KFV
Kuratorium für Verkehrssicherheit

KFV - Sicher Leben #21

KFV SCHRIFTENREIHE NUMMER 21

Cybercrime und Viktimisierung

Versuch einer Typologisierung aus gendersensibler Perspektive

KFV (Kuratorium für Verkehrssicherheit)

KFV - Sicher Leben #21

Cybercrime und Viktimisierung

Versuch einer Typologisierung aus gendersensibler Perspektive

KFV - Sicher Leben. Band #21. Cybercrime und Viktimisierung. Wien, 2019

Medieninhaber und Herausgeber
KFV (Kuratorium für Verkehrssicherheit)

Autorin
Dr. Irmgard Wetzstein

Co-Autoren
Sabine Fuger, Mag. Dagmar Lehner, Mag. Monika Pilgerstorfer, Dr. Georg Plattner

KFV
Kuratorium für Verkehrssicherheit

INHALTSVERZEICHNIS

1 ABSTRACT 9
1.1 Problemstellung und Zielsetzung 9
1.2 Forschungsfragen 10
1.3 Theoretisches Fundament 11
1.4 Methoden 11

2 RELEVANZ DES THEMAS 15
2.1 Politische Relevanz 15
2.2 Gesellschaftliche Relevanz, Forschungsstand und Forschungslücken 15

3 CYBERKRIMINALITÄT 19
3.1 Zur Vielfalt des Phänomens Cyberkriminalität 19
3.2 Täter und Opfer 21
3.3 Zahlen und Fakten 22

4 RELEVANTE VORPROJEKTE IM KFV-FORSCHUNGSBEREICH EIGENTUMSSCHUTZ 27
4.1 Cybercrime-Barometer 27
4.2 Tatort Social Media 29

5 ERGEBNISSE 33
5.1 Ergebnispräsentation Teil 1: Typenbildung („Opfer-Profile“) 33
5.1.1 Archetypen 33
5.1.2 Gefährdungstypen 34
5.2 Ergebnispräsentation Teil 2: Validierung der Typen durch ExpertInnen 36
5.2.1 Kritische Reflexion der „Opfer-Typen“ 36
5.2.2 Typologisierung anhand von Risikofaktoren 36
5.2.3 Ergebnisse 39
5.3 Ergebnispräsentation Teil 3: Repräsentative Befragung 40
5.3.1 Internetnutzung, Internetsicherheit und die Rolle digitaler Kompetenz 41
5.3.2 Präventionsmaßnahmen und praktische Empfehlungen für UserInnen 46
5.3.3 Konkrete Sicherheitsmaßnahmen und Gefahren 48
5.3.4 Fragwürdige/illegale Inhalte im Netz 49
5.3.5 Viktimisierung insgesamt 49
5.3.6 Folgen von Cyberkriminalität 52
5.4 Resümee 54
5.4.1 Erste Schritte für Opfer 54
5.4.2 Anlaufstellen für Hilfesuchende 54

6 LITERATURVERZEICHNIS 59

7 TABELLENVERZEICHNIS 65

8 ABBILDUNGSVERZEICHNIS 69

9 ANHANG **73**
9.1 Typenbildung **73**
9.2 Fälle in den Medien **74**
9.3 Interviewleitfaden **76**
9.4 Fragebogen **81**

IMPRESSUM **90**

1

1 ABSTRACT 9

1.1 Problemstellung und Zielsetzung 9

1.2 Forschungsfragen 10

1.3 Theoretisches Fundament 11

1.4 Methoden 11

1 ABSTRACT

Das in der Folge beschriebene Forschungsprojekt befasste sich multiperspektivisch mit dem Phänomen der Cyberkriminalität und nahm dabei eine opferfokussierte Perspektive ein. Besonderes Augenmerk lag hier auf der Kategorie „Gender". Im Zentrum stand vor allem die Frage, welche Merkmale und Bedingungen die Viktimisierung beeinflussen können. Im Rahmen einer umfassenden Recherche in Medien, einschlägigen Publikationen und öffentlich zugänglichen Informationen wurden zunächst eine Typenbildung im Sinne archetypischer Muster und eine Sammlung von Delikt- und Gefahrenmustern identifiziert und erläutert. Das Meinungsforschungsinstitut IFES wurde beauftragt, die vorgeschlagene Typenbildung anschließend von ExpertInnen verschiedener Fachrichtungen kritisch validieren zu lassen, sowie anhand einer zusätzlichen repräsentativen Befragung der österreichischen Bevölkerung Internetnutzungsmuster und entsprechende Gefahrengeneigtheiten herauszuarbeiten. Ein besonderes Interesse lag darin, herauszufinden, inwieweit die Kategorie Gender einen Erklärungsrahmen in Bezug auf Cybercrime-Viktimisierung darstellt bzw. welche Rolle Gender in diesem Kontext spielt. Die Ergebnisse zeigen unter anderem, dass Gender sowie soziodemografische Merkmale weitgehend nicht als alleinige Kriterien zur Prognose eines besonderen Risikos für Cybercrime-Viktimisierung herangezogen werden können. Jedoch können Aussagen darüber gemacht werden, welche Personengruppen, kategorisiert nach Alter und Geschlecht, von welchen Arten von Cybercrime eher betroffen sind. Aufgrund der in umfassendem Ausmaß gewonnenen Erkenntnisse konnten unter anderem konkrete Empfehlungen abgeleitet werden. Mit den Ergebnissen eines Online-Tests („Welcher Typ sind Sie?") soll eine breitere Öffentlichkeit bewusstseinsbildend erreicht werden.

1.1 Problemstellung und Zielsetzung

Genderzugehörigkeit ist ein zentraler Identitätsbestandteil jedes Menschen: Es gibt kein gesellschaftliches Phänomen, das vom Aspekt Gender völlig unbetroffen ist. Das trifft auch auf Fragestellungen zu Internetnutzung, Cybersecurity und Cyberkriminalität zu. Die Verknüpfung beider Bereiche durch die evidenzbasierte und detaillierte Analyse von Nutzungsmustern in diesem Zusammenhang, die somit auch das kritische Hinterfragen möglicher klischeehafter Annahmen „männlicher" und „weiblicher" Internetnutzung beinhalten muss, wurde daher in diesem Projekt angestrebt. Hinsichtlich des Internetnutzungsverhaltens zielte das Projekt vor allem darauf ab, die Rolle der Kategorie Gender im Zusammenhang mit Cybercrime-Viktimisierung näher zu beleuchten. Mit der empirischen Umsetzung des Projekts wurde das Meinungsforschungsinstitut IFES beauftragt. In Absprache mit dem KFV hat IFES-Projektleiterin Teresa Schaup gemeinsam mit ihrem Team (Evelyn Dawid, Nikolaus Eder, Teresa Leist) die Erhebungsinstrumente gestaltet sowie die Daten gesammelt und ausgewertet.

Menschen stellen bekanntermaßen das schwächste Glied in der Cybersecurity-Kette dar. Zwischen Frauen und Männern sind Unterschiede im Umgang mit sicherer Internetnutzung bekannt. Ein umfassendes und differenzierteres Bild zur Rolle von Gender bzw. Geschlecht[1] im Umgang mit Cyberkriminalität war bisher jedoch noch nicht vorhanden. Die Möglichkeit eines detaillierten fallbasierten „Profiling" (Gefährdungstypen) männlicher und weiblicher InternetnutzerInnen im Kontext Cyberkriminalität sollte deshalb anhand dokumentierter Cybercrime-Fälle sondiert und mit ExpertInnen bzw. ProfessionistInnen für Cybersecurity diskutiert werden. Zusätzlich sollten Männer und Frauen

1 Das Projekt fokussiert Männer und Frauen und bleibt somit auf ein binäres Gender-Konzept beschränkt.

hinsichtlich ihres Internetnutzungsverhaltens befragt werden, um letztlich, aufgrund der identifizierten Eigenschaften, differenziert und unter besonderer Berücksichtigung der Kategorie Gender für InternetnutzerInnen idealerweise Warnsignale (Prodrome) für mögliche Berührungspunkte mit Cyberkriminalität sowie Maßnahmen/Empfehlungen im Sinne einer möglichst frühen Gefährdungserkennung bzw. der Vermeidung, Opfer zu werden, abzuleiten. Einer breiteren Öffentlichkeit werden die Ergebnisse anhand eines Online-Selbsttests zugänglich gemacht, verknüpft mit praktischen Empfehlungen für UserInnen.

Zusammenfassend lauteten die konkreten inhaltlichen Projektziele wie folgt:

- Identifizieren von Gefährdungstypen im Hinblick auf Cyberkriminalität unter besonderer Berücksichtigung der Kategorie Gender bzw. Sondierung dahingehender Unterschiede zwischen Frauen und Männern (geschlechterspezifisches Internetnutzungsverhalten).
- Gendersensibles Erstellen von detaillierten „Opfer-Profilen" im Zusammenhang mit Cyberkriminalität anhand dokumentierter Fälle (Medien, öffentlich zugängliche Berichte/Dokumentationen von wesentlichen Playern, Einrichtungen und Behörden, vorhandene Studien) unter Berücksichtigung von Aspekten wie Alter, Selbstwirksamkeit, digitale Kompetenz bzw. Bildung/beruflicher Werdegang (z.B. IT-Kenntnisse), Social-Media-Nutzungsverhalten (z.B. privat/beruflich, Einstellung/Verhalten bzgl. Privatsphäre, genutzte Social-Media-Kanäle).
- Detektion konkreter gefahrengeneigter Aktivitäten zur Katalogisierung von Warnsignalen und Empfehlungen sowie Präventionsmaßnahmen im Sinne einer möglichst frühzeitigen Gefährdungserkennung für Frauen/Mädchen und Männer/Burschen.

1.2 Forschungsfragen

Folgende Forschungsfragen standen im Zentrum des Projekts:

- Welche Rolle spielt die Kategorie Gender im Zusammenhang mit Cybercrime-Viktimisierung? Welche unterschiedlichen „Gefährdungstypen" und „Opfer-Profile" sind unter besonderer Berücksichtigung der Kategorie Gender identifizierbar?
  - Welche Fälle von Cyberkriminalität sind dokumentiert?
  - Inwieweit sind weibliche und männliche InternetnutzerInnen Opfer bzw. gefährdet im Zusammenhang mit der jeweiligen Form von Cyberkriminalität?
  - Welche gefahrengeneigten Aktivitäten führen dazu, Opfer von Cyberkriminalität zu werden, und welche Unterschiede gibt es diesbezüglich zwischen weiblichen und männlichen InternetnutzerInnen?
  - Was ist über diese Frauen/Mädchen und Männer/Burschen in Bezug auf Aspekte wie Alter, Selbstwirksamkeit, digitale Kompetenz bzw. Bildung/beruflicher Werdegang (z.B. IT-Kenntnisse) und Social-Media-Nutzungsverhalten (z.B. privat/beruflich, Einstellung/Verhalten bzgl. Privatsphäre, genutzte Social-Media-Kanäle) bekannt?
  - Wie schätzen ExpertInnen die erstellten Typen und „Profile" im Hinblick auf deren Richtigkeit, Repräsentativität und Vollständigkeit ein?
  - Inwieweit spiegeln sich die erstellten Typen und „Profile" in der Einstellung und dem Verhalten von NutzerInnen wider?
- Welche Warnsignale (Prodrome) für Berührungspunkte mit Cybercrimes können aus den validierten Profilen abgeleitet werden?
- Welche sinnvollen Empfehlungen und Präventionsmaßnahmen im Sinne einer möglichst frühen Gefährdungserkennung ergeben sich daraus?

1.3 Theoretisches Fundament

Zur theoretischen Verortung des Projekts wird das aus der Kriminologie stammende sogenannte Routine Activity Framework[2] herangezogen, das besagt, dass Kriminalität im Allgemeinen und somit auch Cyberkriminalität drei Vorbedingungen aufweist, die ein Opferwerden wahrscheinlicher machen:

1. Einen motivierten Täter
2. Das Fehlen von Schutzmechanismen (physisch oder technisch, z.B. Eltern, protektive Software)
3. Ein passendes bzw. verfügbares Opfer bzw. Ziel (relevant ist die Nähe zum Opfer, sei es räumlich oder durch einfache Verfügbarkeit)

Sowohl die Frage guter und geeigneter Schutzmechanismen (Punkt 2) als auch die Frage der Angreifbarkeit (Punkt 3) waren im Projekt zentral.

Die Intersektionalitätsperspektive[3] gibt Aufschluss darüber, dass die Geschlechts- bzw. Genderzugehörigkeit nur einen Teil von umfassenden individuellen Identitätsstrukturen darstellt, dass also beispielsweise Alter und ethnische oder religiöse Zugehörigkeit gemeinsam mit der Gender-Zugehörigkeit eines Menschen verknüpft sind und entsprechend beeinflussen, wie dieser Mensch wahrgenommen wird und welche gesellschaftlichen Erwartungen an ihn herangetragen werden. Zur Veranschaulichung dieser Perspektive: Eine ältere muslimische Frau mit Kopftuch wird gesellschaftlich mit anderen Stereotypen verknüpft als eine junge „westlich" anmutende Frau, wiewohl es sich bei beiden Menschen um Frauen handelt.

Die Gender-Dimension im Zusammenhang mit Cyberkriminalität und Internetnutzung abgekoppelt von anderen Identitätsmerkmalen zu sehen, hätte bloß zu stark stereotypisierenden, verallgemeinernden und simplifizierenden Forschungsergebnissen geführt, weswegen andere wesentliche Identitätsmerkmale aus einschlägiger wissenschaftlicher Literatur identifiziert und mitbedacht und entsprechend bereits in der Gestaltung des Methodendesigns berücksichtigt wurden (siehe Anhang – Typenbildung).

1.4 Methoden

Folgende Methoden bzw. Arbeitsschritte kamen zum Einsatz:

- (Online-)Recherchen (mediale Berichterstattung, öffentlich zugängliche Dokumente/Berichte/Studien/Statistiken, wissenschaftliche Publikationen, Identifizierung möglicher ProjektpartnerInnen/ExpertInnen)
- Interviews mit relevanten ExpertInnen (Behörden, Polizei, JuristInnen, SicherheitsforscherInnen, PsychologInnen, KriminologInnen) im Sinne einer Evaluierung/Validierung der erstellten „Opfer-Profile"
- Quantitative repräsentative Befragung männlicher und weiblicher InternetnutzerInnen ab 16 Jahren (zur Identifizierung gefahrengeneigter Aktivitäten und Gefährdungstypen)

2 Vgl. z. B. Arntfield, M. (2015). Toward a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media. *Canadian Journal of Communication*, 40(3), 371–388.
3 Vgl. z. B. Gopaldas, A. (2013). Intersectionality 101. Journal of Public Policy & Marketing, 32, 90-94.

2

2 RELEVANZ DES THEMAS 15

2.1 Politische Relevanz 15

2.2 Gesellschaftliche Relevanz, Forschungsstand und Forschungslücken 15

2 RELEVANZ DES THEMAS

2.1 Politische Relevanz

Gender Mainstreaming und digitale Sicherheit stehen weit oben auf der politischen Agenda. Im vorliegenden Projekt wurden diese beiden Bereiche erstmalig für Österreich umfassend verknüpft.

Geschlechterspezifik. Dass Frauen und Männer im gesellschaftlichen Leben unterschiedliche Bedarfe und Bedürfnisse haben, ist sowohl in der österreichischen als auch in der EU-Politik längst angekommen. In den vergangenen österreichischen Regierungsprogrammen spiegelte sich dies unterschiedlich wider: Im bislang letzten Programm (Regierung ÖVP/FPÖ bis Mitte 2019) wurden geschlechterspezifische gesellschaftliche Bedürfnisse und die Schaffung entsprechender Rahmenbedingungen in der Gesundheitspolitik („Gender-Medizin") und im Zusammenhang mit geschlechtergerechter Sprache sowie Gleichberechtigung im Erwerbsleben thematisiert. Auf Seite 105 desselben Regierungsprogramms findet sich folgendes Statement: *„Die Besonderheit beider Geschlechter macht den Mehrwert für die Gesellschaft sichtbar. Die Verschiedenheit von Mann und Frau zu kennen und anzuerkennen, ist ein Bestandteil menschlichen Lebens und damit unantastbar mit der Würde des Menschen verbunden."*[4] Auf EU-Ebene ist die Thematik der Gleichberechtigung zwischen den Geschlechtern im Rahmen des European Institute for Gender Equality (EIGE) längst institutionalisiert: *„Equality between women and men is a fundamental value of the European Union."*[5]

Digitale Sicherheit. Das vergangene österreichische Regierungsprogramm definierte Cybersecurity als Schwerpunkt der österreichischen EU-Ratspräsidentschaft. Seite 30 dieses Regierungsprogramms definierte die Entwicklung einer gesamtgesellschaftlichen Strategie zur digitalen Sicherheit als Ziel. Dafür sollte mit Wissenschaft, Forschung, Unternehmen und staatlichen Institutionen zusammengearbeitet werden.

Durch die Relevanz der Dimensionen „Gender" und „Digitale Sicherheit" auf (gesellschafts-)politischer Ebene ist eine forschungsgeleitete Verknüpfung beider Dimensionen im Rahmen eines Forschungsprojekts angezeigt.

2.2 Gesellschaftliche Relevanz, Forschungsstand und Forschungslücken

Konkrete (und repräsentative) Zahlen zu geschlechterspezifischer Internetnutzung und Cyberkriminalität fehlen für Österreich.

Bisherige Studien legen Unterschiede zwischen Frauen und Männern im (sicheren) Umgang mit dem Internet nahe. Sie beschränken sich zumeist auf das Abfragen von Befürchtungen und Eintrittsfällen oder auf bestimmte Altersgruppen (Teenager) oder Rollen (Angestellte), während unterschiedliche Gefahrengeneigtheiten sowie ExpertInnenperspektiven weitgehend außen vor bleiben und Nutzungstypen nicht detailliert untersucht werden.

4 Österreichisches Regierungsprogramm (2017-2022), mittlerweile auf der Seite des Bundeskanzleramts nicht mehr auffindbar, dzt. noch hier abrufbar (Stand: 2.7.2019): https://www.dieneuevolkspartei.at/download/Regierungsprogramm.pdf

5 European Institute for Gender Equality (EIGE) (2019). About EIGE. https://eige.europa.eu/about-eige (zuletzt abgerufen am 2.7.2019).

3

3 CYBERKRIMINALITÄT 19

3.1 Zur Vielfalt des Phänomens Cyberkriminalität 19

3.2 Täter und Opfer 21

3.3 Zahlen und Fakten 22

3 CYBERKRIMINALITÄT

3.1 Zur Vielfalt des Phänomens Cyberkriminalität

Ganz allgemein sind mehrere Deliktarten im Zusammenhang mit dem Internet zu unterscheiden. Dazu zählen Cyberwar, Cyberterrorismus, Nutzung von Kinderpornografie im Netz, Wirtschaftskriminalität, Cybermobbing, Cyberstalking, klassische Computerkriminalität und Urheberrechtsverletzungen.[6] Im Sinne unserer Arbeit im Bereich Eigentumsschutz liegt der Projektfokus auf klassischer Computerkriminalität sowie Urheberrechtsverletzungen, wobei im Zusammenhang mit der Dimension Gender auch die (sozialwissenschaftlich weitaus besser erforschten) Phänomene Cybermobbing und Cyberstalking keinesfalls ignoriert werden dürfen.

Entsprechend der unterschiedlichen Ausgestaltung von Cybercrimes fällt auch der rechtliche Rahmen vielfältig aus:[7]

Tatbestand	Wortherkunft	Bedeutung	Motive	Rechtsgrundlagen
Hasspostings	Hassrede	Wer z.B. im Internet zu Gewalt oder Hass gegen Personen aufgrund ihrer Religionszugehörigkeit, Nationalität, ethnischer Zugehörigkeit, Weltanschauung bzw. sexueller Orientierung oder Hautfarbe aufstachelt. Beschimpfungen, Diskriminierungen	Hass, Hetze, Beleidigung	• § 283 StGB Verhetzung • § 111 StGB Üble Nachrede • § 115 StGB Beleidigung • § 297 StGB Verleumdung • § 152 StGB Kreditschädigung • § 107c StGB Cybermobbing • Verstoß gegen Verbotsgesetz
Cybermobbing	Engl. anpöbeln, fertigmachen	Absichtliches, über einen längeren Zeitraum anhaltendes Beleidigen, Bedrohen, Bloßstellen, Belästigen oder Ausgrenzen anderer über digitale Medien	Spaß, Rache, Zorn, Zugehörigkeit, Macht	§ 107c StGB Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems (FS bis zu 1 Jahr/ Geldstrafe bis zu 720 TS)
Happy Slapping	Engl. fröhliches Schlagen	Veröffentlichung eines mitgefilmten Körperverletzungsdelikts	Erniedrigung des Opfers	z.B. • § 83 StGB Körperverletzung • § 105 StGB Nötigung • § 107 StGB Gefährliche Drohung • § 115 StGB Beleidigung
Cybergrooming	„Internet-Anbahnung" (engl. vorbereiten)	Anbahnung sexueller Kontakte (Vergewaltigung, geschlechtliche Nötigung, sexueller Missbrauch, Herstellung von pornografischen Darstellungen) durch Erwachsene zu Kindern und Jugendlichen	„Pädophilie"	§ 208a StGB Anbahnung von Sexualkontakten zu Unmündigen (Freiheitsstrafe von bis zu 2 Jahren)

Tabelle 1: *Formen von Cyberkriminalität (eigene Darstellung)*

6 Vgl. dazu Huber, E. (2012). Cybercrime – Wer sind die Täter. Abrufbar unter: http://itsecx.fhstp.ac.at/downloads_2012/01_huber.pdf (zuletzt abgerufen am 2.7.2019).
7 Vgl. ebd.

Tatbestand	Wortherkunft	Bedeutung	Motive	Rechtsgrundlagen
Sexting	„Sex" + „Texting" (Engl. Senden von SMS)	Verschicken und Tauschen von eigenen Nacktaufnahmen über Internet und Handy	Kennenlernen, Flirten, Beziehungspflege, Sexuelle Aufreizung, Selbstdarstellung	§ 207a StGB: Pornografische Darstellung Minderjähriger (Strafdrohung je nach Delikt Freiheitsstrafe von bis zu 10 Jahren)
Sextortion	„Sex" + „Extortion" (Engl. Erpressung)	Betrugsmasche -Geld-erpressung durch heimlich aufgezeichnetes Sex-Material	Gelderpressung	• § 144 StGB Erpressung • § 105 StGB Nötigung • § 111 StGB Üble Nachrede • § 207a StGB
Pornografische Darstellungen Minderjähriger		z.B. wirklichkeitsnahe Abbildungen einer geschlechtlichen Handlung oder der Genitalien oder Schamgegend		§ 207a StGB
Weitergabe u. Besitz best. Inhalte an/von Jugendliche/n, jugendgefährdender Medien (Gewalt-Videos)		Insbes. von z.B. pornografischen, nationalsozialistischen oder gewaltverherrlichenden Inhalten		Jugendschutzgesetze der Bundesländer
Verbot der nationalsozialistischen Wiederbetätigung		Z.B.: „Wer öffentlich oder vor mehreren Leuten, in Druckwerken, verbreiteten Schriften oder bildlichen Darstellungen zu einer der nach § 1 oder § 3 verbotenen Handlungen auffordert, aneifert oder zu verleiten sucht, insbesondere zu diesem Zweck die Ziele der NSDAP, ihre Einrichtungen oder Maßnahmen verherrlicht oder anpreist (. . .)"		Verbotsgesetz (z.B. § 3d)

Tabelle 1: *Formen von Cyberkriminalität (eigene Darstellung)*

Die unterschiedlichen Deliktarten lassen eine Zuordnung bzw. Strukturierung nach Angriffsziel und Täter-Opfer-Interaktion zu, wie die folgende Abbildung illustriert[8].

8 Bzgl. möglicher Rollen und Interaktionen von Mensch und Computer im Cybercrime-Kontext vgl. z.B. Moura, G., Sadre, R. & Pras, A. (2014). Bad neighborhoods on the internet. *IEEE Communications Magazine*, 52(7), 132–139.

Keine Täter-Opfer-Interaktion	Hacking (z.B. Social Media-Profil, Online-Banking zwecks Datenklau etc.) Phishing (per E-Mail) (Link Baiting als mögliche Strategie)	Identitätsdiebstahl / Klonen von Online-Identitäten, sich online als eine andere Person ausgeben (via E-Mail, Social Media, …) (mögliche Strategie: Informationsdiebstahl via Messengerdienste, Abgreifen von dort möglicherweise gespeicherten sensiblen Daten) Veröffentlichung falscher Informationen über eine Person (auch: Photo Morphing) Online-Betrug (Versandhandel, Wohnungsmarkt/Airbnb, Online-Auktionen, Kreditkartenbetrug
Täter-Opfer-Interaktion	„Social Engineering“ (z.B. telefonische Kontaktaufnahme mit dem Ziel, Zugang zum Computer zu erhalten, Passwörter, Kontodaten etc. zu erfahren) Ransomware (Verschlüsseln von Dateien bzw. des Computers, um für die Entschlüsselung Geld zu erpressen)	Cyberstalking Cybergrooming Cybermobbing / Beleidigung / Hass / (sexualisierte) Gewalt / Drohungen Love/Romance/Dating Scamming Verbreitung von kompromittierendem Bildmaterial zwecks Erpressung Sextortion (z.B. via Webcam, Photo Morphing)
	Angriff auf Computersysteme	**Angriff auf Personen** **(Kein Angriff auf Computersysteme)**

Tabelle 2: *Modell zur Struktur und Zuordnung von Cyberkriminalität (eigene Darstellung)*

3.2 Täter und Opfer

Generell ist die Täterperspektive im Sinne eines „Profiling“ besser erforscht als die Opferperspektive. Weitgehend Konsens besteht darüber, dass Hacker zumeist junge Männer (Teenageralter bis in die 20er) sind. Motive für deren Handeln sind Neugier oder wirtschaftliches Interesse. Hacking-Opfer sind alle Gruppen – sowohl Privatpersonen als auch öffentliche Einrichtungen oder Firmen können betroffen sein.[9] Für den Bereich (Cyber-)Stalking wird unter anderem berichtet, dass Täter eher männlich und ihre Opfer oftmals ehemalige Beziehungspartnerinnen sind und Belästigung sowohl online als auch offline stattfindet[10].

In einer Studie aus dem Jahr 2015 werden Frauen als kommunikativer im Internet beschrieben, verwenden das Internet also etwa, um ihre sozialen Kontakte zu erweitern oder zu verbessern, Neuigkeiten und Sorgen (mit) zu teilen oder auch Veranstaltungen zu planen.[11] Durch ihr kommunikativeres Online-Verhalten geben Frauen daher zumeist mehr von sich preis als Männer. Männer kommunizieren eher im „Special Interest“-Umfeld, das heißt vor allem zur Suche und zum Rezipieren von Informationen und Entertainment. Einer älteren und daher ob deren Aktualität zu hinterfragenden Studie aus dem Jahr 2005 zufolge nutzen Männer das Internet eher für Transaktionen bzw. Handel und sind sicherer im Umgang und kompetenter in der Kenntnis von Internettools und -technologien.[12]

9 Vgl. Bundeskriminalamt Deutschland / Kriminalistisches Institut / Forschungs- und Beratungsstelle Cybercrime KI16 (4.12.2015). Täter im Bereich Cybercrime. Eine Literaturanalyse. Abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Internetkriminalitaet/internetkriminalitaet_node.html, zuletzt abgerufen am 19.9.2019.

10 Vgl. Der Standard (21.2.2019). Stalking: Wenn das Trachten nach Nähe zu Gewalt wird (verfasst von Nicole Schöndorfer, abrufbar unter https://www.derstandard.at/story/2000098049042/wenn-das-trachten-nach-naehe-zu-gewalt-wird), zuletzt abgerufen am 19.9.2019.

11 Vgl. Danoglidis, S. A. (2015). Internetnutzung: Frauen vs. Männer. (3.2.2015). Abrufbar unter: https://entwickler.de/online/webmagazin/internetnutzung-frauen-vs-maenner-39308.html (zuletzt abgerufen am 2.7.2019).

12 Vgl. Fallows, D. (2005). How Women and Men use the Internet. (28.12.2005). Abrufbar unter: http://www.pewinternet.org/2005/12/28/how-women-and-men-use-the-internet/ (zuletzt abgerufen am 2.7.2019).

3.3 Zahlen und Fakten

- In Österreich ist die Anzahl angezeigter Cybercrime-Fälle tendenziell steigend, während die Aufklärungsrate in absoluten Zahlen zwar wächst, anteilig bzw. prozentual jedoch tendenziell zurückgeht: Konnten im Jahr 2006 noch 2.312 von insgesamt 3.257 angezeigten Fällen geklärt werden (Aufklärungsquote: 71%), waren es im Jahr 2017 6.470 von 16.804 Fällen (Aufklärungsquote: 38,5%)[13]. Angenommen werden kann, dass die meisten Cyberkriminalitätsfälle im Dunkelfeld bleiben bzw. nicht angezeigt werden und nur ein kleiner Teil ins Hellfeld gelangt.
- Special Eurobarometer 464a (Europeans' attitudes towards cyber security)[14]: 87% der EU-BürgerInnen halten Cybercrimes für eine bedeutende Herausforderung. Nur 49% finden, dass die Strafverfolgung bzw. der Gesetzesvollzug bereits ausreichen. Generell steigt das Bewusstsein, aber hier gibt es noch Luft nach oben. Die meisterlebten Situationen sind Schadsoftware auf Geräten sowie Phishing (per E-Mail bzw. telefonisch unter dem Begriff Social Engineering).
- Generell ist das Internetnutzungsverhalten von Frauen eher kommunikativ geprägt (hohe Nutzungsintensität sozialer Medien), während jenes von Männern eher unterhaltungsorientiert geprägt ist (hoher Gaming-, Video- und Musikkonsum). Einer Umfrage unter 2.871 InternetnutzerInnen aus dem Jahr 2015 zufolge haben sich 10% der Männer und 8% der Frauen mit einem Computervirus infiziert, nachdem sie eine gehackte Website besucht haben. 17% der befragten Männer und 14% der Frauen gaben an, nach einer Computervirusinfektion einen finanziellen Verlust erlitten zu haben. Frauen sind daher eher der Gefahr des Accountdaten-Phishings sozialer Netzwerke ausgesetzt, während sich Männer eher vor Drive-by-Download-Angriffen, das heißt einer Computervirusinfektion allein durch den Besuch einer kompromittierenden Website, in Acht nehmen müssen.[15]
- Eine weitere Umfrage unter deutschen Männern und Frauen aus dem Jahr 2018 legt nahe, dass sich Frauen misstrauischer im Netz bewegen als Männer, wenn es um IT-Sicherheit und Datenschutz geht: 18% der befragten Frauen und 15% der befragten Männer halten einen Hack ihres Online-Banking-Accounts in den nächsten 12 Monaten für wahrscheinlich. 71% der Frauen und 64% der Männer halten den Missbrauch ihrer persönlichen Daten nach einem Social-Media-Account-Hack für wahrscheinlich.[16]
- Insgesamt schätzen Frauen bzw. Mädchen ihre Fähigkeiten und Ressourcen für eine sichere Internetnutzung bzw. aktiv dazu beitragen zu können schwächer ein als Männer bzw. Burschen (Selbstwirksamkeit).[17] Entsprechende Studien beziehen sich speziell entweder auf Teenager oder auf Männer und Frauen als Angestellte.

13 Vgl. statista. Entwicklung der Anzahl der angezeigten und geklärten Fälle von Cybercrime (gesamt) in Österreich von 2006 bis 2018. (mit Verweis auf das Bundeskriminalamt, Cybercrime-Report) Abrufbar unter: https://de.statista.com/statistik/daten/studie/680927/umfrage/angezeigte-und-geklaerte-faelle-von-cybercrime-in-oesterreich/ (zuletzt abgerufen am 2.7.2019).

14 Vgl. European Commission / Migration and Home Affairs (2017). Europeans' attitudes towards cyber security. (19.9.2017). Abrufbar unter https://ec.europa.eu/home-affairs/news/europeans%E2%80%99-attitudes-towards-cyber-security_en (letztes Update: 2.7.2019).

15 Vgl. Danoglidis, S. A. (2015). Internetnutzung: Frauen vs. Männer. (3.2.2015). Abrufbar unter: https://entwickler.de/online/webmagazin/internetnutzung-frauen-vs-maenner-39308.html (zuletzt abgerufen am 2.7.2019).

16 Vgl. Kaspersky Lab (2018). Männer sind leichtfertiger als Frauen – bei Datenschutz und IT-Sicherheit. (Pressemitteilung vom 6.12.2018). Abrufbar unter: https://www.kaspersky.de/about/press-releases/2018_men-are-more-reckless-than-women-in-privacy-and-it-security (zuletzt abgerufen am 2.7.2019).

17 Vgl. Amo, L. (2016). Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy. *IEEE Security & Privacy*, 14 (1), 72-75.
Vgl. Anwar, M. et al. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

4

4 RELEVANTE VORPROJEKTE IM KFV-FORSCHUNGSBEREICH EIGENTUMSSCHUTZ 27

4.1 Cybercrime-Barometer 27

4.2 Tatort Social Media 29

4 RELEVANTE VORPROJEKTE IM KFV-FORSCHUNGSBEREICH EIGENTUMSSCHUTZ

Studien im Bereich Cyberkriminalität mit explizitem Fokus auf der Dimension Gender wurden im KFV-Forschungsbereich Eigentumsschutz bislang noch nicht durchgeführt, jedoch wurde dieser Aspekt in einigen Projekten am Rande mitbedacht bzw. miterhoben. Dazu zählen die Projekte **„Cybercrime-Barometer" (CyBar)** sowie **„Tatort Social Media"** (beide durchgeführt im Jahr 2018).

4.1 Cybercrime-Barometer

Das als Pilot-Befragung definierte Projekt „Cybercrime-Barometer" (2018) wurde im September 2018 vom Österreichischen Gallup Institut im Auftrag des KFV durchgeführt. Die Befragung der Privatpersonen erfolgte online. Die Stichprobe bestand aus 1.000 ÖsterreicherInnen repräsentativ für die österreichische Bevölkerung ab 14 Jahren, zusätzlich wurde in allen Bundesländern auf eine Stichprobe von mindestens 100 Personen aufgestockt, um Aussagen auch auf Bundesländer-Ebene treffen zu können. Insgesamt wurden 1.210 Personen befragt.

Die Pilot-Befragung ergab, dass unter 30-jährige Menschen sozialen Medien gegenüber weniger kritisch eingestellt sind als ältere Befragte. So sind sie auch eher von Delikten in diesem Zusammenhang betroffen. Mehr als jeder Zehnte von ihnen wurde bereits über soziale Medien angegriffen (Mobbing), Männer und Frauen sind davon gleichermaßen betroffen. Andere Delikte wie Identitätsdiebstahl und Grooming betreffen vor allem junge Frauen. Insbesondere junge Männer (14 bis 29 Jahre) sind aber teilweise zu sorglos in Bezug auf mögliche Attacken. Hingegen sind junge Frauen eher besorgt, Opfer zu werden.

Bezüglich der Nutzung von Hardware gibt es Unterschiede zwischen Frauen und Männern: Tablet und Notebook werden zwar gleichermaßen von Frauen und Männern genutzt. Unterschiede gibt es aber bei Desktop-PCs und Spielkonsolen, mit denen Männer häufiger mit dem Internet verbunden sind als Frauen. Bei Personen im Alter ab 30 Jahren sind Männer auch häufiger per Smart-TV im Internet als Frauen. Bei den jungen Nutzern unter 30 sind Frauen und Männer gleichermaßen im Internet aktiv.

Junge NutzerInnen wissen über viele Arten von Internetkriminalität weniger gut Bescheid als der Durchschnitt. Allerdings ist auffällig, dass sie über psychische Angriffe gegen Personen (Grooming und Mobbing) besser informiert sind. Junge Frauen geben zudem häufiger als junge Männer an, diese Form der Kriminalität zu kennen.

Wesentliche genderrelevante CyBar-Ergebnisse im Überblick:[18]

- Männer (49%) sind von Viren und Trojanern häufiger betroffen als Frauen (44%).
- Frauen erhalten häufiger Spam-Mails (57%) als Männer (46%).
- Nahezu jede vierte Frau (23%) unter 30 wurde bereits Opfer eines Identitätsdiebstahls auf sozialen Netzwerken (Männer 11%), 42% davon sogar öfter als einmal.
- Jede fünfte Frau (20%) wurde online in unangebrachter Weise angesprochen oder belästigt (Männer 10%), 30% davon sogar öfter als 4 Mal.

Häufigste Folgen der Cybercrime-Aktivitäten sind emotionale Verletzungen und hoher organisatorisch-bürokratischer Aufwand.

- Emotionale Verletzungen resultieren häufig aus Mobbing- oder Grooming-Angriffen.
- Organisatorischer Aufwand entsteht am häufigsten durch Trojaner/Viren und Hacken von Geräten.
- Finanzieller Verlust durch Phishing ist bei jungen Männern größer als bei jungen Frauen.
- Frauen nehmen eher ExpertInnen-Hilfe in Anspruch als Männer.

Entsprechend den Erfahrungen mit Internetkriminalität zeichnet sich auch das Bild der Sorge, Opfer zu werden.

- Am meisten Sorge besteht hinsichtlich Viren und Trojanern (54%) – hier sorgen sich Männer und Frauen gleichermaßen, gefolgt von Spam-Mails (43%) und Phishing-Mails (35%).
- Insgesamt jedoch haben Frauen mehr Sorge, (wieder) Opfer zu werden als Männer.
- Männer finden eine digitale und vernetzte Welt besser (30%) als Frauen (20%).
- 55% der Männer und 38% der Frauen sind gegenüber sozialen Medien negativ eingestellt. Am deutlichsten zeigt sich dieser Unterschied bei den älteren Befragten, wo 68% der Männer und 52% der Frauen nichts von sozialen Medien halten.

18 https://www.kfv.at/wp-content/uploads/2019/07/Bericht_Internetkriminalität_Internet.pdf

4.2 Tatort Social Media

Während sich das Projekt CyBar dem Phänomen Cyberkriminalität alters- und medienübergreifend widmete, setzte sich das Projekt „Tatort Social Media“ speziell mit der Social-Media-Nutzung von Kindern bzw. Jugendlichen ab 12 Jahren auseinander. Hier stellte sich unter anderem heraus, dass Mädchen eher mit ungewollten „Komplimenten“ belästigt werden (auch nachdem darum gebeten wurde, damit aufzuhören) als Burschen. Dennoch sind auch Burschen davon betroffen. Insbesondere Mädchen haben bereits unangenehme Situationen im Internet erlebt, möglicherweise sind sie aber auch weniger gehemmt, darüber zu sprechen. Von „Body Shaming“ und Mobbing sind vor allem Mädchen betroffen, während Buben Erzählungen von Mädchen zufolge eher Täter sind.

Generell nutzen Jugendliche WhatsApp sehr stark, unter anderem zur Koordination mit der peer group oder des Familienalltags oder etwa zum Austausch von Informationen betreffend Hausaufgaben. Die Nutzung von Videotelefonie, etwa zur Kommunikation mit der besten Freundin, ist eher mädchenspezifisch, ebenso wie die „spielerische“ Nutzung sozialer Medien (z.B. TikTok).

Um jugendliche Internetnutzung und Gefahren, die sich daraus ergeben, zu verstehen sowie möglichst früh sensibilisierend und bewusstseinsbildend agieren zu können, ist es jedenfalls wichtig, auch jugendspezifische Plattformen im Sinne von Online-Lebenswelten und Funktionalitäten zu kennen. Dazu zählen aktuell etwa TikTok[19], Discord[20], Twitch[21] sowie FaceTime (bei iPhones) oder Houseparty[22] als Video-Chat-Kanäle, die, wie zuvor erwähnt, vor allem von Mädchen genutzt werden.

19 https://www.tiktok.com/de/
20 https://discordapp.com
21 https://www.twitch.tv/
22 https://houseparty.com/

5

5 ERGEBNISSE 33

5.1 Ergebnispräsentation Teil 1: Typenbildung („Opfer-Profile“) 33

5.1.1 Archetypen 33

5.1.2 Gefährdungstypen 34

5.2 Ergebnispräsentation Teil 2: Validierung der Typen durch ExpertInnen 36

5.2.1 Kritische Reflexion der „Opfer-Typen“ 36

5.2.2 Typologisierung anhand von Risikofaktoren 36

5.2.3 Ergebnisse 39

5.3 Ergebnispräsentation Teil 3: Repräsentative Befragung 40

5.3.1 Internetnutzung, Internetsicherheit und die Rolle digitaler Kompetenz 41

5.3.2 Präventionsmaßnahmen und praktische Empfehlungen für UserInnen 46

5.3.3 Konkrete Sicherheitsmaßnahmen und Gefahren 48

5.3.4 Fragwürdige/illegale Inhalte im Netz 49

5.3.5 Viktimisierung insgesamt 49

5.3.6 Folgen von Cyberkriminalität 52

5.4 Resümee 54

5.4.1 Erste Schritte für Opfer 54

5.4.2 Anlaufstellen für Hilfesuchende 54

5 ERGEBNISSE

5.1 Ergebnispräsentation Teil 1: Typenbildung („Opfer-Profile“)

Anhand umfassender Analysen wissenschaftlicher Literatur sowie öffentlich zugänglicher Studien und Statistiken (beispielsweise des 2017 publizierten Eurobarometers speziell zum Thema Cybersecurity[23] sowie des Cybercrime-Reports des österreichischen Bundeskriminalamtes[24]) und thematisch relevanter medialer Berichterstattung wurden genderfokussiert Muster zum Thema Cyberkriminalität identifiziert, die schließlich in folgende **zwei Archetypen und drei delikt- und verhaltensbasierte Gefährdungstypen** zusammengefasst werden konnten (Details dazu siehe Anhänge 1 und 2). Archetypen beschreiben dabei Personengruppen, die aufgrund immanenter, nicht veränderbarer Wesensmerkmale eher Opfer werden; Gefährdungstypen beschreiben vor allem Verhaltensweisen, die dazu führen können, Opfer bestimmter Delikte (siehe dazu Abbildung 1) zu werden:

5.1.1 Archetypen

5.1.1.1 Das Zufalls-Opfer

Ein zufälliges Opferwerden betrifft vor allem Deliktarten, die Computersysteme angreifen und keine Täter-Opfer-Interaktion beinhalten, wie etwa **Hacker- und Phishing**-Attacken (zur im Projekt verwendeten Einordnung von Deliktarten vgl. Abbildung 1):

Bei Angriffen auf Computersysteme ohne Täter-Opfer-Interaktion, also Hacking- oder Phishing-Angriffen, spielt der Zufall mehr als in anderen Bereichen eine Rolle (vgl. dazu Abbildung 1). Es ist also nicht absehbar, wer Opfer werden kann. Potenziell kann jeder bzw. jede sowohl im privaten als auch im beruflichen Umfeld betroffen sein. Opfer in diesem Bereich sind also weniger durch Geschlecht, Alter oder Status zu charakterisieren als durch ihren **Umgang mit dem Internet** bzw. inwieweit ihnen entsprechende Tools und Technologien geläufig sind, inwieweit sie darin geübt sind und ihr Blick für entsprechende Phishing-Versuche geschärft und Software (z.B. Anti-Viren-Schutz) auf dem neuesten Stand ist. Schlüsselkriterium für den Schutz vor Phishing oder Hacker-Angriffen ist also digital-technologische Kompetenz (*„technological fluency“*).

Anfällig sind also sowohl Frauen als auch Männer, die entweder ungeübt/unerfahren mit dem Internet sind, fahrlässig/sorglos mit Hard- und Software oder auch ihren persönlichen Daten (Passwörtern, SV-Nummern, Kontonummern etc.) umgehen oder mangelnde digitale Kompetenz aufweisen (z.B. im Zusammenhang mit Nicht-Erkennen von Phishing-Mails, kein Anti-Viren-Schutz, Passwörter in Dateiordnern mit „auffälligem“ Namen wie etwa „privat“ oder „Eigene Dateien“, allgemeine Gutgläubigkeit in Bezug auf E-Mail-Anfragen und Link Baiting).

Zusammengefasst kann gesagt werden: Der Zufall entscheidet über potenzielle Opfer. Sorglosigkeit bzw. übersteigertes Sicherheitsgefühl (Eigenschaften, die beispielsweise vor allem bei Männern zwischen 14 und 29 Jahren beobachtet werden können), Unachtsamkeit bzw. mangelndes Wissen/Bewusstsein über Phishing- und Hacking-Angriffe (vor allem bei jungen Leuten bemerkbar), Ungeübtheit und Gutgläubigkeit/Naivität sowie (mangelnde) technologische Kompetenz können aber darüber entscheiden, ob die Falle letztendlich zuschnappt.

23 Vgl. European Commission / Migration and Home Affairs (2017). Europeans' attitudes towards cyber security. (19.9.2017). Abrufbar unter https://ec.europa.eu/home-affairs/news/europeans%E2%80%99-attitudes-towards-cyber-security_en (letztes Update: 2.7.2019)

24 Vgl. Bundesministerium für Inneres (2017). IT-Sicherheit. Cybercrime-Report 2016: Zahl der Anzeigen 2016 fast um ein Drittel gestiegen. Artikel Nr. 15260 vom Montag, 30. Oktober 2017. Abrufbar unter: https://www.bmi.gv.at/news.aspx?id=5062565A4F35476A2B38453D (zuletzt abgerufen am 2.7.2019).

5.1.1.2 Das weibliche Opfer

Oft reicht der Umstand, eine **Frau** zu sein, aus, um Opfer von Cyberkriminalität zu werden. Das betrifft vor allem Deliktarten, die Angriffe auf Personen (und nicht auf Computersysteme) mit Täter-Opfer-Interaktion verknüpfen. Am deutlichsten wird dieser Umstand anhand **sexualisierter Gewalt** und entsprechenden Drohungen und Beleidigungen, die etwa Frauen mit hohem **sozioökonomischem Status** treffen, mit dem Ziel, diese abzuwerten. Täter sind in solchen Fällen zumeist Männer, die ihre Opfer über unterschiedliche Medienkanäle (z.B. Social-Media-Kanäle, E-Mail, Messenger-Dienste) kontaktieren. Zudem spielt **Ethnizität** eine Rolle: Frauen bzw. Mädchen mit nicht weißer Hautfarbe werden eher Opfer sexualisierter Gewalt im Internet.

Überdies sind vor allem (junge) Frauen potenzielle Opfer von Cybergrooming und Cybermobbing. Vor allem Mädchen nutzen soziale Medien eher „spielerisch" (z.B. TikTok) und chatten eher mit Unbekannten, was zusätzlich Angriffsfläche für Täter bietet (Experimentierfreude). Zu beobachten ist etwa auch, dass Mädchen, die bereits als Cybermobberinnen in Erscheinung getreten sind, später eher selbst Opfer von Cybermobbing werden, beispielsweise, wenn sich frühere Opfer an ihnen rächen[25]. Anders das Phänomen Cyberstalking: Jenes betrifft zwar eher Frauen, aber auch Männer, über weibliche Opfer wird jedoch mehr berichtet. Das typische Cyberstalking-Opfer ist angestellt und in einer Partnerschaft lebend oder verheiratet.

5.1.2 Gefährdungstypen

5.1.2.1 Die Arglosen/Die Vertrauensvollen/Die Unbedachten/Die Gutgläubigen („Die Vertrauens-Falle")

Die **„Vertrauens-Falle"** betrifft sowohl Angriffe auf Computersysteme mit Täter-Opfer-Interaktion (in Form von Social Engineering) als auch Angriffe auf Computersysteme ohne Täter-Opfer-Interaktion (z.B. Phishing) und Angriffe auf Personen mit Täter-Opfer-Interaktion (z.B. Love/Romance/Dating Scamming).

Social Engineering braucht eine erfolgreiche Kontaktaufnahme des Täters mit dem Opfer insofern, dass ersterer genug Vertrauen aufbauen kann, um Zugriff auf den Computer des Opfers zu erhalten. Besonders offenes Kommunikationsverhalten bzw. die bereitwillige Inanspruchnahme von „Hilfe" bzw. „Hilfsangeboten" auch von Fremden begünstigen die Viktimisierung. Neben allgemeiner (Un-)Sicherheit im Umgang mit Computern (digitaler Kompetenz) entscheidet also der Grad kommunikativer Offenheit bzw. entsprechendes Vertrauen auch Fremden gegenüber darüber, ob ein Schaden eintritt. Dadurch, dass Männer ihre Selbstwirksamkeit im Umgang mit dem Internet (also ihre Fähigkeit, selbst etwas zum sicheren Umgang mit dem Internet beitragen zu können) höher einschätzen als Frauen und möglicherweise eher versuchen, entsprechende Probleme selbst zu lösen, könnten (möglicherweise vor allem ältere) Frauen eher von dubiosen „Hilfsangeboten" in Form von Social Engineering betroffen sein.

Love/Romance/Dating Scamming betrifft Frauen und Männer gleichermaßen, wobei unterschiedliche Strategien beobachtet werden können:

- Männer werden mit falschen Frauen-Profilen dazu animiert, anstößige Bilder zu schicken, es folgt die Drohung, diese Bilder an Familie, Ehefrau, Firma etc. zu schicken. Ziel und Strategie ist die Erpressung von Geld über eine Anbahnung sexueller Kontakte.
- Frauen werden von vermeintlichen Verehrern darum gebeten, Geld zu überweisen. Ziel und Strategie ist es hier, Frauen in eine emotionale Abhängigkeit zu führen, sodass diese letztlich freiwillig Geld transferieren.

Frauen und Männer, die Dating-Portale nutzen, sind naturgemäß besonders gefährdet. Ältere, ein-

25 Vgl. z.B. Landesmedienzentrum Baden-Württemberg: Wer mobbt? Wer leidet? Wer schaut zu? Täterinnen und Täter (https://www.lmz-bw.de/medien-und-bildung/jugendmedienschutz/cybermobbing/wer-mobbt-wer-leidet-wer-schaut-zu/), abgerufen am 18.9.2019.

same und ev. geschiedene Frauen werden bei zweiterer Variante als besonders gefährdet eingeschätzt. Online-Betrug ist andererseits sicherlich weniger genderspezifisch zu fassen. Hier sind Unachtsamkeit und Gutgläubigkeit bzw. Impulsivität und Eile wohl eher relevante Schlüsselkriterien.

5.1.2.2 Die Unvorbereiteten/Fahrlässigen („Die Fahrlässigkeits-Falle")

Die **„Fahrlässigkeits-Falle"** betrifft vor allem Angriffe auf Computersysteme mit Täter-Opfer-Interaktion (z.B. Einsatz von Ransomware zur Erpressung von Geld).

Wenn etwa Dateien bzw. der Computer mittels Ransomware verschlüsselt werden und für die Wiederentschlüsselung Geld erpresst wird, ist es nicht ratsam, sich auf solche Deals einzulassen. Anfällig dafür, dies trotzdem zu tun, sind vor allem solche Personen, die aus Unwissenheit bzw. aus mangelndem Gefahrenbewusstsein sensible Firmen- oder Privatinformationen nicht zusätzlich gesichert bzw. geschützt haben. Wer erpressbar ist, ist letztendlich nicht gender- oder altersabhängig. Erpressbarkeit betrifft vielmehr solche Leute, die Verantwortung oder Verfügung über sensible Informationen bzw. Daten haben (z.B. Firmendaten, die von Geschäftsleuten bzw. Personen mit gehobenem sozioökonomischem Status verwaltet werden bzw. jene betreffen).

Während im Fall von Social Engineering eher noch der Zufall über potenzielle Opfer entscheidet, kann angenommen werden, dass der gezielte Einsatz von Ransomware unter anderem dort erfolgen kann, wo „interessante" (im Sinne für das Opfer unverzichtbare) Informationen vermutet werden.

5.1.2.3 Die Impulsiv-Offenen/Die Kommunikations- und Experimentierfreudigen („Die Impuls -Falle")

Die **„Impuls-Falle"** schnappt vor allem bei Angriffen auf Personen ohne (z.B. Online-Identitätsdiebstahl) und mit Täter-Opfer-Interaktion (z.B. Sextortion, Verbreitung von kompromittierendem Bildmaterial, Cybergrooming) zu.

Online-Identitätsdiebstahl und das Verbreiten falscher, rufschädigender Informationen über bestimmte Personen finden vermehrt auf Social-Media-Kanälen statt und betreffen vor allem jene, die entsprechende Social-Media-Services intensiv und vorwiegend öffentlich, also uneingeschränkt einsehbar, nutzen und deren Social-Media-Präsenz aus unterschiedlichen Gründen auffällt (z.B. auch politisches Engagement, Prominenz). Neben öffentlich zugänglichen verbalen/schriftlichen Inhalten (auch sensiblen Daten) sind auch öffentliche visuelle Inhalte (z.B. Fotos/Selfies, Videos, Profilbilder) „nützlich" für Identitätsdiebstahl und können für das Verbreiten von Falschinformationen entsprechend nutzbar gemacht werden (z.B. durch „Photo Morphing"). Gefährdet sind tendenziell junge weibliche Social-Media-Nutzerinnen unter 30, oftmals mit öffentlichem Social-Media-Profil (das erst dann auf „privat" umgestellt wird, wenn etwas passiert ist) und impulsivem, unvorsichtigem Handeln bzgl. des Teilens von Informationen über sich selbst. Generell sind Frauen eher gefährdet als Männer, wenn mit der Online-Identität sexuelle Aspekte (Morphing von Bildmaterial zu pornografischem Material oder das Anbieten von sexuellen Dienstleistungen im Namen des Opfers) verknüpft werden. Generell nutzen junge Frauen bzw. Mädchen soziale Medien eher „spielerisch" (z.B. TikTok) als junge Männer bzw. Burschen und chatten eher mit Unbekannten, was eine zusätzliche Angriffsfläche für Täter bietet (Experimentierfreude).

5.2 Ergebnispräsentation Teil 2: Validierung der Typen durch ExpertInnen

Die oben beschriebenen, mithilfe relevanter Quellen kreierten Typen wurden von IFES den folgenden fünf ExpertInnen aus den Bereichen Opferschutz, Ermittlungsbehörden und Forschung in jeweils rund einstündigen leitfadengestützten Interviews zur Validierung vorgelegt: Edith Huber (Expertin für Cybercrime und Cybersecurity an der Donau-Universität Krems), Dina Nachbaur (Weißer Ring), Thorsten Behrens (Österreichisches Institut für Angewandte Telekommunikation), einem in einem Landeskriminalamt ansässigen IT-Experten sowie einem Experten des im Bundeskriminalamt angesiedelten Cyber Crime Competence Center. Die beiden letztgenannten Experten möchten anonym bleiben bzw. haben die Zustimmung zur Nennung ihres Namens nicht explizit erteilt. Zuvor wurden in Frage kommende ExpertInnen durch Recherche in österreichischen Medien identifiziert. Im Rahmen des Validierungsvorhabens wurde eruiert, inwieweit ExpertInnen die unterschiedlichen Typen als realistisch bzw. lebensnah einstufen, was sie am Typenmodell ändern würden und welche Erfahrungen sie anhand der Typen in ihrem beruflichen Kontext selbst bereits gemacht bzw. welche Fälle sie erlebt haben. Für Letzteres wurden neben den oben beschriebenen Typen auch Fälle aus den Medien (siehe Anhang 2) skizziert und zur Diskussion gestellt. Die leitfadengestützten Interviews wurden nach Transkription qualitativ-inhaltsanalytisch (nach Mayring) ausgewertet.

5.2.1 Kritische Reflexion der „Opfer-Typen"

Die weiter oben vorgeschlagenen Opfer-Typen sind aus der Sicht der ExpertInnen schlüssig beschrieben, allerdings in der Realität meist nicht klar voneinander abzugrenzen, da etwa oft mehr als ein Typ zutrifft. Am kritischsten wurde der Typ der „Impulsiv-Offenen" („Die Impuls-Falle") gesehen, hier urgieren die ExpertInnen, dass auch Fahrlässigkeit eine große Rolle spielt, wodurch dieser Typ schwierig vom Typ „Die Unvorbereiteten/Fahrlässigen" abzugrenzen ist. Die vorgeschlagenen Typen sind also explizit als Idealtypen zu sehen, die zwar Orientierung geben können, zu denen einzelne Personen aber selten eindeutig und trennscharf zuordenbar sein werden. Ergänzend wurden auch besonders offene und digital unerfahrene Menschen als Risikogruppen genannt.

5.2.2 Typologisierung anhand von Risikofaktoren

Auf Basis der ExpertInneninterviews bietet sich neben der idealtypischen Klassifizierung von Opfer-Typen eine flexiblere und damit eindeutig zuordenbarere Definition unterschiedlicher Risikofaktoren an, die gemeinsam und in unterschiedlicher Kombination auftreten können. Detailliertere Beschreibungen sind dann möglich, wie etwa jene, dass offene und neugierige Menschen nur dann stark gefährdet sind, wenn sie auch leichtsinnig sind. Aus den Interviews konnten für das jeweilige Risikoverhalten charakteristische Eigenschaften und Risikofaktoren für die jeweiligen Arten von Cybercrime abgeleitet werden.

Die folgende Aufstellung fasst zusammen, welche Risikofaktorgruppen bei den häufigsten Formen von Cybercrime eine Rolle spielen können:

- Identitätsdiebstahl: Arglosigkeit, Fahrlässigkeit, Leichtsinnigkeit, Offenheit, digitale Unerfahrenheit
- Cyber-Betrug: Arglosigkeit, Leichtfertigkeit, digitale Unerfahrenheit
- Cybergrooming: Offenheit
- Phishing: Arglosigkeit, Leichtfertigkeit, digitale Unerfahrenheit
- Erpressungen: Leichtfertigkeit, digitale Unerfahrenheit (bei Ransomware: Fahrlässigkeit)
- Love-Scamming: Arglosigkeit, Offenheit
- Cybermobbing & Cyberstalking: Leichtfertigkeit, Offenheit
- Hasspostings, Diskriminierung & Verhetzung: Offenheit
- Social Hacking: Arglosigkeit, digitale Unerfahrenheit
- „Computer-based"-Crime: Fahrlässigkeit, digitale Unerfahrenheit

Aus den ExpertInneninterviews ergibt sich eine empirisch ausgerichtete Typologie, die sich wie folgt an den Faktorengruppen Arglosigkeit, Fahrlässigkeit (in technischer Hinsicht), Leichtfertigkeit (im Umgang mit Daten und Inhalten), Offenheit sowie digitale Unerfahrenheit orientiert:

5.2.2.1 Eine Typologie der Risikofaktoren

Faktorengruppe 1: **Digital-Leichtsinnig**

NutzerInnen, die sich im Internet **vertrauensvoll und gutgläubig** verhalten und z.B.

- Hilfsangebote (auch von Fremden) annehmen, ohne sie zu hinterfragen, und Hilfe leisten, ohne misstrauisch zu werden
- Anleitungen für Online-Zahlungen oder Online-Buchungen befolgen, ohne sie in Frage zu stellen, solange die Websites (halbwegs) professionell wirken
- Aufforderungen nachkommen, wenn diese von vermeintlichen Banken oder ähnlichen Institutionen mit „Autorität" an sie per E-Mail geschickt werden

Gefährdet sind diese Personen vor allem von Social Hacking (insbesondere, wenn andere Faktoren hinzukommen, z.B. geringe digitale Kompetenz), Phishing, Cyber-Betrug (insbesondere, wenn andere Faktoren hinzukommen), Love-Scamming (wenn die persönliche Lebenssituation dies fördert) und Identitätsdiebstahl (bei dem die Daten in der realen Welt gestohlen werden, der Missbrauch aber in der Online-Welt stattfindet).

Ein **höheres Risiko** tragen

- nach Alter: eher ältere Personen

Es müssen nicht alle Kriterien erfüllt sein, aber mindestens zwei von ihnen.

5.2.2.2 Eine Typologie der Risikofaktoren 2

Faktorengruppe 2: **Sicherheits-Leichtsinnig**

NutzerInnen, die z.B.

- vor der Nutzung neuer Hard- oder Software keine oder kaum Informationen einholen
- grundsätzlich kein Interesse an IT-Themen haben
- in dem falschen Bewusstsein leben, dass ihnen schon nichts passieren wird

· keine ausreichenden oder die falschen Vorsichtsmaßnahmen technischer Natur ergreifen, z.B. auf Anti-Viren-Programme, Sicherheitskopien oder Passwörter verzichten
Gefährdet sind sie vor allem von Viren, Trojanern, Malware, Hacking, Datendiebstahl, Identitätsdiebstahl oder Ransomware.

Ein **höheres Risiko** tragen

Es müssen nicht alle Kriterien erfüllt sein, aber mindestens zwei von ihnen.

- nach Geschlecht: eher Frauen

5.2.2.3 Eine Typologie der Risikofaktoren 3

Faktorengruppe 3: **Digital-Impulsiv**

NutzerInnen, die z.B.

· im Internet impulsgesteuert handeln
· Inhalte von Webseiten nur ungenau oder gar nicht lesen
· unbedacht auf Links klicken, ohne diese genau anzusehen oder zu überprüfen
· viele Fotos (auch in lächerlichen Lebenslagen) von sich veröffentlichen bzw. intimes Bildmaterial an andere weitergeben
· Schnäppchen kaufen, ohne über die Shops zu recherchieren
· Videos und Ratgeber, etwa zu Schönheits- und Gesundheitsthemen (z.B. zum Abnehmen), erstehen, ohne die Expertise der Produzenten*innen zu überprüfen
· PIN-Codes gemeinsam mit den dazugehörigen Kredit-/Bankomatkarten aufbewahren oder offen herumliegen lassen

Gefährdet sind sie vor allem von Betrug, Identitätsdiebstahl, Sextortion, Phishing, Mobbing sowie durch den schnellen Klick auf einen Link von *computer-based* crime.

Ein **höheres Risiko** tragen

Es müssen nicht alle Kriterien erfüllt sein, aber mindestens zwei von ihnen.

- nach Geschlecht: eher Frauen
- nach Alter: eher junge und Menschen mittleren Alters

5.2.2.4 Eine Typologie der Risikofaktoren 4

Faktorengruppe 4: **Digital-Naiv**

NutzerInnen, die z.B.

· neugierig und experimentierfreudig sind
· bereitwillig und offen kommunizieren
· Social-Media-Angebote intensiv nutzen
· ihre Social-Media-Aktivitäten uneingeschränkt einsehbar (also öffentlich) halten
· eine auffallend starke Medienpräsenz zeigen
· soziale Kontakte zu einem beträchtlichen Teil über die sozialen Medien knüpfen und bewahren
· ihr Alltagsleben mithilfe des Smartphones organisieren

Gefährdet sind sie vor allem von Cybergrooming, Cybermobbing, der Verbreitung bzw. Schaffung von kompromittierendem Bildmaterial, Identitätsdiebstahl (Fake-Profilen), Love-Scamming und Hasspostings.

Ein **höheres Risiko** tragen

- nach Alter: eher junge Menschen bis 35

Es müssen nicht alle Kriterien erfüllt sein, aber mindestens zwei von ihnen.

5.2.2.5 Eine Typologie der Risikofaktoren 5

Faktorengruppe 5: **Internet als Neuland**

NutzerInnen, die z.B.

- erst seit kurzem im Internet aktiv sind, weil sie z.B. noch sehr jung sind oder erst spät im Leben mit dem Internet in Berührung gekommen sind
- eine sehr niedrige Online-Aktivität aufweisen
- das Internet für ihren Beruf nicht benötigen
- nicht zwischen redaktionellen Inhalten und Werbung unterscheiden können
- auch in schlecht gemachte Fallen tappen (z.B. bei Fake-Shops)
- ohne Bedenken gefährliche Links anklicken

Sie sind von allen Cybercrime-Formen überdurchschnittlich hoch gefährdet, besonders aber von Fake-Shops, Social Hacking, Erpressung, Phishing und Ransomware.

Ein **höheres Risiko** tragen

- nach Alter: eher sehr junge und ältere Menschen

Es müssen nicht alle Kriterien erfüllt sein, aber mindestens zwei von ihnen.

5.2.3 Ergebnisse

Die befragten ExpertInnen stellten konsensual fest, dass sich Opfer von Cyberkriminalität mit soziodemografischen Merkmalen meist nicht (ausreichend) beschreiben lassen, denn jedeR könne Opfer werden. Ausnahmen stellen Erpressungen in erotischem Kontext dar, die überwiegend Männer betreffen (z.B. Sextortion), sowie vorgetäuschte Online-Liebesbeziehungen mit dem Ziel des Geldtransfers, die meistens Frauen betreffen (Love-Scamming). Cybermobbing trifft meist und Cybergrooming stets Kinder und Jugendliche. Unter den Opfern fast aller Deliktformen finden sich zudem laut ExpertInnen viele ältere Menschen, da deren digitale Kompetenz häufig mangelhaft ist.

Dass soziodemografische Merkmale allein keine ausreichende Erklärung für Viktimisierungsprognosen im Kontext Cyberkriminalität liefern, lässt sich beispielsweise anhand des sozialen Status einer Person illustrieren: Dieser spiele per se keine Rolle, sehr wohl jedoch für die Vulnerabilität potenzieller Opfer, denn je höher der soziale Status, desto eher greifen Erpressungsversuche. Auch spiele sozialer Status für den Verlauf der kriminellen Handlungen eine Rolle, denn je höher der soziale Status und damit auch das Vermögen, desto höher die Geldforderungen. Tendenziell treffe dies eher männliche Opfer, da sie im Allgemeinen mehr verdienen als Frauen und öfter von Erpressungen betroffen sind. Die Ergebnisse der repräsentativen Fragebogenerhebung (siehe folgendes Kapitel) bestätigen diesen Befund: Männer tragen in Folge von Cyberkriminalität höhere finanzielle Schäden davon. Für die Antizipation bzw. Prädiktion von Cybercrime-Viktimisierung spielen Merkmale wie Geschlecht, Alter oder ökonomische Ausstattung allein also keine Rolle. Vielmehr lassen sich, wie auch aus den oben erläuterten Faktorengruppen ersichtlich, Muster am ehesten betroffener Alters- und Geschlechtergruppen je nach konkretem Tatbestand ableiten.

So wie der eben erläuterte Befund spiegeln auch viele andere Erkenntnisse aus den ExpertInneninterviews die Ergebnisse der im nächsten Kapitel präsentierten repräsentativen Online-Befragung wider: Männer sind in stärkerem Ausmaß von Cyber-Kriminalität betroffen als Frauen, was aber auch auf deren höhere Online-Aktivität zurückzuführen ist. Cybermobbing und Cybergrooming betreffen eher jüngere bis mittlere Altersgruppen, Cyber-Betrug eher ältere Personen, die allgemein eine eher geringe digitale Kompetenz aufweisen.

5.3 Ergebnispräsentation Teil 3: Repräsentative Befragung

Eine vom Umfrageinstitut IFES durchgeführte österreichweite quantitative repräsentative Online-Befragung männlicher und weiblicher InternetnutzerInnen von 16 bis 65 Jahren (n=1000, max. Schwankungsbreite: ± 3,1 Prozentpunkte) diente vor allem zur Identifizierung gefahrengeneigter Aktivitäten bezogen auf relevante persönliche Merkmale (siehe Anhang 1) und Gefährdungstypen (siehe Ergebnispräsentation Teil 1). In Zusammenhang mit relevanten, aus einschlägigen Quellen extrahierten Merkmalen erfragt wurden zudem das allgemeine Internetnutzungsverhalten (genutzte Kanäle, Dauer, Intensität, Zweck), spezifische Vorerfahrungen als Cyberkriminalitätsopfer (siehe Abbildung 1), die Kenntnis relevanter Delikte bzw. Gefahren sowie die Sorge, Opfer unterschiedlicher Delikte zu werden. Abbildungen 1 – 4 zeigen die Zusammensetzung der repräsentativen Stichprobe nach Geschlecht, Alter, Bildung und Tätigkeit. Aufgrund des Gender-Bezugs des Projekts wurde vor allem auf ein quantitatives Gleichgewicht von Männern und Frauen geachtet.

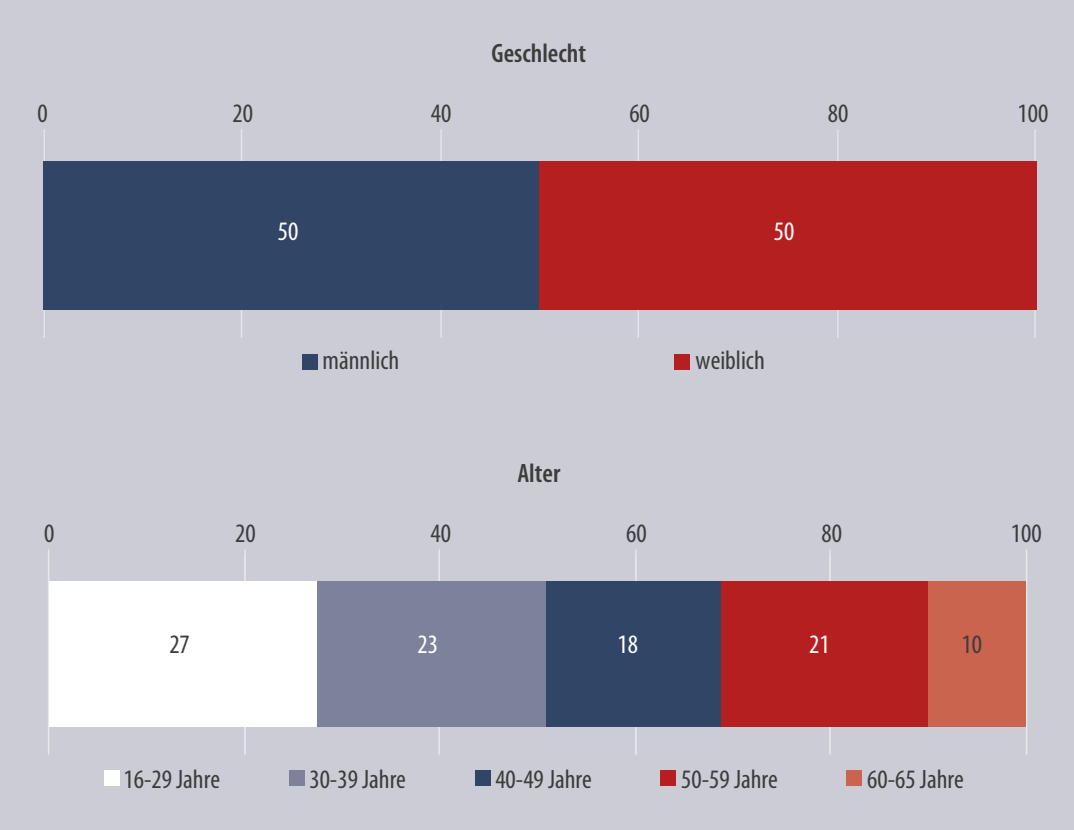

Abbildung 1: *Darstellung der Stichprobe nach Geschlecht und Alter in % (n=1000)*

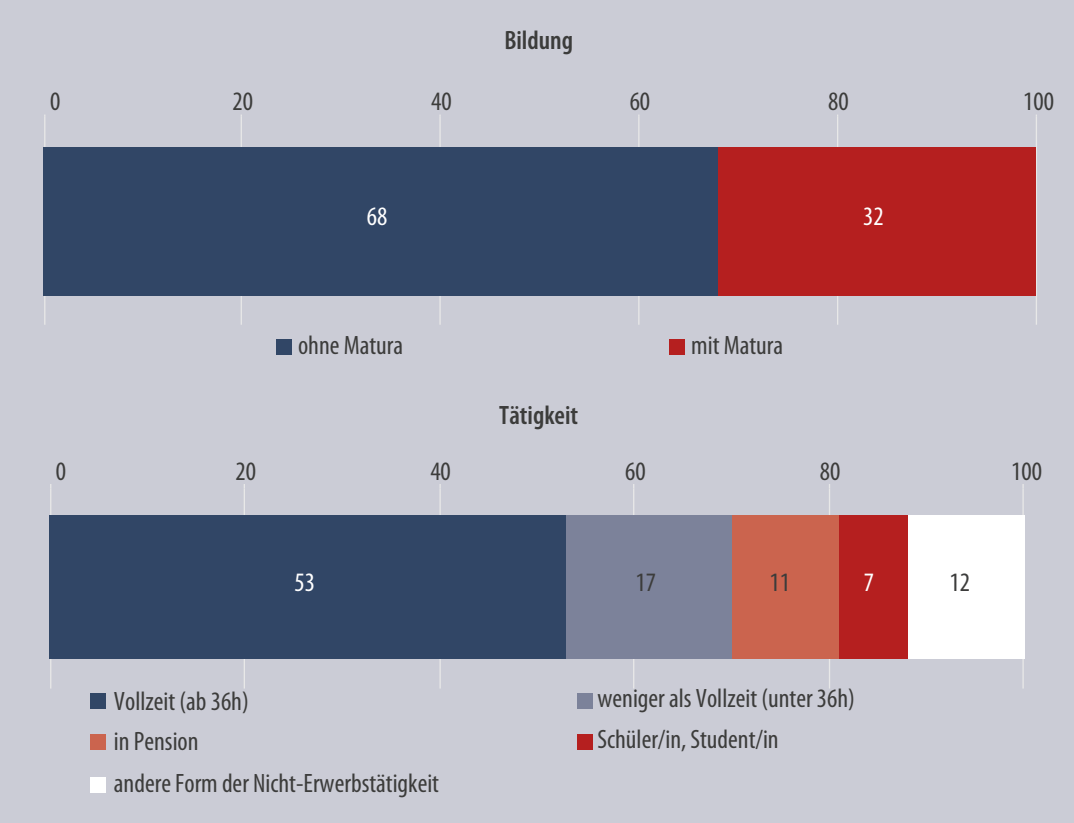

Abbildung 2: *Darstellung der Stichprobe nach Bildungsgrad und Tätigkeit in % (n=1000)*

5.3.1 Internetnutzung, Internetsicherheit und die Rolle digitaler Kompetenz

Durchschnittlich wird das Internet drei Stunden pro Tag privat genutzt. Abbildung 3 zeigt, dass mehr als ein Drittel der Befragten täglich mehr als drei Stunden online ist. Abbildung 4 zeigt, dass viele davon Jüngere (unter 30-Jährige) und Personen mit vergleichsweise niedrigem formalem Bildungsniveau sind. Das Geschlecht ist bzgl. der Internetnutzungsintensität kein Unterscheidungskriterium: Männer und Frauen nutzen das Internet weitgehend ähnlich viel.

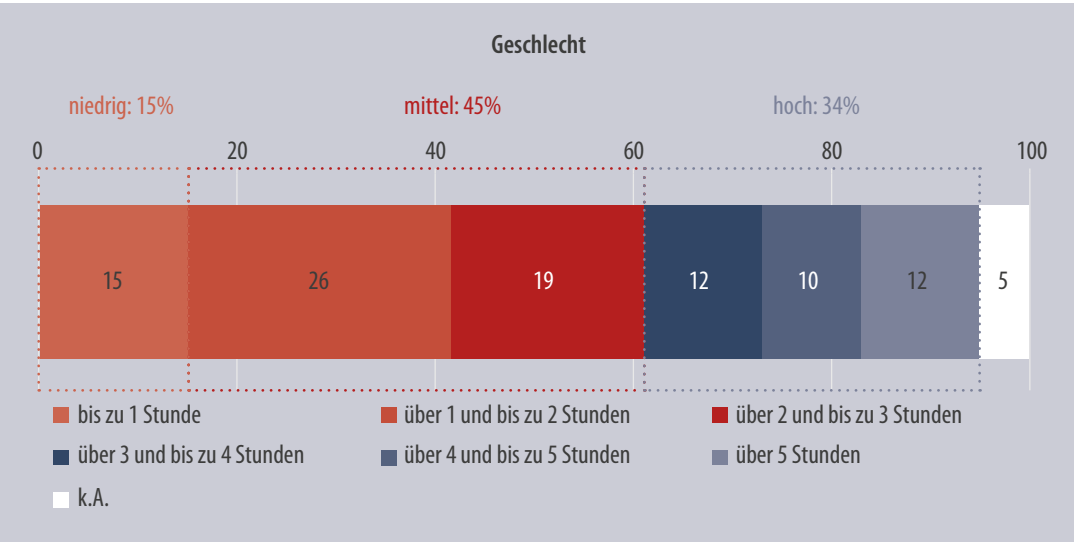

Abbildung 3: *Intensität der Internetnutzung pro Tag in % (n=1000)*

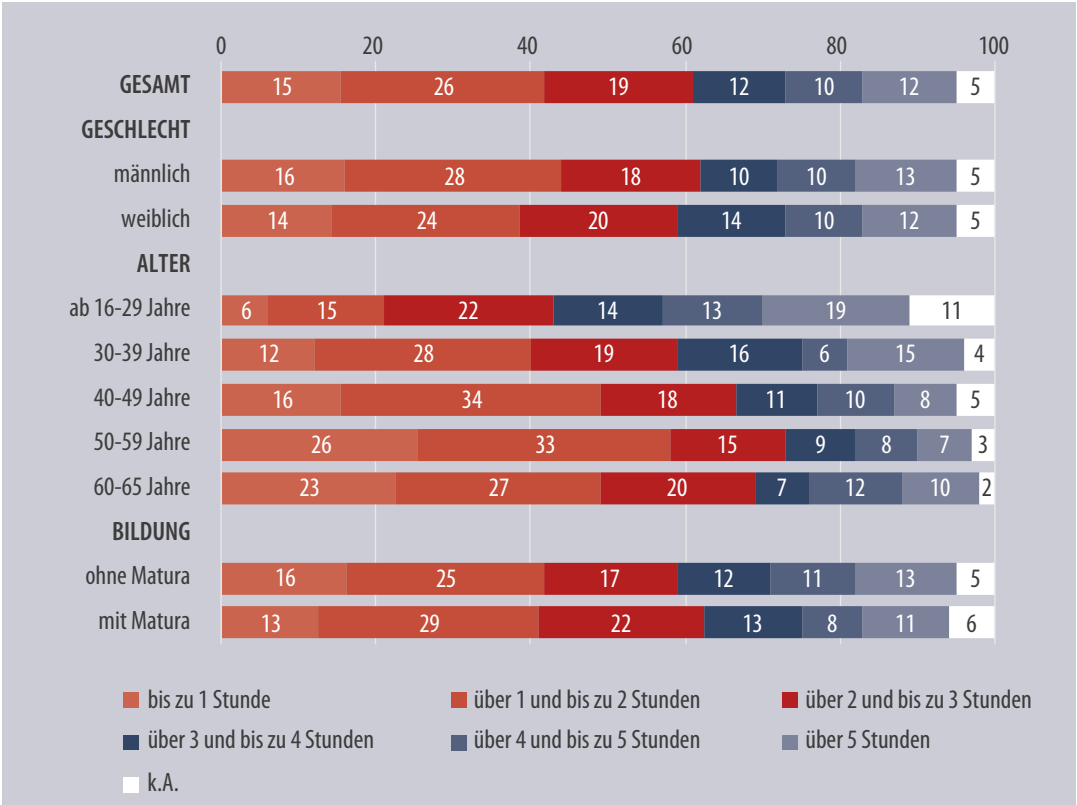

Abbildung 4: *Intensität der Internetnutzung pro Tag nach Alter, Geschlecht und Bildung in % (n=1000)*

Im Rahmen der Internetnutzung nimmt Instant Messaging quantitativ einen besonders hohen Stellenwert ein – sieben von zehn Personen nutzen entsprechende Dienste (fast) täglich. Informationssuche (59%), das Verfassen und Empfangen von E-Mails (57%) und Social-Media-Plattformen (54%) spielen ebenfalls eine große Rolle. Messaging-Dienste und soziale Medien werden vor allem von den unter 30-Jährigen und von Frauen oft genutzt. Jüngere Befragte nutzen zudem überdurchschnittlich oft täglich das Internet, um Videos oder Musik zu streamen bzw. herunterzuladen.

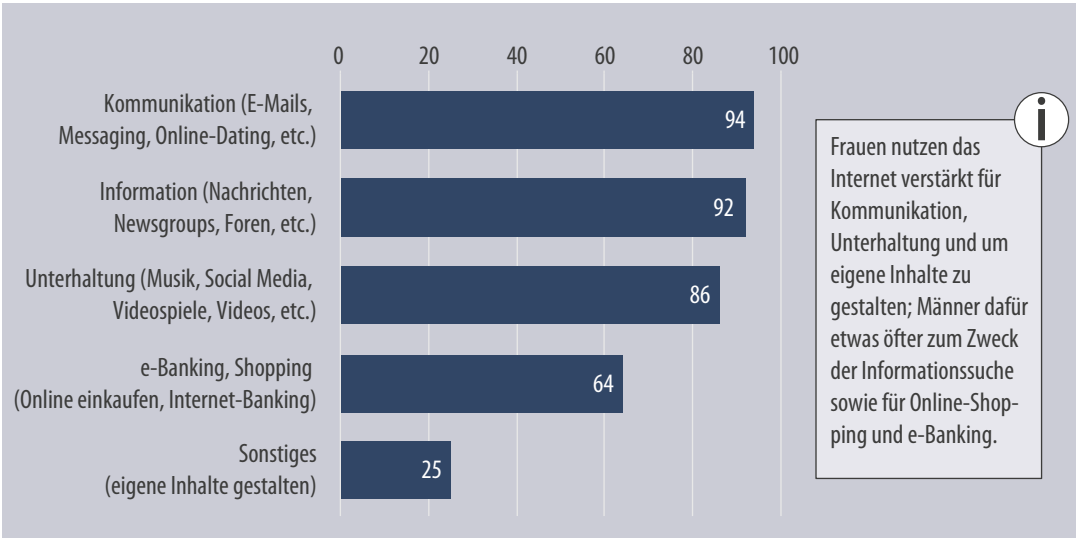

Abbildung 5: *Internet-Nutzungsmotive in % (n=1000)*

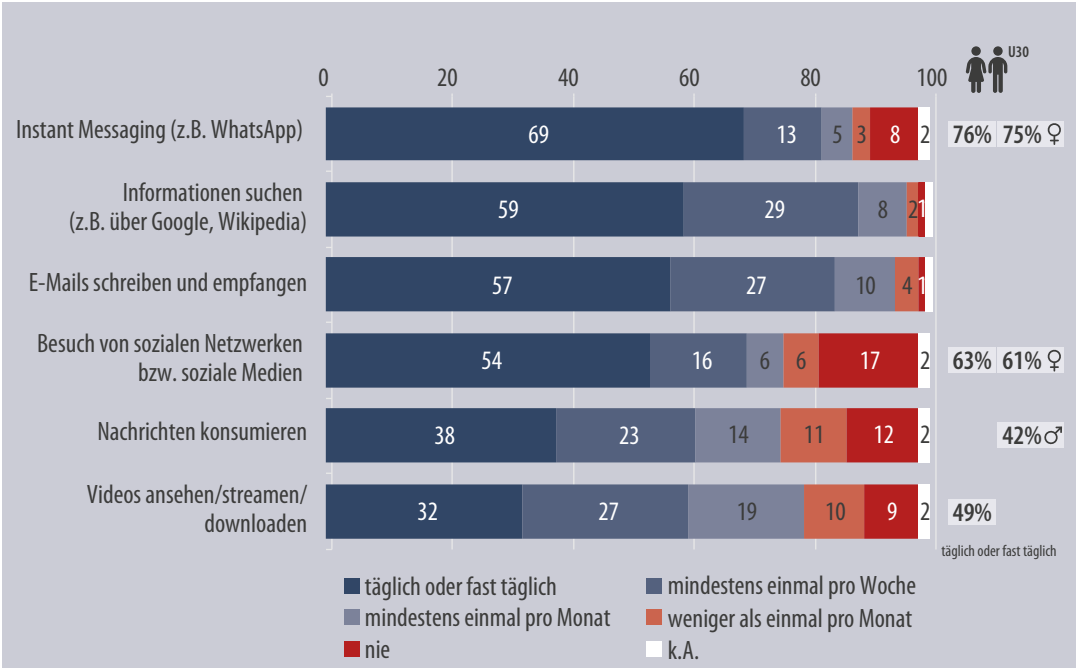

Abbildung 6: *Nutzungshäufigkeit von Internet-Angeboten in % (n=1000)*

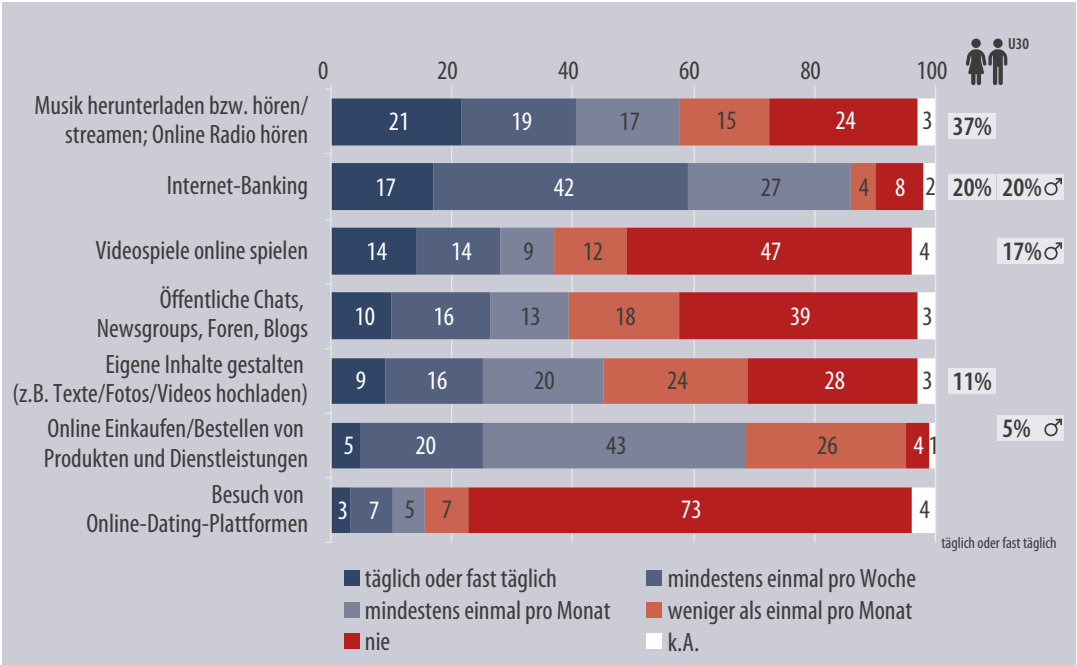

Abbildung 7: *Häufigkeit unterschiedlicher Nutzungsaktivitäten in % (n=1000)*

Mehr als 50 Prozent der Befragten geben an, sich gerne mit neuen Technologien zu beschäftigen bzw. keine Probleme damit zu haben, Software selbst zu installieren. Hier besteht jedoch ein auffälliger Unterschied zwischen Männern und Frauen, der darauf hinweist, dass digitale Kompetenz – geht es um den technischen Umgang mit dem Internet bzw. Internetsicherheit sowie technologisches Interesse – männlich besetzt ist. Auch Personen mit höherem formalem Bildungsniveau weisen eine signifikant höhere digitale Kompetenz auf. Einen weniger starken Unterschied gibt es zwischen jüngeren und älteren Befragten.

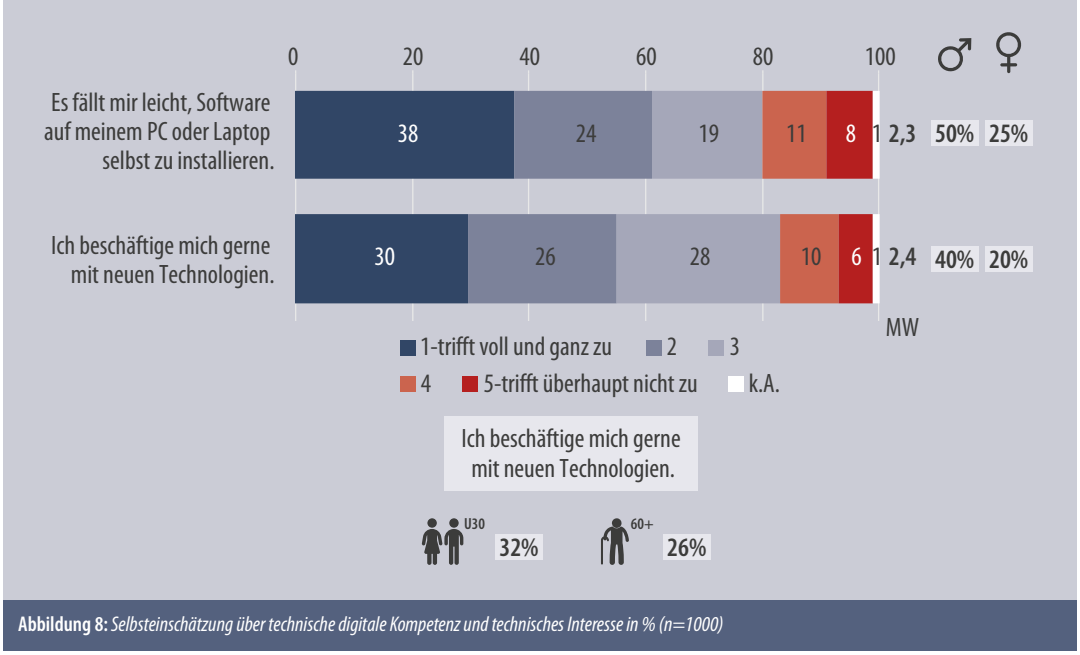

Abbildung 8: *Selbsteinschätzung über technische digitale Kompetenz und technisches Interesse in % (n=1000)*

Während Männer sich als technisch kompetenter einschätzen, weisen Frauen bei inhaltlicher digitaler Kompetenz ein selbstsichereres Antwortverhalten auf: Frauen geben weit weniger häufig als Männer an, dass es ihnen schwerfällt, vertrauenswürdige Informationen im Internet selbst zu finden, und sie befürchten weniger, im Umgang mit ihren internetfähigen Geräten etwas falsch zu machen.

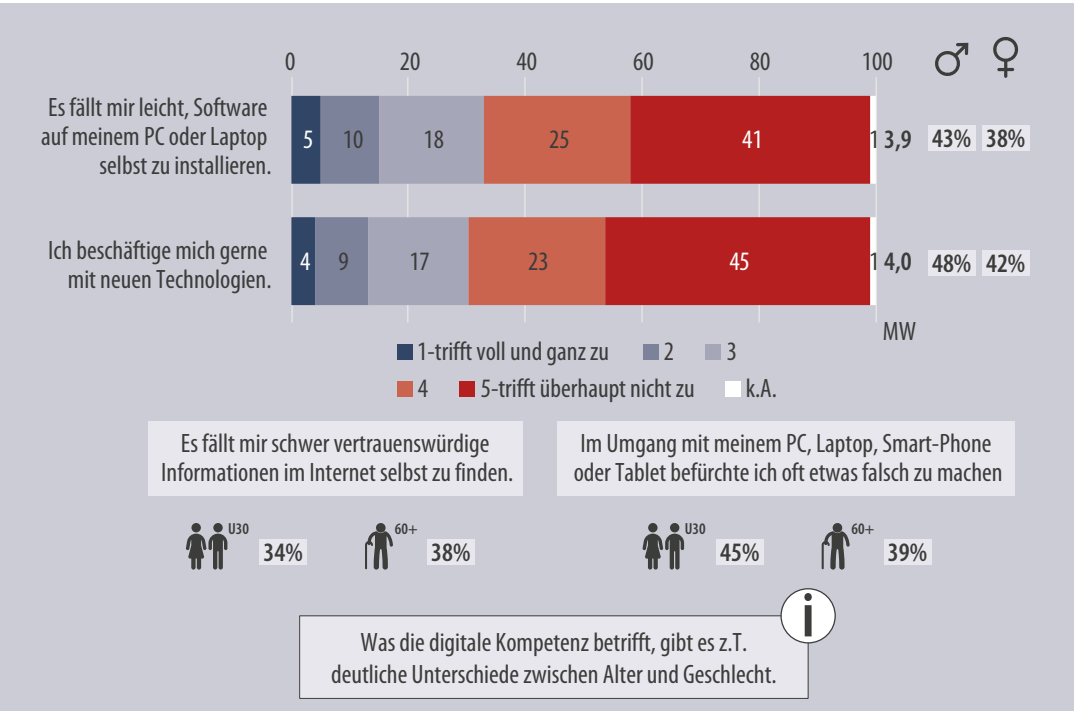

Abbildung 9: *Selbsteinschätzung über inhaltliche digitale Kompetenz und Selbstsicherheit in % (n=1000)*

Wenig überraschend fühlen sich Menschen mit geringer digitaler Kompetenz nicht nur deutlich schlechter über die Risiken von Cyberkriminalität informiert, sondern zeigen auch vermehrt unvorsichtiges Verhalten im Internet hinsichtlich des Ergreifens konkreter Sicherheitsmaßnahmen. Auch Befragte unter 30 Jahren setzen diese weniger häufig.

Sicherheitsbedenken gibt es vor allem hinsichtlich Hacking von Bank- oder Kreditkartendaten (große Sorgen machen sich 30% der Befragten), der weltweiten Weitergabe von elektronisch erfassten persönlichen Daten, des Missbrauchs von persönlichen Einträgen im Internet, des Zugriffs fremder Personen auf den eigenen Computer und der Auswertung von Nutzerdaten im Web (jeweils rund 25% der Befragten machen sich in diesen Hinsichten große Sorgen). Jüngere Menschen und Personen, die selbst noch nicht Opfer von Internetkriminalität geworden sind, haben allgemein weniger starke Sicherheitsbedenken, was sich auf das Ergreifen konkreter Sicherheitsmaßnahmen auswirkt.

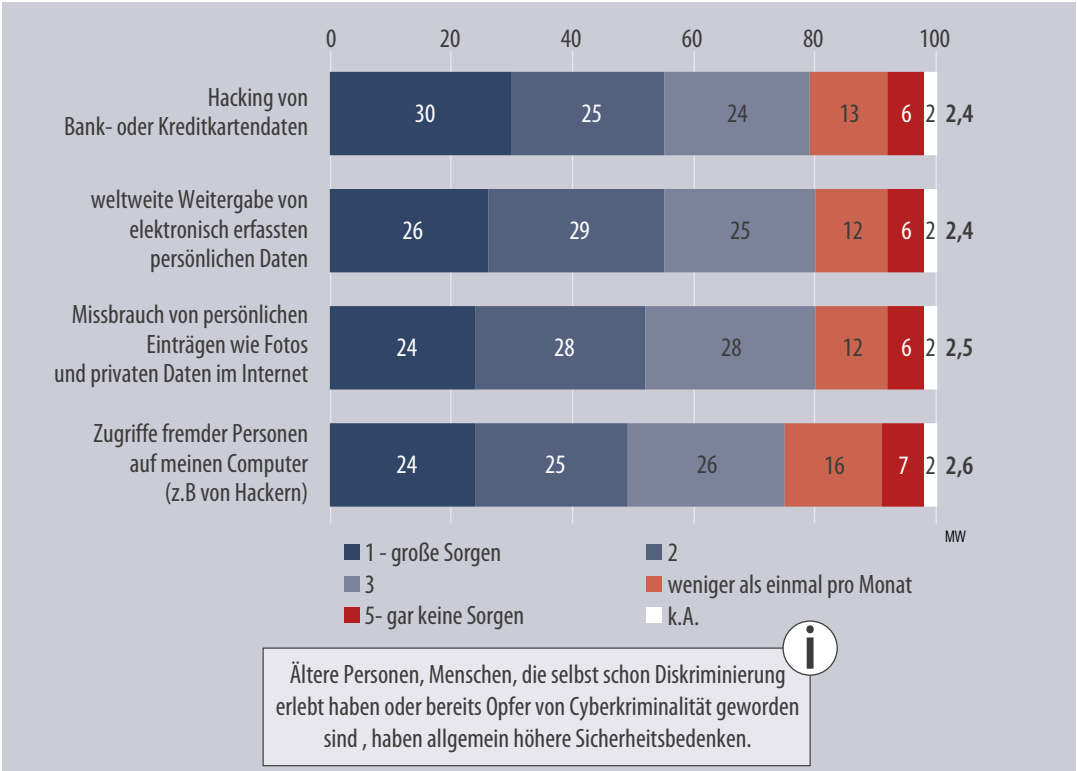

Abbildung 10: *Sicherheitsbedenken im Rahmen der Internetnutzung in % (n=1000)*

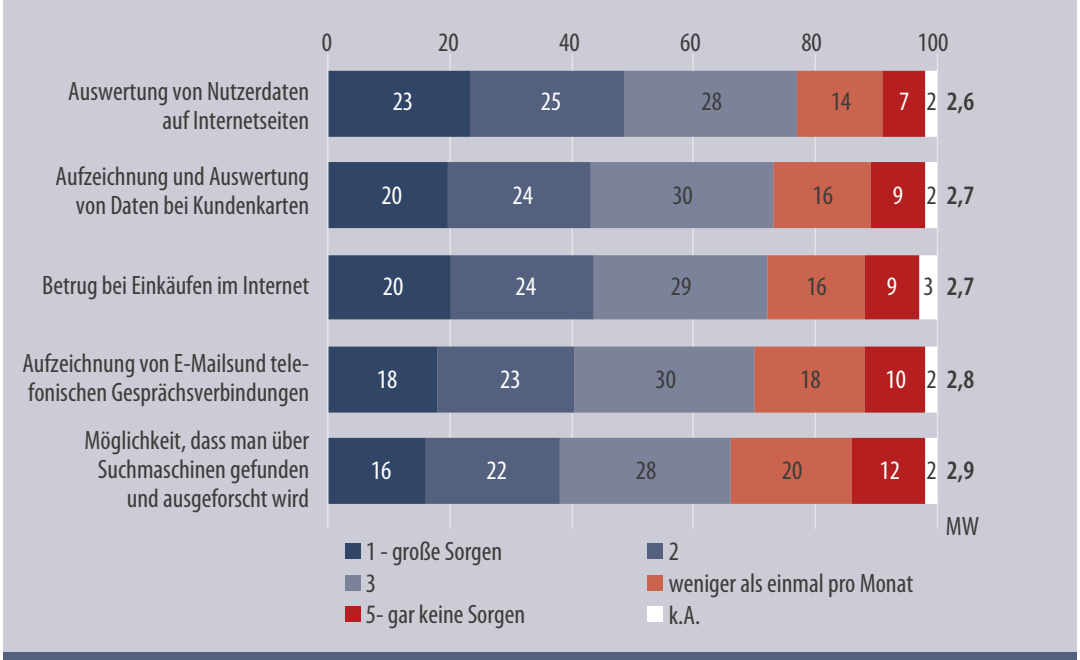

Abbildung 11: *Sicherheitsbedenken im Rahmen der Internetnutzung in % (n=1000)*

5.3.2 Präventionsmaßnahmen und praktische Empfehlungen für UserInnen

Im Zuge der Interviews wurden sowohl praktisch anwendbare Tipps für einzelne UserInnen, aber auch mögliche Präventionsmaßnahmen aufgrund bereits bestehender Ansätze und Strategien auf institutioneller und gesellschaftlicher Ebene thematisiert.

5.3.2.1 Präventionsmaßnahmen

Folgende mögliche Präventionsmaßnahmen wurden von den ExpertInnen ins Treffen geführt:

- (Schnellere) Anpassung von Gesetzen: Cyberkriminalitätsphänomene entwickeln sich in hohem Tempo weiter.
- Ausbau der bereits guten Kooperation und Vernetzung von Ermittlungsbehörden, Opferschutzeinrichtungen und Beratungsstellen
- Die verstärkte Bekanntmachung bereits vorhandener Angebote und Informationsquellen, wie etwa der Watchlist Internet (https://www.watchlist-internet.at), die aufgrund von Meldungen von Online-KonsumentInnen Warnmeldungen publiziert, des österreichischen E-Commerce-Gütezeichens und des European Trust Mark auf EU-Ebene (sowie die damit verbundene Propagierung von Einkäufen in zertifizierten Online-Shops). Online-Shops sind auch unter https://www.guetezeichen.at zu überprüfen, sollten Zweifel an der Echtheit des E-Commerce-Gütezeichens in einem Online-Shop bestehen.
- Erweiterung des Angebots an Vorträgen, Schulungen und Informationsveranstaltungen, insbesondere für Erwachsene 40+, die durch solche noch zu wenig erreicht werden
- Präsenz in und Kooperation mit Massenmedien: Durch eine breite mediale Streuung des Themas sind nach Ansicht der befragten ExpertInnen auch Erwachsene 40+ am besten erreichbar.
- Verbreitung von Warnungen via Smartphone und Social Media zur Erreichung der jüngeren Zielgruppe.

5.3.2.2 Praktische Empfehlungen

Folgende für einzelne UserInnen praktisch umsetzbare Empfehlungen konnten aus den Interviews zusammengetragen werden:

Immer und überall

- Erst denken, dann klicken!
- Verdächtige E-Mail-Adressen und URLs von Webseiten googeln. Meist finden sich Hinweise, ob sie bereits in betrügerischer Absicht verwendet wurden (z.B. auf der Watchlist Internet unter https://www.watchlist-internet.at).
- Internetfähige Endgeräte (Computer, Tablets, Smartphones) durch starke Passwörter schützen.
- Virenschutzprogramme und/oder Firewalls installieren.
- Regelmäßig Sicherheitskopien anfertigen.

Fürs Lesen von E-Mails

- E-Mails von unbekannten AbsenderInnen nicht öffnen. Links, Attachments und Fotos in derartigen E-Mails auf keinen Fall anklicken.
- Banken, Versicherungen und ähnliche Institutionen schicken niemals E-Mails, die dazu auffordern, die Zugangsdaten zu den Konten oder Kreditkarten einzutragen. Alle derartigen E-Mails sind Fälschungen, die in Betrugsabsicht verschickt werden.

Bei Computerproblemen

- Nur persönlich bekannten Personen und Firmen einen Fernzugang zu Computern oder Smartphones gewähren. Auf AnruferInnen, die angeben, im Namen von Microsoft oder Apple anzurufen, und technischen Support anbieten, niemals eingehen, sondern SpezialistInnen vor Ort um Rat fragen.

Fürs Shoppen

- Wenn Waren, Ferienunterkünfte oder Dienstleistungen über Internet-Plattformen angeboten werden, die den KonsumentInnen Schutz gewähren (z.B. Amazon Marketplace, Airbnb, Willhaben), stets im System dieser Plattformen bleiben – bei Kommunikation und Bezahlung.
- Bei zu günstigen Preisen für Markenprodukte misstrauisch werden.
- Beim Online-Einkauf stets die URL des Shops im Auge behalten und darauf überprüfen, ob sie zum Shop passt und welche TLD (Top Level Domain: letzter Abschnitt, rechts vom Punkt wie z.B. .com) sie hat. Russische und chinesische Seiten zum Beispiel besonders überprüfen.
- Auf Gütezeichen (European Trust Mark, E-Commerce-Gütezeichen) achten und Online-Shops gegebenenfalls überprüfen (https://www.guetezeichen.at).
- Das Impressum der Online-Shops genau durchlesen.

Fürs Zahlen

- Bei Zahlungen mit Kreditkarte stets überprüfen, ob das Design der Seite, auf die man weitergeleitet wird, vertraut ist, und ob die URL passt.
- Möglichst über PayPal zahlen. Wo kein PayPal angeboten wird, ist Misstrauen angesagt.
- Keine Zahlungen via Western Union durchführen und größte Vorsicht bei Zahlungen mit Bitcoins.

Für Online-Beziehungen

- Entfernte Verwandte und Bekannte, die sich per E-Mail an einen wenden, immer persönlich treffen, bevor man Geld überweist – und im Gespräch überprüfen, ob es sich tatsächlich um diese Personen handelt.
- Auch beim nettesten Online-Flirt oder der intensivsten Online-Liebesbeziehung ist die Bitte um Geld ein untrügliches Zeichen für einen Betrug.
- Bei Beziehungen mit persönlichem Charakter zuerst einen Face-to-Face-Kontakt herstellen – und erst dann vertrauliche bzw. intime Daten und Bilder austauschen.
- Wenn intimes Bildmaterial verschickt wird, möglichst darauf achten, dass das Gesicht verdeckt oder nicht auf dem Foto ist, sodass man nicht individuell erkennbar wird.

Und wenn doch einmal etwas schief gegangen ist, …

- zum Beispiel bei Erpressungen, keinesfalls zahlen, sondern Anzeige erstatten und/oder Unterstützungseinrichtungen wie den Internetombudsmann kontaktieren.
- Evtl. Screenshots von verdächtigen Chat-Konversationen anfertigen bzw. Sicherung von E-Mail-Konversationen.

5.3.3 Konkrete Sicherheitsmaßnahmen und Gefahren

Im Allgemeinen werden viele Sicherheitsmaßnahmen bereits breit umgesetzt: Ein Großteil der Befragten gibt an, regelmäßige Software-Updates durchzuführen, einen Malware-/Virenscanner bzw. eine Firewall installiert zu haben, die Seriosität von Webseiten und Online-Shops zu überprüfen, keine E-Mails zu öffnen, wenn der Absender unbekannt ist und für verschiedene Webseiten unterschiedliche Passwörter zu benutzen, wobei Passwörter oftmals nicht regelmäßig geändert werden.

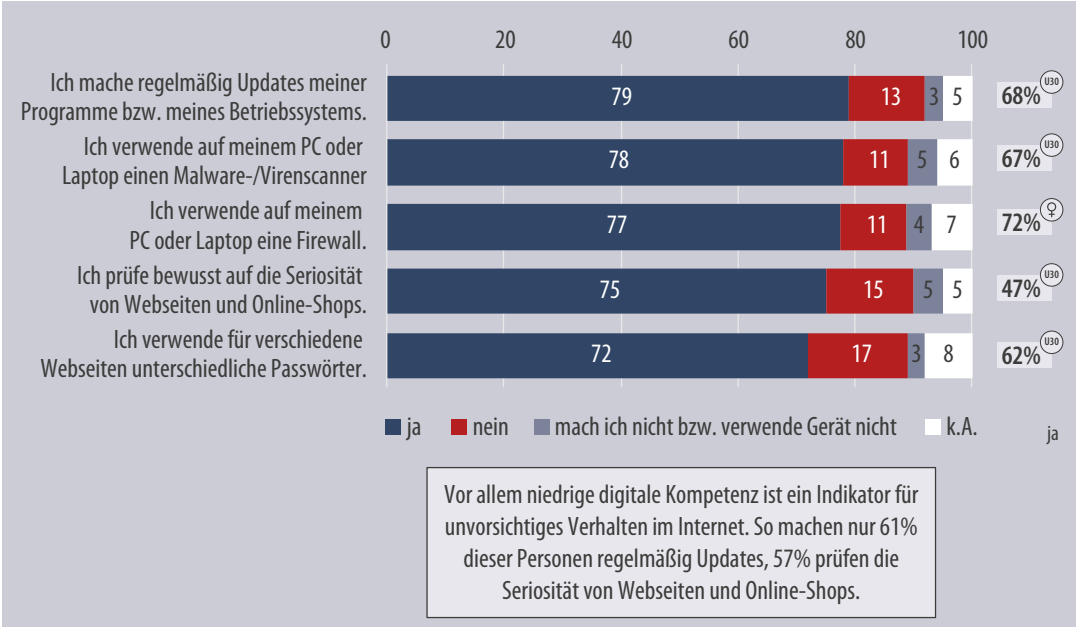

Abbildung 12: *Umsetzung von Sicherheitsmaßnahmen in % (n=1000)*

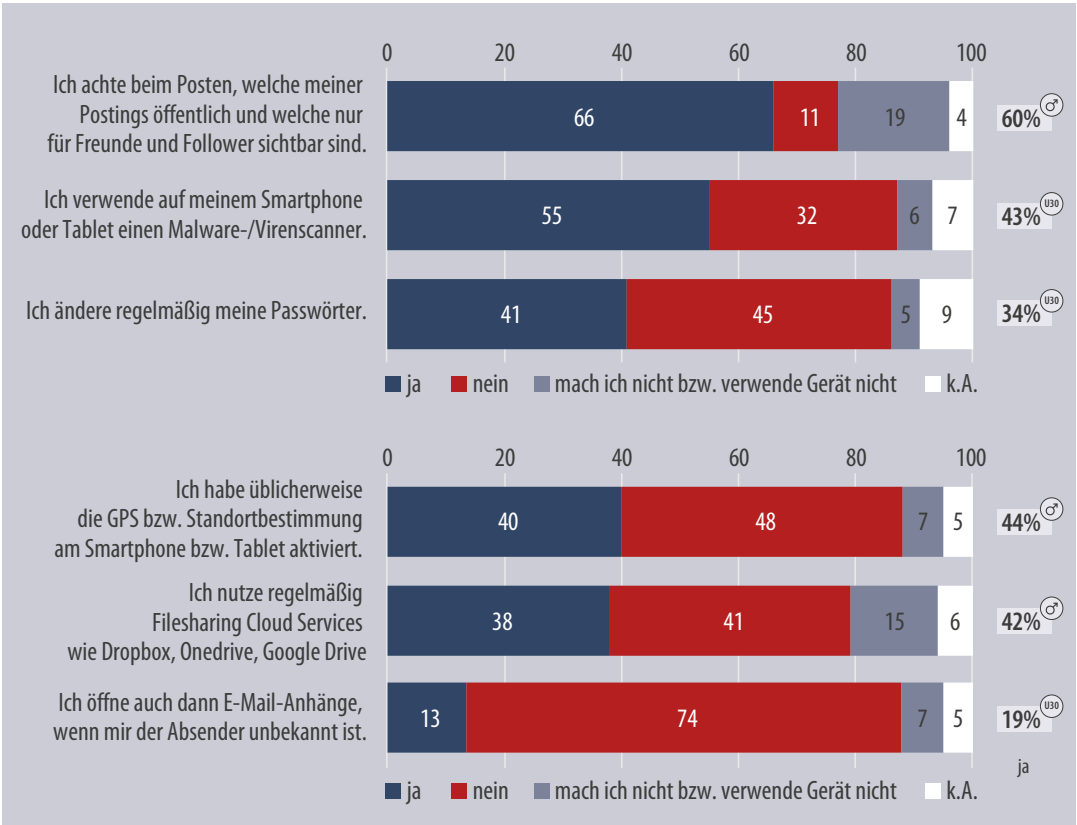

Abbildung 13: *Umsetzung von Sicherheitsmaßnahmen in % (n=1000)*

5.3.4 Fragwürdige/illegale Inhalte im Netz

Dass Frauen eher als Männer beim Posten darauf achten, welche ihrer Postings für wen bzw. öffentlich oder privat sichtbar sind, steht im Einklang mit deren höherer „inhaltlicher" digitaler Kompetenz, wenn es also um einen umsichtigeren Umgang mit Internetinhalten geht.

Mehr als die Hälfte der Befragten (57%) ist im Internet bereits mit fragwürdigen oder illegalen Inhalten in Berührung gekommen, vorwiegend mit Pornografie (32%, Männer: 39%), Nacktheit (30%, Männer 35%), Videos, auf denen eine Schlägerei zu sehen ist (28%) oder fremdenfeindlichen Inhalten (25%). Häufigste Gegenmaßnahmen waren das Blocken von Inhalten, „Unfollowen" von Accounts, das Vermeiden entsprechender Websites und das Melden beim Betreiber.

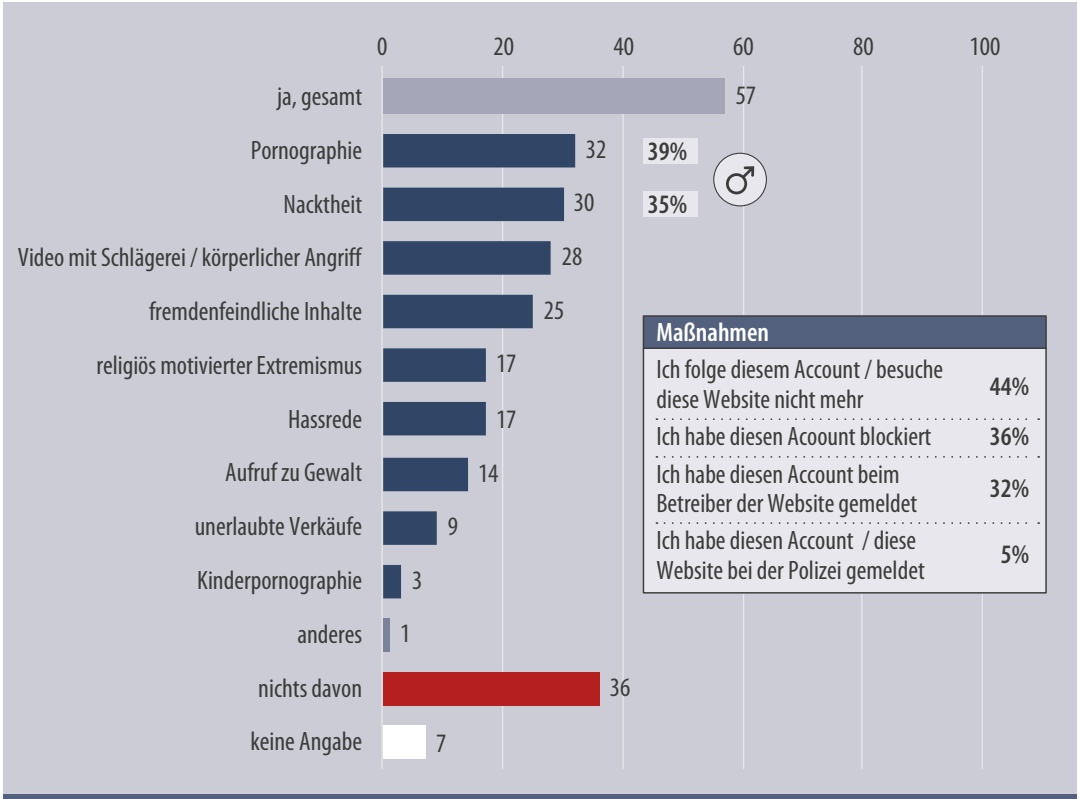

Abbildung 14: *Konfrontation und Umgang mit fragwürdigen/illegalen Inhalten im Internet in % (n=1000)*

5.3.5 Viktimisierung insgesamt

Die häufigste Art erlebter Cyberkriminalität bezieht sich auf Viren, Trojaner oder Malware (39% der Befragten waren in der Vergangenheit betroffen). Etwa 20% bis 25% der Befragten haben andere Formen von Cybercrime erlebt, beispielsweise Versuche, an Zugangsdaten zu gelangen oder zu Geldzahlungen zu bewegen, entweder, indem Erbschaften, Lotteriegewinne und Ähnliches versprochen wurden oder aber, indem Waren und Dienstleistungen bezahlt, aber nicht geliefert wurden.

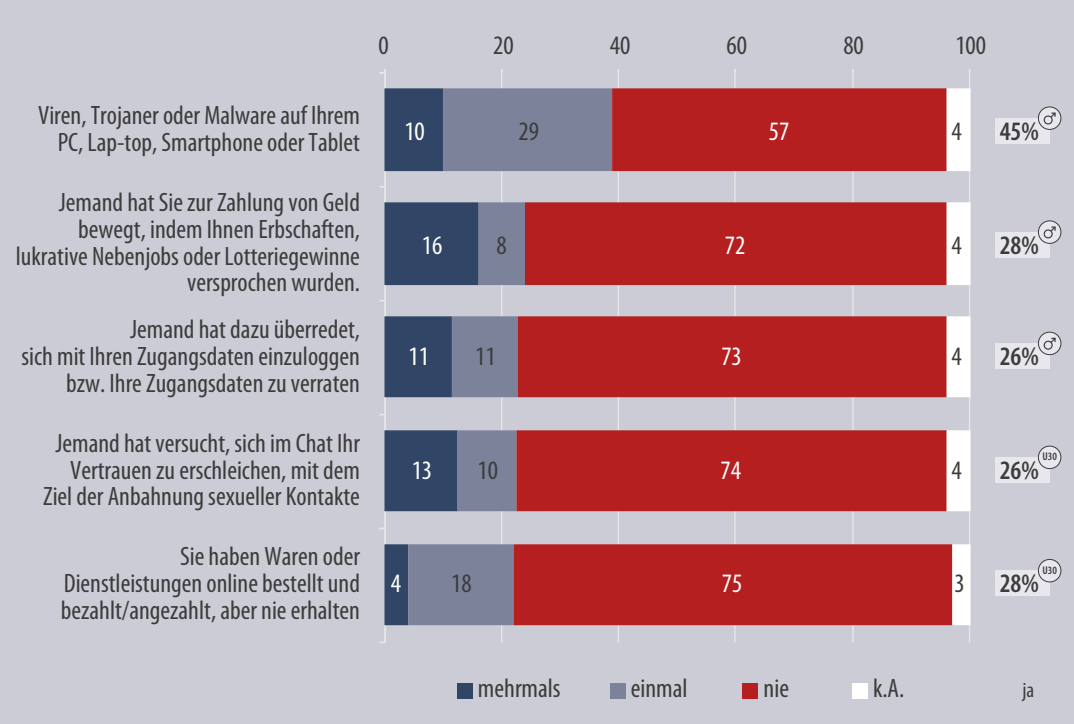

Abbildung 15: *Eigene Betroffenheit von Cyberkriminalität in % (n=1000)*

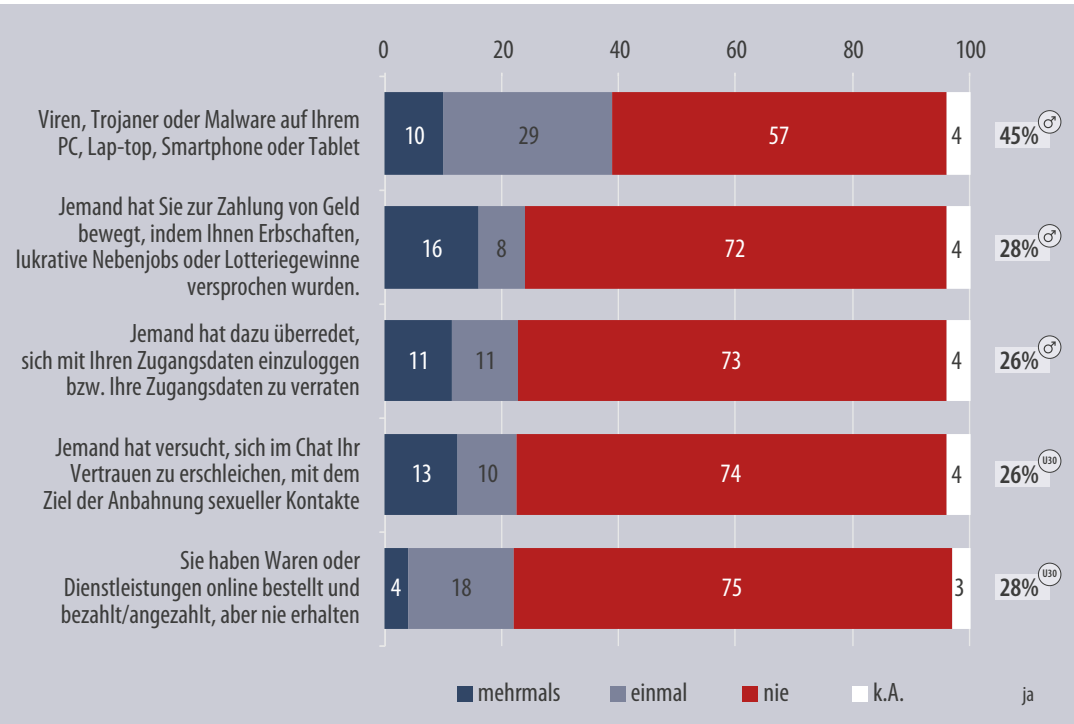

Abbildung 16: *Eigene Betroffenheit von Cyberkriminalität in % (n=1000)*

Abbildung 16: *Eigene Betroffenheit von Cyberkriminalität in % (n=1000)*

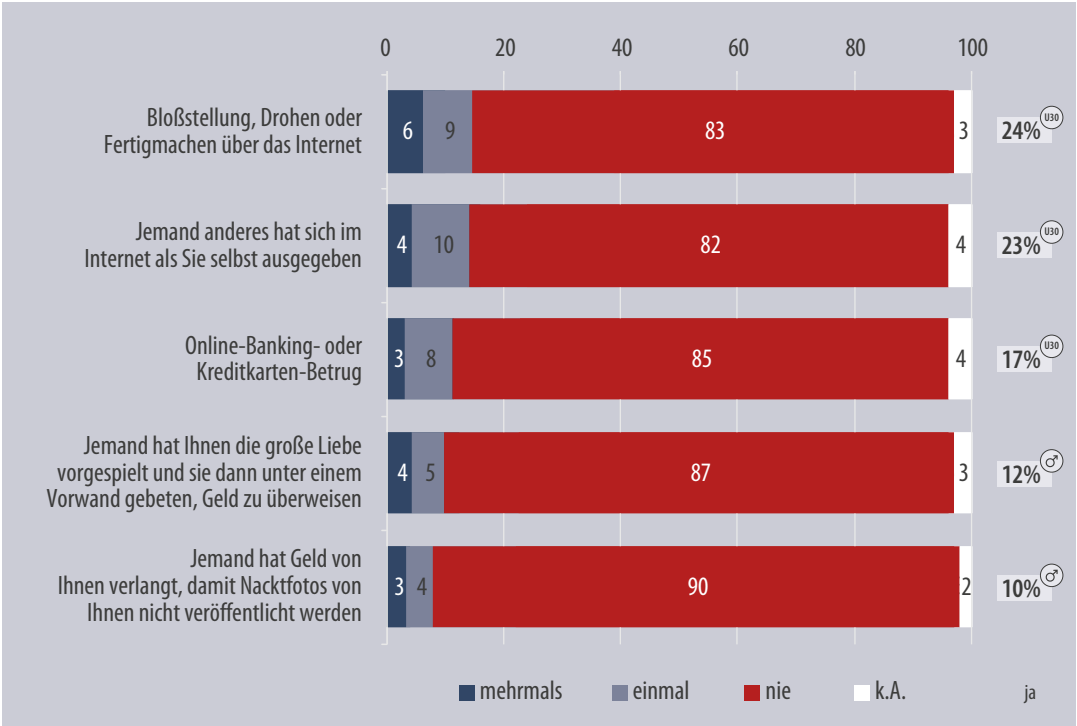

Abbildung 17: *Eigene Betroffenheit von Cyberkriminalität in % (n=1000)*

„Computer-based"-Cybercrimes (Angriffe auf Computersysteme) kommen im Allgemeinen öfter vor (63%) als „person-based"-Cybercrimes (kein Angriff auf Computersysteme, Angriff auf Personen) (54%). Wie im vorigen Kapitel bereits angedeutet, lässt sich anhand der vorliegenden Daten nicht bestätigen, dass Geschlecht und sozialer Status direkten Einfluss auf die Wahrscheinlichkeit haben, Opfer von „person-based"-Cybercrimes zu werden.

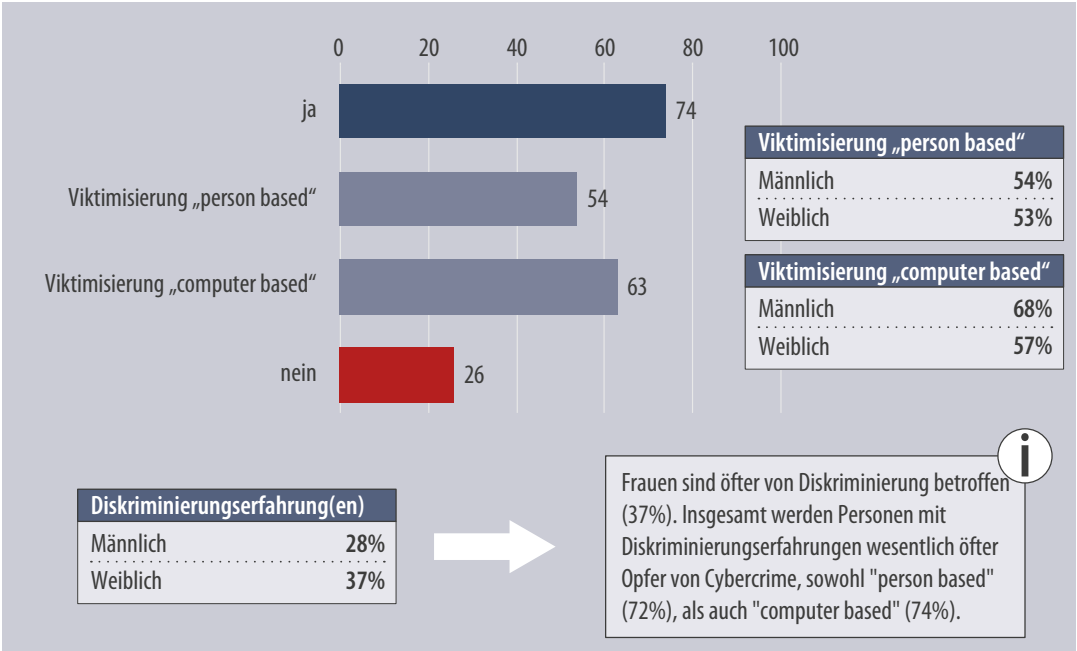

Abbildung 18: *Betroffenheit von „computer-based" und „person-based" Cybercrimes in % (n=1000)*

5.3.6 Folgen von Cyberkriminalität

Insgesamt wurden rund drei Viertel der Befragten (74%) bereits einmal Opfer von Cyberkriminalität, wobei damit nicht zwangsläufig finanzielle, rechtliche oder emotionale bzw. psychische Folgen verbunden waren. Junge Menschen, intensive Online-NutzerInnen und impulsive Menschen (jeweils rund 8 von 10) sind vergleichsweise häufiger davon betroffen, ebenso wie Personen mit Diskriminierungserfahrungen (84%), wobei Frauen allgemein stärker von Diskriminierung betroffen sind als Männer (56% vs. 44%).

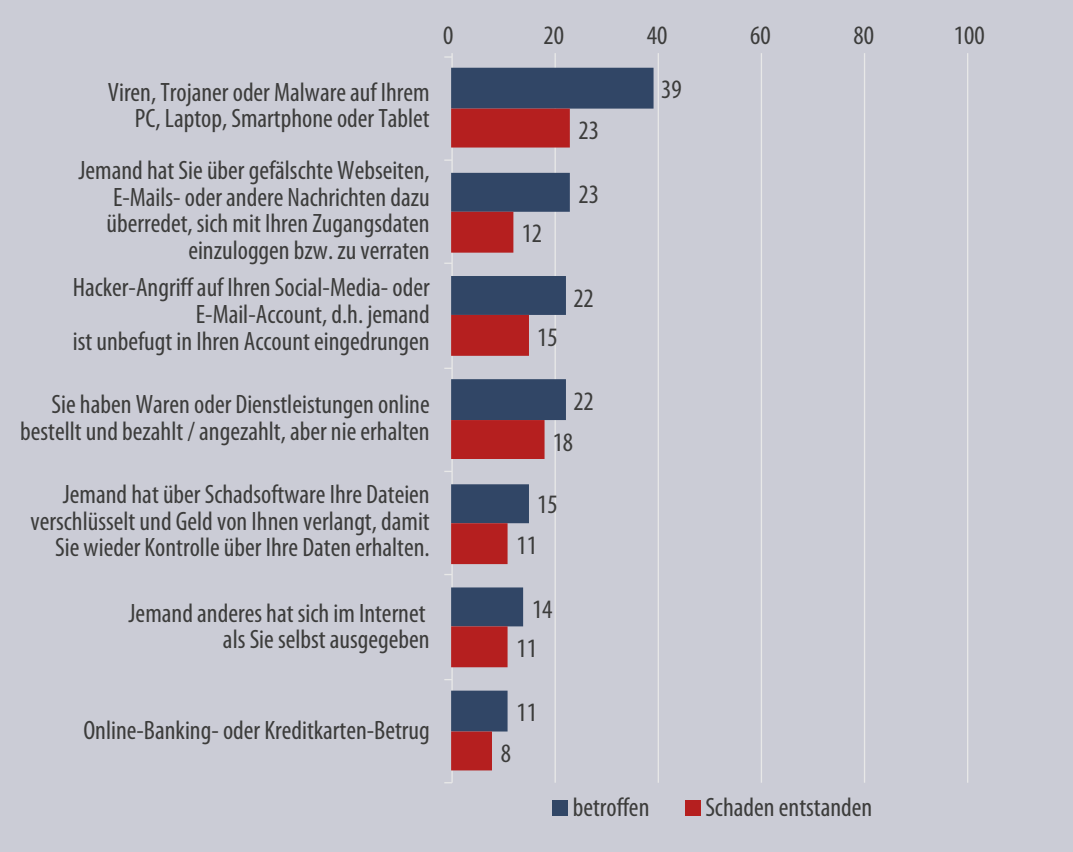

Abbildung 19: *Betroffenheit und Schäden durch Cybercrime in % (n=1000)*

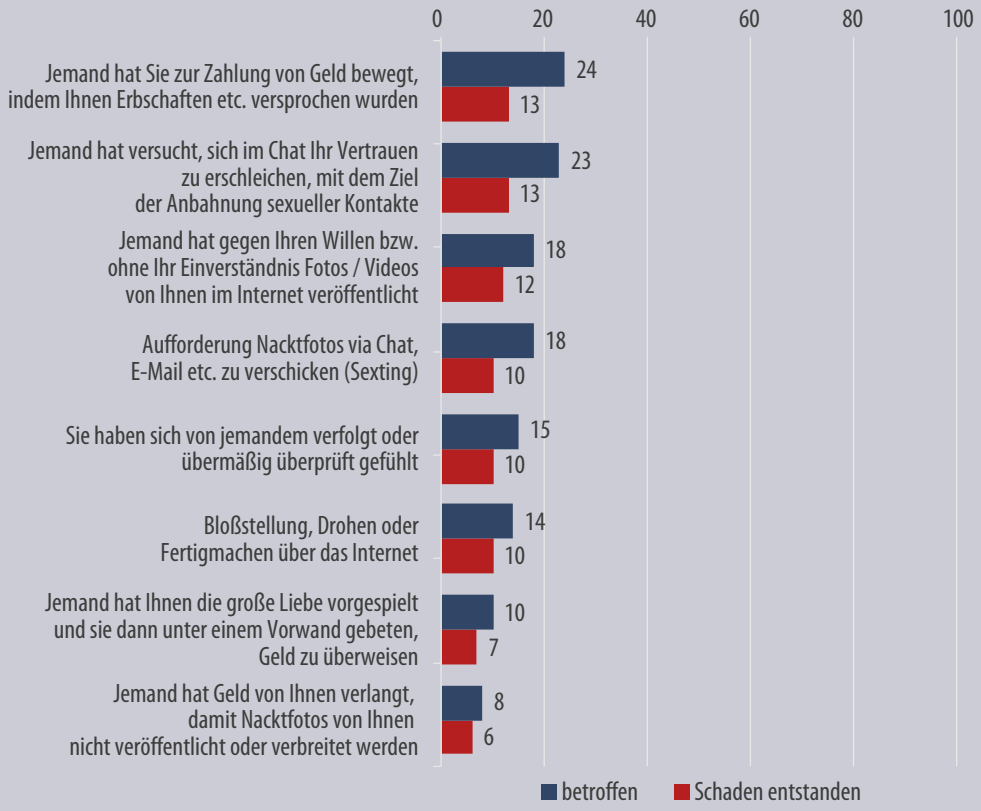

Abbildung 20: *Betroffenheit und Schäden durch Cybercrime in % (n=1000)*

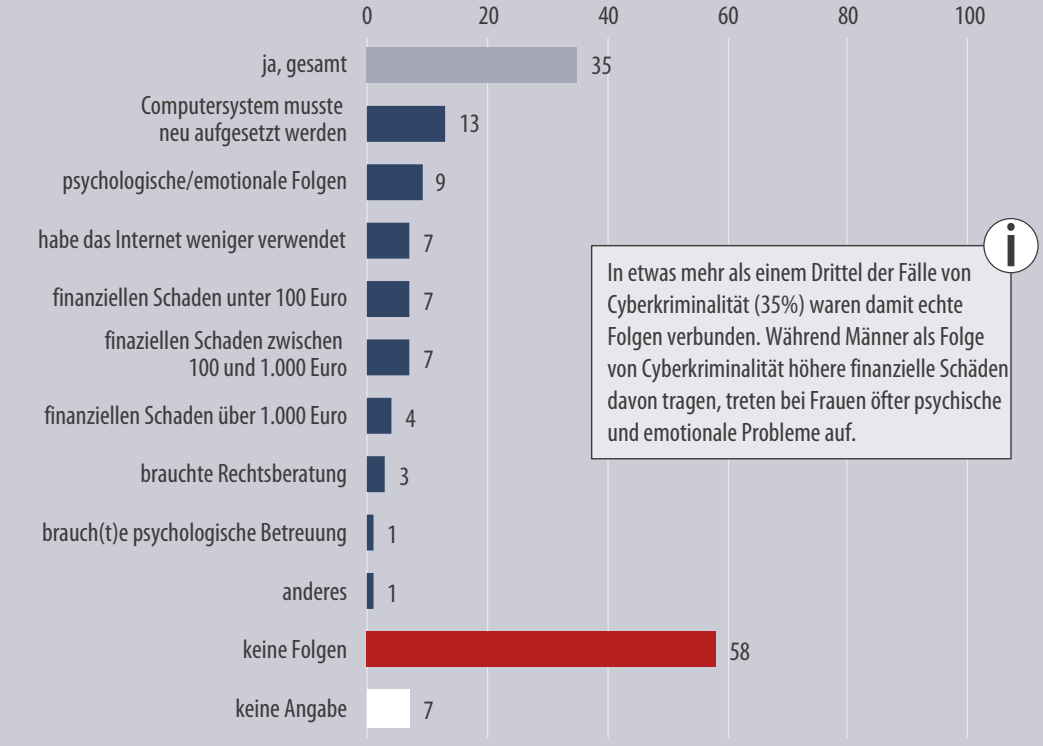

Abbildung 21: *Folgen von Cyberkriminalität (Basis: in den letzten 3 Jahren von Cyberkriminalität betroffen, n=739)*

5.4 Resümee

Die vorliegende Studie hat gezeigt, dass eine Opfer-Typologisierung von Cyberkriminalität mit soziodemografischen Merkmalen wie Geschlecht, Alter oder sozialem Status über Idealtypen, die sich empirisch überschneiden bzw. zu denen Personen nicht eindeutig zuordenbar sind, nicht hinausgehen kann. Die Identifizierung dieser Idealtypen anhand nur eines soziodemografischen Merkmals, wie etwa des Geschlechts bzw. Gender, ist – aus Intersektionalitätsperspektive erwartungsgemäß – unmöglich. Zu komplex sind Menschen, untrennbar und komplex verwoben sind Identitätskategorien wie Gender, Alter, Status, Herkunft oder sexuelle Orientierung.

Sowohl die qualitative ExpertInnenbefragung als auch die österreichrepräsentative Bevölkerungsumfrage haben ergeben, dass soziodemografische Merkmale prognostisch bzw. zur Antizipation von Cybercrime-Viktimisierung nicht herangezogen werden können, wiewohl unterschiedliche nach Alter und Geschlecht definierte Personengruppen eher von konkreten Tatbeständen betroffen sind. Ein solides Erklärungsfundament zur Prognose möglicher Viktimisierung bietet vielmehr beispielsweise das Merkmal der digitalen (inhaltlichen oder technischen) Kompetenz, die jeweils nach Geschlecht, aber auch Alter und Bildung unterschiedlich ausgeprägt sein kann.

Eine Ausnahme bilden hier das betrügerische sogenannte „Love-Scamming“ sowie die erpresserische „Sextortion“, dem bzw. der eindeutig entweder Frauen (Love-Scamming) oder Männer (Sextortion) zum Opfer fallen. Diese Phänomene sollten aus Genderperspektive näher unter die Lupe genommen werden.

Einer näheren Betrachtung muss auch das große Dunkelfeld im Cybercrime-Bereich unterzogen werden, das laut ExpertInneneinschätzung so groß ist, weil TäterInnen – oftmals in Form organisierter Banden – schwer auszuforschen sind, aber auch, weil Opfer entweder zu große Scham empfinden, um Anzeige zu erstatten oder Hilfe etwa von Beratungsstellen in Anspruch zu nehmen (vermutlich vor allem bei „person-based“ Cybercrimes) oder sich selbst nicht als Opfer wahrnehmen (vermutlich vor allem bei „computer-based“ Cybercrimes, bei denen kein (großer) finanzieller Schaden entstanden ist). Bewusstseinsbildung muss hier ansetzen.

5.4.1 Erste Schritte für Opfer

- **Sichern von Beweisen:** Speichern von Mails, Bildmaterial, Chat-Texten usw. als Beweismaterial (auf einem Speichermedium wie bspw. Cloud-Dienst, externer Festplatte, USB-Stick)
- **Blockieren von Nutzern** in sozialen Medien
- **Melden von Verstößen** in sozialen Medien

5.4.2 Anlaufstellen für Hilfesuchende[26]

- **Watchlist Internet, www.watchlist-internet.at:** Informationsplattform zu Internetbetrug und betrugsähnlichen Online-Fallen, die über aktuelle Betrugsfälle im Internet informiert und Tipps zur Vorbeugung gibt; Anlaufstelle für Betrugs-Opfer, diese erhalten konkrete Anleitungen für weitere Schritte
- **Internet Ombudsmann, www.ombudsmann.at:** Hilfe zu Online-Shopping und Internetbetrug, aber auch Unterstützung bei Verstößen in Social-Media-Plattformen (Melden von Fake-Seiten, Nutzerprofilen etc.)
- **Saferinternet, www.saferinternet.at:** Hilfe und Anregungen, wie Kinder bei der sicheren und verantwortungsvollen Verwendung von Internet, Handy usw. unterstützt werden können

26 *Geyerhofer, Alexander.* Kinder sicher im Internet (2019), 274 ff.

- **Viren, Hoax, www.hoax-info.tubit.tu-berlin.de/hoax:** Informationen über Computer-Viren, die keine sind, Falschmeldungen und Gerüchte
- **Anzeige erstatten:** bei jeder Polizeidienststelle, die weitere Bearbeitung übernimmt das Bundeskriminalamt
- **Bundeskriminalamt, Cyber Crime Competence Center (C4):** Hilfe und Informationen bzw. Meldestelle bei Verdacht auf Internetkriminalität; **against-cybercrime@bmi.gv.at**

6

6 LITERATURVERZEICHNIS 59

6 LITERATURVERZEICHNIS

Amo, L. (2016). Addressing Gender Gaps in Teens' Cybersecurity Engagement and Self-Efficacy. *IEEE Security & Privacy, 14 (1)*, 72-75.

Anwar, M. et al. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.

Arntfield, M. (2015). Toward a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media. *Canadian Journal of Communication*, 40(3), 371–388.

Bundeskriminalamt Deutschland / Kriminalistisches Institut / Forschungs- und Beratungsstelle Cybercrime KI16 (4.12.2015). Täter im Bereich Cybercrime. Eine Literaturanalyse. Abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/Internetkriminalitaet/internetkriminalitaet_node.html, zuletzt abgerufen am 19.9.2019.

Bundesministerium für Inneres (2017). IT-Sicherheit. Cybercrime-Report 2016: Zahl der Anzeigen 2016 fast um ein Drittel gestiegen. Artikel Nr. 15260 vom Montag, 30. Oktober 2017. Abrufbar unter: https://www.bmi.gv.at/news.aspx?id=5062565A4F35476A2B38453D (zuletzt abgerufen am 2.7.2019).

Danoglidis, S. A. (2015). Internetnutzung: Frauen vs. Männer. (3.2.2015). Abrufbar unter: https://entwickler.de/online/webmagazin/internetnutzung-frauen-vs-maenner-39308.html (zuletzt abgerufen am 2.7.2019).

Der Standard (21.2.2019). Stalking: Wenn das Trachten nach Nähe zu Gewalt wird (verfasst von Nicole Schöndorfer, abrufbar unter https://www.derstandard.at/story/2000098049042/wenn-das-trachten-nach-naehe-zu-gewalt-wird), zuletzt abgerufen am 19.9.2019.

European Commission / Migration and Home Affairs (2017). Europeans' attitudes towards cyber security. (19.9.2017). Abrufbar unter https://ec.europa.eu/home-affairs/news/europeans%E2%80%99-attitudes-towards-cyber-security_en (letztes Update: 2.7.2019).

European Institute for Gender Equality (EIGE) (2019). About EIGE. https://eige.europa.eu/about-eige (zuletzt abgerufen am 2.7.2019).

Fallows, D. (2005). How Women and Men use the Internet. (28.12.2005). Abrufbar unter: http://www.pewinternet.org/2005/12/28/how-women-and-men-use-the-internet/ (zuletzt abgerufen am 2.7.2019).

Gopaldas, A. (2013). Intersectionality 101. *Journal of Public Policy & Marketing*, 32, 90-94.

Huber, E. (2012). Cybercrime – Wer sind die Täter. Abrufbar unter: http://itsecx.fhstp.ac.at/downloads_2012/01_huber.pdf (zuletzt abgerufen am 2.7.2019).

Kaspersky Lab (2018). Männer sind leichtfertiger als Frauen – bei Datenschutz und IT-Sicherheit. (Pressemitteilung vom 6.12.2018). Abrufbar unter: https://www.kaspersky.de/about/press-releases/2018_men-are-more-reckless-than-women-in-privacy-and-it-security (zuletzt abgerufen am 2.7.2019).

Landesmedienzentrum Baden-Württemberg: Wer mobbt? Wer leidet? Wer schaut zu? Täterinnen und Täter (https://www.lmz-bw.de/medien-und-bildung/jugendmedienschutz/cybermobbing/wer-mobbt-wer-leidet-wer-schaut-zu/), abgerufen am 18.9.2019.

Moura, G., Sadre, R., & Pras, A. (2014). Bad neighborhoods on the internet. IEEE Communications Magazine, 52(7), 132–139.

Österreichisches Regierungsprogramm (2017-2022), dzt. noch hier abrufbar (Stand: 2.7.2019): https://www.die-neuevolkspartei.at/download/Regierungsprogramm.pdf

Statista. Entwicklung der Anzahl der angezeigten und geklärten Fälle von Cybercrime (gesamt) in Österreich von 2006 bis 2018. (mit Verweis auf das Bundeskriminalamt, Cybercrime-Report) Abrufbar unter: https://de.statista.com/statistik/daten/studie/680927/umfrage/angezeigte-und-geklaerte-faelle-von-cybercrime-in-oesterreich/ (zuletzt abgerufen am 2.7.2019).

7

7 TABELLENVERZEICHNIS 65

7 TABELLENVERZEICHNIS

Tabelle 1: Formen von Cyberkriminalität (eigene Darstellung) 19
Tabelle 2: Modell zur Struktur und Zuordnung von Cyberkriminalität (eigene Darstellung) 21

8

8 ABBILDUNGSVERZEICHNIS 69

8 ABBILDUNGSVERZEICHNIS

Abbildung 1: Darstellung der Stichprobe nach Geschlecht und Alter in % 40
Abbildung 2: Darstellung der Stichprobe nach Bildungsgrad und Tätigkeit in % 41
Abbildung 3:Intensität der Internetnutzung pro Tag in % 41
Abbildung 4: Intensität der Internetnutzung pro Tag nach Alter, Geschlecht und Bildung in % 42
Abbildung 5: Internet-Nutzungsmotive in % 42
Abbildung 6: Nutzungshäufigkeit von Internet-Angeboten in % 43
Abbildung 7: Häufigkeit unterschiedlicher Nutzungsaktivitäten in % 43
Abbildung 8: Selbsteinschätzung über technische digitale Kompetenz und technisches Interesse in % 44
Abbildung 9: Selbsteinschätzung über inhaltliche digitale Kompetenz und Selbstsicherheit in % 44
Abbildung 10: Sicherheitsbedenken im Rahmen der Internetnutzung in % 45
Abbildung 11: Sicherheitsbedenken im Rahmen der Internetnutzung in % 45
Abbildung 12: Umsetzung von Sicherheitsmaßnahmen in % 48
Abbildung 13: Umsetzung von Sicherheitsmaßnahmen in % 48
Abbildung 14: Konfrontation und Umgang mit fragwürdigen/illegalen Inhalten im Internet in % 49
Abbildung 15: Eigene Betroffenheit von Cyberkriminalität in % 50
Abbildung 16: Eigene Betroffenheit von Cyberkriminalität in % 50
Abbildung 17: Eigene Betroffenheit von Cyberkriminalität in % 51
Abbildung 18: Betroffenheit von „computer-based“ und „person-based“ Cybercrimes in % 51
Abbildung 19: Betroffenheit und Schäden durch Cybercrime in % 52
Abbildung 20: Betroffenheit und Schäden durch Cybercrime in % 53
Abbildung 21: Folgen von Cyberkriminalität 53

9

9 ANHANG 73

9.1 Typenbildung 73

9.2 Fälle in den Medien 74

9.3 Interviewleitfaden 76

9.4 Fragebogen 81

9 ANHANG

9.1 Typenbildung

Unterscheidungskriterien (wesentliche Merkmale) zur Typenbildung und für den standardisierten Fragebogen

(extrahiert aus deutsch- und englischsprachiger wissenschaftlicher Literatur via u:search und auseinschlägigen öffentlich zugänglichen Online-Quellen):

Unterscheidungsmerkmal (Variable)	Erläuterung (Wissenschaftliche Fragestellungen, Hypothesen und Erkenntnisse)
Geschlecht (Mann/Frau)	Frauen/Mädchen werden eher Opfer von person-based Cybercrimes (Angriff auf Personen). Frauen geraten eher in emotionale Abhängigkeitsfallen („Love-Scamming").
Ethnizität (white / non-white)	Nicht-Weiße werden eher Opfer von person-based Cybercrimes.
Sozialer Status	Menschen mit hohem sozialem Status (insbesondere Frauen) werden eher Opfer von Hass im Netz (person-based Cybercrimes). V.a. Frauen mit hohem ökonomischem Status, die noch dazu in der Öffentlichkeit stehen, sollen durch sexistische Hassreden eingeschüchtert werden. Expertin dazu: Caroline Lasen Diaz, Leiterin für Gendergleichstellung im Europarat. Siehe auch Fälle Sigi Maurer oder Internet-Postings gegen ÖVP-Ministerin Köstinger.
Alter	Junge werden eher Opfer bzw. haben eher Angst, Opfer von person-based Cybercrimes zu werden.
Digitale Kompetenz / Eigenwahrnehmung digitaler Kompetenz („technological fluency", „confidence in ability to use internet" = Selbstwirksamkeit)	Bei Jüngeren und Männern ausgeprägter.
Vorerfahrung als Opfer	Menschen mit „victimization experiences" haben eher Angst, wieder Opfer zu werden.
Vorerfahrung als Täter	Wer schon einmal Täter war, wird eher Opfer (bei Mädchen / person-based Cybercrimes).
Selbstkontrolle/Impulskontrolle	Impulsive Menschen begeben sich eher ohne ihr Wissen in die Nähe von motivierten Tätern.
Kommunikationsverhalten	Mädchen chatten eher mit ihnen Unbekannten (Gefahr person-based Cybercrimes); Männer sehen sich eher beabsichtigt (sexuelle) Inhalte an (Gefahr computer-based Cybercrimes).
Nutzungsmotive	Eskapismus/Unterhaltung und/oder Information, Kommunikation
Nutzungsintensität	Je intensiver die Nutzung, desto eher wird man Opfer/Täter.
Nutzungsart/Umgang	Privatsphäreeinstellungen bei Social Media, Klarname oder nickname
Deliktart	„Person-based" (personal interaction/"contact risks"): Cyberstalking, Grooming bei Erwachsenen und Kindern, Mobbing, Hass im Netz/Beleidigung/Drohung, Sexting/Sextortion, Love/Romance Scamming, Radikalisierung; „Content risks": Verletzung von Urheberrechten, Verletzung von Bildrechten/Verletzen des Rechts am eigenen Bild) oder computer-based (Hacking, Datenklau, Identitätsdiebstahl, Phishing; auch hier können „contact risks" ausschlaggebend sein).

9.2 Fälle in den Medien

Notizen zur journalistischen Berichterstattung:

Fälle aus den Medien (1.1.2014-1.1.2019, extrahiert aus österreichischen Medien mit den Suchbegriffen „Mann" und „Cyber" bzw. „Frau" und „Cyber" via APAdefacto-Datenbank.)

- 55-jährige Frau als willkürliches Opfer eines Cyber-Stalkers, der von ihr ein fingiertes Facebook-Profil erstellt und dort im Namen der Frau Sexdienste angeboten hat. Zudem meldete er sein Opfer via E-Mails von fingierten Hinterbliebenen bei der Energie AG, Gaswerk und Telekom ab und veröffentlichte auf einer Trauerwebsite einen Partezettel mit dem Foto der angeblich Verstorbenen.
- Derselbe Mann verleumdete im Internet drei Neos-KandidatInnen für eine Gemeinderatswahl (1 Frau, 2 Männer), beschuldigte sie neonazistischer Umtriebe, was diese zur Aufgabe zwang. Staatsanwaltschaft reagierte spät, Weißer Ring ergriff Initiative.
- Frau (eines Prominenten) bucht über Airbnb ein Ferienhaus, das in Wirklichkeit gar nicht existierte. Ließ sich auf eine Seite außerhalb des Portals locken und überwies von dort die Miete.
- Ähnlicher Fall: Mietbetrug, gefälschte Airbnb-Profilseite, Frau überweist Miete im Voraus, Überweisung per Western Union (betrügerische Wohnungsangebote).
- Männer werden in Sexchats (gefälschte Profile) überredet, intimes Bildmaterial zu schicken, mit dem sie dann erpresst werden (z.B. Überweisen von 5000 Euro, sonst bleibt Video online). Gefahr Videochat (via Webcam) mit Unbekannten. Tipp: Screenshots der Betrüger-Accounts machen und Chatprotokolle sichern.
- Ähnlich: Männer werden mit falschen Frauen-Profilen „in die Falle gelockt", Drohung, anstößige Bilder an Familie, Ehefrau, Firma zu schicken
- Frau kommuniziert mit einem Mann (lt. Foto) über Flirtplattform, Treffen wird vereinbart, Mann behauptet, er sei auf einer Geschäftsreise bestohlen worden und fragt nach Geld, Frau schickt ihm Geld, Treffen kam nicht zustande. Frau musste von der Polizei davon überzeugt werden, dass sie einer Betrügermasche aufgesessen war. Info: Cybercrime generiert weltweit Umsatz, der dem österreichischen BIP von ca. 330 Milliarden Euro entspricht)
- „Black Shades" werden dafür genutzt, via Webcam Fotos von jungen Frauen zu machen oder zu stehlen.
- In der Redaktion der Tageszeitung TAZ wurden 19 Frauen (zumeist Praktikantinnen) und 4 Männer mittels Keylogger (Tastatureingaben werden mitprotokolliert) ausgespäht. Täter war ein Mann, EDV-Mitarbeiter entdeckte dies.
- Andere Beispiele: Naivität: vermeintlichen Mitarbeitenden von Software-Firmen wird am Telefon Zugang zu Computer gestattet, Zugang via Teamviewer, Opfer überweist dafür Geld (ein 33-jähriger Mann erlaubte vermeintlichen Microsoft-Mitarbeitern einen Remote-Zugang zu seinem Computer, als er dann aufgefordert wurde, via Kreditkarte Geld an ein Konto der Western Union Bank zu überweisen, brach er den Kontakt jedoch ab. Computer und Laptop waren aber bereits geschädigt und mussten um teures Geld repariert werden), Täter lesen Zugangscodes mit und leeren Bankkonto. Polizei-Tipp: Immer gleich auflegen!
- Unbedacht: Öffnen von vermeintlich echten Rechnungs-E-Mails von Telefonanbietern bzw. entsprechenden Dokumenten (Phishing) – Sicherheitsupdates und Anti-Viren-Software wichtig (besser als keine!)
- Verschwindende Grenzen online – offline (Fall aus Wien): 16-jähriges Mädchen brüstet sich online damit, der besten Freundin den Freund ausgespannt zu haben. Die Freundin stellt daraufhin die Tötung des Mädchens auf Facebook zur Debatte. Junge, perspektivlose Männer (v.a. Muslime) als Radikalisierungsziele (werden vom Opfer zum Täter)

- Cyber-Attacke 2016: Bei 900.000 deutschen Telekom-Kunden wurde das Internet lahmgelegt (Es kann jeden treffen!); Online-Kommunikation Geflüchtete/Schlepper; Anstieg Bestell-Betrug; Cyberkriminalität als Problem für Banken, KMUs, Firmen, Social Engineering (digitale Sicherheit ist reaktiv), Klonen von Kreditkarten.

  Täter sind in den Medienberichten entweder nicht als Frauen oder Männer ausgewiesen oder männlich (IT-interessierte Burschen, die Hacking, Passwortklau etc. als Spiel sehen und nicht wissen, was sie anrichten können; kriminelle Netzwerke; „der Täter"; 18-jähriger Niederländer, 24-jähriger Schwede, Hackergruppe von weniger als einem Dutzend Männern unter 30 Jahren, …).

9.3 Interviewleitfaden

9.3.1 Interviewleitfaden Cyberkriminalität „Opfertypologie“

[Die Fragen sind absichtlich in „gesprochener“ Alltagssprache verfasst, um ein möglichst natürliches Gesprächsklima zu schaffen.]

OFFENER EINSTIEG

Unsere Studie befasst sich mit Cyberkriminalität **im privaten Bereich, also nicht gegen Firmen**. Wir versuchen herauszufinden, wer besonders gefährdet ist, Opfer zu werden – natürlich mit einem Blick auf die verschiedenen Formen von Cyberkriminalität, die wir heute kennen.

OPFER

- Aus Ihrer Berufserfahrung: Wer ist in welcher Art besonders gefährdet, Opfer zu werden?
  - o Fallen Ihnen noch weitere Gruppen ein? Wenn Sie jetzt z.B. an das Verhalten im Internet oder in Social Media denken?
  - o Spielt die Vertrautheit mit dem Computer, dem Handy, dem Internet oder den Social-Media-Angeboten da auch eine Rolle oder kann das heute eh schon jede und jeder?
    - Mir fällt jetzt ein, vielleicht liege ich da völlig falsch, dass da ältere Menschen eher gefährdet sein könnten, die ja noch nicht mit dem Computer aufgewachsen sind. Oder vielleicht auch ganz junge, weil für die der Umgang mit dem Handy z.B. selbstverständlicher Teil des Alltags ist. Liege ich da richtig oder ist das zu einfach?

- Sehen Sie eigentlich auch Unterschiede in der Gefährdung von Männern und Frauen?
  - o Gibt es Cyberkriminalitätsformen, von denen eher Männer oder eher Frauen betroffen sind? [mehrmals fragen]
  - o Wie würden Sie diese Unterschiede erklären?
  - o Gibt es auch ein unterschiedliches Nutzungsverhalten, das da zum Tragen kommt?

FALLVIGNETTEN

Ich möchte Ihnen jetzt einige Szenarien vorstellen, die sich an realen Fällen anlehnen. Könnten Sie mir bitte sagen, was aus Ihrer Sicht an diesem Fall eher typisch und was daran eher atypisch ist? Beginnen wir mit dem ersten Fall:

Fall 1

Es handelt sich hier um **Cyberstalking und Identitätsdiebstahl**: Ein Mann sucht zufällig eine 55-jährige Frau aus, erstellt von ihr ein fingiertes Facebook-Profil und bietet dort in ihrem Namen Sexdienstleistungen an. Gleichzeitig gibt er andernorts im Internet vor, die Frau sei verstorben: Er veröffentlicht auf einer Trauerwebseite einen Partezettel inklusive Foto und meldet sie als angeblicher Hinterbliebener bei den Energie-, Gas- und Telekommunikationslieferanten ab.

- Ist das ein eher typischer Fall?
  - o Was ist daran typisch/atypisch?
  - o Alter und Geschlecht des Opfers?
  - o Zufälligkeit bei der Auswahl des Opfers?
  - o Was mit der gestohlenen Identität gemacht wird?
  - o Gibt es etwas, was das Opfer besonders verwundbar macht und daher für den Täter geeignet erscheinen lässt?

- *Erinnern Sie sich vielleicht an einen konkreten Fall, der aussagekräftiger ist? [falls die anderen Fragen keine Ergebnisse bringen.]*

- Hätte die Frau im Vorfeld etwas anders machen können, um das zu verhindern?
- Wie darf ich mir einen Täter oder eine Täterin vorstellen, der/die so etwas macht?

Fall 2

Als nächstes ein klassischer **Betrugsfall**: Eine 70-jährige Frau möchte über Airbnb eine Ferienwohnung buchen, sie überweist die Miete im Voraus per Western Union. Die Airbnb-Seite ist gefälscht, das Geld verloren.

- Ist das ein eher typischer Fall?
  - Was ist daran typisch/atypisch?
  - Geschlecht des Opfers?
  - *Erinnern Sie sich vielleicht an einen konkreten Fall, der aussagekräftiger ist? [falls die anderen Fragen keine Ergebnisse bringen.]*
- Hätte die Frau im Vorfeld etwas anders machen können, um das zu verhindern?
- Wie darf ich mir einen Täter oder eine Täterin vorstellen, der/die so etwas macht?

Fall 3

Der nächste Fall fällt in die Kategorie **Sextortion**: Ein 21-jähriger Kellner lernt im Chatroom eine Frau kennen, der Chat wird zunehmend schlüpfrig. Die Frau lässt so viel von sich sehen, dass der Mann Lust auf mehr bekommt und gerne ihrer Aufforderung nachkommt, sich vor der Webcam auszuziehen und zu masturbieren. Kurz darauf erhält er die Aufforderung, eine Geldsumme zu überweisen, andernfalls bleibt das Video online. Der Mann zahlt und sieht sich mit der nächsten Erpressung konfrontiert: Das Video stehe zwar nicht mehr online, sei aber noch nicht gelöscht. Zahlt er nicht noch einmal, wird das Video an seine Frau und die Kollegen in der Firma geschickt.

- Ist das ein eher typischer Fall?
  - Was ist daran typisch/atypisch?
  - Alter, Geschlecht und sozialer Status des Opfers?
  - Zufälligkeit bei der Auswahl des Opfers?
  - *Erinnern Sie sich vielleicht an einen konkreten Fall, der aussagekräftiger ist? [falls die anderen Fragen keine Ergebnisse bringen.]*
- Hätte der Mann im Vorfeld etwas anders machen können, um das zu verhindern?
- Wie darf ich mir einen Täter oder eine Täterin vorstellen, der/die so etwas macht?

Fall 4

Hier hätte ich einen Fall von **Love-Scamming**: Eine 51-jährige Ärztin kommuniziert über eine Flirtplattform seit drei Monaten mit einem Mann. Sie vereinbaren ein persönliches Treffen. Kurz vor dem Date meldet sich der Mann verzweifelt aus dem Ausland: Er sei auf einer Geschäftsreise bestohlen worden, habe kein Geld und keine Kreditkarte und bitte um finanzielle Hilfe. Die Frau überweist, der Mann meldet sich noch einige Male: Er habe weitere Kosten und stecke im Ausland fest. Das persönliche Treffen kommt niemals zustande, der Kontakt bricht ab.

- Ist das ein eher typischer Fall?
  - Was ist daran typisch/atypisch?
  - Alter, Geschlecht und sozialer Status des Opfers?

- *Erinnern Sie sich vielleicht an einen konkreten Fall, der aussagekräftiger ist?*

· Hätte die Ärztin im Vorfeld etwas anders machen können, um das zu verhindern?

· Wie darf ich mir einen Täter oder eine Täterin vorstellen, der/die so etwas macht?

Fall 5

Der nächste Fall fällt auch in die Kategorie **Social Engineering bzw. Social Hacking**: Ein 33-jähriger Kfz-Mechaniker erhält einen Anruf. Der Mann am anderen Ende der Leitung behauptet, für Microsoft zu arbeiten, und möchte Zugang zum Computer des Mechanikers, um ein gravierendes Microsoftproblem zu lösen, das unerwartet bei einigen Kunden aufgetreten sei. Der Mechaniker gewährt den Zugang, wird aber stutzig, als für die „Reparatur" Geld von ihm verlangt wird, das via Kreditkarte an Western Union zu überweisen sei. Er bricht den Kontakt ab, aber PC und Laptop sind bereits schwer beschädigt.

· Ist das ein eher typischer Fall?

- Was ist daran typisch/atypisch?
- Alter, Geschlecht und sozialer Status des Opfers?
- *Erinnern Sie sich vielleicht an einen konkreten Fall, der aussagekräftiger ist? [falls die anderen Fragen keine Ergebnisse bringen.]*

· Hätte der Mechaniker im Vorfeld etwas anders machen können, um das zu verhindern?

· Wie darf ich mir einen Täter oder eine Täterin vorstellen, der/die so etwas macht?

OPFERTYPOLOGIE

Wir haben versucht, eine Typologie der Opfer von Cyber-Kriminalität zu erstellen. Das ist ein erster Versuch, eine Basis, die wir dann aufgrund der Interviews schärfen und verfeinern wollen. Ich möchte Ihnen diese Basistypologie vorstellen und Sie bitten, zu sagen, was Sie von dieser Einteilung halten. *[Den InterviewpartnerInnen wird zuerst ein Typ nach dem anderen zur Kommentierung vorgelegt. Nach der Diskussion der einzelnen Typen folgt das Vorzeigen der Gesamtübersicht anhand einer Grafik.]*

Wir schlagen eine Unterscheidung in **drei Gefährdungstypen** vor, je nach Art der Falle, in die die Opfer geraten:

1. die Vertrauensfalle

In die Vertrauensfalle geraten vor allem Internet- und Social-Media-Nutzer und -Nutzerinnen, die

· arglos, vertrauensvoll und gutgläubig sind.

· Hilfsangebote (auch von Fremden) annehmen, ohne sie zu hinterfragen, und Hilfe leisten, ohne misstrauisch zu werden.

· Anleitungen für Online-Zahlungen oder Online-Buchungen befolgen, ohne sie in Frage zu stellen, solange die Websites (halbwegs) professionell wirken.

Das ist jene Gruppe, bei der es am wahrscheinlichsten ist, dass sie Opfer von **Social Hacking, Phishing, Cyber-Betrug und Love-Scamming** wird.

· Ist das so lebensnah, ist das aus Ihrer Erfahrung realistisch?

· Haben Sie dazu bereits konkrete Fälle erlebt?

- Würden Sie da etwas verändern und ergänzen wollen?
- Spielt bei den Opfern eine Rolle …
  - o Geschlecht?
  - o Ethnizität?
  - o sozioökonomischer Status?
  - o Alter?

2. die Fahrlässigkeitsfalle
In die Fahrlässigkeitsfalle geraten vor allem Internet- und Social-Media-Nutzer und -Nutzerinnen, die

- sich vor der Nutzung nicht oder nur oberflächlich informieren.
- in dem falschen Bewusstsein leben, dass ihnen schon nichts passieren wird.
- keine ausreichenden oder die falschen Vorsichtsmaßnahmen technischer Natur ergreifen, z.B. auf Anti-Viren-Programme, Sicherheitskopien oder Passwörter verzichten.

Das ist jene Gruppe, bei der es am wahrscheinlichsten ist, dass sie Opfer von **Viren, Trojanern, Malware, Hacking, Datendiebstahl oder Ransomware** wird.

- Ist das so lebensnah, ist das aus Ihrer Erfahrung realistisch?
- Haben Sie dazu bereits konkrete Fälle erlebt?
- Würden Sie da etwas verändern und ergänzen wollen?
- Spielt bei den Opfern eine Rolle …
  - o Geschlecht?
  - o Ethnizität?
  - o sozioökonomischer Status?
  - o Alter?

3. die Impulsfalle
In die Impulsfalle geraten vor allem Internet- und Social-Media-Nutzer und -Nutzerinnen, die

- impulsiv, neugierig und experimentierfreudig sind.
- bereitwillig und offen kommunizieren.
- Social-Media-Angebote intensiv nutzen
- und somit auch, weil sie ihre Social-Media-Aktivitäten uneingeschränkt einsehbar (also öffentlich) halten, eine auffallend starke Medienpräsenz haben.

Das ist jene Gruppe, bei der es am wahrscheinlichsten ist, dass sie Opfer von I**dentitätsdiebstahl, Sextortion, Verbreitung bzw. Schaffung (Morphing) von kompromittierendem Bildmaterial oder Cybergrooming** wird.

- Ist das so lebensnah, ist das aus Ihrer Erfahrung realistisch?
- Haben Sie dazu bereits konkrete Fälle erlebt?
- Würden Sie da etwas verändern und ergänzen wollen?

- Spielt bei den Opfern eine Rolle …
  - o Geschlecht?
  - o Ethnizität?
  - o sozioökonomischer Status?
  - o Alter?

4. die drei Typen auf einen Blick

[Grafik oder übersichtliche Tabelle mit allen drei Typen vorlegen.]

- o Hier sind jetzt die drei Typen nebeneinandergestellt. Würden Sie sagen, dass damit die Opfer und deren Merkmale, so wie Sie sie aus Ihrer Arbeit kennen, gut abgebildet werden? [Alternativ: Scheinen Ihnen die Typen jetzt realitätsnäher, wo sie nebeneinanderstehen?]
- o Was ist gut daran?
- o Was ist schlecht daran?
- o Was würden Sie ändern oder ergänzen?

PRÄVENTION & GEGENMASSNAHMEN

- Von den verschiedenen gefährdeten Gruppen, über die wir jetzt gesprochen haben: Wie kann sich [Gruppe 1, 2, 3, …] selbst am besten schützen?

- Wird insgesamt eigentlich genug Prävention gegen Cyber-Kriminalität betrieben? Wie sehen Sie das?
  - o Was wird da schon gemacht?
  - o Reicht das aus?
  - o Was könnte noch zusätzlich unternommen werden?
  - o Fällt Ihnen noch etwas ein?

OFFENES ENDE

Fällt Ihnen irgendetwas ein, das wir noch nicht angesprochen haben, das Ihnen aber noch wichtig ist, das Sie gerne unterbringen möchten?

9.4 Fragebogen

Institut für empirische Sozialforschung	Untersuchungs-Nr.	2	7	4	0	0	0	2	2	CAWI
1010 Wien, Teinfaltstraße 8	Listen Nr.									
54 670 D.V.R. 0049492	Laufende Nr.									
2019-04-02	Interviewer-Nr.									

In der folgenden Umfrage geht es um das Thema Internetnutzung und mögliche Gefahren im Internet. Sie wird in etwa 15 Minuten dauern, und wir möchten Sie herzlich einladen, daran teilzunehmen. Es gibt keine richtigen oder falschen Antworten, von Interesse ist einfach nur Ihre persönliche Meinung. Selbstverständlich werden Ihre Angaben völlig vertraulich behandelt und nur gemeinsam mit anderen statistisch ausgewertet.

SAMPLE: n=1.000, Örep. ab 15 Jahren

EINSTIEG

Zu Beginn ein paar Fragen für die Statistik.

1. Geschlecht

männlich 1
weiblich 2

2. Wie alt sind Sie?

3. In welchem Bundesland befindet sich Ihr Hauptwohnsitz?

Vorarlberg 1
Tirol 2
Salzburg 3
Oberösterreich 4
Kärnten 5
Steiermark 6
Burgenland 7
Niederösterreich 8
Wien 9

4. Welche ist Ihre höchste abgeschlossene Schulbildung?

Pflichtschule 1
Pflichtschule mit Lehre 2
Fachschule (mittlere Schule, BMS) 3
AHS, BHS ohne Matura 4
Matura (AHS, BHS) 5
Hochschule, Fachhochschule, Akademie 6

5. **Haben Sie selbst Kinder unter 18 Jahren, die mit Ihnen im gemeinsamen Haushalt leben?**
Dazu zählen auch Pflege- oder Stiefkinder. Wenn ja, wie viele?

|__|__|

keine Kinder 999

6. (WENN F5 >0) **Geben Sie bitte Alter und Geschlecht Ihrer Kinder an!**

ONLINE-NUTZUNG UND DIGITALE KOMPETENZ

7. **Man kann das Internet auf verschiedenen Geräten nutzen, wie beispielsweise Computern, Tablets, Handys. Wie viele Stunden pro Tag nutzen Sie das Internet im Durchschnitt für private Zwecke?**

|__|__| Stunden

keine Angabe 999

8. **Wie häufig haben Sie selbst im Schnitt in den letzten drei Monaten folgende Online-Aktivitäten unternommen? Egal, ob zu Hause, in der Arbeit, bei Freunden oder unterwegs über mobiles Internet, z.B. am Smartphone, Laptop oder Tablet.**

		täglich oder fast täglich	mindestens einmal pro Woche	mindestens einmal pro Monat	weniger als einmal pro Monat	nie	k.A.
1.	Nachrichten konsumieren (z.B. Online-Auftritt von TV-, Radiosendern, Zeitungen)	1	2	3	4	5	999
2.	Informationen suchen (z.B. über Google, Wikipedia)	1	2	3	4	5	999
3.	öffentliche Chats, Newsgroups, Foren, Blogs	1	2	3	4	5	999
4.	Musik herunterladen bzw. hören/ streamen; online Radio hören	1	2	3	4	5	999
5.	eigene Inhalte gestalten (z.B. Texte / Fotos / Videos hochladen)	1	2	3	4	5	999
6.	Besuch von sozialen Netzwerken bzw. sozialen Medien, z.B. Facebook, Google+, Instagram, Twitter etc.	1	2	3	4	5	999
7.	Instant Messaging, z.B. WhatsApp, Facebook-Messenger, Snap-Chat, Instagram Direct Messenger	1	2	3	4	5	999
8.	Online Einkaufen / Bestellen von Produkten und Dienstleistungen (z.B. Urlaub, Bücher, Musik)	1	2	3	4	5	999
9.	Online Verkaufen von Waren oder Dienstleistungen (z.B. auf eBay, willhaben)	1	2	3	4	5	999
10.	Videospiele online spielen	1	2	3	4	5	999

11.	Internet-Banking	1	2	3	4	5	999
12.	Videos ansehen / streamen / downloaden (z.B. Youtube, Netflix, Amazon Prime)	1	2	3	4	5	999
13.	Besuch von Online-Dating-Plattformen (z. B. Parship, Tinder, OKCupid, Once, Grindr)	1	2	3	4	5	999

9. **Wie sehr stimmen Sie den folgenden Aussagen zu?**

		trifft voll und ganz zu	2	3	4	trifft überhaupt nicht zu	k.A.
1.	Ich beschäftige mich gerne mit neuen Technologien.	1	2	3	4	5	999
2.	Im Umgang mit meinem PC, Laptop, Smartphone oder Tablet befürchte ich oft, etwas falsch zu machen.	1	2	3	4	5	999
3.	Ich erledige Amtswege gerne online (z.B. Anträge stellen).	1	2	3	4	5	999
4.	Es fällt mir schwer, vertrauenswürdige Informationen im Internet selbst zu finden (z.B. über Suchmaschinen).	1	2	3	4	5	999
5.	Es fällt mir leicht, Software auf meinem PC oder Laptop selbst zu installieren.	1	2	3	4	5	999

DATENSCHUTZ UND CYBERSECURITY

10. **Wenn Sie an die Erfassung und Speicherung Ihrer elektronischen Daten denken, wie sehr fühlen Sie sich da von Folgendem bedroht?**

		sehr bedroht	2	3	4	gar nicht bedroht	k.A.
1.	weltweite Weitergabe von elektronisch erfassten persönlichen Daten	1	2	3	4	5	999
2.	Aufzeichnung und Auswertung von Daten bei Kundenkarten	1	2	3	4	5	999
3.	Austausch von Kundendaten zwischen Unternehmen	1	2	3	4	5	999
4.	Missbrauch von persönlichen Einträgen wie Fotos und privaten Daten im Internet	1	2	3	4	5	999
5.	Betrug bei Einkäufen im Internet (z.B. bezahlte Ware wird nicht geliefert)	1	2	3	4	5	999
6.	Hacking von Bank- oder Kreditkartendaten	1	2	3	4	5	999
7.	Zugriffe fremder Personen auf meinen Computer (z.B. von Hackern)	1	2	3	4	5	999
8.	Aufzeichnung von E-Mails und telefonischen Gesprächsverbindungen	1	2	3	4	5	999
9.	Auswertung von Nutzerdaten bei Internetseiten wie Facebook, Google oder Amazon	1	2	3	4	5	999
10.	Möglichkeit, dass man über Suchmaschinen gefunden und ausgeforscht wird	1	2	3	4	5	999

11. Welche der folgenden Aussagen trifft auf Sie zu?

		ja	nein	mache ich nicht bzw. verwende Gerät nicht	k.A.
1.	Ich verwende auf meinem PC oder Laptop einen Malware-/Virenscanner.	1	2	3	999
2.	Ich verwende auf meinem PC oder Laptop eine Firewall.	1	2	3	999
3.	Ich verwende auf meinem Smartphone oder Tablet einen Malware-/Virenscanner.	1	2	3	999
4.	Ich ändere regelmäßig meine Passwörter.	1	2	3	999
5.	Ich verwende für verschiedene Webseiten unterschiedliche Passwörter.	1	2	3	999
6.	Ich achte darauf, dass Webseiten sicher sind, bevor ich mich mit meinen Zugangsdaten einlogge (z.B. https statt http, Vorhandensein von Sicherheitszertifikaten).	1	2	3	999
7.	Ich prüfe bewusst die Seriosität von Webseiten und Online-Shops.	1	2	3	999
8.	Ich öffne keine E-Mail-Anhänge, wenn mir der Absender suspekt oder unbekannt ist.	1	2	3	999
9.	Ich habe üblicherweise GPS bzw. Standortbestimmung am Smartphone bzw. Tablet aktiviert.	1	2	3	999
10.	Ich achte beim Posten darauf, welche meiner Postings öffentlich und welche nur für Freunde und Follower sichtbar sind.	1	2	3	999
11.	Ich mache regelmäßig Updates meiner Programme bzw. meines Betriebssystems.	1	2	3	999
12.	Ich nutze regelmäßig Filesharing Cloud Services wie Dropbox, Onedrive, Google Drive (dabei werden Daten online in der "Cloud" gespeichert, und man kann von jedem Computer oder Smartphone darauf zugreifen).	1	2	3	999

12. Wenn Sie eine Wahlmöglichkeit haben: Verwenden Sie bei Benutzerkonten im Internet lieber Ihren echten Namen oder einen fiktiven Namen (Nickname)?

echter Vor- und Zuname 1
frei erfundener Name (Nickname) 2
k.A. 999

13. Von allen Personen, mit denen Sie über Instant-Messaging-Dienste (z.B. Facebook Messenger, Instagram DM, WhatsApp, Snap-Chat) chatten, wie viele davon, schätzen Sie, kennen Sie persönlich, d.h. haben Sie schon einmal getroffen?

(fast) alle (91%-100%) 1
sehr viele (61%-90%) 2
etwa die Hälfte (51%-60%) 3
eher wenige (21%-50%) 4
sehr wenige (0%-20%) 5
k.A. 999

CYBERKRIMINALITÄT

14. Wie gut fühlen Sie sich im Allgemeinen über die Risiken von Cyberkriminalität informiert?

sehr gut informiert 1
eher gut informiert 2
eher weniger gut informiert 3
gar nicht gut informiert 4
k.A. 999

15. Sind Sie beim Surfen im Netz schon einmal auf Webseiten oder Benutzer-Accounts gestoßen, auf denen fragwürdige oder illegale Inhalte verbreitet wurden? Wenn ja, was waren das für Inhalte?

fremdenfeindliche Inhalte 1
religiös motivierter Extremismus (z.B. gegen Juden, Moslems gerichtet) 2
Aufruf zu Gewalt 3
Hassrede 4
Video, auf dem eine Schlägerei oder ein körperlicher Angriff zu sehen ist 5
Nacktheit 6
Pornografie (sexuelle Handlungen zwischen Erwachsenen) 7
Kinderpornografie 8
unerlaubte Verkäufe (z.B. illegale Substanzen) 9
anderes (NOTIEREN) 10
nichts davon 11
keine Angabe 999

16. (WENN F15≠11**) Wie haben Sie darauf reagiert, welche der folgenden Handlungen haben Sie gesetzt?**

gar nichts 1
Ich folge diesem Account nicht mehr / besuche diese Website nicht mehr. 2
Ich habe diesen Account blockiert. 3
Ich habe diesen Account beim Betreiber der Website gemeldet. 4
Ich habe diesen Account/diese Website bei der Polizei gemeldet 5
anderes (NOTIEREN) 6
keine Angabe 999

17. Es gibt unterschiedliche Arten von Cyberkriminalität. Waren Sie in den letzten 3 Jahren schon einmal von folgenden Arten betroffen? Uns geht es darum, ob Sie tatsächlich Opfer wurden. Bloße kriminelle Versuche, denen Sie rechtzeitig ohne Schaden entgehen konnten, sind damit nicht gemeint.

		mehrmals	einmal	nie	k.A.
1.	Viren, Trojaner oder Malware auf Ihrem PC, Laptop, Smartphone oder Tablet	1	2	3	999
2.	Hacker-Angriff auf Ihren Social-Media- oder E-Mail-Account, d.h., jemand ist unbefugt in Ihren Account eingedrungen	1	2	3	999
3.	Jemand hat Sie über gefälschte Webseiten, E-Mails oder andere Nachrichten dazu überredet, sich mit Ihren Zugangsdaten einzuloggen bzw. Ihre Zugangsdaten zu verraten	1	2	3	999
4.	Jemand hat Sie zur Zahlung von Geld bewegt, indem Ihnen per E-Mail oder Chats Erbschaften, lukrative Nebenjobs oder Lotteriegewinne versprochen wurden	1	2	3	999
5.	Jemand hat über Schadsoftware Ihre Dateien verschlüsselt und Geld von Ihnen verlangt, damit Sie wieder Kontrolle über Ihre Daten erhalten	1	2	3	999
6.	Jemand anderes hat sich im Internet als Sie selbst ausgegeben	1	2	3	999
7.	Jemand hat gegen Ihren Willen bzw. ohne Ihr Einverständnis Fotos/Videos von Ihnen im Internet veröffentlicht	1	2	3	999
8.	Rufschädigung über das Internet	1	2	3	999
9.	Online-Banking- oder Kreditkarten-Betrug	1	2	3	999
10.	Sie haben Waren online bestellt und bezahlt, aber nie die Ware erhalten	1	2	3	999
11.	Bloßstellung, Drohen oder Fertigmachen über das Internet	1	2	3	999
12.	Sie haben sich von jemandem verfolgt oder übermäßig überprüft gefühlt	1	2	3	999
13.	Sexuelle Belästigung über das Internet	1	2	3	999
14.	Jemand hat versucht, sich im Chat Ihr Vertrauen zu erschleichen (z.B. mit Fake-Profilen), mit dem Ziel der Anbahnung sexueller Kontakte	1	2	3	999
15.	Aufforderung, Nacktfotos via Chat, E-Mail etc. zu verschicken (Sexting)	1	2	3	999
16.	Jemand hat Geld von Ihnen verlangt, damit Nacktfotos von Ihnen nicht veröffentlicht oder verbreitet werden	1	2	3	999
17.	Jemand hat Ihnen in sozialen Netzwerken oder Online-Partnerbörsen die große Liebe vorgespielt und sie dann unter einem Vorwand (z.B. finanz. Notlage) gebeten, Geld zu überweisen	1	2	3	999

18. (WENN F17=1-2) Welche Folgen hatte/n diese Form/en der Cyberkriminalität für Sie?

keine Folgen 1
finanziellen Schaden unter 100 Euro. 2
finanziellen Schaden zwischen 100 und 1.000 Euro. 3
finanziellen Schaden über 1.000 Euro. 4
habe das Internet weniger verwendet bzw. meine Online-Aktivitäten eingeschränkt 5
psychische/emotionale Folgen 6
Computersystem musste neu aufgesetzt werden 7
brauchte Rechtsberatung 8
brauch(t)e psychologische Betreuung 9
andere (NOTIEREN) 10
k.A. 999

19. Manchmal macht man Dinge, bei denen man erst im Nachhinein bemerkt, dass man vielleicht etwas zu weit gegangen ist. Kennen Sie jemanden in Ihrem Umfeld, der Folgendes schon einmal gemacht hat? (siehe Tabelle Frage 20)

20. Und wie sieht es mit Ihnen aus? Haben Sie selbst schon einmal eines der folgenden Dinge getan?

		ja	nein	k.A.
1.	Viren, Trojaner oder Malware auf einem PC, Laptop, Smartphone oder Tablet installiert	1	2	999
2.	Social-Media- oder E-Mail-Accounts gehackt	1	2	999
3.	Jemanden zu überreden versucht, die Zugangsdaten zu verraten	1	2	999
4.	Sich im Internet als jemand anderes ausgegeben, ein Fake-Profil erstellt	1	2	999
5.	Von jemandem gegen seinen Willen bzw. ohne Einverständnis Fotos/Videos im Internet veröffentlicht	1	2	999
6.	Falsche Behauptungen über eine andere Person im Internet verbreitet	1	2	999
7.	Jemanden/m im Internet bloßgestellt oder gedroht	1	2	999
8.	Jemanden über das Internet (z.B. in sozialen Netzwerken, per E-Mail) gestalkt	1	2	999
9.	Jemandem übermäßig viele E-Mails, SMS oder andere Nachrichten geschrieben, ohne dass die andere Person je darauf geantwortet hat	1	2	999
10.	Jemanden über das Internet sexuell belästigt (z.B. Aufforderung zu sexuellen Handlungen, unaufgefordertes Verschicken von Nacktfotos/sexuellen Inhalten, ungefragte Thematisierung körperlicher Geschlechtsmerkmale einer anderen Person)	1	2	999
11.	Versuch, von jemandem via Chat, E-Mail etc. Nacktfotos zu bekommen	1	2	999

21. Haben Sie sich in den letzten drei Jahren in Österreich aus einem der folgenden Gründe diskriminiert oder ungleich behandelt gefühlt?

Hautfarbe 1
Ethnische Herkunft oder Migrationshintergrund 2
Religion oder Glaube 3
Alter 4
Geschlecht 5
Behinderung oder körperliche Einschränkung 6
Sexuelle Orientierung (z.B. weil man schwul, lesbisch, bisexuell, transsexuell etc. ist) 7
andere Gründe 8
nein, nichts davon .....

22. Inwieweit treffen die folgenden Aussagen auf Sie zu?

		trifft voll und ganz zu	2	3	4	trifft überhaupt nicht zu	k.A.
1.	Ich mache mir nicht viele Gedanken über die Zukunft.	1	2	3	4	5	999
2.	Ich handle oft spontan, denke aber trotzdem mit.	1	2	3	4	5	999
3.	Aufregung und Abenteuer sind für mich wichtiger als Sicherheit.	1	2	3	4	5	999
4.	Ich finde es manchmal aufregend, Sachen zu machen, für die ich Ärger bekommen könnte.	1	2	3	4	5	999
5.	Wenn ich eine ernsthafte Auseinandersetzung mit jemandem habe, ist es normalerweise schwierig für mich, ruhig zu reden und nicht zu explodieren.	1	2	3	4	5	999

23. (WENN F5≠999) **Denken Sie an verschiedene Gefahren aus dem Internet, z.B. Online-Mobbing, Erpressung oder andere Gefahren. Tun Sie etwas der folgenden Dinge, um Ihr Kind/Ihre Kinder vor diesen Gefahren zu schützen?**

		ja	nein	trifft nicht zu (d.h., Kind darf z.B. gar nicht ins Internet)	k.A.
1.	darauf achten, was das Kind genau im Internet tut	1	2	3	999
2.	mit dem Kind ausführlich und regelmäßig über die Gefahren des Internets sprechen	1	2	3	999
3.	Internet-Benutzung des Kindes zeitlich begrenzen	1	2	3	999
4.	Browser- und Suchmaschinen-Einstellung kindersicher gestalten	1	2	3	999
5.	auf sozialen Medien mit dem Kind / den Kindern befreundet sein	1	2	3	999
6.	Regeln über die Internetnutzung mit dem Kind / den Kindern vereinbaren	1	2	3	999

24. (WENN F5≠999) **Hat Ihr Kind/Haben Ihre Kinder schon einmal negative Erfahrungen im Internet gemacht? Beispielsweise in Chats oder bei der Nutzung sozialer Netzwerke. Wenn ja, was ist da passiert?**

keine negativen Erfahrungen 999

STATISTIK

25. Was ist Ihre hauptsächliche Tätigkeit?

voll berufstätig (36 Stunden oder mehr) 1
Teilzeit berufstätig (unter 36 Stunden) 2
geringfügig beschäftigt 3
andere Form der Berufstätigkeit (z.B. Werkvertrag, mithelfende Familienangehörige) 4
Lehrling.....5
arbeitslos 6
in Karenz.....7

in Pension 8
im Haushalt tätig OHNE eigenes Einkommen 9
Schüler/in, Student/in 10
andere Form der Nicht-Erwerbstätigkeit .....

26. (WENN F25=1-5) **Was ist Ihre derzeitige Stellung im Beruf?/ Was war Ihre letzte Stellung im Beruf?**

Freie Berufe 1
InhaberIn/DirektorIn größerer Unternehmen 2
InhaberIn kleinerer Firmen 3
Angestellte (einfache) + Lehrlinge f. Angestelltenberufe 4
Angestellte (qualifizierte) 5
Angestellte (leitende) 6
Beamte/öffentlich Bedienstete (nicht leitend) 7
Beamte/öffentlich Bedienstete (leitend) 8
Landwirte (+ Mithelfende) 9
ArbeiterIn (ungelernte, angelernte) 10
FacharbeiterIn + Lehrlinge für Arbeiterberufe 11
ArbeiterIn: Meister, Vorarbeiter 12
ArbeiterIn im öffentlichen Dienst 13
freier Dienstvertrag/neue Selbstständige 14
War noch NIE berufstätig: z.B. Kind / SchülerIn / StudentIn / (nur) im Haushalt tätig 15
k.A.....

27. In welche Kategorie fällt das monatliche Netto-Einkommen Ihres Haushaltes? Rechnen Sie dazu bitte alle Einkommen zusammen (inkl. Familienbeihilfe, Kinderbetreuungsgeld, Wohnbeihilfe, Mindestsicherung etc.)!

bis 750 Euro 1
bis 1.000 Euro 2
bis 1.300 Euro 3
bis 1.600 Euro 4
bis 2.000 Euro 5
bis 2.500 Euro 6
bis 3.000 Euro 7
bis 3.500 Euro 8
bis 4.000 Euro 9
bis 4.500 Euro 10
bis 5.000 Euro 11
über 5.000 Euro 12
keine Angabe 999

28. (WENN F3≠9) **Ortsgröße Ihres Wohnortes:**

bis 2.000 Einwohner 1
bis 5.000 Einwohner 2
bis 10.000 Einwohner 3
bis 20.000 Einwohner 4
bis 50.000 Einwohner 5
bis 300.000 Einwohner 6

IMPRESSUM

Medieninhaber und Herausgeber
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien
Tel: +43 (0)5 77 0 77-1919
Fax: +43 (0)5 77 0 77-8000
kfv@kfv.at
www.kfv.at

Vereinszweck und Richtung
Der Verein ist eine Einrichtung für alle Vorhaben der Unfallverhütung und eine Koordinierungsstelle für Maßnahmen, die der Sicherheit im Verkehr sowie in sonstigen Bereichen des täglichen Lebens dienen. Er gliedert sich in die Bereiche Verkehr und Mobilität, Heim, Freizeit, Sport, Eigentum und Feuer sowie weitere Bereiche der Sicherheitsarbeit.

Geschäftsführung
Dr. Othmar Thann, Dr. Louis Norman-Audenhove

ZVR-Zahl
801 397 500

Grundlegende Richtung
Die Publikationsreihe „KFV – Sicher Leben" dient der Veröffentlichung von Studien aus dem Bereich Eigentumsschutz, die vom KFV oder in dessen Auftrag durchgeführt wurden.

Autorin
Dr. Irmgard Wetzstein

Co-Autoren
Sabine Fuger, Mag. Dagmar Lehner, Mag. Monika Pilgerstorfer, Dr. Georg Plattner

Fachliche Verantwortung
Dr. Armin Kaltenegger

Redaktion
Mag. Andrea Feymann
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18
1100 Wien

Verlagsort
Wien, 2019

Lektorat
Mag. Eveline Wögerbauer
Angela Dickinson

Grafik
Catharina Ballan .com

Fotos
Titelbild: iStock

ISBN – pdf-Version
978-3-7070-0165-5

Zitiervorschlag
KFV - Sicher Leben. Band #21. Cybercrime und Viktimisierung. Wien, 2019

Aufgrund von Rundungen kann es bei Summenbildungen zur Unter- oder Überschreitung des 100%-Wertes kommen.

ISBN (PDF) 978-3-7070-0165-5

KEYLESSCUBIETENDEUENUMMER 21