Victims and the Scams. In F. G., & K. Pease, Repeat Victimization (pp. 133-152). New York: Criminal Justice Press.

van de Weijer, S., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology, 1-23.

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology, 53(4), 665-684.

Whitty, M. (2015). Anatomy of the online dating romance scam. Security Journal, 28(4), 443-455.

Whitty, M. (2018). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, behavior, and social networking, 21(2), 105-109.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass marketing scam. Journal of Experimental Psychology: applied, 24(2), 196-206.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass masketing scam. Journal of Experimental Psychology: Aplied, 24(2), 196-206.

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the american society for information science and technology, 59(4), 1-12.

Yeboah-Boateng, E., & Amanor, P. (2014). Phishing, SMishing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.

CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN