Wenn Liebe teuer wird

Moderner Heiratsschwindel im Internet

Wien, Juni 2023

Durchgeführt im Auftrag von: Dr. Armin Kaltenegger

Wenn Liebe teuer wird

Moderner Heiratsschwindel im Internet

Autorin
Patricia Jeßner, BA

Fachliche Verantwortung
Patricia Jeßner, BA

Im Auftrag von
Dr. Armin Kaltenegger

Inhaltsverzeichnis

1. Einleitung

Die Evolution des Internets hat tiefgreifende Auswirkungen auf die zwischenmenschliche Kommunikation und den Aufbau von Beziehungen. In der Ära des Online-Dating und der sozialen Medien haben Menschen aus verschiedenen Teilen der Welt die Möglichkeit, miteinander in Kontakt zu treten und potenzielle Partner*innen kennenzulernen. Leider haben sich im Zuge dieser Entwicklung auch Individuen herausgebildet, die das Internet als Werkzeug zur Ausbeutung und Täuschung anderer nutzen.

Im Bereich der Online-Betrügereien haben sich E-Mail-Scams traditionell auf negative Emotionen wie Gier (z. B. in zahlreichen 419-Betrügereien[1]), Einsamkeit (Romance Scams) und Angst (Sicherheitswarnungen, Phishing usw.) gestützt (Jakobsson, 2016, p. XIV). Insbesondere Romance Scams oder Love Scams werden von den Medien häufig thematisiert, wenn besonders drastische Fälle ans Licht kommen und betrügerische Täter*innen ihre Opfer um beträchtliche Geldsummen bringen. Diese Geschichten finden dann ihren Platz in den Zeitungsspalten.

Das FBI definiert „Romance Scam“ als „die Annahme gefälschter Online-Identitäten durch Kriminelle mit dem Ziel, die Zuneigung und das Vertrauen eines Opfers zu erschleichen“. Die Betrüger*innen täuschen eine enge, romantische Beziehung vor, um das Opfer zu manipulieren und/oder zu bestehlen. Die Liebesbetrüger sind Experten auf ihrem Gebiet. Sie wirken aufrichtig, fürsorglich und glaubwürdig. Sie sind auf den meisten Dating- und Social-Media-Seiten präsent. Ihre Absicht ist es, so schnell wie möglich eine Beziehung aufzubauen, Zuneigung bei ihrem Opfer hervorzurufen und sich Vertrauen zu erschleichen. (FBI, 2021)

Das Konzept des Kennenlernens und des Beziehungsaufbaus hat sich mit dem Aufkommen des Internets grundlegend gewandelt. Während Menschen früher hauptsächlich über den Arbeitsplatz, den Freundeskreis oder gemeinsame Interessen potenzielle Partner*innen kennenlernten, hat Online-Dating die Möglichkeiten des Beziehungsaufbaus erweitert und verändert. Im Gegensatz zu den traditionellen analogen Methoden, die meist örtlich begrenzt waren, eröffnet das Internet Liebessuchenden die gesamte Welt als potenziellen Pool an Partnern.

Mithilfe einer Betroffenenstudie und einer Dunkelfeldstudie möchte das Kuratorium für Verkehrssicherheit diese perfide Form des Onlinebetrugs näher beleuchten, die Auswirkungen dieser modernen Verbrechensart im Detail darstellen und somit einen wesentlichen Beitrag zur Bewusstseinsbildung, Information und Prävention in puncto Cybercrime leisten.

[1] Bei 419-Betrügereien handelt es sich um einen Vorschuss-Betrug, bekannt durch die Mails vom berühmten “nigerianischen Prinzen“. Benannt ist diese Form des Betrugs nach dem Paragraphen des nigerianischen Strafgesetzbuchs, mit dem dieses Vergehen festgehalten wird.

2. Cyberkriminalität in Österreich

Cyberkriminalität ist auch in Österreich ein in den letzten Jahren stark gewachsenes Kriminalitätsfeld. Dies zeigt auch die vom Innenministerium im Cybercrime Report 2019 veröffentlichte Anzeigenstatistik: „Die Abbildung der Entwicklung von Cybercrime in den letzten zehn Jahren zeigt, dass mit 28.439 Delikten 2019 gegenüber dem Vorjahr ein Anstieg von 44,9 Prozent zu verzeichnen ist (2018: 19.627)“ (Bundeskriminalamt, 2022, p. 14). Und auch im Vergleich von 2019 mit 2020 zeigt sich erneut ein steiler Anstieg der angezeigten Straftaten.

Die Aufklärungsquote bewegte sich in den letzten Jahren stets um die 30 Prozent (siehe auch Abbildung 1). Diese Zahlen fassen jedoch alle Arten von Cyberkriminalität zusammen, sowohl im privaten als auch im wirtschaftlichen Bereich, darüber hinaus auch nur jene, die der engen österreichischen Definition entsprechen.

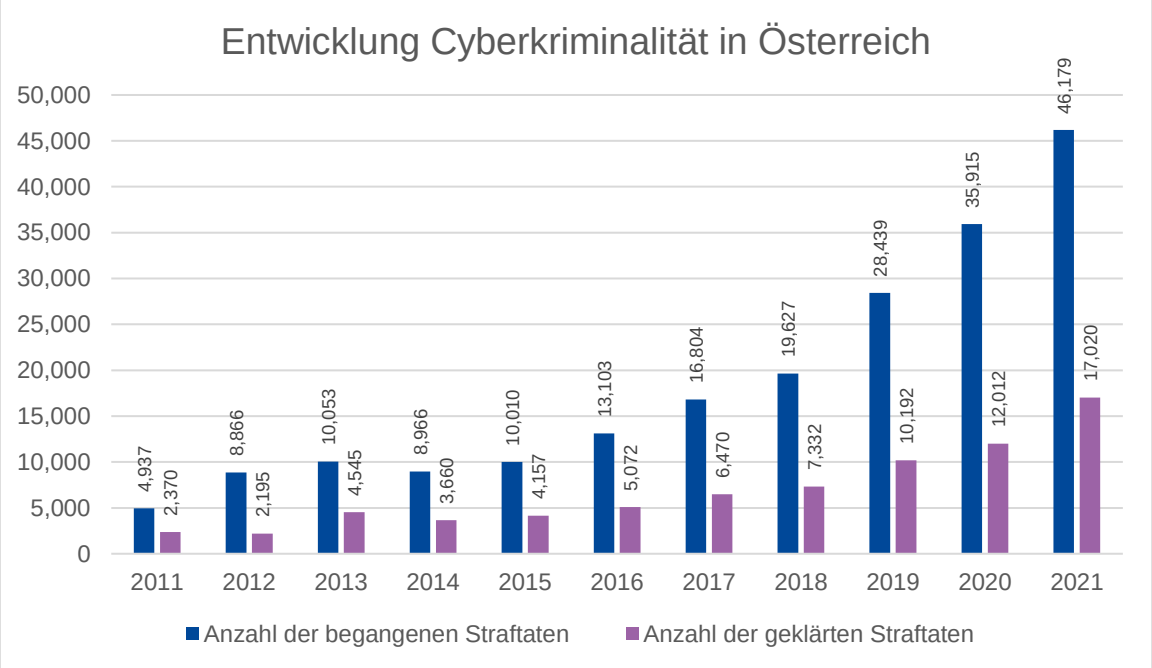


Abbildung 1: Entwicklung der Cyberkriminalität in Österreich. Quelle: Bundeskriminalamt

Die österreichische Gesetzgebung unterscheidet nämlich in ihrer Klassifizierung zwischen Cybercrime „im engeren“ und „im weiteren“ Sinn:

Ersteres bedeutet, wie im obigen Zitat bereits angedeutet, dass sowohl Tatinstrument als auch Angriffsziel IT-Systeme oder Daten sein müssen. Hierfür existiert im Bundeskriminalamt ein spezielles Kompetenzzentrum, das Cyber Crime Competence Center (C4), das als nationale und internationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität dient. „2019 musste bei Tatbeständen zu Cybercrime im engeren Sinn ein (…) Anzeigenanstieg von 148,3 Prozent gegenüber dem Vorjahr verzeichnet werden. Die beiden häufigsten Deliktsarten waren

der widerrechtliche Zugriff auf ein Computersystem § 118a Strafgesetzbuch (StGB) und der betrügerische Datenverarbeitungsmissbrauch § 148a StGB“ (Bundeskriminalamt, 2022, p. 15).

Cybercrime im weiteren Sinne bedeutet, dass ein*e Täter*in IT-Systeme zur Tatverwirklichung nutzt, das Ziel jedoch kein IT-System ist. Während unter erstere Definition klassisches Hacking oder auch DDoS-Attacken fallen, fällt unter die zweite Definition die klassische Erpressung (Ransomware) oder Betrug (Phishing), wobei ein IT-System genutzt wird, um eine originär „klassische“ Straftat zu begehen. „Der Internetbetrug (Phishing, Scam, Betrug beim Einkauf im Internet etc., Anm.) erreichte 2019 mit 16.831 Anzeigen einen neuen Höchststand. (…) Auf den gesamten Bereich Cybercrime gerechnet, stellt somit der Internetbetrug etwas mehr als 59 Prozent der Anzeigen dar“ (Bundeskriminalamt, 2022, p. 15 f.).

Die zwei in Österreich am häufigsten auftretenden spezifischen Formen von Cyberkriminalität sind Cyberverbrechen „im weiteren Sinn“:

- Zum einen ist dies Ransomware, also Schadsoftware, die auf IT-Systeme geschleust wird und die darauf befindlichen Daten verschlüsselt. Meist geschieht dies über eine infizierte Datei, die per E-Mail gesendet wird. Die Täter*innen machen sich nun bemerkbar und erpressen ihre Opfer, indem klar gemacht wird, dass die Daten nur gegen Lösegeldzahlungen wieder freigegeben werden. Dies ist vor allem im Wirtschaftsbereich ein großes Problem, weil diese Schadsoftware ganze Produktionsketten zum Erliegen bringen kann.
- Phishing, die zweite massiv steigende Deliktform, ist der Versuch, Geheimdaten abzuziehen. Klassischerweise geschieht dies über eine E-Mail, in der die Adressat*innen aufgefordert werden, ihre Daten auf einer Homepage einzugeben. Dabei wird vorgetäuscht, eine seriöse Institution (bspw. ein Gesundheitsinstitut oder ein Zulieferungsbetrieb) zu sein. Die Seite, die in der E-Mail verlinkt wird, ist meistens täuschend echt nachgebaut und wirkt seriös. Werden die Daten eingegeben, erhalten die Betrüger*innen Zugriff auf das Bankkonto, den Datenserver oder ähnliches.

Diese beiden Delikte steigen auch weiterhin stark an, da sie verhältnismäßig leicht und ohne besondere Vorkenntnisse gesetzt werden können und durch ihren Massencharakter eine sehr große Zahl an potenziellen Opfern in sehr kurzer Zeit erreichen können.

2.1. Spam vs Social Engineering

Das gezielte Scamming, bei dem Betrüger*innen ihre Bemühungen auf eine ausgewählte Anzahl potenzieller Opfer konzentrieren, hat sich als effizienter erwiesen als der Versuch, eine breite Masse durch Massenspam-Mails zu erreichen. Es gibt verschiedene Faktoren, die erklären, warum mehr Menschen auf gezieltes Scamming anspringen.

Ein entscheidender Grund liegt in der Blockierungsrate bei ungerichteten Angriffen. Wenn Betrüger eine große Anzahl von Massenspam-Mails versenden, um möglichst viele Menschen zu erreichen, werden diese E-Mails häufig von Spamfiltern erkannt und blockiert. Spamfilter verwenden verschiedene Kriterien, um unerwünschte E-Mails zu identifizieren, wie zum Beispiel die Reputation des Absenders oder die Anzahl der von diesem Absender in kurzer Zeit versendeten Nachrichten. Da Massenspam-Mails oft dieselben Merkmale aufweisen und in großer Anzahl versendet werden, steigt die Wahrscheinlichkeit, dass sie von Spamfiltern erkannt und aussortiert werden. Dies führt dazu, dass die Wirksamkeit solcher Massenspam-Angriffe erheblich eingeschränkt wird (Jakobsson, 2016, S. 1-2).

Im Gegensatz dazu nutzen gezielt agierende Betrüger den Vorteil, Spamfilter effektiver zu umgehen. Indem sie ihre Bemühungen auf eine ausgewählte Gruppe von potenziellen Opfern konzentrieren, können sie personalisierte E-Mails senden, die weniger verdächtig wirken und somit weniger wahrscheinlich von Spamfiltern erkannt werden. Gezielt agierende Betrüger investieren Zeit und Mühe in die Recherche ihrer Opfer, um deren Interessen, Hobbys, Hintergrundinformationen oder sogar persönliche Beziehungen zu verstehen. Dadurch können sie E-Mails verfassen, die individuell angepasst sind und den Eindruck erwecken, von einer vertrauenswürdigen Quelle zu stammen. Durch diese personalisierten Ansätze können gezielt agierende Betrüger die Aufmerksamkeit und das Vertrauen der potenziellen Opfer effektiver gewinnen.

Ein weiterer Aspekt, der die Effektivität gezielter Scams erhöht, ist die psychologische Manipulation. Gezielt agierende Betrüger nutzen geschickt menschliche Emotionen wie Vertrauen, Sehnsucht nach Liebe oder den Wunsch nach finanzieller Sicherheit aus, um ihre Opfer zu täuschen. Sie geben vor, eine enge Beziehung oder Liebe zu entwickeln, um eine emotionale Bindung herzustellen und das Vertrauen der Opfer zu gewinnen. Diese manipulative Vorgehensweise kann dazu führen, dass die Opfer ihre kritische Denkfähigkeit einschränken und weniger misstrauisch werden, da sie glauben, eine authentische Beziehung aufzubauen.

3. Love Scam

Der Love Scam oder Romance Scam ist eine Betrugsvariante, die im Bereich des Online-Datings stattfindet. Menschen werden über Online-Datingseiten oder soziale Medien zum Ziel der Scammer. Die Online-Beziehung entwickelt sich schnell weiter, da der Scammer seinem potenziellen Opfer sehr viel Zeit und Aufmerksamkeit widmet. Durch vorgeblich ähnliche Lebensziele, Interessen und Hobbys entwickelt sich schnell eine enge Bindung. Die Persona, die dabei von den Scammern angenommen wird, ist bei weiblichen Opfern häufig ein Militärzugehöriger, Arzt oder Verkäufer, häufig verwitwet und alleinerziehend. Bei männlichen Opfern ist die Persona häufig eine junge, hilfsbedürftige Frau. (Dove, 2021)

Der grundsätzliche Ablauf bewegt sich stets in diesem Muster:

1. **Phase – Mr/Ms Perfect**
   In gefälschten Profilen mit attraktiven, meist gestohlenen Fotos stellt sich der Scammer als der perfekte Partner dar. Meist schreibt der*die Scammer*in das potenzielle Opfer an. In dieser Phase widmen sich die Täter*innen intensiv ihrem Gegenüber. Der Täter oder die Täterin gesteht der betroffenen Person rasch seine bzw. ihre Liebe, es findet ein regelrechtes „Love Bombing“[2] statt.
2. **Phase – Beziehung**
   Die Beziehung intensiviert sich in dieser Zeit, findet aber nach wie vor rein online statt. Auch (Video-)Telefonate können dabei stattfinden, der*die Scammer*in verwendet dazu beispielsweise im Internet verfügbare Videoausschnitte und erklärt die mögliche Gespräch-Bild-Schere mit schlechter Übertragungsqualität. In dieser Phase kündigt der*die Täter*in einen persönlichen Besuch an.
3. **Phase – Katastrophe**
   Der versprochene Besuch wird angekündigt, doch eine Katastrophe droht diesen zu verhindern: Das Militär genehmigt den Urlaub nicht, bei der Durchreise in einem anderen Land wird die Persona des Scammers vorgeblich verhaftet, ein vermeintlicher Unfall ereignet sich, … Die Konsequenz bleibt immer gleich: Der*die Täter*in benötigt dringend Geld.
4. **Phase – Dauerschleife**
   Die so vielversprechend begonnene Beziehung bleibt stetig in Gefahr. Krankheiten, Schulden oder Verhaftungen bedrohen konstant das Liebesglück. Und stets ist die einzige Lösung der Misere die Bezahlung oft hoher Summen durch den*die Betroffene*n.
5. **Phase – Verbrannte Erde**
   Kann das Betrugsopfer irgendwann nicht mehr zahlen, verschwindet der Scammer. Die Online-Profile werden gelöscht, und die Handynummer führt plötzlich ins Leere.

   Auch wenn der Romance Scam immer auf ähnliche Weise abläuft, finden Variationen innerhalb dieses Musters statt. Oft verschwindet der*die Scammer*in nicht einfach,

[2] Love Bombing: Als Love Bombing (Kompositum aus englisch love und bombing, deutsch: ‚Liebesbombardement‘, in diesem Zusammenhang aber auch im Deutschen Love Bombing genannt) wird eine Methode bezeichnet, die oft beim Dating angewandt wird, häufig mit psychischer Manipulation einhergeht und zu emotionalem Missbrauch führen kann. Der sogenannte Love Bomber überschüttet seine Partnerin bzw. seinen Partner oft schon kurze Zeit nach dem ersten Kennenlernen mit Liebesbekundungen oder Geschenken, mit dem Ziel, die andere Person an sich zu binden sowie Kontrolle und Macht über die Person zu bekommen. (Wikipedia, 2022)

sondern das Opfer wird bedroht. Manchmal verwenden die Täter auch die Konten ihrer Opfer zur Geldwäsche. (Geld wird auf ihr Konto überwiesen, der*die Täter*in bittet die betroffene Person, diese Geldsumme auf ein anderes Konto weiter zu überweisen).

3.1. Typische Szenarien für den Online-Liebesbetrug

Klassische Beispiele für Love Scams umfassen verschiedene Situationen, in denen Betrüger*innen gefälschte Identitäten annehmen, um das Vertrauen und die Zuneigung ihrer Opfer zu gewinnen. Hier sind einige typische Szenarien:

Der "ausländische Soldat": In diesem Fall gibt sich der Betrüger als Soldat aus, der angeblich im Ausland stationiert ist. Er knüpft online Kontakt zu potenziellen Opfern, meist über Dating-Plattformen, und entwickelt eine romantische Beziehung. Der Betrüger behauptet, in Gefahr zu sein oder finanzielle Schwierigkeiten zu haben und bittet das Opfer um Geld für vermeintliche Notfälle, medizinische Kosten oder Flugtickets, um sich mit dem Opfer zu treffen. Oft verwenden diese Betrüger gestohlene Fotos echter Soldaten, um ihre Geschichte zu unterstützen.

Der/die "Witwer/Witwe": Hier gibt sich der Betrüger als verwitwete Person aus, die nach Liebe und Trost sucht. Er knüpft Kontakt zu einsamen Menschen, insbesondere älteren Singles, und spielt eine einfühlsame Rolle. Der Betrüger gewinnt das Vertrauen des Opfers und behauptet schließlich, dringende finanzielle Probleme zu haben, wie zum Beispiel hohe Schulden oder medizinische Kosten für sich oder ein erfundenes Familienmitglied. Das Opfer wird gebeten, Geld zu leihen oder zu überweisen, um die vermeintlichen Notlagen zu bewältigen.

Der "Online-Liebhaber": In diesem Szenario gibt sich der Betrüger als attraktive Person aus und entwickelt über Online-Plattformen oder soziale Medien eine romantische Beziehung zum Opfer. Der Betrüger investiert Zeit und Mühe, um eine emotionale Bindung aufzubauen, und gewinnt so das Vertrauen des Opfers. Nach einer gewissen Zeit bittet der Betrüger das Opfer um Geld, angeblich für Reisekosten, medizinische Behandlungen oder andere dringende Ausgaben. Oft behaupten diese Betrüger, dass sie das Geld benötigen, um sich endlich mit dem Opfer zu treffen.

Der "Lotto-Gewinner": In diesem Fall gibt sich der Betrüger als glücklicher Lotto-Gewinner aus und kontaktiert das potenzielle Opfer, um ihm mitzuteilen, dass er in einem Gewinnspiel eine hohe Summe gewonnen hat. Der Betrüger behauptet, dass er aus altruistischen Gründen einen Teil des Geldes mit dem Opfer teilen möchte, aber vorher bestimmte Gebühren oder Auslagen beglichen werden müssen. Das Opfer wird gebeten, Geld zu überweisen, um angebliche Steuern, Bearbeitungsgebühren oder Anwaltskosten zu decken. Letztendlich gibt es jedoch keinen echten Lottogewinn, und das Opfer verliert das überwiesene Geld.

3.2. Die Tricks der Täter

Die Täter beim Liebesbetrug im Internet verwenden verschiedene Tricks, um ihre Opfer zu täuschen und auszunutzen. Unter anderem werden folgende Tricks verwendet:

1. **Falsche Identität:** Die Betrüger erstellen gefälschte Profile und Identitäten, die attraktiv und glaubwürdig wirken sollen. Sie verwenden gestohlene Fotos oder Bilder von anderen Personen, um ihre erfundene Identität zu unterstützen. Sie können auch gefälschte Namen, Berufe, Wohnorte und Lebensgeschichten verwenden, um ihre Opfer zu täuschen.
2. **Liebe und Romantik:** Die Täter spielen die Rolle des perfekten Partners, der alles sagt und tut, um die Gefühle des Opfers zu gewinnen. Sie verwenden romantische und liebevolle Worte, um eine starke emotionale Bindung herzustellen. Sie geben vor, tiefe Gefühle für das Opfer zu haben und stellen eine intensive Beziehung her, um das Vertrauen des Opfers zu gewinnen.
3. **Schnelle Entwicklung der Beziehung:** Die Betrüger drängen darauf, die Beziehung schnell voranzutreiben. Sie investieren viel Zeit und Aufmerksamkeit, um eine enge Bindung herzustellen und das Opfer dazu zu bringen, sich verliebt zu fühlen. Sie nutzen oft romantische und sentimentale Gesten, um die Beziehung zu intensivieren.
4. **Finanzielle Notlage:** Die Täter nutzen oft finanzielle Notlagen als Vorwand, um Geld von ihren Opfern zu verlangen. Sie können behaupten, dass sie in Schwierigkeiten stecken, medizinische Behandlungen benötigen oder Schulden haben. Sie bitten das Opfer um Geld, angeblich um ihre Probleme zu lösen, und appellieren an das Mitgefühl des Opfers.
5. **Druck und Erpressung:** Einige Betrüger wenden Druck und Erpressungstaktiken an, um ihre Opfer zur Zusammenarbeit zu zwingen. Sie drohen beispielsweise damit, die Beziehung zu beenden, wenn das Opfer nicht nachgibt oder kein Geld gibt. Sie können auch damit drohen, intime Fotos oder Nachrichten zu veröffentlichen, um das Opfer einzuschüchtern.
6. **Geheimhaltung:** Die Täter fordern oft ihre Opfer auf, die Beziehung geheim zu halten und niemandem davon zu erzählen. Sie versuchen, das Opfer zu isolieren und zu verhindern, dass es Hilfe von anderen Personen sucht oder Rat einholt. Dadurch können sie ihre betrügerischen Aktivitäten länger fortsetzen, ohne entdeckt zu werden.

Diese Tricks der Täter beim Liebesbetrug dienen dazu, das Vertrauen und die Emotionalität ihrer Opfer auszunutzen. Es ist wichtig, sich dieser Taktiken bewusst zu sein und skeptisch zu bleiben, wenn man online neue Beziehungen eingeht. Wenn etwas zu schön erscheint, um wahr zu sein, ist es möglicherweise ein Indiz für einen Betrug.

3.3. Die psychologischen Aspekte des Liebesbetrugs

Um ihre Opfer an sich zu binden, nutzen die Täter verschiedene Mechanismen, die einerseits den emotionalen Status ausnützen, andererseits eine scheinbar enge Bindung zwischen Täter und Betroffenen erschaffen.

Menschen, die sich in einer emotionalen oder einsamen Situation befinden, sind anfälliger für Liebesbetrug. Betrüger nutzen dies aus, indem sie eine romantische Beziehung vortäuschen und die Sehnsucht des Opfers nach Liebe und Zuneigung ansprechen. Sie bieten emotionale Unterstützung, Komplimente und Aufmerksamkeit, um eine enge Bindung herzustellen.

Betrüger geben sich große Mühe, Vertrauen aufzubauen. Sie erschaffen gefälschte Identitäten und Geschichten, die glaubwürdig wirken sollen. Sie können gestohlene Fotos verwenden, um ihre erfundene Persönlichkeit zu untermauern. Indem sie sich als aufrichtig, fürsorglich und vertrauenswürdig darstellen, gewinnen sie das Vertrauen der Opfer.

Betrüger nutzen oft Taktiken des emotionalen Drucks, um ihre Opfer gefügig zu machen. Sie können beispielsweise behaupten, dass sie ohne finanzielle Unterstützung in Gefahr sind oder dass ihre Liebe und Beziehung gefährdet ist, wenn das Opfer nicht nachgibt. Durch die Schaffung einer emotionalen Abhängigkeit versuchen sie, das Opfer unter Kontrolle zu halten und es dazu zu bringen, Geld oder andere Ressourcen bereitzustellen.

Opfer von Love Scams schämen sich meist, über ihre leidvollen Erfahrungen zu sprechen. Die Täter nutzen dies aus, indem sie ihre Opfer dazu bringen, ihre Beziehung geheim zu halten und niemandem davon zu erzählen. Indem sie ein Klima der Scham schaffen, versuchen sie, das Opfer zu isolieren und zu verhindern, dass es Hilfe sucht oder andere Personen um Rat fragt.

Betrüger können ihren Opfern das Gefühl geben, etwas Besonderes und Einzigartiges zu sein. Sie behaupten oft, dass sie nur mit dem Opfer eine außergewöhnliche Verbindung haben und dass ihre Beziehung etwas Einmaliges ist. Dies verstärkt das Gefühl des Opfers, etwas Besonderes gefunden zu haben, und macht es weniger misstrauisch gegenüber den betrügerischen Absichten.

3.4. Experteninterview Birgit Wohler

Der vorliegende Text basiert auf einem Interview mit Birgit Wohler, einer Expertin und Unterstützerin von Romance-Scam-Betroffenen. Der Fokus des Interviews lag auf den wichtigsten Erkenntnissen bezüglich des Romance Scams, einschließlich der Mechanismen des Betrugs, der Profilerstellung der Täterinnen und Täter sowie der Auswirkungen auf die Opfer.

Birgit Wohler kam erstmals mit dem Thema Romance Scam in Berührung, als sie auf einer Online-Partnerbörse von einem vermeintlichen Autohändler aus Irland angeschrieben wurde, der tatsächlich die gestohlene Identität eines Freundes annahm. Als Reaktion darauf hat sie eine geschlossene Facebook-Gruppe für Betroffene gegründet und betreibt nun auch eine öffentliche Seite zur Aufklärung über Romance Scam.

Romance-Scam-Betroffene lassen sich nicht einheitlich beschreiben, jedoch leiden viele von ihnen unter Einsamkeit. Der Betrug verläuft typischerweise in mehreren Phasen. Die Täterinnen und Täter nehmen Kontakt zu potenziellen Opfern auf und stellen ihnen viele Fragen, um eine leichtere Beeinflussung zu ermöglichen. Nach kurzer Zeit beginnen sie mit intensiven Liebesbekundungen ("Love Bombing"). Sobald das Vertrauen aufgebaut ist, bitten sie die Opfer um finanzielle Unterstützung in vermeintlichen Notlagen.

Jede*r kann zum Opfer von Romance Scam werden, unabhängig von Alter oder sozialem Hintergrund. Die Täterinnen und Täter präsentieren sich in verschiedenen Rollen wie Soldat*in, Chirurg*in oder Ingenieur*in auf einer Bohrinsel. Eine gemeinsame Taktik besteht darin, die Geschichte eines verstorbenen Partners und eines zurückgelassenen Kindes zu verwenden, das von einer Nanny oder in einem Internat betreut wird. Die Täterinnen und Täter nutzen gezielte Fragen und Informationen aus den Profilen der Opfer, um eine vertraute Beziehung aufzubauen.

Die Opfer lösen sich aus dem Betrug, indem sie Ungereimtheiten und Widersprüche bemerken oder zufällig die wahre Identität der Täterinnen und Täter entdecken. Misstrauen kann auch durch das Einwirken von Familienangehörigen oder Freunden entstehen. Opfer geraten in den Betrug, da sie oft einsam sind und sich nach einer Beziehung sehnen. Die Täterinnen und Täter verwenden raffinierte Taktiken und vorgefertigte Texte, um die Echtheit ihrer Gefühle vorzutäuschen.

Birgit Wohler unterstützt Betroffene, indem sie ihnen zuhört und bei Bedarf bei der Suche nach Beweisen und professioneller Hilfe wie Schuldnerberatung oder psychologischer Betreuung hilft. Besonders häufig wenden sich Familienmitglieder an Frau Wohler, die Beweise für ihren Verdacht brauchen, dass jemand Opfer eines Scams geworden ist. Im Rahmen ihrer Hilfstätigkeit rät Frau Wohler stets dazu, dass Familienangehörige keine Vorwürfe machen, sondern zuhören und Unterstützung bei der Suche nach Hilfe bieten sollten, beispielsweise durch den Kontakt mit Organisationen wie dem "Weißen Ring".

Leider erstattet nur etwa jede*r dritte bis vierte Betroffene eine Anzeige bei der Polizei. Die Erfahrungen mit den Behörden variieren. Einige Polizeireviere verfügen über eine spezialisierte Abteilung für Cyberkriminalität, wo es für Betroffene einfacher ist, eine Anzeige zu machen. Bei anderen, oft kleineren Revieren wie z.B. in einer Kleinstadt oder in einem Dorf stößt der*die Betroffene leider häufig auf Unverständnis.

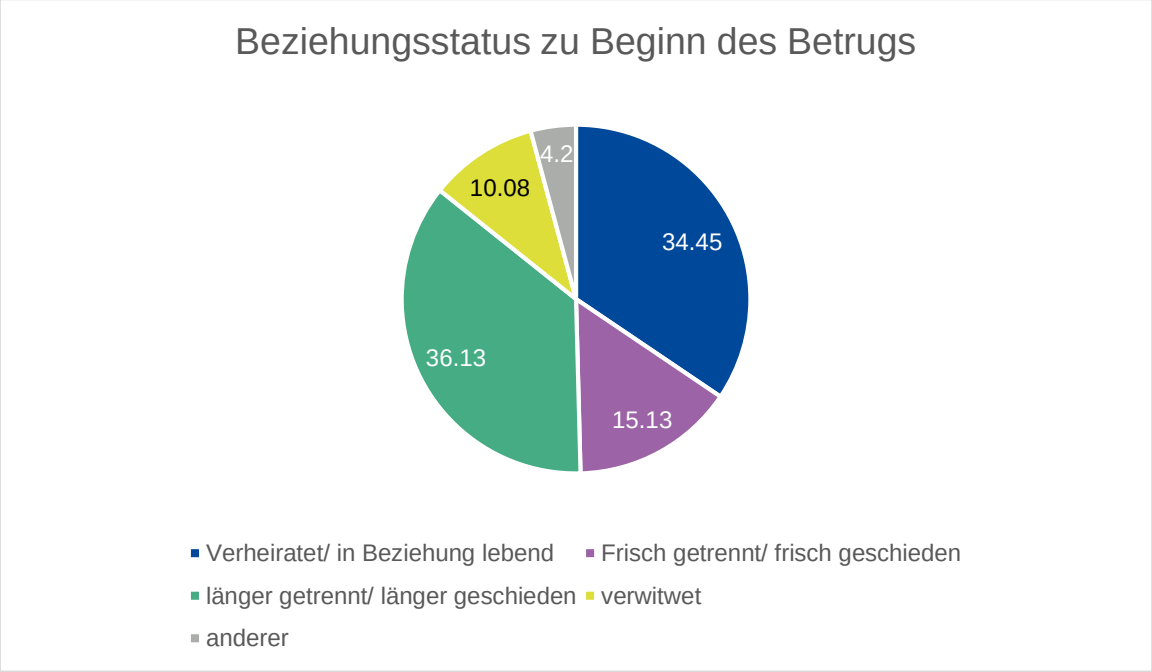
Die dramatischen Konsequenzen dieses Betrugs sind Vertrauensverlust, Depression und Armut bis hin zum Suizid. Gerade aufgrund dieser gravierenden Konsequenzen würde sich Frau Wohler eine verstärkte Aufklärung via Presse, Internet und TV (ev. auch Radiospots) wünschen.

4. Ergebnisse

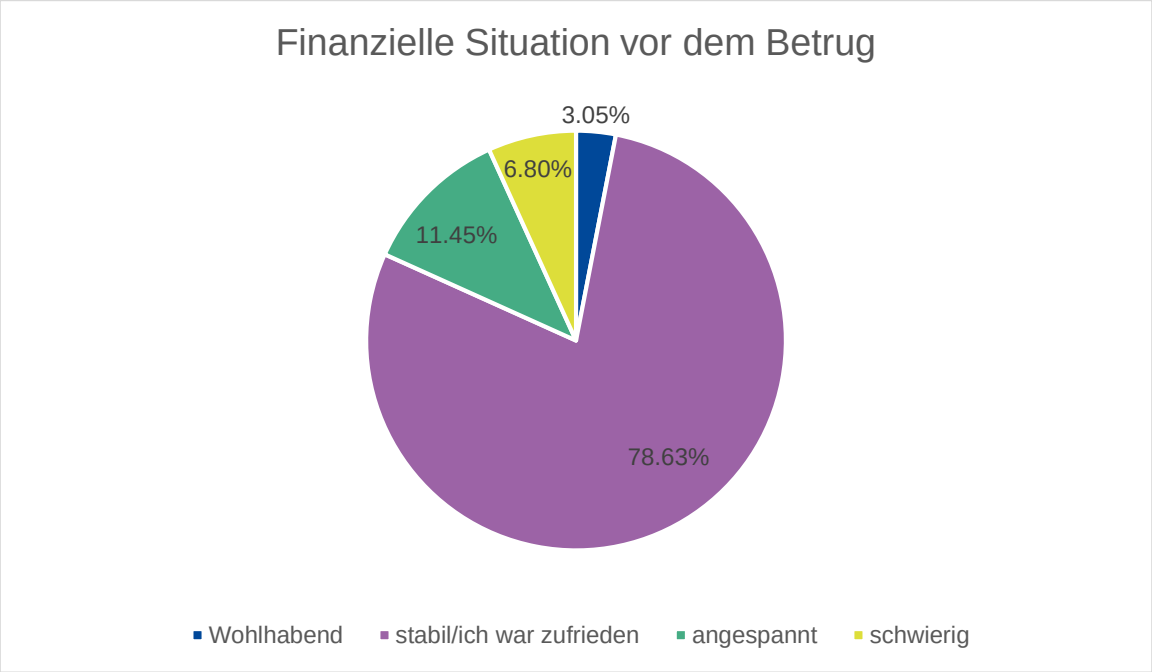
4.1. Betroffenenstudie

Persönliche Situation der Betroffenen

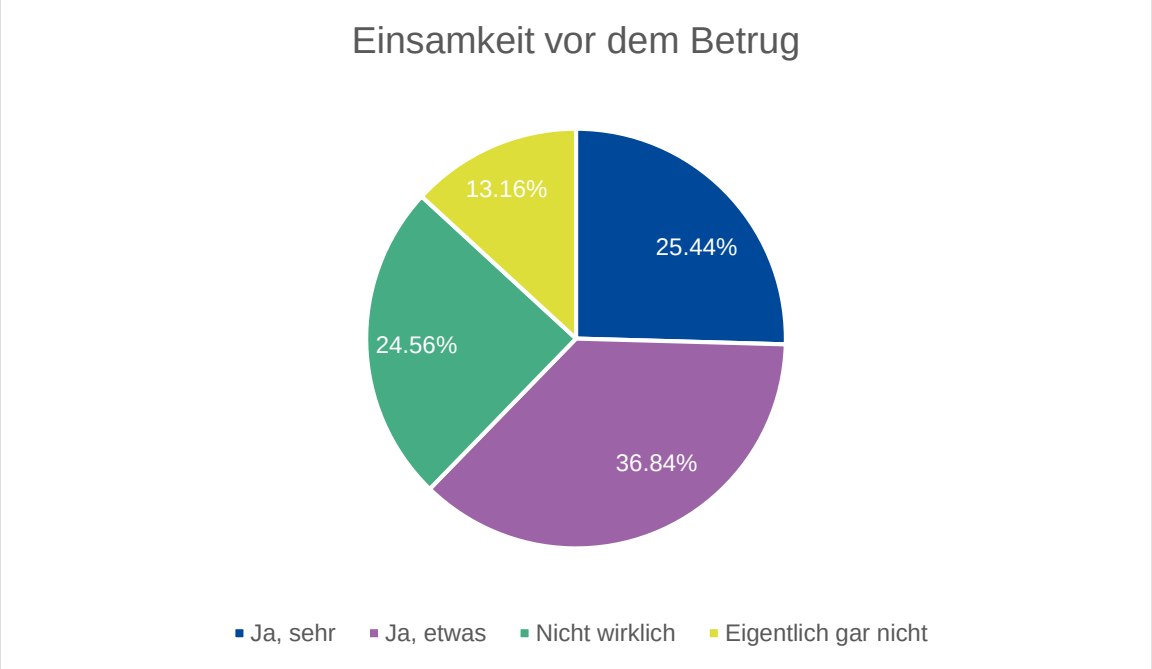
Die vom KFV durchgeführte Betroffenenstudie, die primär in Selbsthilfegruppen auf Facebook und in Foren geteilt wurde, zeigt in auffälliger Weise: Die Betroffenen waren zu 96 % weiblich. 70 % der Befragten haben ein oder mehrere Kinder, dennoch lebte die Mehrheit zur Zeit des Romance Scams allein (54 %).



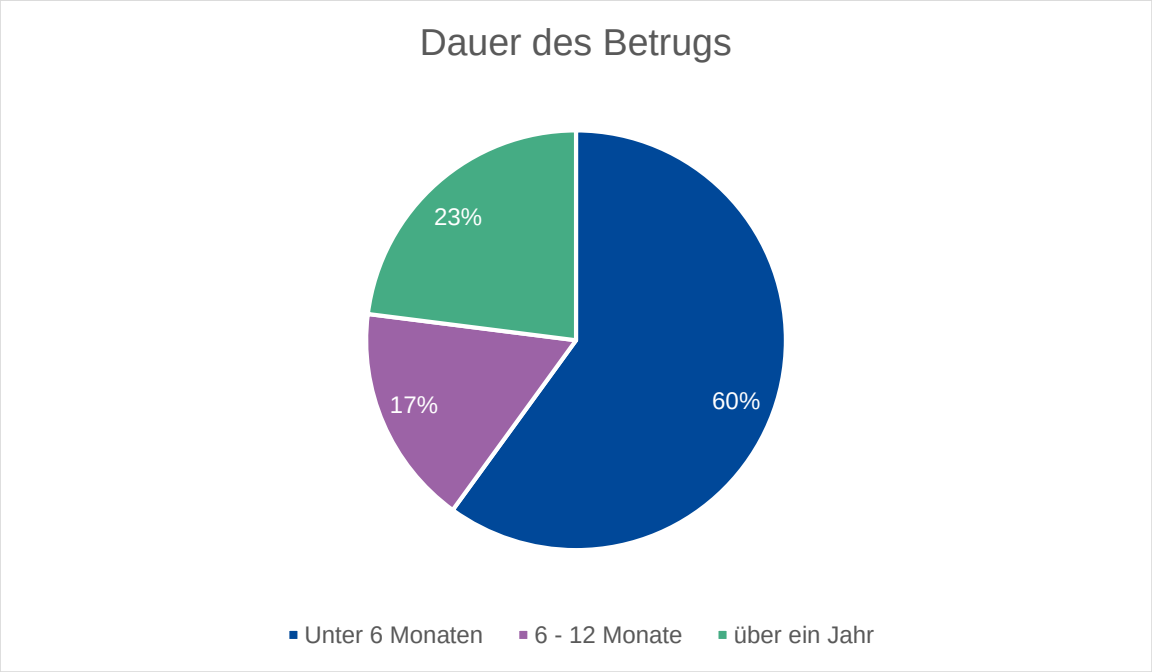
Mit 36 Prozent waren auffällig viele Betroffene zu Beginn des Betrugs in einer Beziehung. Ein ähnliches Bild zeigt die Frage, ob die Betrugsopfer aktiv auf Partnersuche waren. Knapp 75 % der Betroffenen waren nicht aktiv auf der Suche nach einem neuen Lebenspartner, dies galt nur für ein Viertel.



Die finanzielle Situation der Betroffenen wurde mehrheitlich als „stabil/ich war zufrieden“ beschrieben.

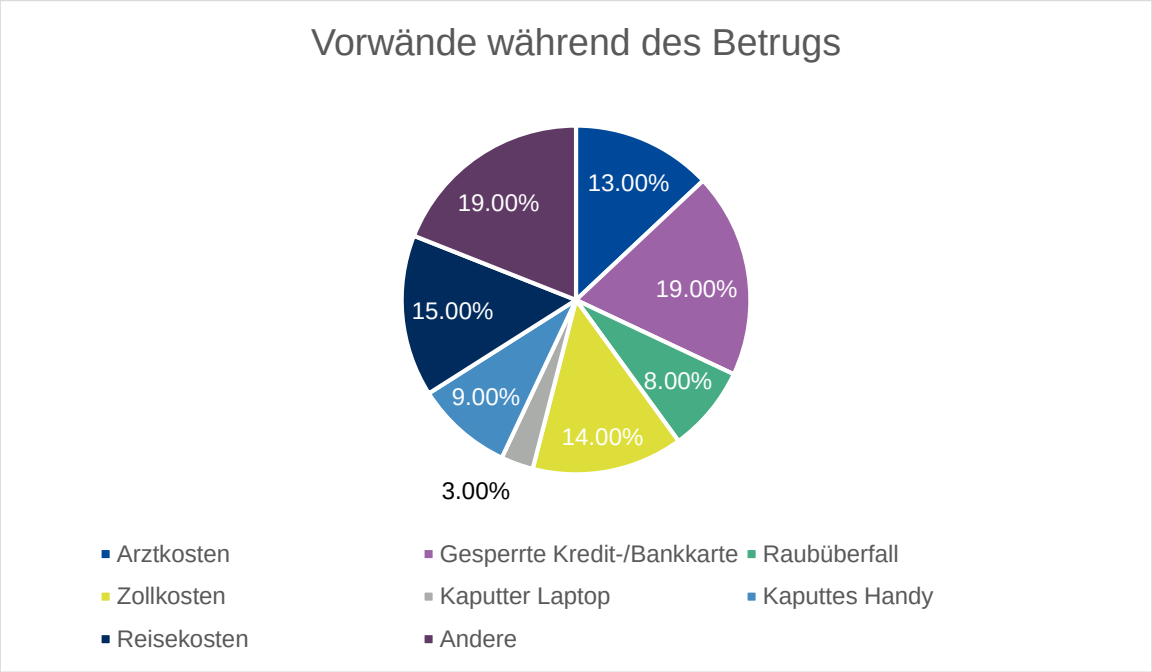


Mehr als die Hälfte der Betroffenen gaben in der Befragung an, dass sie sich vor dem Betrug einsam gefühlt hätten (62 %).



Etwa 60 % der Betroffenen gaben an, dass der Betrug weniger als 6 Monate andauerte. Bei rund 17 % der Betroffenen erstreckte sich der Betrug über einen Zeitraum von 6 bis 12 Monaten, während bei etwa 23 % der Opfer der Betrug länger als ein Jahr andauerte.

Diese Ergebnisse zeigen, dass es beträchtliche Variationen in der Dauer des Romance Scams gibt. Während die Mehrheit der Betroffenen innerhalb weniger Monate Opfer des Betrugs wurde, gab es auch eine signifikante Anzahl von Opfern, bei denen der Betrug über einen längeren Zeitraum hinweg stattfand. Dies deutet darauf hin, dass es keine einheitliche Zeitspanne gibt, in der Menschen dem Romance Scam zum Opfer fallen, sondern dass dies von verschiedenen individuellen Faktoren abhängt.



Es zeigt sich, dass die Betrüger in Liebesbetrugsfällen eine Vielzahl von Vorwänden nutzen, um Betroffene dazu zu bringen, Geld zur Verfügung zu stellen. Von den untersuchten Fällen gaben 13 % der Betroffenen an, dass der Täter Arztkosten als Grund nannte, um finanzielle Unterstützung zu erbitten. Dies deutet darauf hin, dass die Täter die problematische Gesundheitssituation vortäuschten, um Mitgefühl und finanzielle Hilfe zu erlangen.

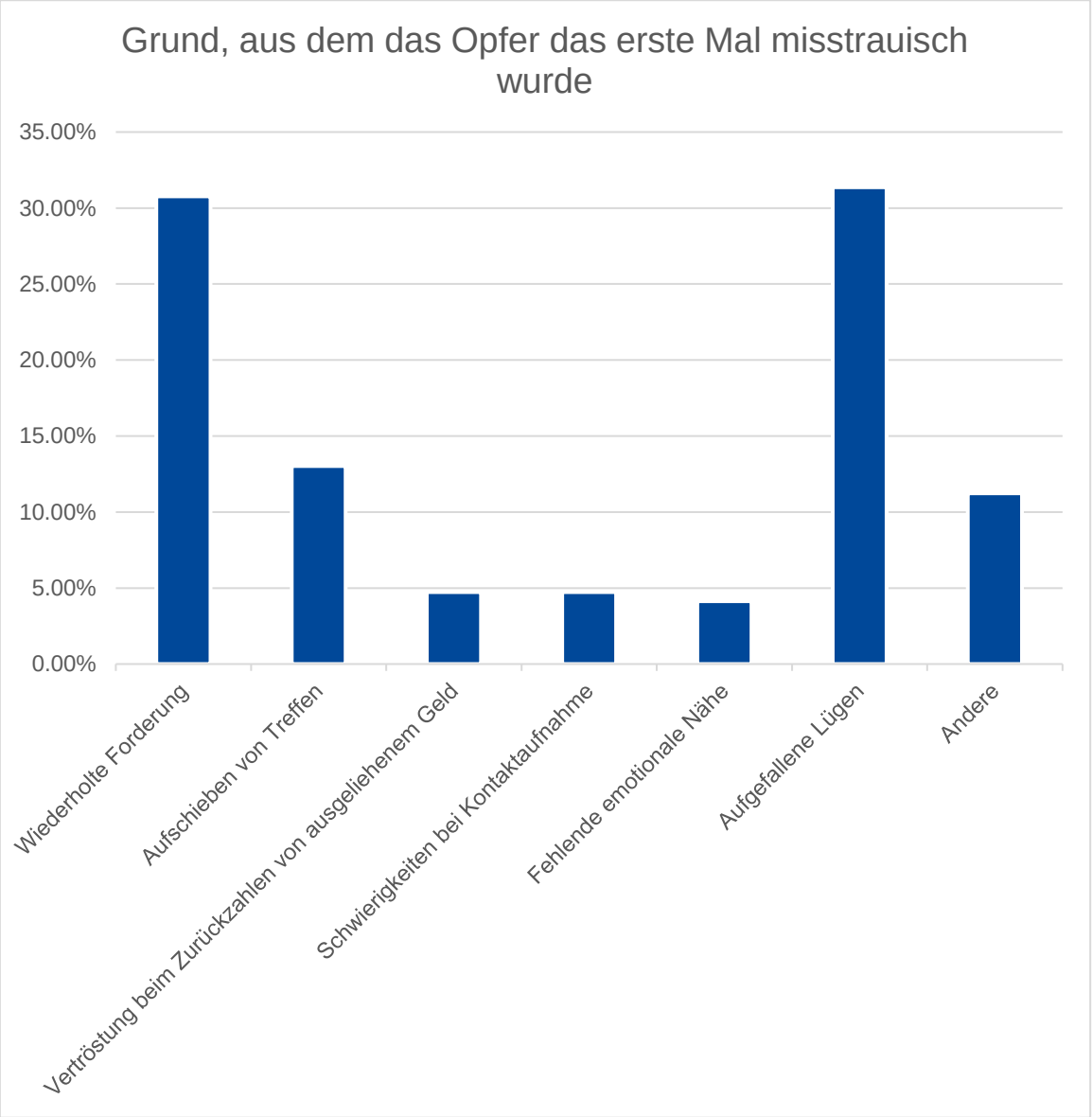
Weitere 19 % der Betroffenen berichteten, dass der Täter vorgab, eine gesperrte Kredit- oder Bankkarte zu haben. Dieses Szenario wurde verwendet, um die Dringlichkeit der Geldanfrage zu betonen und die Betroffenen dazu zu bringen, finanzielle Hilfe für den angeblichen Zugriff auf ihr Konto bereitzustellen.

Ein weiterer häufig verwendeter Vorwand war ein Raubüberfall, der bei 8 % der Betroffenen genannt wurde. Die Täter gaben vor, Opfer eines Raubüberfalls geworden zu sein und baten um finanzielle Unterstützung, um gestohlene Wertgegenstände oder Ausweisdokumente zu ersetzen. Dieser Vorwand zielt darauf ab, das Mitgefühl der Betroffenen zu wecken und sie dazu zu bringen, finanzielle Hilfe anzubieten.

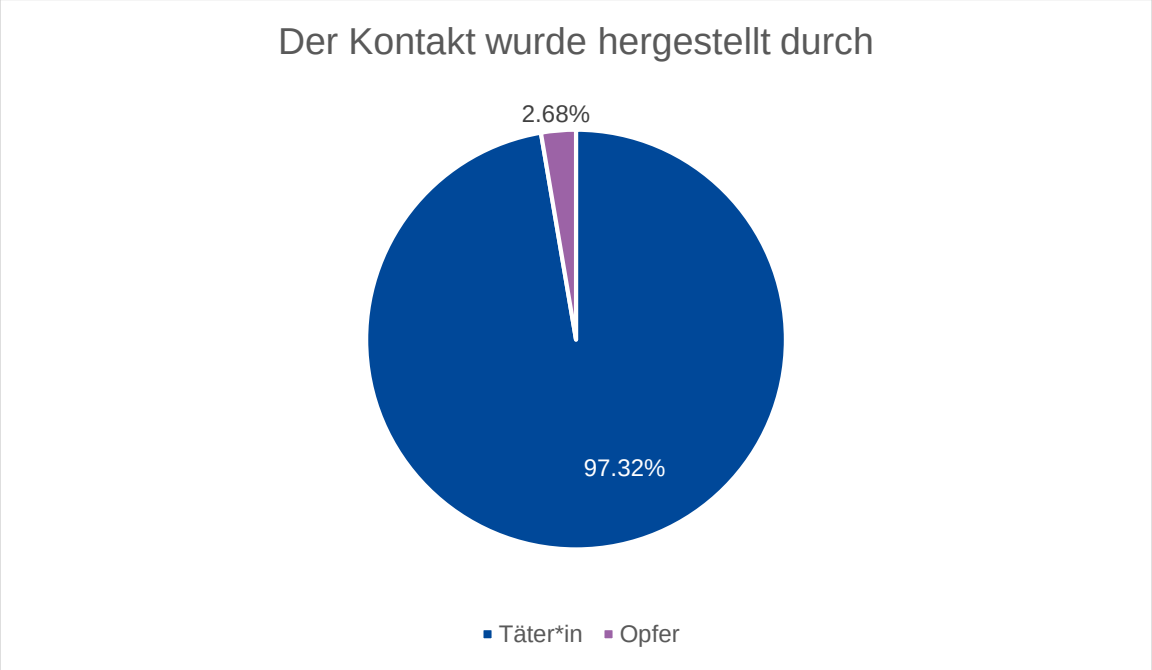
Zollkosten wurden von 14 % der Betroffenen als Vorwand angegeben. Die Täter behaupteten, dass ein Koffer mit Geld, Dokumenten oder anderen wertvollen Gegenständen an die Betroffenen gesendet wurde, aber am Zoll feststeckte. Um den Koffer freizugeben, wurden finanzielle Mittel von den Betroffenen verlangt. Dieser Vorwand diente dazu, die Betroffenen zu verunsichern und sie dazu zu bringen, Geld zur Lösung des angeblichen Problems bereitzustellen.

Weitere Vorwände, die von den Romance-Scam-Tätern verwendet wurden, waren ein kaputter Laptop (3 %), ein kaputtes Handy (9 %) und Reisekosten (15 %). Es ist anzumerken, dass 19 % der Betroffenen andere Vorwände angaben, die in dieser Studie nicht weiter spezifiziert wurden.

Dies unterstreicht die Vielfalt und Kreativität der Täter bei der Entwicklung von Vorwänden, um finanzielle Unterstützung von den Betroffenen zu erlangen.



Wiederholte Forderungen und aufgefallene Lügen sind die häufigsten Gründe, aus denen Betroffene erstmals auf den Betrug aufmerksam wurden. Auch das Aufschieben von Treffen machte Betroffene stutzig.

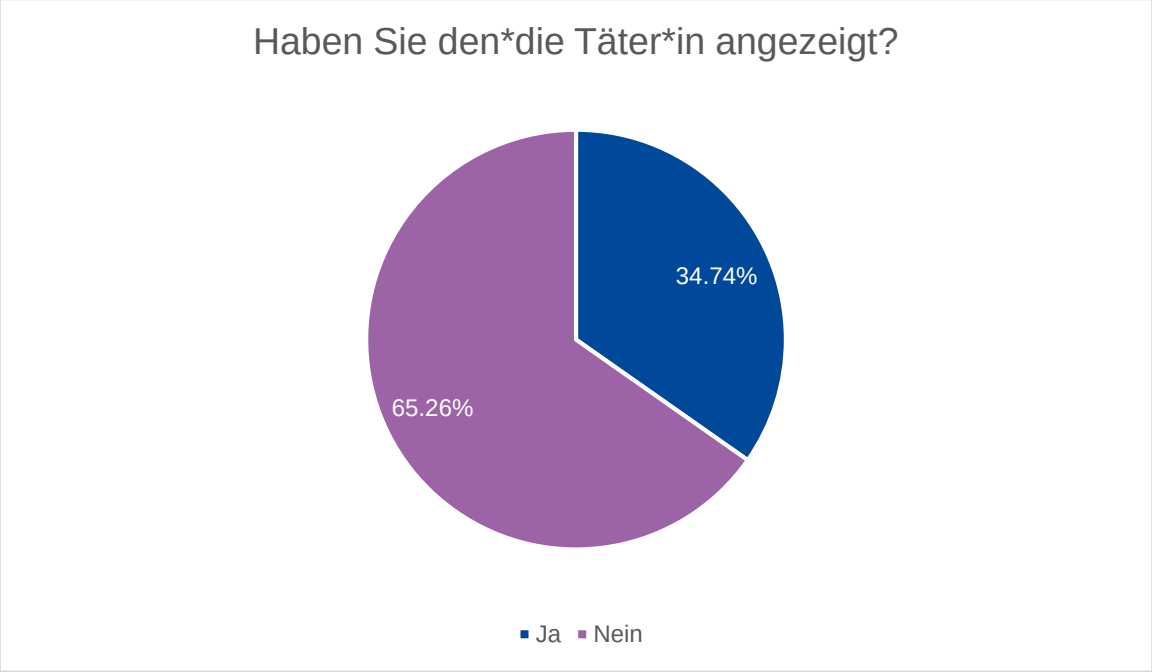


Die überwiegende Anzahl der Kontaktaufnahmen im Rahmen von Love Scams geht von den Tätern aus. Diese Tatsache lässt sich auf verschiedene Faktoren zurückführen und lässt einige Interpretationen zu: Die Täter von Love Scams sind in der Regel organisiert und professionell in ihrem Vorgehen. Sie setzen gezielte Strategien ein, um potenzielle Opfer zu identifizieren und anzusprechen. Durch den Einsatz von gefälschten Profilen, manipulativen Taktiken und emotionalen Ansprachen können sie das Interesse und die Aufmerksamkeit der potenziellen Opfer wecken.

Love-Scam-Täter*innen nutzen oft Situationen aus, in denen Menschen verletzlich sind oder nach emotionaler Verbundenheit und Liebe suchen. Sie zielen auf Menschen ab, die möglicherweise einsam sind, sich nach einer Beziehung sehnen oder durch persönliche Umstände wie Trennung, Verlust oder Unsicherheit emotional beeinflusst werden. Diese Menschen sind anfälliger für romantische Versprechungen und suchen aktiv nach Kontakten.

Das Internet und soziale Medien bieten den Tätern eine breite Plattform, um potenzielle Opfer zu erreichen. Sie können mühelos Profile erstellen, in Online-Communities und Dating-Plattformen agieren und so eine große Anzahl von Menschen erreichen. Durch ihre aktive Kontaktaufnahme können sie ihre Chancen erhöhen, auf jemanden zu stoßen, der anfällig für ihre Betrugsmasche ist.

Die Täter von Love Scams können ihre Identität leicht verschleiern und Distanz wahren, da sie oft in anderen Ländern operieren. Diese Anonymität ermöglicht es ihnen, ihre wahren Absichten zu verbergen und eine vertrauensvolle Beziehung aufzubauen, ohne persönliche Verantwortung übernehmen zu müssen.



Wie schon im Experteninterview mit Frau Wohler dargelegt wurde, zeigt sich eine besorgniserregende Tendenz bei den vom Online-Liebesbetrug Betroffenen, die Täter viel zu selten anzuzeigen. Diese Beobachtung wirft einige Fragen auf und erfordert eine vertiefte Analyse.

Ein möglicher Grund für die geringe Anzeigebereitschaft könnten Scham und das Stigma sein, das mit der Opferrolle im Falle von Love Scam einhergeht. Opfer könnten sich möglicherweise schuldig oder peinlich naiv fühlen, da sie auf die raffinierten Täuschungsmethoden der Betrüger*innen hereingefallen sind. Die Offenlegung dieses Vorfalls könnte mit einem Gefühl der Demütigung und dem Verlust des Selbstwertgefühls einhergehen. Dies kann dazu führen, dass sich die Betroffenen zurückziehen und aus Angst vor negativen Reaktionen aus ihrem sozialen Umfeld die Strafverfolgungsbehörden nicht einschalten.

Ein weiterer Grund könnte in der Hoffnung der Opfer liegen, dass sie das verlorene Geld oder die entstandenen Schäden auf anderem Wege wiedererlangen können. Dies könnte dazu führen, dass die Betroffenen den Vorfall nicht melden, in der Hoffnung, dass sich die Situation von selbst löst oder dass sie das Geld durch andere Mittel zurückerhalten. Diese Hoffnung auf eine unabhängige Lösung kann dazu führen, dass die Anzeige als eine mühsame und aussichtslose Option betrachtet wird.

Des Weiteren können die Erfahrungen der Betroffenen mit den Strafverfolgungsbehörden eine Rolle spielen. Wie Frau Wohler im Interview betont, sind die Erfahrungen der Opfer mit den Behörden unterschiedlich. Während einige Polizeireviere spezialisierte Abteilungen für Cyberkriminalität haben und die Betroffenen bei der Anzeigenerstattung umfassend unterstützen, kann es bei kleineren Revieren zu Unverständnis oder mangelnder Kompetenz im Umgang mit solchen Fällen kommen. Dies kann die Hemmschwelle erhöhen, eine Anzeige zu erstatten, da die Betroffenen möglicherweise Zweifel haben, dass ihre Situation angemessen behandelt wird.

4.2. Dunkelfeldstudie

4.2.1. Allgemeine Internetnutzung und Risikobewusstsein

Ganz gleich, ob zu Hause, in der Arbeit, bei Freunden oder unterwegs, das Internet hält in Österreich immer mehr Einzug in den Alltag. Der Zugang zur digitalen Welt wird fortlaufend erleichtert, sodass es kaum eine Bevölkerungsgruppe gibt, die noch nicht mit dem Internet in Berührung gekommen wäre. Die Nutzung erfolgt entweder über Standcomputer oder über mobiles Internet, z.B. am Smartphone, mit dem Laptop oder Tablet. Dementsprechend sind auch die Nutzungsmöglichkeiten sehr vielfältig.

4.2.2. Häufigkeit der Online-Aktivitäten

Das Internet wird von der österreichischen Bevölkerung pro Tag im Durchschnitt drei Stunden lang für private Zwecke genutzt, und zwar unabhängig davon, ob dies über PC, Tablet oder Handy geschieht.

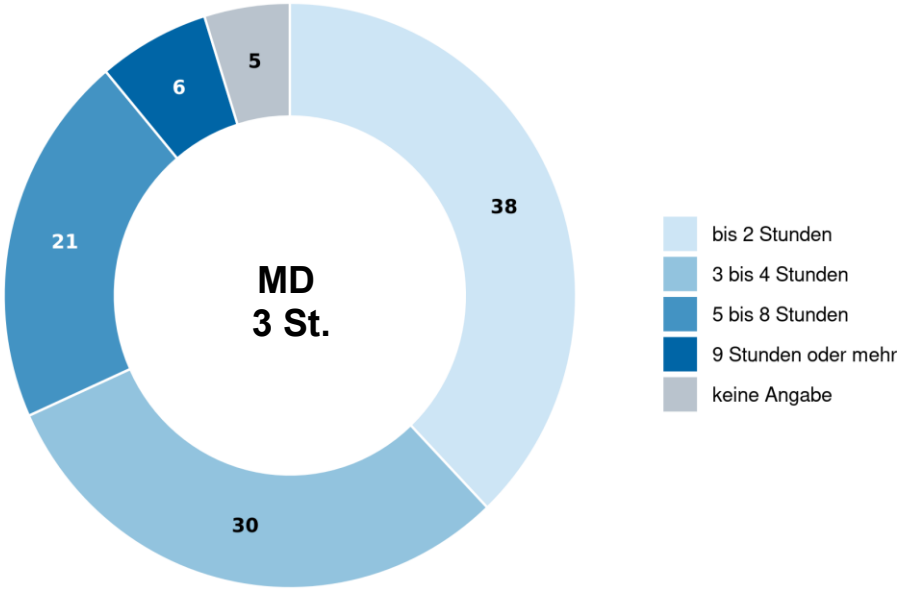


Abbildung 2: Durchschnittliche Internetnutzung pro Tag

Etwas mehr als ein Drittel der Befragten gab an, das Internet bis zu 2 Stunden am Tag für private Zwecke zu nutzen. Ein knappes Drittel bezifferte die tägliche private Verweildauer im digitalen Raum mit 3-4 Stunden, und mehr als ein Viertel der Bevölkerung verbringt privat sogar mehr als fünf Stunden pro Tag im World Wide Web.

Mit 77 % steht die Nutzung von Messenger-Diensten an der Spitze der (fast) täglichen Anwendungen, knapp gefolgt von E-Mails (70 %) und der Informationssuche (69 %). Soziale Netzwerke werden von 59 % der Österreicher*innen, Online-Dating-Plattformen von 5 % der Nutzer*innen hierzulande beinahe täglich genutzt. 4 % der Befragten sind mindestens einmal in der Woche auf digitalen Partnerbörsen unterwegs, 3 % tun dies mindestens einmal im Monat, und 5 % verkehren seltener als einmal im Monat auf Dating-Plattformen im Internet. Von den befragten Personen gaben 79 % an, noch nie eine Online-Partnerbörse besucht zu haben.

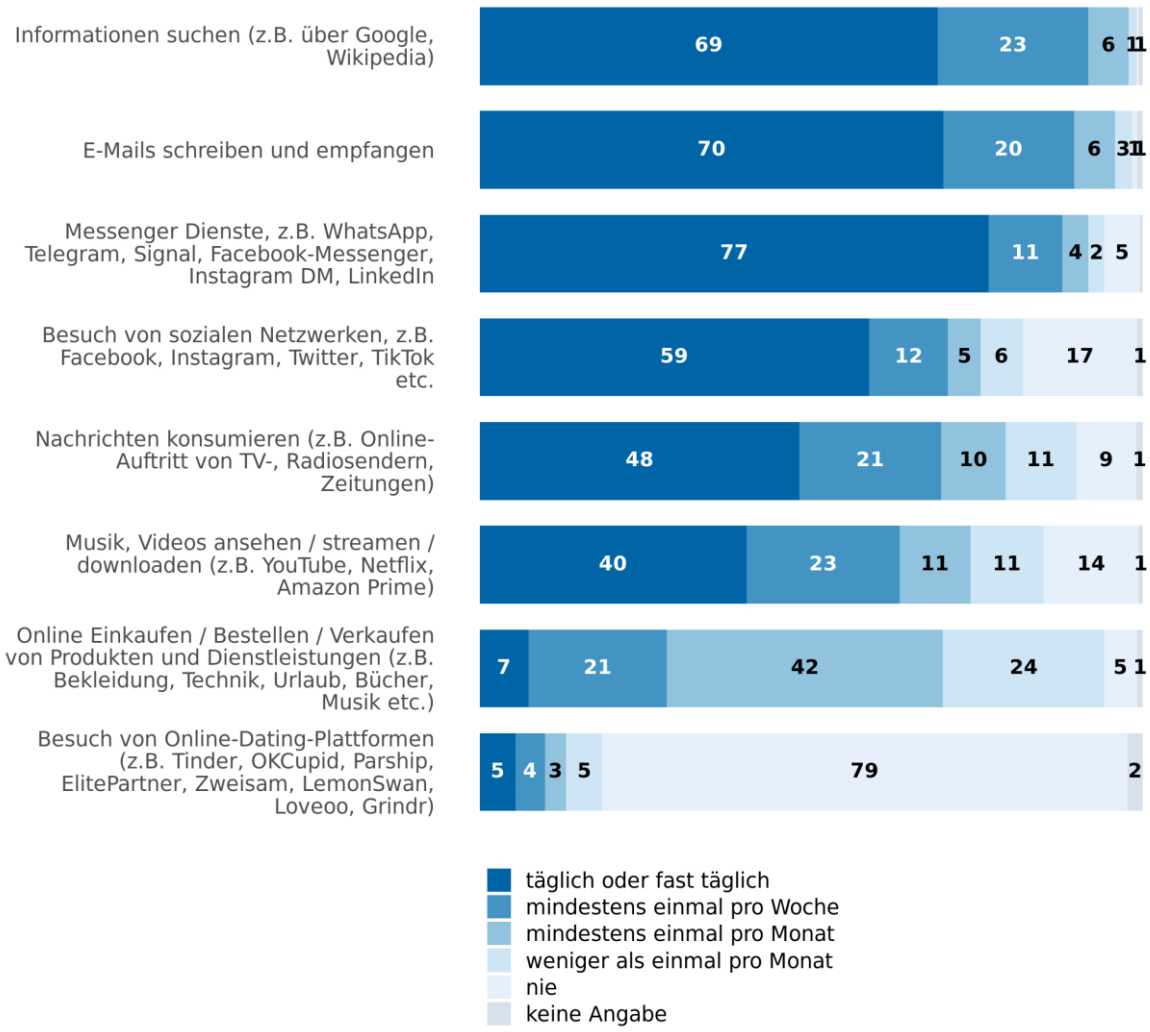


Abbildung 3: Häufigkeit der Online-Aktivitäten

4.2.3. Sicherheitsbedenken

Das Bewusstsein um mögliche Risiken im Zusammenhang mit der Internetnutzung scheint bei der mehrheitlichen Bevölkerung vorhanden zu sein. Lediglich 13-15 % der befragten Personen gaben an, sich wenige Sorgen zu machen, wenn es um Phishing, Hacking, die Auswertung von Nutzerdaten, Betrug bei Online-Einkäufen oder den Missbrauch von persönlichen Informationen im Internet geht. Für 5-6 % der Befragten gibt es gar keinen Grund, sich besorgt zu fühlen.

Abbildung 4: Sicherheitsbedenken unter Internetnutzern

Romance Scam wird im Vergleich zu anderen Deliktformen im Bereich Cybercrime weniger stark als Gefahr wahrgenommen. Während sich beispielsweise rund die Hälfte der Befragten im Hinblick auf Phishing (51 %) oder Hacking (49 %) (sehr) große Sorgen macht, sind es bei anderen Betrugsformen wie der Vortäuschung von lukrativen Aktiengeschäften, Erbschaften oder Liebesbeziehungen nur 32 %. Mit 42 % sticht die Anzahl jener Menschen signifikant heraus, die wenige oder keinerlei Bedenken im Zusammenhang mit dieser Art der Täuschungen im Onlinebereich hegen: 21 % der Interviewpartner*innen sind ganz und gar nicht bekümmert, ob sie Opfer in Folge von betrügerischen Geschäften oder Partnerschaften im Internet werden könnten. Weitere 21 % fühlen sich relativ sicher und machen sich wenige Sorgen hierzu.

Betrachtet man nun das Verhalten und die Einstellung der Internetnutzer*innen nach demografischen Merkmalen, so zeigt sich, dass junge Frauen im Alter von 17 bis 29 Jahren die meisten Sicherheitsbedenken haben (42 %), wenn es um die Vortäuschung einer Liebesbeziehung, angebliche Erbschaften oder den Betrug mit lukrativen Aktiengeschäften geht.

Das diesbezügliche Angstbefinden weiblicher Personen nimmt mit dem Alter der Frauen allerdings wieder ab. So sind es unter Frauen mittleren Alters nur noch 28 % und unter Frauen höheren Alters nur noch 23 %, die sich bezüglich derartiger Täuschungen im Internet Sorgen machen. Bei den männlichen Interviewpartnern zeigt sich ein umgekehrtes Bild. Als besonders arglos erweisen sich junge Männer unter 30 Jahren (29 %). Das Risikobewusstsein, möglicherweise Opfer solcher Täuschungen zu werden, nimmt bei Männern im Alter zu.

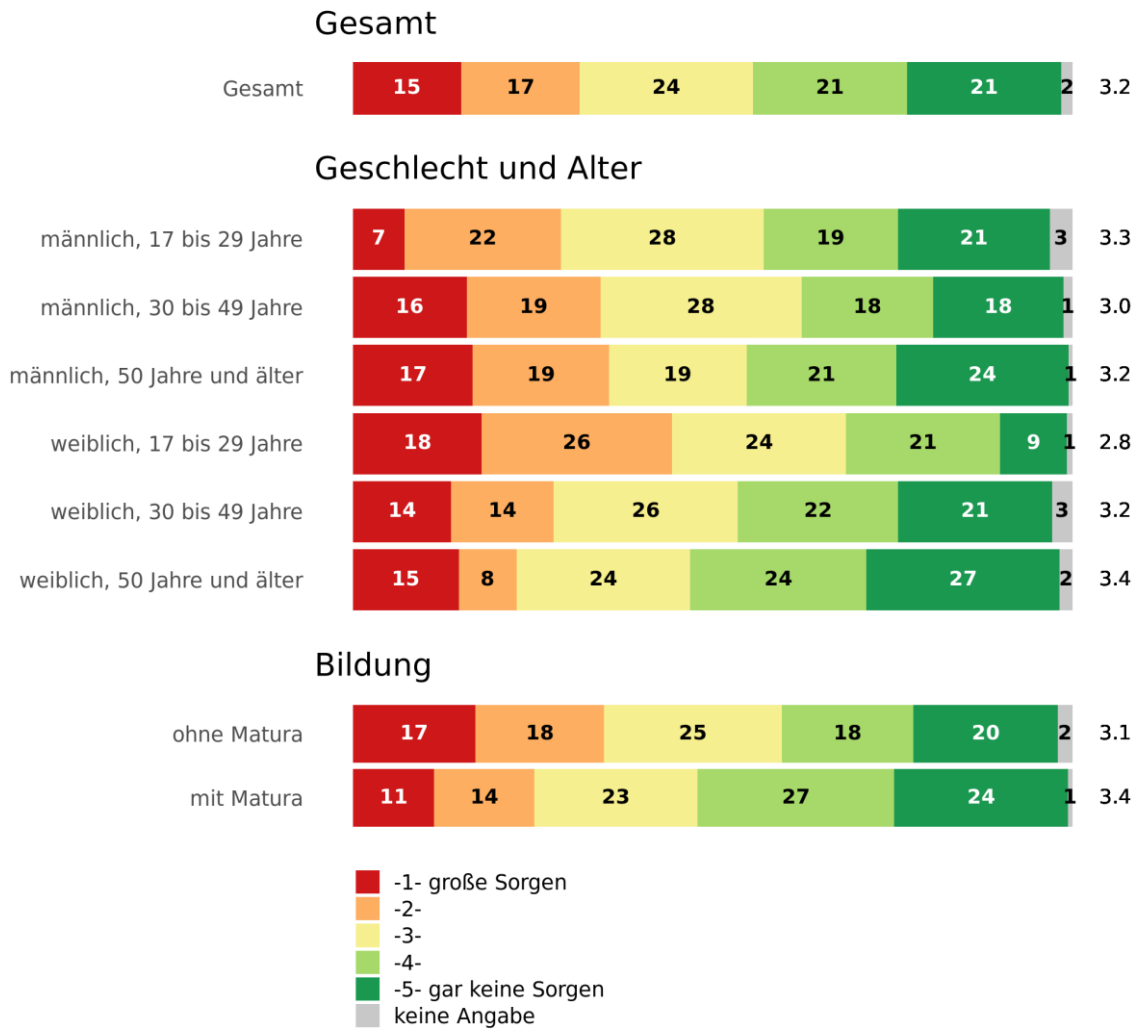


Abbildung 5: Sicherheitsbedenken nach Alter und Bildung

Interessant ist auch, dass ein höherer Bildungsgrad offenbar nicht mit einem höheren Risikobewusstsein einhergeht. Im Gegenteil, denn bei der Befragung zeigte sich, dass sich jene Interviewpartner, die die Matura erfolgreich abgelegt hatten, am wenigsten Sorgen machen, von Internetbetrügern getäuscht und geschädigt zu werden (11 %).

Der Summenindex zu den Sicherheitsbedenken im Umgang mit persönlichen elektronischen Daten im Internet zeigt, dass knapp ein Drittel der Bevölkerung (30 %) geringe Bedenken hat, wobei sich insbesondere junge Männer und ältere Frauen am wenigsten sorglos zeigen.

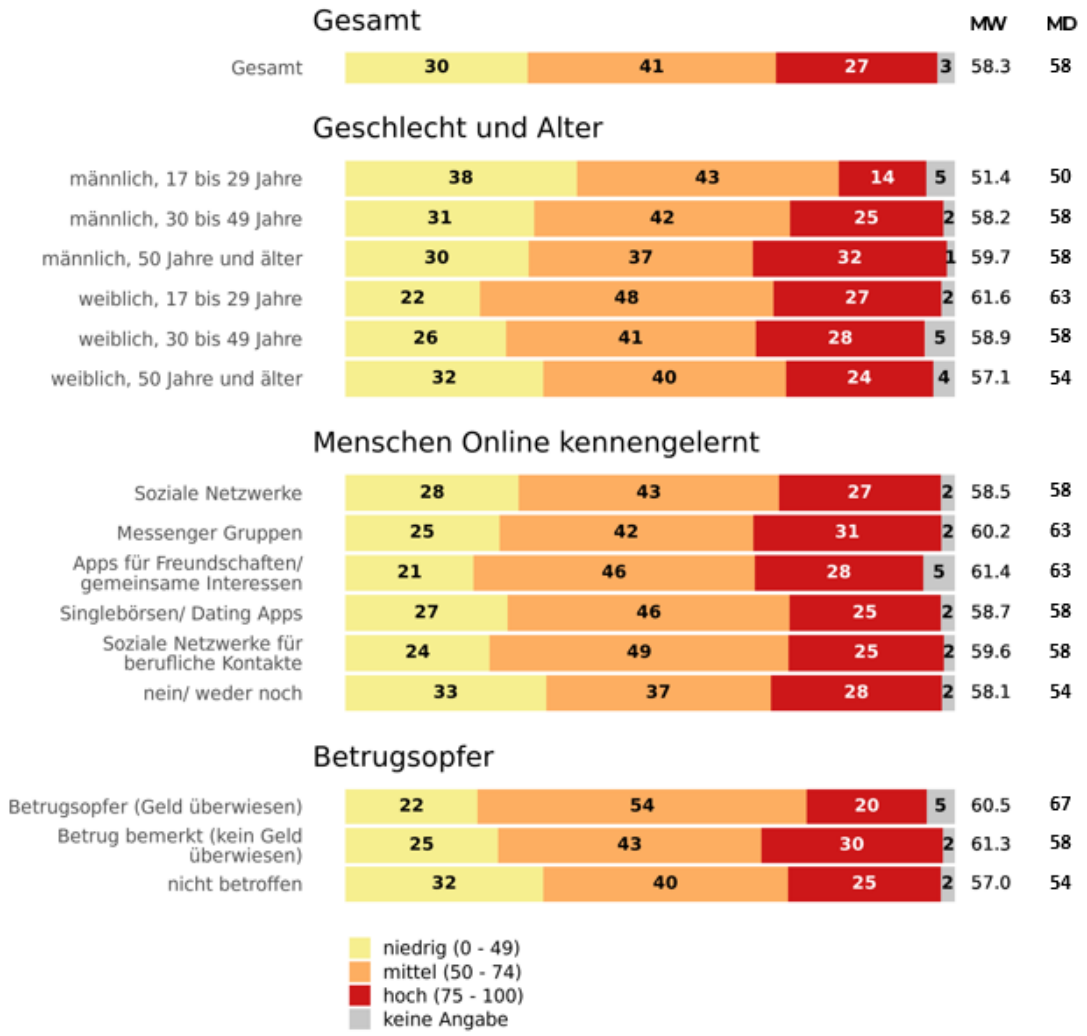


Abbildung 6: Summenindex zu Sicherheitsbedenken im Umgang mit persönlichen Daten

Sorglosigkeit, ein Mangel an Awareness und ein gewisses Maß an Naivität im Umgang mit Kontakten, die man im Netz knüpft, werden als wesentliche Risikofaktoren angesehen, wenn es um Opferwerdung geht. Daher wurden diese Themen in den Interviews auch abgefragt.

4.2.4. Online-Bekanntschaften

Vier von zehn Befragten (40 %) haben bereits Menschen entweder für private Freundschaften, zur beruflichen Vernetzung oder im Rahmen der Partnersuche über soziale Netzwerke (z.B. Facebook, Instagram, Twitter, TikTok) kennengelernt. Über soziale Netzwerke für berufliche Kontakte (z.B. LinkedIn, Xing) schlossen 15 % der Befragten Bekanntschaften, und 9 % taten dies

über Apps für Freundschaften oder gemeinsame Interessen (z.B. Xperience, Bumble BFF, Unblnd, Meetup).

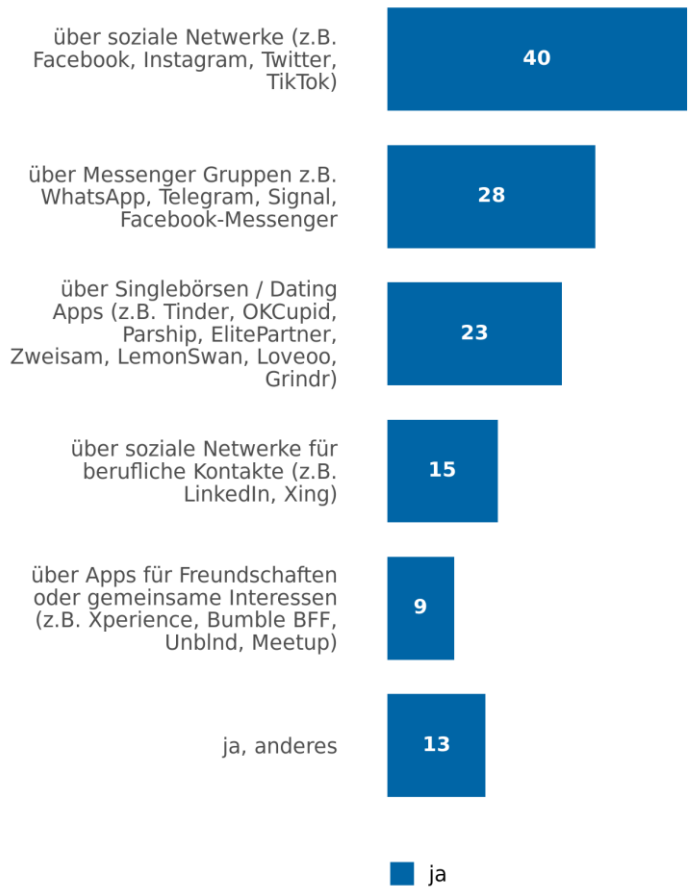


Abbildung 7: Bekanntschaften über das Internet geschlossen

4.2.5. Bekanntschaften über Dating-Apps

Von den Interviewpartnern gaben 23 % an, sich über Singlebörsen oder Dating Apps (z.B. Tinder, OKCupid, Parship, ElitePartner, Zweisam, LemonSwan, Lovoo, Grindr) schon einmal mit anderen Usern befreundet zu haben. Drei Viertel der Internetnutzer*innen (75 %) waren hingegen noch nie auf Partnersuche via Dating-Apps.

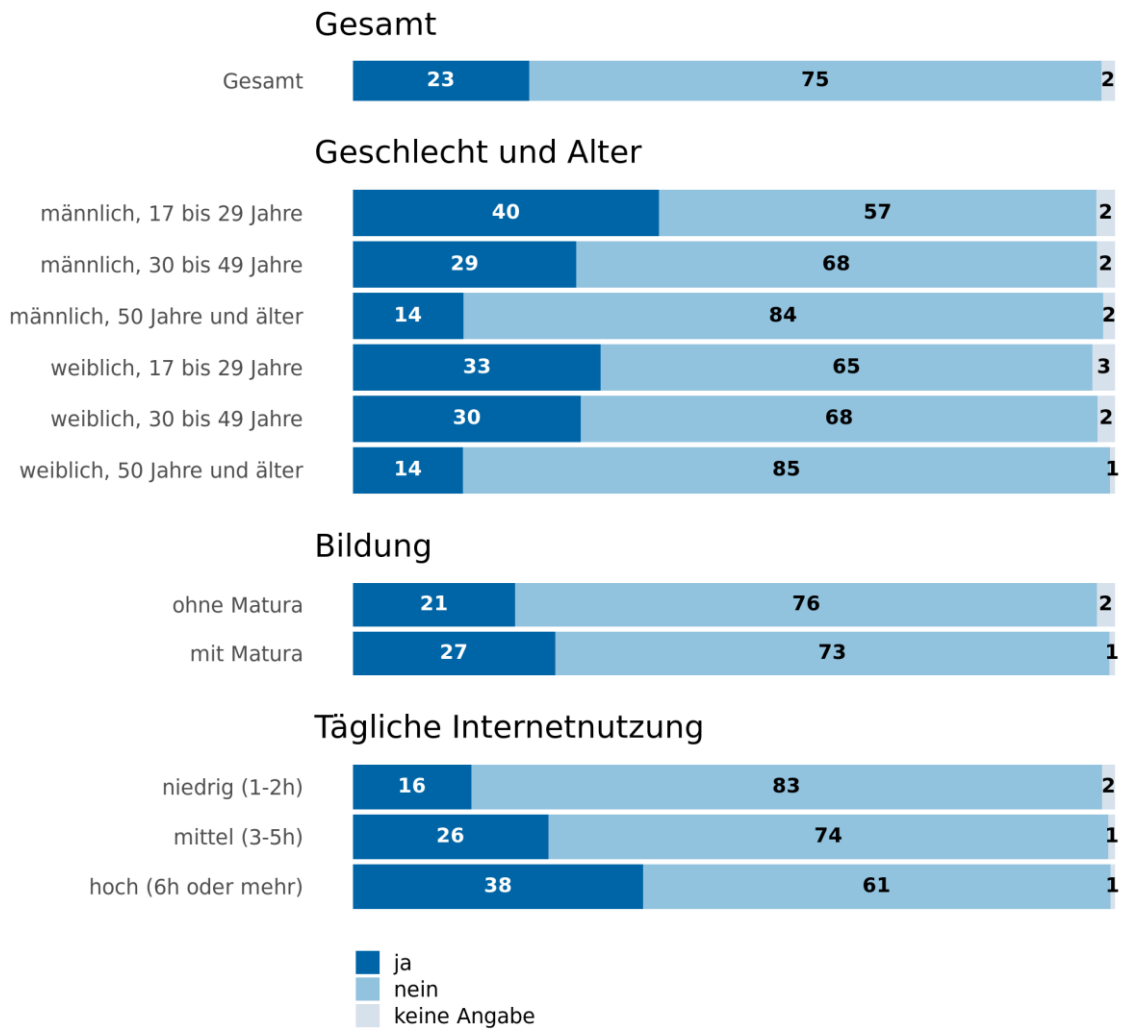


Abbildung 8: Kennenlernen über Dating-Apps

Junge Männer nutzen Dating-Apps stärker als Frauen der gleichen Altersgruppe. Der Prozentsatz an jungen männlichen Nutzern unter 30 Jahren beträgt 40 %. Bei Frauen unter 30 Jahren sind es 33 %, die zumindest einmal bereits eine Online-Partnerbörse aufsuchten. Der Anteil der Nutzer*innen mit einem Matura-Abschluss liegt mit einem Plus von 6 % etwas höher als jener der Personen, die keine Reifeprüfung nach einer höheren Schulausbildung abgelegt haben.

Etwas mehr als ein Drittel (36 %) der Dating-App-Verwender*innen nutzt das Internet täglich 6 Stunden oder mehr. Rund ein Viertel (26 %) aller Dating-App-Nutzer*innen ist 3-5 Stunden pro Tag im virtuellen Netz unterwegs.

4.2.6. Annahme von Freundschaftsanfragen

Weniger als die Hälfte der Bevölkerung (45 %) nimmt Freundschaftsanfragen von Fremden im Internet an, 44 % gehen zumindest manchmal bis selten Bekanntschaften online ein. Insgesamt

geben 9 % an, (fast) immer oder häufig Kontaktanfragen von Fremden auf sozialen Netzwerken (z.B. Facebook, Instagram, TikTok, Twitter, LinkedIn) anzunehmen. Junge Menschen unter 30 Jahren tun dies vergleichsweise öfter als ältere (Männer: 26 %, Frauen: 14 %).

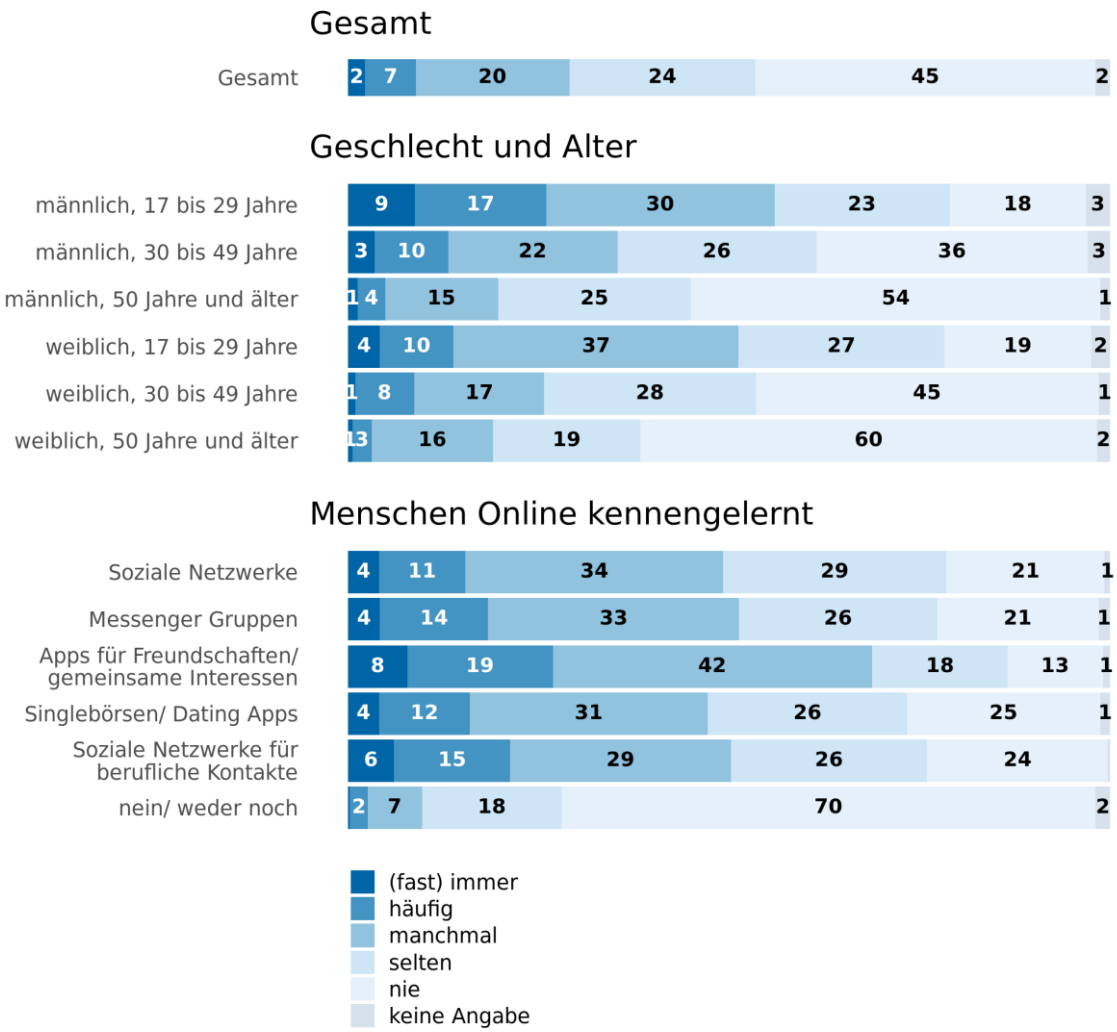


Abbildung 9: Annahme von Kontaktanfragen von Fremden

Ähnliches gilt für Nutzer*innen, die mit Hilfe von Messenger-Diensten in Kontakt mit Fremden treten. Auch hier sind die Jüngeren etwas unvorsichtiger. Immerhin gaben knapp 6 von 10 Befragten (57 %) an, fast alle ihre Chatpartner*innen bereits einmal persönlich getroffen zu haben. Hingegen sind es bei den unter 30-Jährigen weniger als die Hälfte (Männer 44 %, Frauen 47 %). Am ehesten sind es Frauen über 50 Jahren (66 %), die mit ihren Chatpartner*innen, mit denen sie über WhatsApp und ähnliche Dienste kommunizieren, nicht nur online in Verbindung stehen.

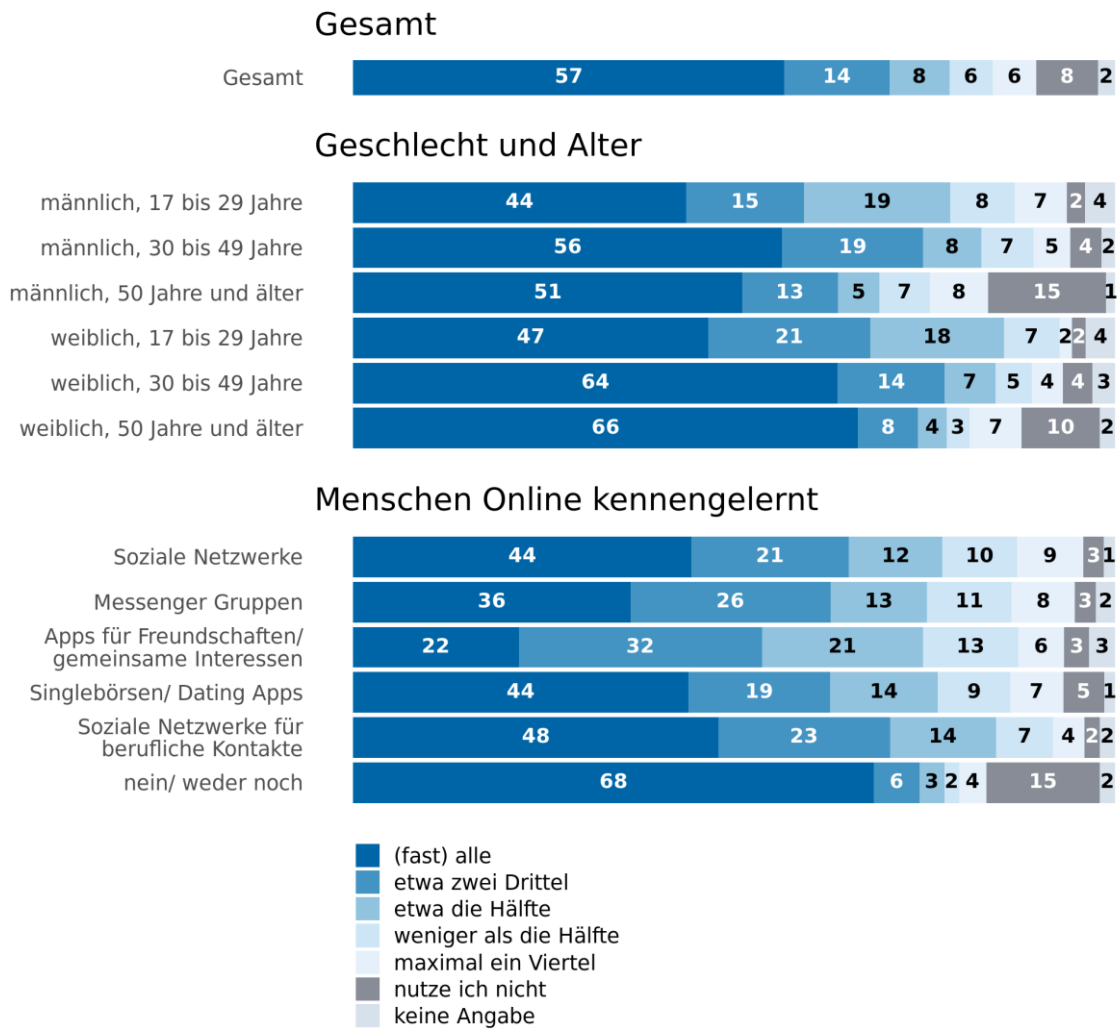


Abbildung 10: Persönliche Bekanntschaft mit Chatpartnern

Unter den Onlinediensten sind es die sozialen Netzwerke für berufliche Kontakte, deren Nutzer*innen mit 48 % am häufigsten ihre Chatpartner*innen auch persönlich kennen. Im Fall von Singlebörsen bzw. Dating-Apps haben 44 % der Nutzer*innen ihre Chatpartner*innen, die sie online kennengelernt haben, ebenfalls schon persönlich getroffen.

Von allen Befragten, die bereits andere Menschen online kennengelernt haben (317 Personen), gab mehr als ein Viertel (26 %) an, (fast) immer Recherchen zu der jeweiligen Person im Internet anzustellen, um mehr über sie herauszufinden. Fast die Hälfte (44 %) beantwortete die Frage nach der Identitätsrecherche mit „ja, eher schon“.

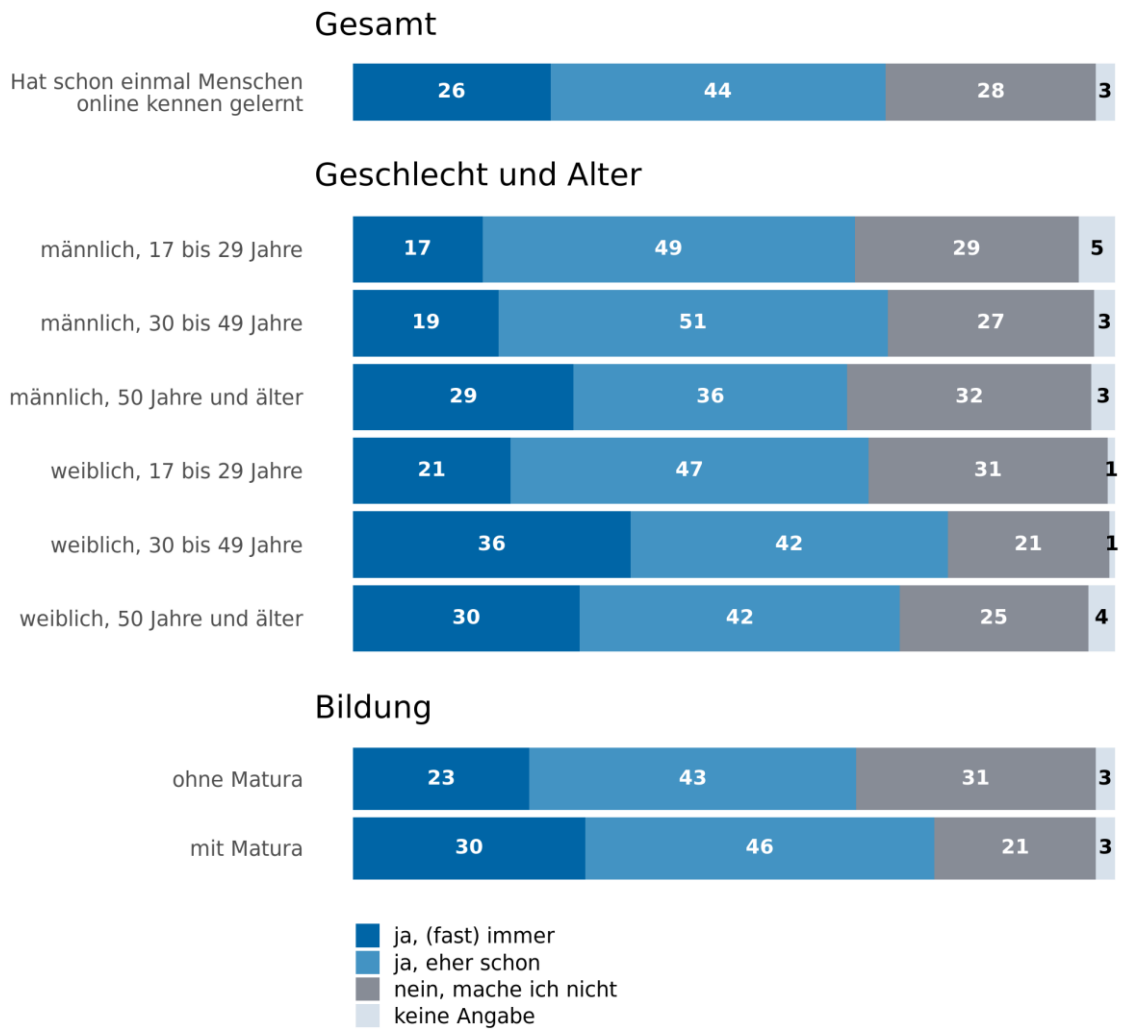


Abbildung 11: Bestätigung der Identität

Etwas weniger verbreitet ist diese Recherche wieder bei jungen Menschen unter 30 Jahren und hier wieder insbesondere bei Männern. Nur 17 % der 17- bis 29-jährigen Männer gaben an, fast immer im Internet nach der Identität des Chatpartners zu suchen. Von den jungen Frauen unter 30 Jahren sind es immerhin 21 %, die sich aktiv auf die Online-Suche nach persönlichen Daten ihrer Chatpartner*innen begeben. Personen mit niedrigerem formalem Bildungsniveau recherchieren online weniger oft (23 %) nach dem Chatpartner als Nutzer*innen mit absolvierter Matura (30 %).

4.2.7. Viktimisierung

Unter Viktimisierung im engeren Sinn versteht man eine finanzielle Schädigung, die auf Basis einer vorgetäuschten Verliebtheit oder Liebesbeziehung zum Zwecke der Bereicherung des Schädigers

entsteht. Das Opfer wird dabei vom Schädiger, etwa unter dem Vorwand einer finanziellen Notlage, um Geld gebeten. Aus Mitleid oder der Hoffnung, dem vermeintlich neuen Partner zu helfen, ergreift der Geschädigte Maßnahmen, die dem Opfer zugutekommen sollen (z.B. Überweisung von Geld).

Viktimisierung im weiteren Sinn trifft auf jene Personen zu, die zwar vom Schädiger kontaktiert, getäuscht und um Geld gefragt werden, jedoch keine finanziellen Zuwendungen tätigen.

4.2.8. Bekanntheit von Romance Scam

Rund 9 von 10 Befragten (88 %) ist das Phänomen der gefälschten Profile auf Singlebörsen und in sozialen Netzwerken mit dem kriminellen Zweck, durch Vortäuschen einer Liebesbeziehung Geld von anderen Menschen zu erschleichen, bekannt. 10 % der Befragten haben noch nie etwas davon gehört, 2 % enthielten sich einer Angabe.

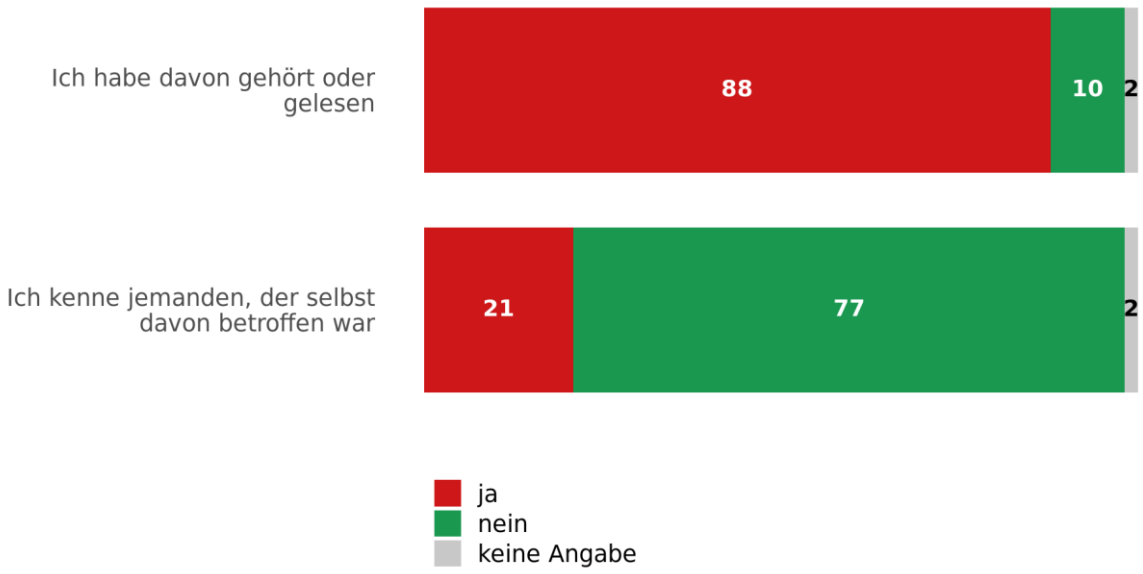


Abbildung 12: Bekanntheit von Romance Scam

Gut ein Fünftel (21 %) der Befragten kennt jemanden im Bekanntenkreis, der selbst schon einmal davon betroffen war. Hingegen ist 77 % der Interviewpartner*innen niemand in ihrer unmittelbaren Umgebung bekannt, der selbst einmal von Romance Scam betroffen gewesen wäre. Auch hier enthielten sich wieder 2 % der Befragten ihrer Stimme.

4.2.9. Betroffenheit und Viktimisierung im engeren Sinn

Auf die Frage, ob man selbst bereits einmal Geld überwiesen hatte, als aus einer lockeren Bekanntheit im Internet mehr wurde beziehungsweise sich eine Liebesbeziehung entwickelte und

die Person nach einiger Zeit um Geld bat (etwa unter dem Vorwand einer finanziellen Notlage), antworteten 5 % der Interviewpartner*innen mit „ja“. Die Mehrheit, nämlich 94 % der Befragten, verneinte diese Frage.

Junge Menschen nutzen öfter Online-Plattformen sowie Dating-Apps und weisen im Allgemeinen eine höhere technische Affinität auf. Zudem sind sie leichtfertiger im Umgang mit Online-Bekanntschaften als ältere Personen. Die junge Generation ist daher in puncto Internet-Betrugsversuchen deutlich exponierter.

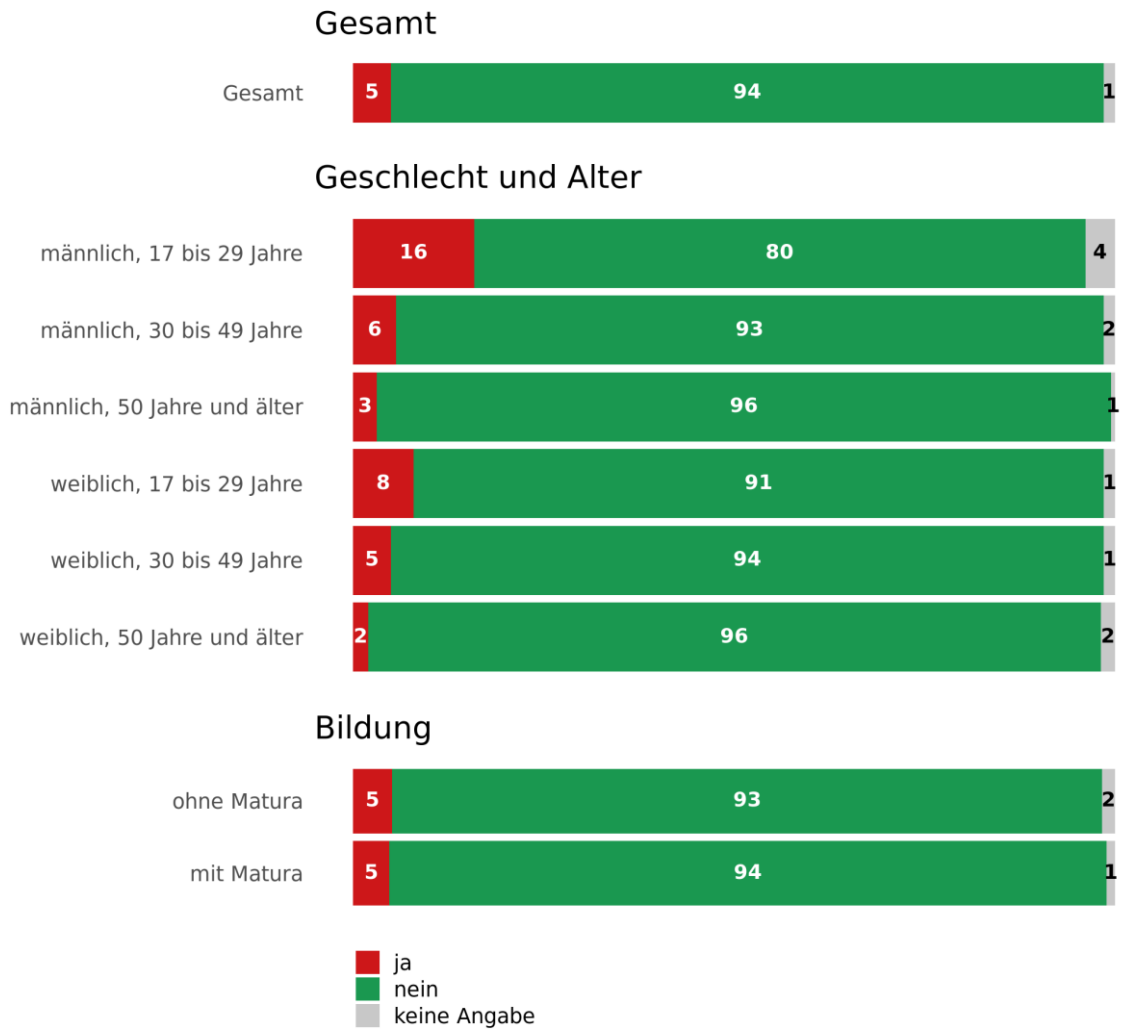


Abbildung 13: Viktimisierung im engeren Sinn (Geld überwiesen) nach Geschlecht, Alter und Bildungsstand

Die am häufigsten mit Viktimisierung im engeren Sinn konfrontierte Kohorte ist jene der jungen Männer unter 30 Jahren. In dieser Altersgruppe ist der Anteil der betroffenen Männer rund dreimal so hoch wie bei älteren. Im Fall von Frauen derselben Altersgruppe (17-29 Jahre) waren es 8 %, die aufgrund von Romance Scam finanziell bereits einmal geschädigt wurden. Grundsätzlich sind

Männer und Frauen ab 30 Jahren vorsichtiger, wenn es darum geht, einer Online-Bekanntschaft Geld zu überweisen.

Bei den 30-49 Jahre alten männlichen Interviewpartnern beträgt der Anteil jener, die schon einmal Geld auf Basis einer vorgetäuschten Online-Romanze überwiesen haben, 6 %. Nur 3 % der älteren Männer ab 50 Jahren fielen auf einen Romance Scam herein. Unter den weiblichen Teilnehmern der Studie zeigt sich ein sehr ähnliches Bild: 5 % der 30- bis 49-jährigen Frauen wurden laut eigenen Angaben Opfer einer im Internet vorgetäuschten Liebesbeziehung. Unter den Frauen ab 50 Jahren sind es sogar lediglich 2 %, die in die Irre geleitet wurden und dadurch finanziellen Schaden erlitten.

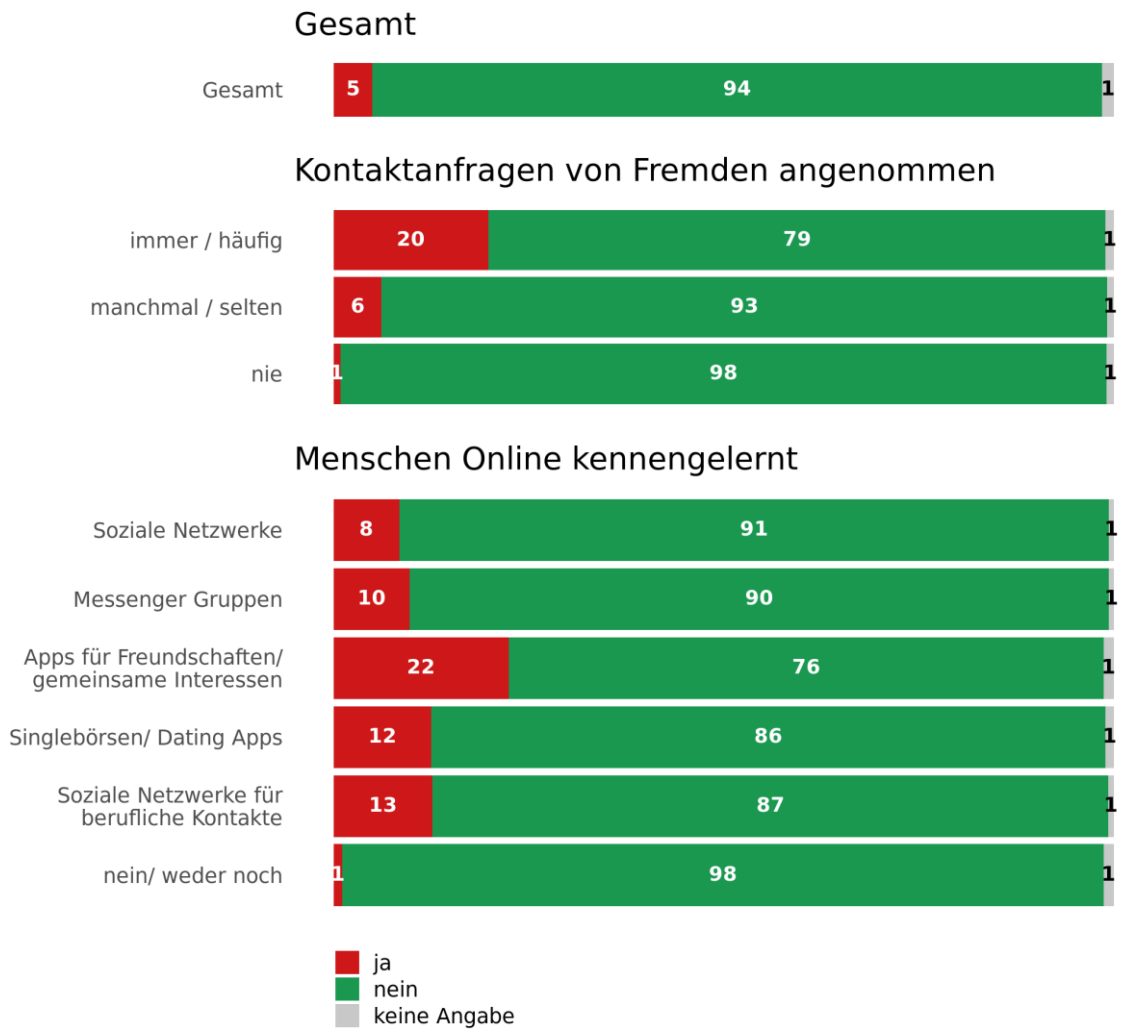


Abbildung 14: Viktimisierung im engeren Sinn (Geld überwiesen) nach Kontaktaufnahme durch Fremde

Von den Geschädigten nehmen 20 % immer bzw. häufig Kontaktanfragen von Fremden an, 6 % lassen sich dazu manchmal oder selten verleiten, und 1 % lässt Anfragen dieser Art gänzlich unberücksichtigt. Die meisten Opfer lernten ihre Schädiger über Apps für Freundschaften und

gemeinsame Interessen kennen (22 %). 13 % der Betroffenen gingen die Bekanntschaft über soziale Netzwerke für berufliche Kontakte ein, und 12 % lernten ihre vermeintlichen Liebespartner über Singlebörsen bzw. Dating Apps kennen. Am wenigsten von Romance Scam im engeren Sinn betroffen waren Internetznutzer*innen, die Verbindungen über soziale Netzwerke eingingen (8 %) und Personen, die neue Bekanntschaften über Messenger-Dienste schlossen.

4.2.10. Betroffenheit und Viktimisierung im weiteren Sinn

Den Betrug nach der ersten Geldforderung bemerkt und kein Geld überwiesen haben 11 % der Befragten. Wieder sind es die jungen Internetnutzer*innen, die vermehrt davon betroffen waren.

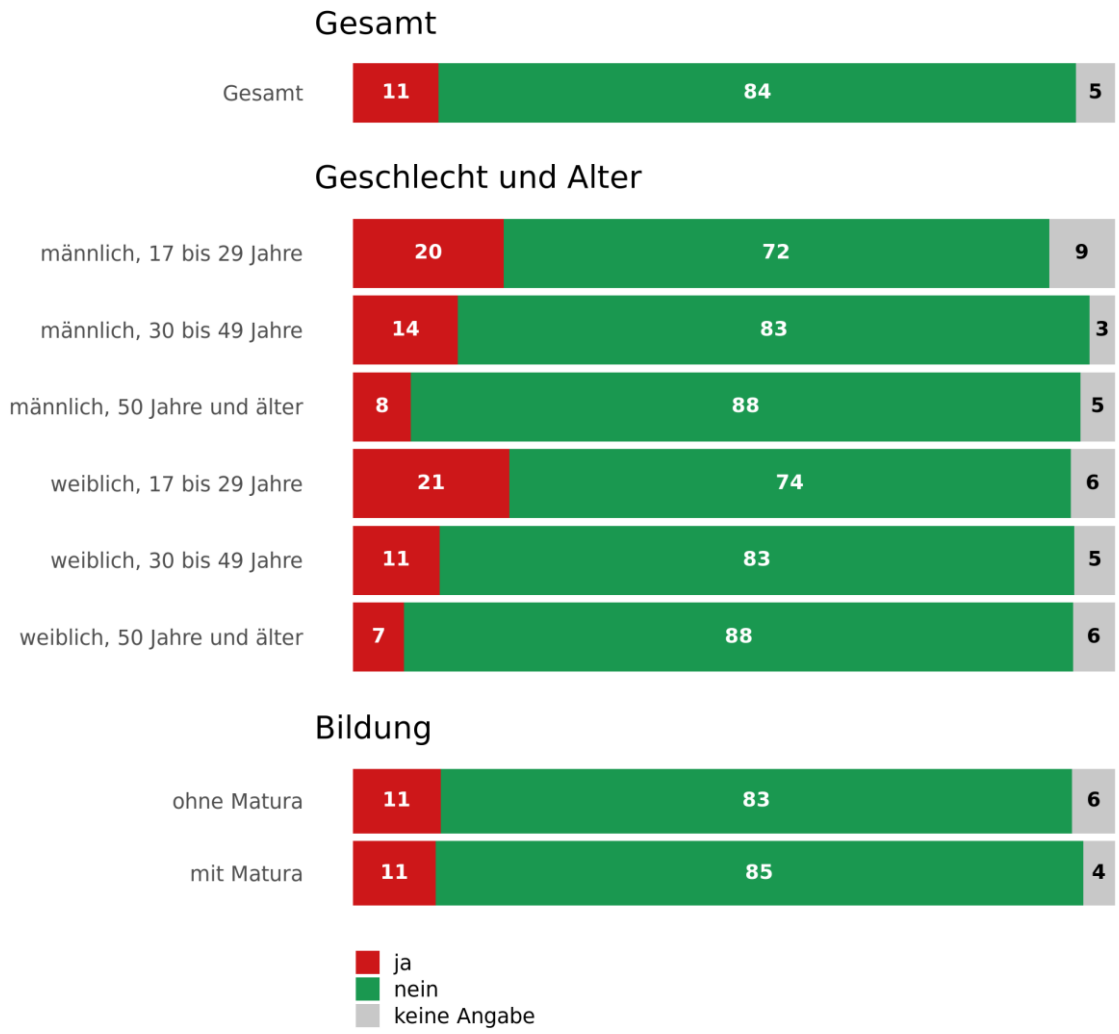


Abbildung 15: Viktimisierung im weiteren Sinn (kein Geld überwiesen) nach Geschlecht, Alter und Bildungsstand

Rund ein Fünftel der jungen Betroffenen zwischen 17 und 29 Jahren (Männer: 20 %, Frauen: 21 %) bemerkte rechtzeitig, dass es sich um einen Betrugsversuch handelte. Männer mittleren Alters (30-49 Jahre) erkannten dies zu 14 %, hingegen waren es nur 11 % der Frauen derselben

Altersgruppe. Bei den älteren Männern und Frauen ab 50 Jahren lag dieser Prozentsatz bei 8 bzw. 7 %.

Von den Betroffenen eines Romance Scam, die kein Geld überwiesen, nahmen 27 % immer oder häufig Kontaktanfragen von Fremden an. Am wenigsten (6 %) waren jene exponiert, die sich nie mit fremden Nutzer*innen online befreunden.

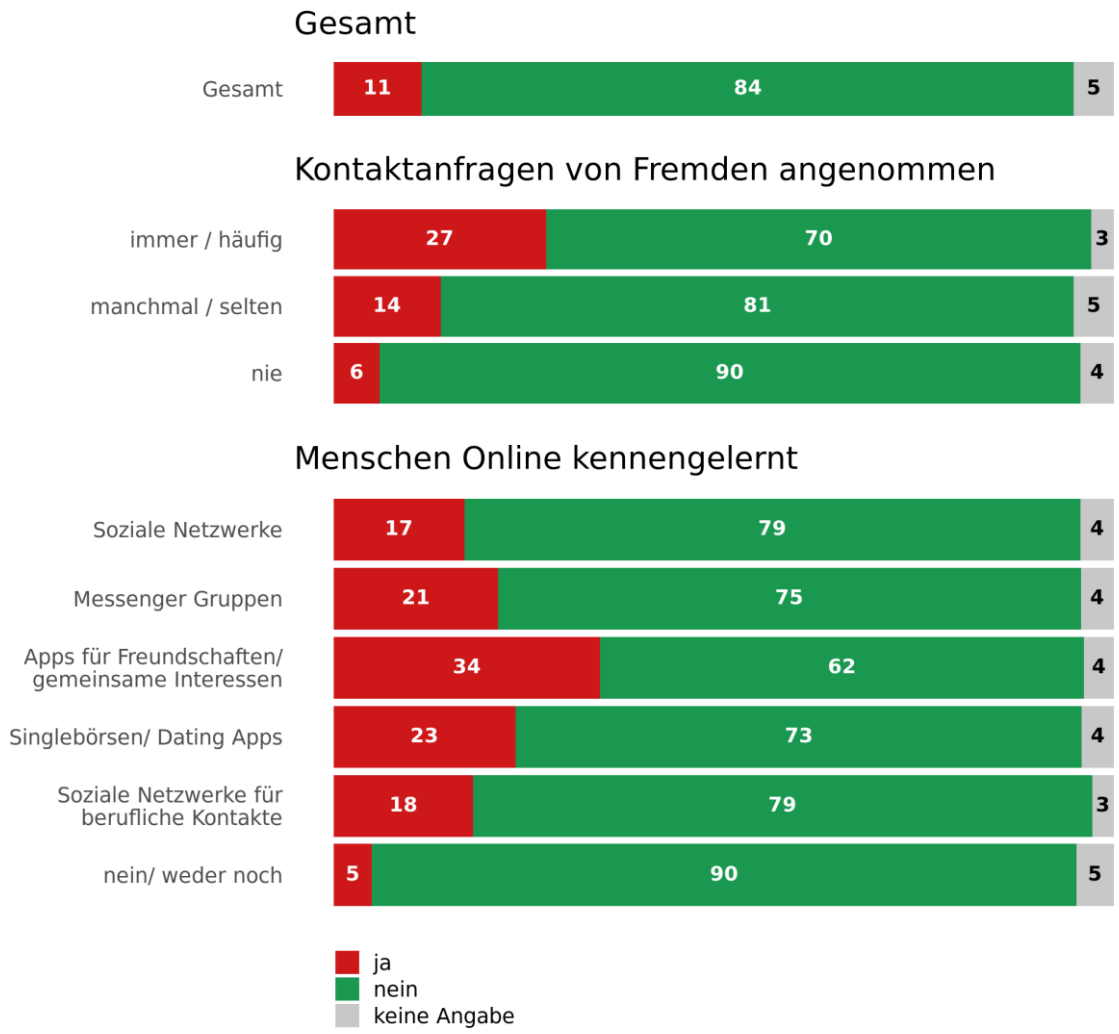


Abbildung 16: Viktimisierung im weiteren Sinn (kein Geld überwiesen) nach Kontaktaufnahme durch Fremde

Stellt man die Viktimisierung im engeren und weiteren Sinn einander gegenüber, so stellt man fest, dass in beiden Fällen die meisten Opfer gezielt über Apps für Freundschaftsanfragen bzw. gemeinsame Interessen kontaktiert wurden: 34 % der Betroffenen, die im Zuge einer sich anbahnenden Romanze nach Geld gefragt wurden, den Betrugsfall jedoch noch im Keim erstickten, lernten die Betrüger*innen über ebensolche Apps kennen. Singlebörsen bzw. Dating-

Apps waren für 23 % die Quelle für unehrliche Liebschaften mit Finanzierungswunsch, und 21 % gingen die falschen Freundschaften über Messenger-Gruppen ein.

Ein Fünftel (20 %) ist selbst schon Opfer eines Romance Scam geworden, hat aber den Betrugsversuch schon früh, d.h., als der Kontakt zustande kam, bemerkt.

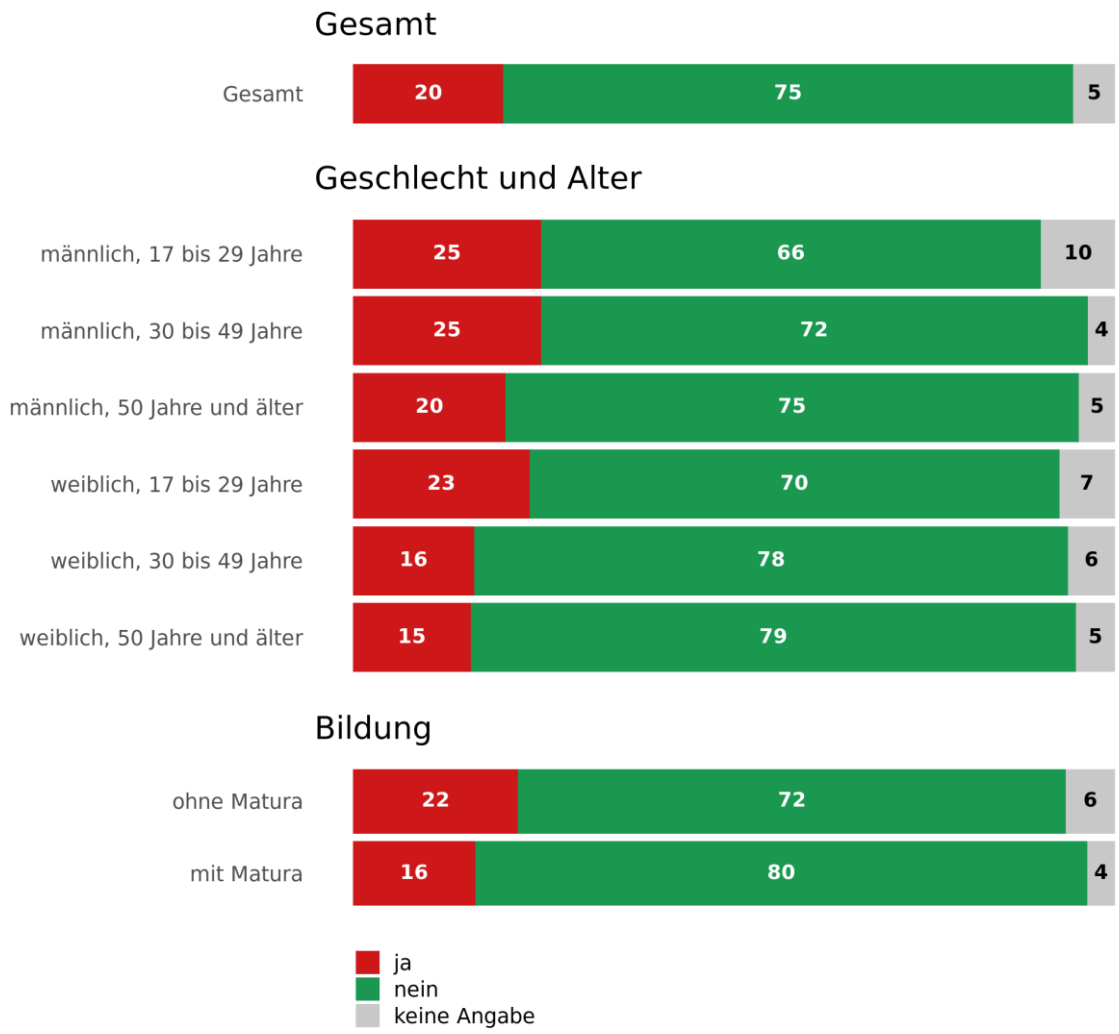


Abbildung 17: Betrug schon bei Kontaktanbahnung bemerkt (nach Geschlecht, Alter und Bildung)

Sowohl unter den jungen Männern (17-29 Jahre) als auch unter den Männern mittleren Alters (30-49 Jahre) zweifelte ein Viertel der Betroffenen (25 %) die Authentizität der Person und ihrer Situation bereits bei der Kontaktanbahnung an. Auch junge Frauen unter 30 Jahren zeigten sich skeptischer, wodurch 23 % den Kontakt sofort nach dem Aufkommen erster Zweifel an der Integrität des Chatpartners unterbrachen. Betroffene ohne Matura scheinen vorsichtiger zu sein und brechen den Kontakt eher ab (22 %) als jene mit Reifeprüfungsabschluss (16 %).

Auch in diesem Fall zeigt sich wieder dasselbe Bild wie schon zuvor: Es sind am ehesten jene Internetnutzer*innen betroffen, die grundsätzlich immer oder häufig Kontaktanfragen von Fremden annehmen (36 %), nämlich vor allem über Apps für Freundschaften und gemeinsame Interessen (44 %), über Messenger-Gruppen (32 %), gefolgt von Singlebörsen und Dating-Apps (31 %).

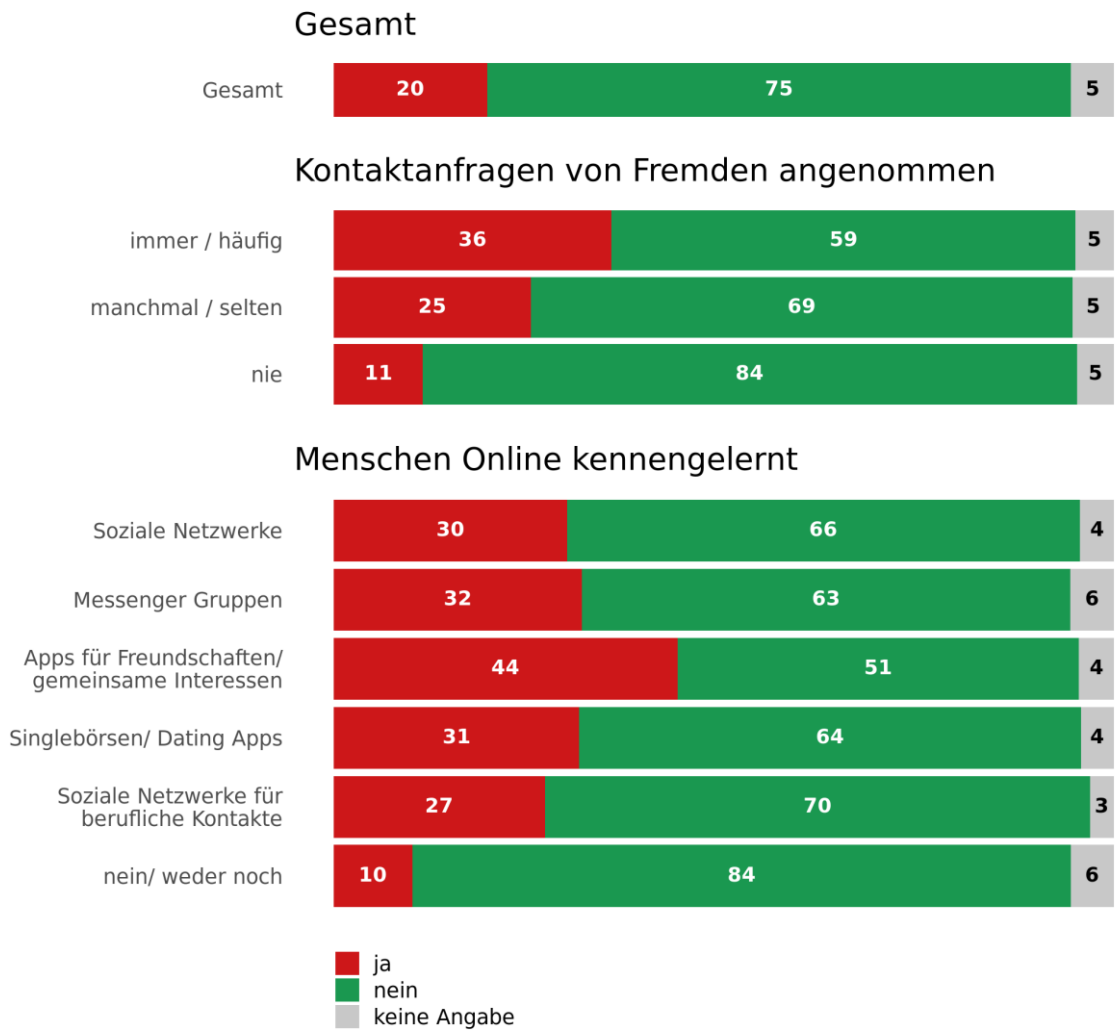


Abbildung 18: Betrug schon bei Kontaktanbahnung bemerkt (Internetdienste)

4.2.11. Häufigkeit des Betrugsversuchs

Jene Personen, die online schon einmal eine Liebesbeziehung eingegangen und um Geld gebeten worden sind, wurden dazu befragt, wie oft sie bereits von Romance Scam oder einem Betrugsversuch betroffen waren.

Erstaunlicherweise wurde rund ein Drittel der getäuschten Dating-Partner (35 %) bereits dreimal oder gar öfter Opfer von Romance Scammern. Für 26 % der Opfer kam es zweimal zu einem

Betrug oder Betrugsversuch, 29 % gaben an, dass sie nur einmal in diese prekäre Lage gekommen waren.

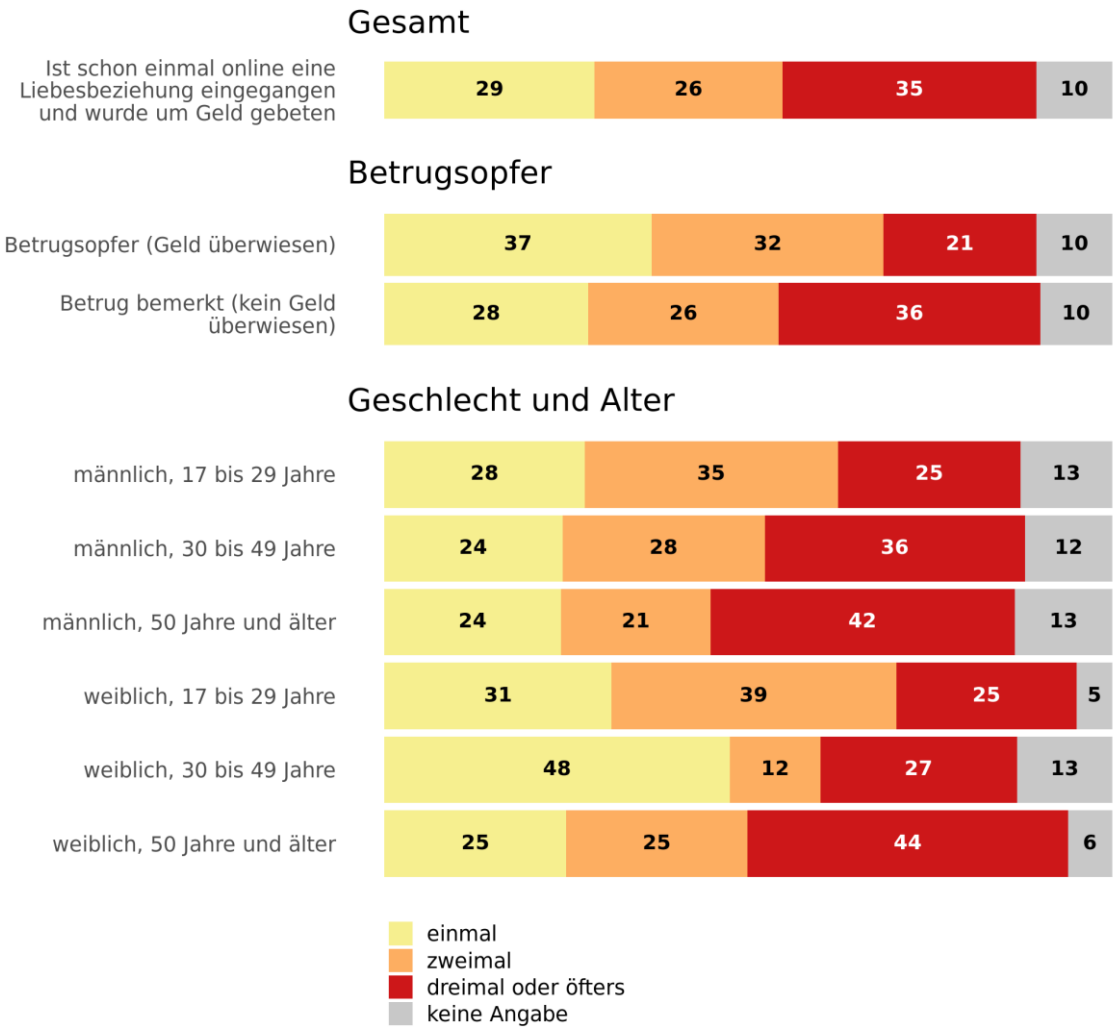


Abbildung 19: Häufigkeit des Betrugs(-versuchs)

Betrachtet man die demografischen Faktoren, so kann man Folgendes feststellen: Von den jungen Personen (17-29 Jahre), die in einer Online-Liebesbeziehung bereits um Geld gebeten worden sind, wurde ein Viertel (25 %) bereits dreimal oder öfter Opfer eines solchen Betrugsversuchs. Auffallend sind im Gegensatz dazu Personen über 50 Jahren. Bei ihnen liegt der Anteil der Betroffenen mit mindestens dreimaligem Betrug oder Betrugsversuch bei 42 % (Männer) bzw. 44 % (Frauen). Wenn ältere Menschen also von Romance Scam betroffen sind, dann passiert ihnen dies in der Regel öfters.

Dort, wo es im Rahmen des Liebesschwindels im Internet zu finanziellen Zuwendungen gekommen ist, war hingegen der Lerneffekt größer, und es kam weniger oft zu wiederholten Betrugsversuchen (dreimal oder öfter Geld überwiesen: 21 %, kein Geld überwiesen: 36 %).

Bei 35 % der Betroffenen, die Geld überwiesen haben, liegt der letzte Betrugsversuch höchstens 12 Monate zurück, bei 21 % maximal drei Jahre. In 38 % der Fälle ist der Betrugsfall schon länger als 4 Jahre her.

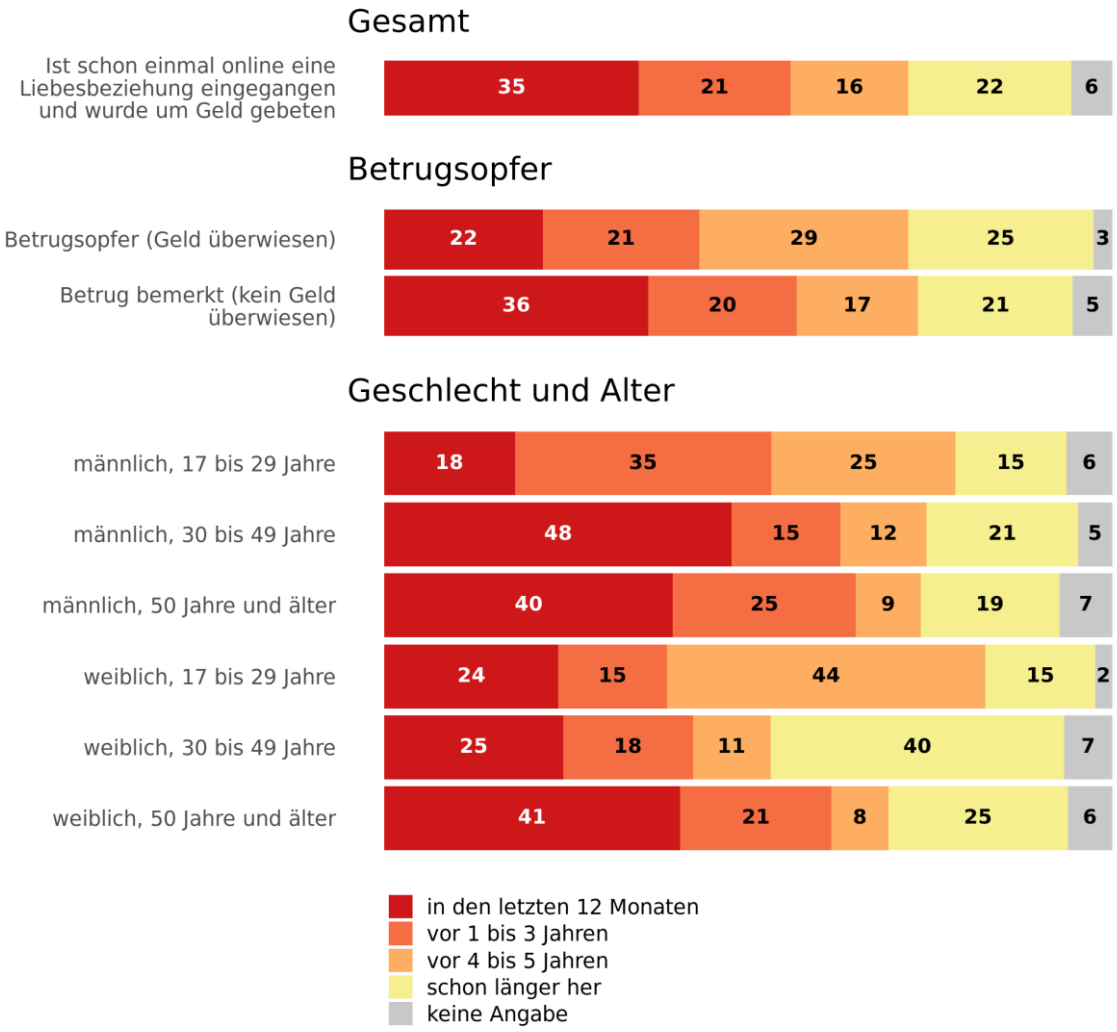


Abbildung 20: Letzter Betrug bzw. Betrugsversuch gegenüber Personen, die bereits eine Online-Beziehung eingegangen sind

Auch hier zeigen sich Differenzen nach Untergruppen. Während in den letzten 12 Monaten ein knappes Fünftel (18 %) der jungen Männer unter 30 Jahren und fast ein Viertel (24 %) aller jungen Frauen derselben Altersgruppe von Romance Scam betroffen waren, sind es bei den älteren Betroffenen ab 50 Jahren doppelt so viele Personen (Männer: 40 %, Frauen: 41 %). Die am stärksten betroffene Kohorte war jene der Männer mittleren Alters (30-49 Jahre), von denen fast jeder zweite (48 %) einem Romance Scam im Internet ausgesetzt war.

Betrachtet man nun alle Betrugsfälle und Betrugsversuche gemeinsam, so fanden 9 % aller Vorfälle in den letzten 12 Monaten statt. Personen ohne Matura waren um 2 % öfter betroffen als jene mit Reifeprüfungsabschluss, wobei der Fokus auf Männern mittleren Alters (14 %) lag.

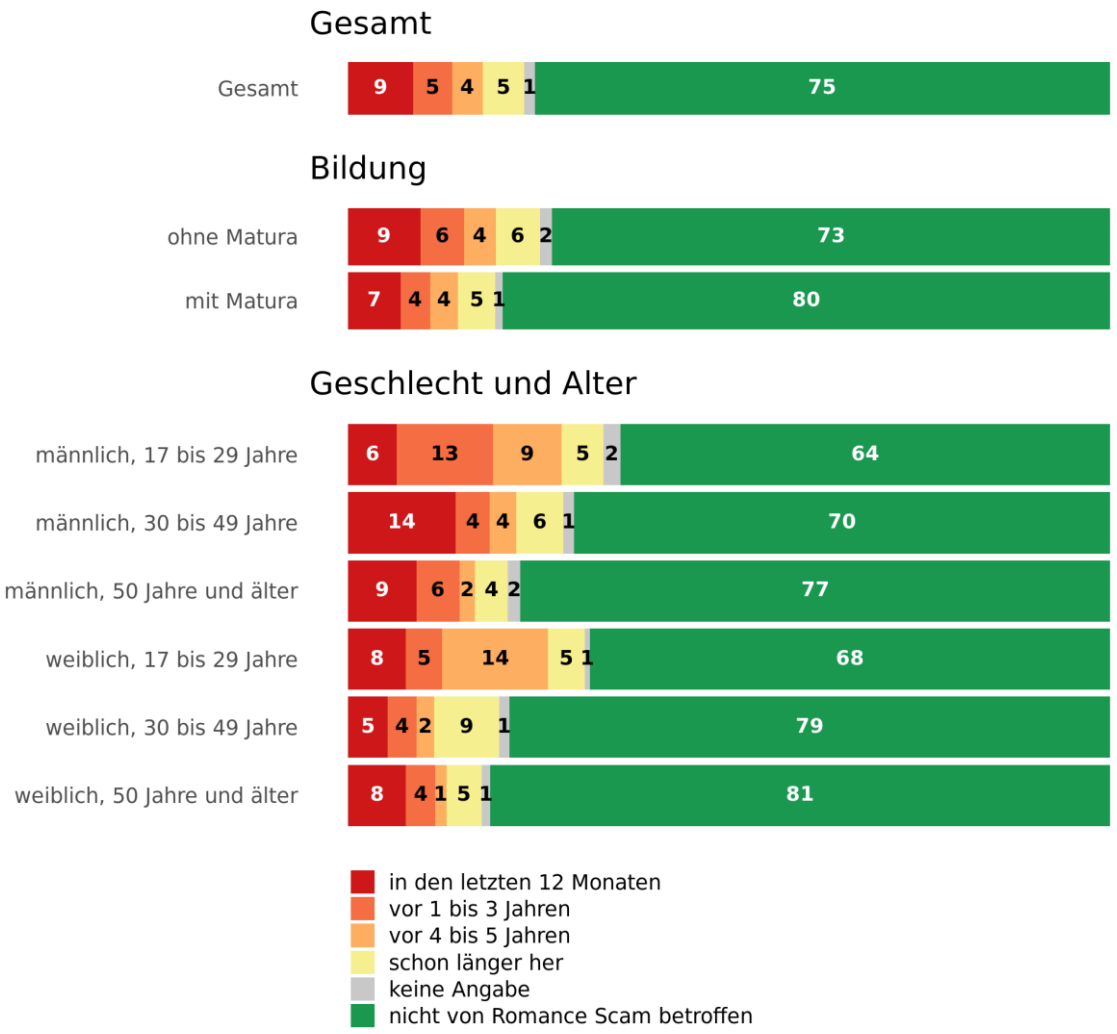


Abbildung 21: Letzter Betrug oder Betrugsversuch gesamt betrachtet

4.2.12. Finanzielle Unterstützung

Die Auswertung der Daten bezüglich des Ausmaßes der Forderungen seitens der Scammer ergab, dass in den meisten Fällen die Täter*innen von sich aus nach einer finanziellen Unterstützung fragten. Von den Betroffenen wurden 51 % um Geld und 17 % um Sachgeschenke gebeten. Für 5 % erstreckten sich die Forderungen über beide Kategorien. In nur 2 % der Fälle haben die Opfer von sich aus finanzielle Unterstützung oder Sachgeschenke angeboten.

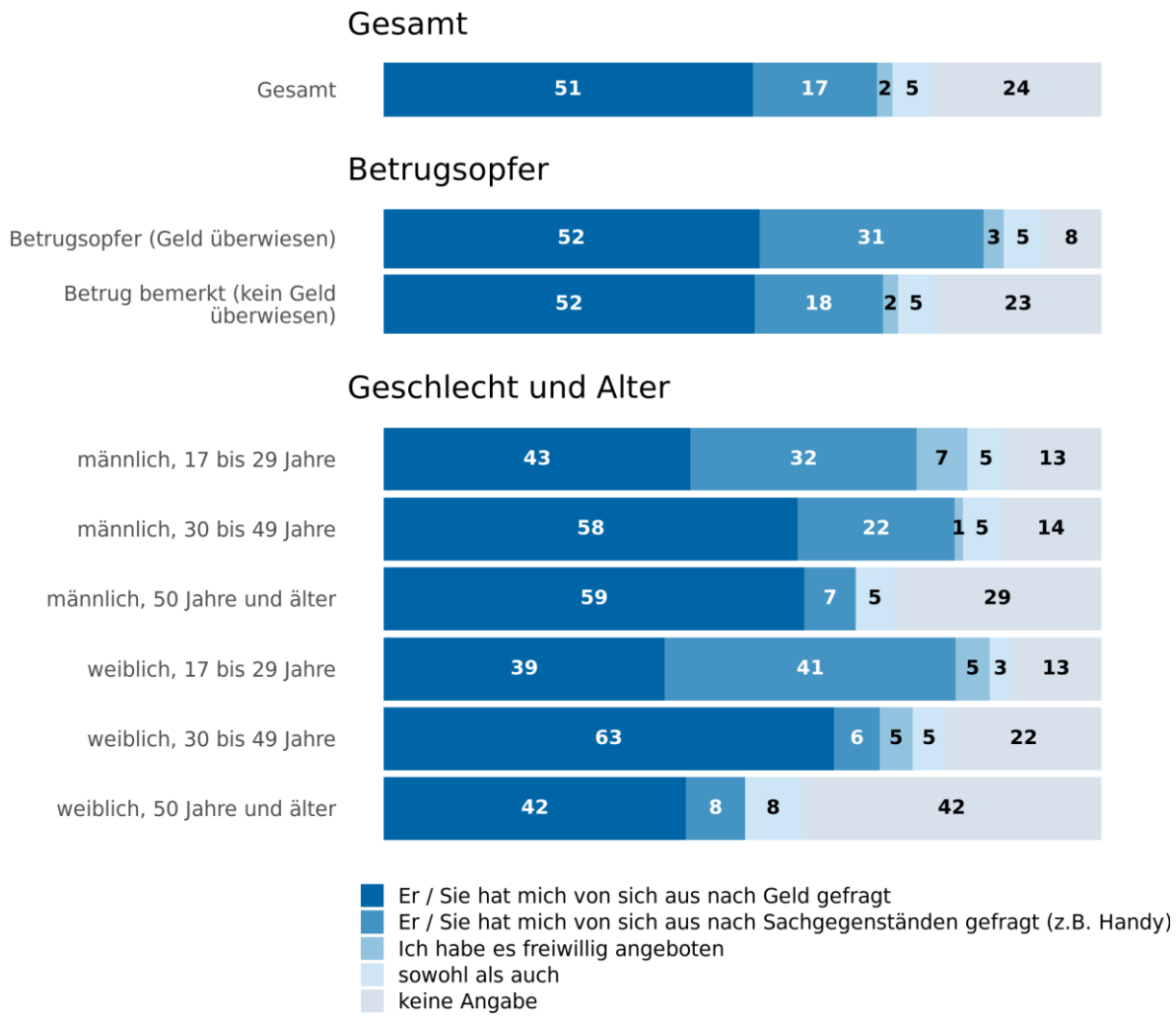


Abbildung 22: Finanzielle Unterstützung

Dem Wunsch nach Geld kamen 52 % der Betroffenen nach, 31 % schenkten Sachgegenstände im Anschluss an die Forderung.

Statistisch gesehen wurden Frauen mittleren Alters (30-49 Jahre) am häufigsten (63 %) nach Geld gefragt, nur 6 % berichteten von Anfragen zu Sachgeschenken. Am zweit- und dritthäufigsten werden Männer ab 50 Jahren (59 %) und Männer von 30 bis 49 Jahren (58 %) um Geld gefragt. Am wenigsten scheinen junge Frauen im Alter von 17 bis 29 Jahren dem Wunsch nach Geldtransfer ausgesetzt zu sein (39 %), allerdings erhielten sie die meisten Anfragen zu Sachgeschenken (41 %).

Die Höhe der Beträge, welche die Scammer erhielten, beläuft sich auf durchschnittlich 400 Euro. Etwas mehr als ein Viertel (26 %) der zahlenden Betroffenen hat maximal 100 Euro überwiesen. Ein weiteres Viertel (25 %) überwies zwischen 101 und 1.500 Euro, und 12 % initiierten einen Geldtransfer mit einem Betrag zwischen 1.501 und 5.000 Euro. 3 % zeigten sich am

spendabelsten und gaben an, eine Summe zwischen 5.001 und 40.000 Euro überwiesen zu haben.

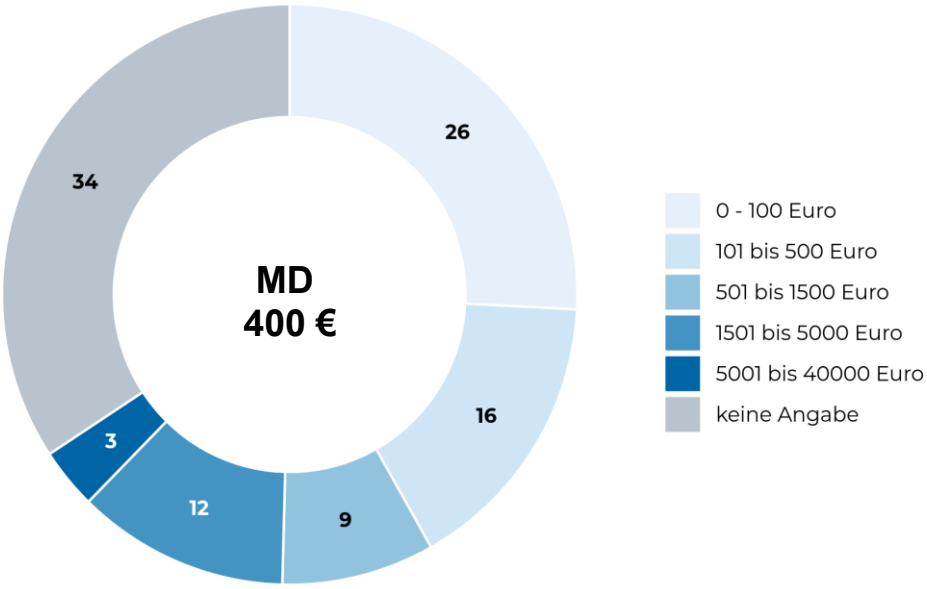


Abbildung 23: Höhe der finanziellen Unterstützung

4.2.13. Reaktion auf den Betrug oder Betrugsversuch

Jene Interviewpartner*innen, die schon einmal online eine Liebesbeziehung eingegangen waren und um Geld gebeten wurden, wurden im Rahmen der KFV-Studie dazu befragt, was sie unternahmen, nachdem sie den Betrug oder Betrugsversuch bemerkt hatten.

Von den Betroffenen wollten etwas mehr als ein Viertel (27 %) den Vorfall der Polizei melden, im Fall derjenigen, die sogar Geld überwiesen hatten, waren dies 30 %. Allerdings erstatteten nur 6 von 10 Personen, die den Betrug bzw. Betrugsversuch der Polizei meldeten, tatsächlich Anzeige.

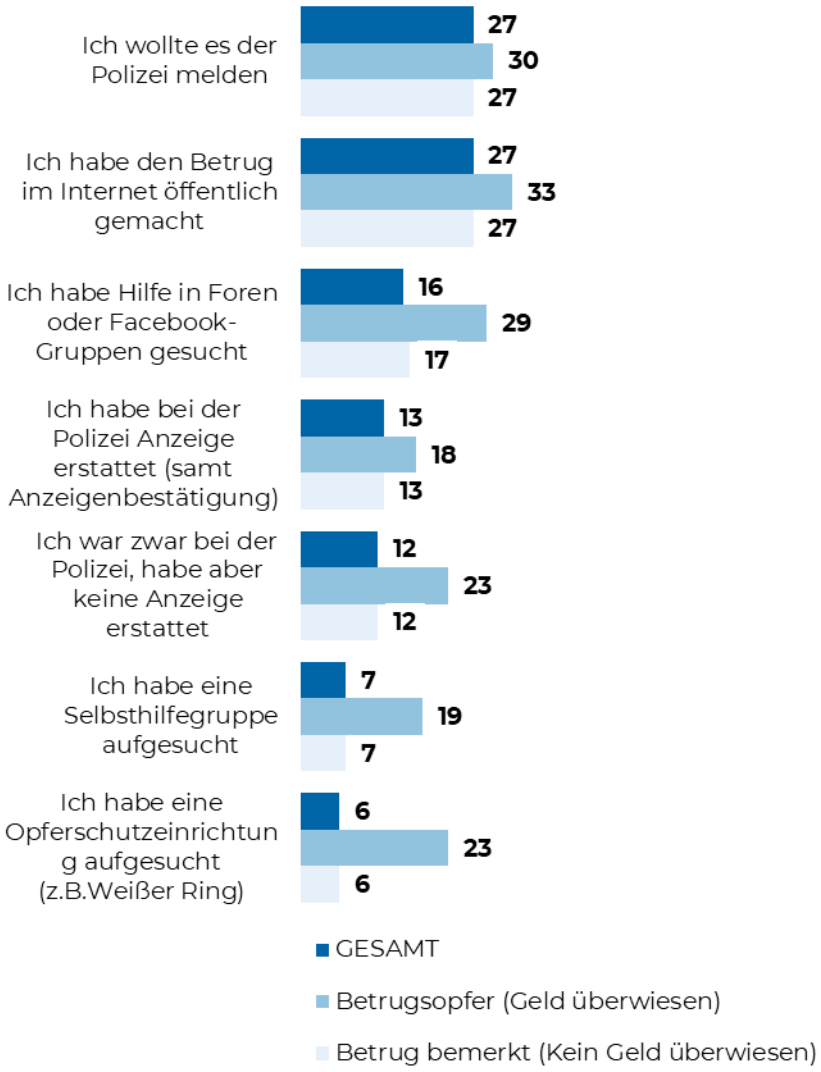


Abbildung 24: Reaktion auf den Betrug

Ebenfalls 27 % machten den Betrug im Internet öffentlich, wobei 16 % Hilfe in einschlägigen Foren oder Facebook-Gruppen suchten. Sich an Selbsthilfegruppen zu wenden, erachteten 7 % aller Betroffenen als notwendig (sogar 19 % derjenigen, die Geld überwiesen hatten), und 6 % suchten eine Opferschutzeinrichtung auf (im Fall einer finanziellen Schädigung waren dies sogar 23 % der Betroffenen).

Im Allgemeinen lässt sich aus den Daten herauslesen, dass jene, die dem Täter Geld überwiesen hatten, vergleichsweise öfter Konsequenzen aus dem Vorfall zogen als jene, bei denen es zu keiner finanziellen Schädigung kam.

4.2.14. Alter bei Betrug

Über ein Fünftel (21 %) der Opfer von Romance Scam, die zuletzt um eine Geldüberweisung gebeten wurden, sind junge Menschen im Alter von 17 bis 29 Jahren. In den restlichen Kohorten verteilt sich der Prozentsatz zu fast gleichen Anteilen (12-13 %). Im Durchschnitt beträgt das Alter der Betroffenen 40 Jahre, wobei junge Internetnutzer*innen öfter als alle anderen von einer vorgetäuschten Liebesbeziehung im Internet samt Geldansuchen betroffen waren.

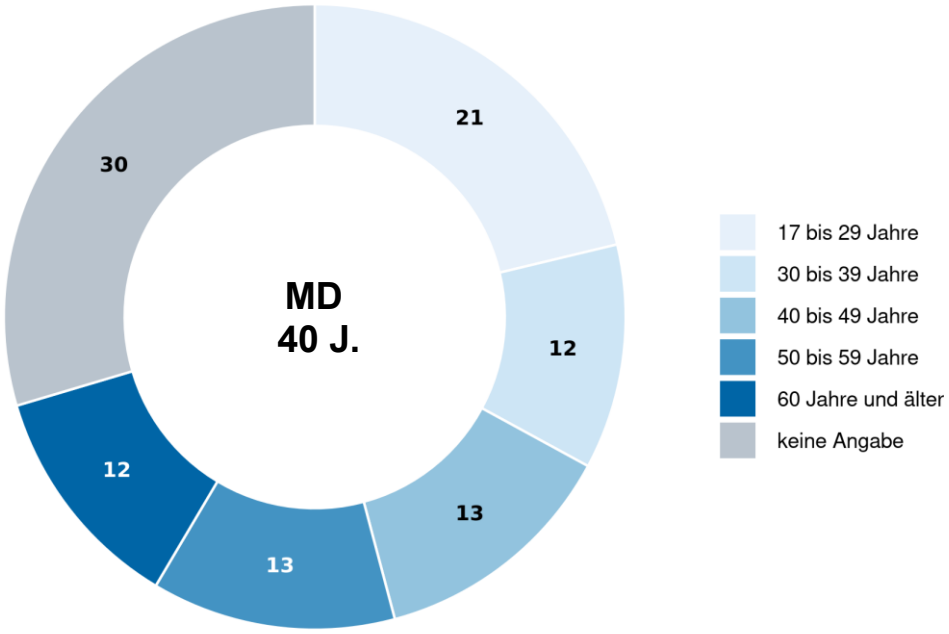


Abbildung 25: Alter bei Betrug

4.2.15. Einsamkeit und Beziehungsstatus zum Zeitpunkt des Betrugs

Gegen Ende des Interviews wurden die Betroffenen nach ihrem Beziehungsstatus und ihrem Befinden unmittelbar vor dem Betrugsfall gefragt, genauer gesagt, ob sie sich damals einsam fühlten oder nicht.

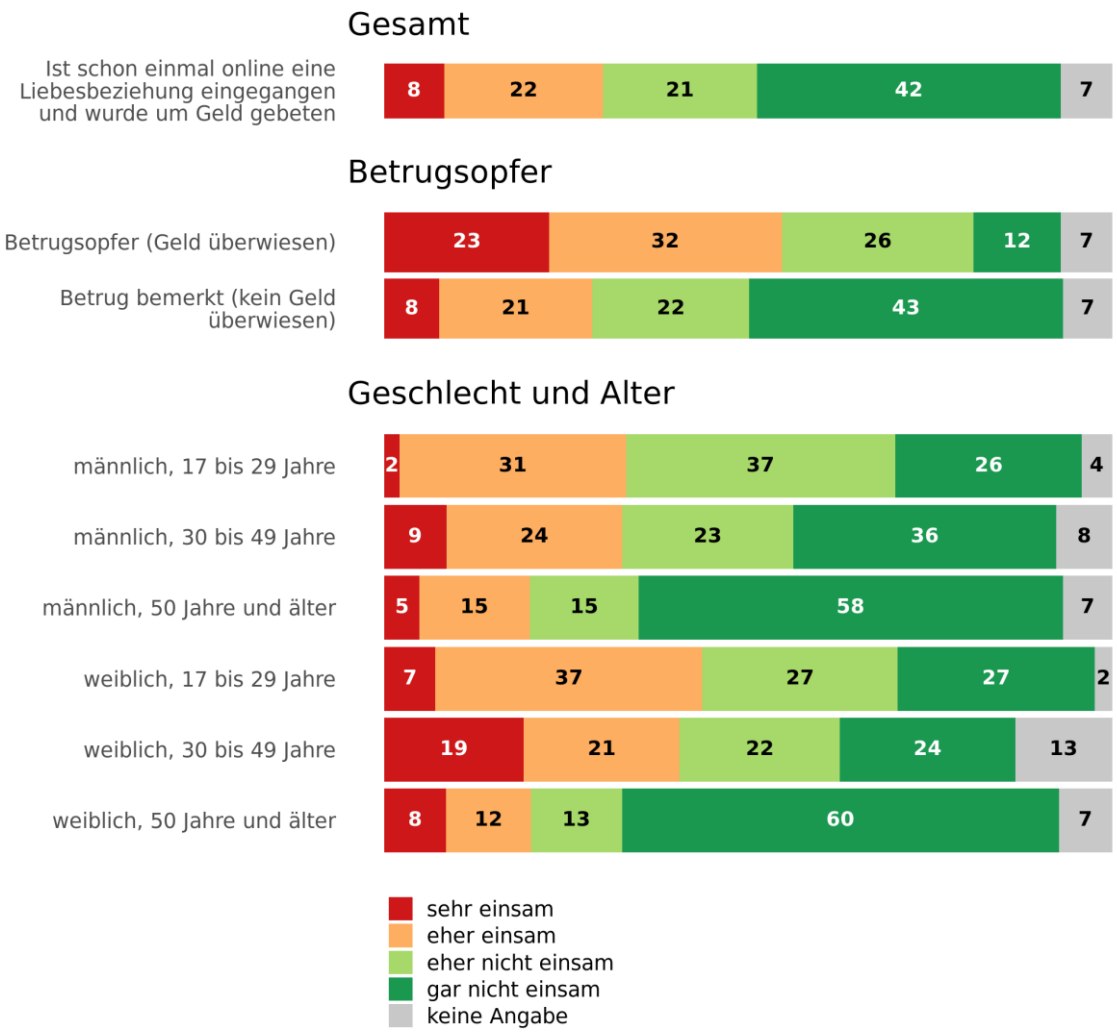


Abbildung 26: Einsamkeit zum Zeitpunkt des Betrugs

3 von 10 Opfern fühlten sich zum Zeitpunkt des Betrugs sehr einsam oder einsam. Hier lässt sich ein Unterschied zwischen jenen erkennen, die Geld überwiesen, und jenen, die den Betrug noch rechtzeitig vor der Transaktion bemerkt haben. So fühlte sich mehr als die Hälfte (55 %) jener Personen, die eine Transaktion veranlassten, einsam bis sehr einsam. Im Gegensatz dazu waren es bei jenen, die der Bitte um finanzielle Unterstützung nicht nachgaben, nur 29 %.

Nach den demografischen Faktoren Alter und Geschlecht betrachtet sind es vor allem Personen der jüngeren und mittleren Altersgruppen (unter 50 Jahren), bei denen Gefühle der Einsamkeit eine stärkere Rolle spielten. Es waren vor allem Frauen mittleren Alters (30-49 Jahre), die sich zum Zeitpunkt der Kontaktaufnahme sehr einsam fühlten (19 %). Am meisten Einsamkeit empfanden jüngere Frauen unter 30 Jahren. In dieser Kohorte gaben insgesamt 44 % an, unmittelbar vor dem Betrug einsam oder sehr einsam gewesen zu sein.

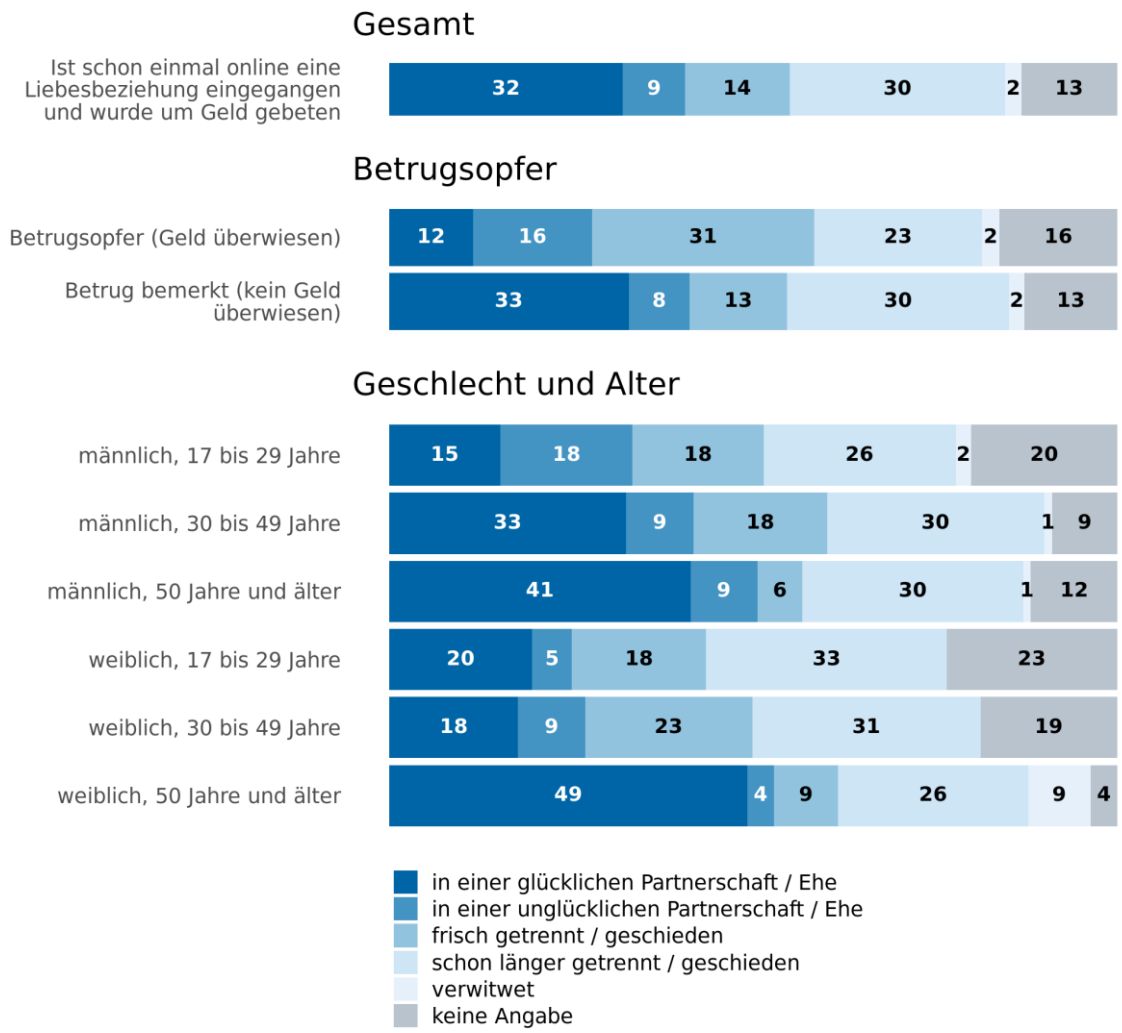


Abbildung 27: Beziehungsstatus zum Zeitpunkt des Betrugs

Knapp ein Drittel (32 %) der Betrugsopfer war zum Zeitpunkt des Betrugs in einer glücklichen Beziehung, 9 % gaben an, in einer unglücklichen Partnerschaft gewesen zu sein, 14 % hatten vor Kurzem eine Trennung durchlebt, und 30 % waren schon länger alleinstehend. Unter den Betrugsopfern im engeren Sinn, sprich jenen, die schon einmal Geld überwiesen haben, ist der Anteil der Alleinstehenden vergleichsweise höher (Geld überwiesen: 56 %, kein Geld überwiesen: 45 %).

Fast die Hälfte der Frauen ab 50 Jahren (49 %) und deutlich mehr als ein Drittel der älteren Männer (41 %) befanden sich zum Zeitpunkt des Betrugsfalls in einer glücklichen Partnerschaft. Hingegen waren es lediglich 15 % der jungen Männer im Alter von 17 bis 29 Jahren, die trotz einer glücklichen Beziehung über neue Kontakte einem Romance Scam ausgesetzt wurden.

Beinahe ein Viertel der Betroffenen (22 %) war damals aktiv auf Partnersuche. Der Anteil der Opfer im engeren Sinn (35 %) sowie der Betroffenen mittleren Alters war auch hier wieder höher. 38 % der 30- bis 49-jährigen Männer und 34 % der 30- bis 49-jährigen Frauen waren aktiv auf Partnersuche, als sie mit einem Romance Scam konfrontiert wurden. In der Gruppe der betroffenen jungen Männer unter 30 Jahren waren es 24 %, die zum Zeitpunkt der aktiven Partnersuche zum Betrugsopfer wurden.

Am seltensten waren es junge Frauen im Alter von 17 bis 29 Jahren, die auf ihrer aktiven Suche nach einem Partner von einem Betrüger in die Falle gelockt wurden. 94 % der betroffenen jungen Frauen waren zum Zeitpunkt des Betrugs nicht auf Partnersuche.

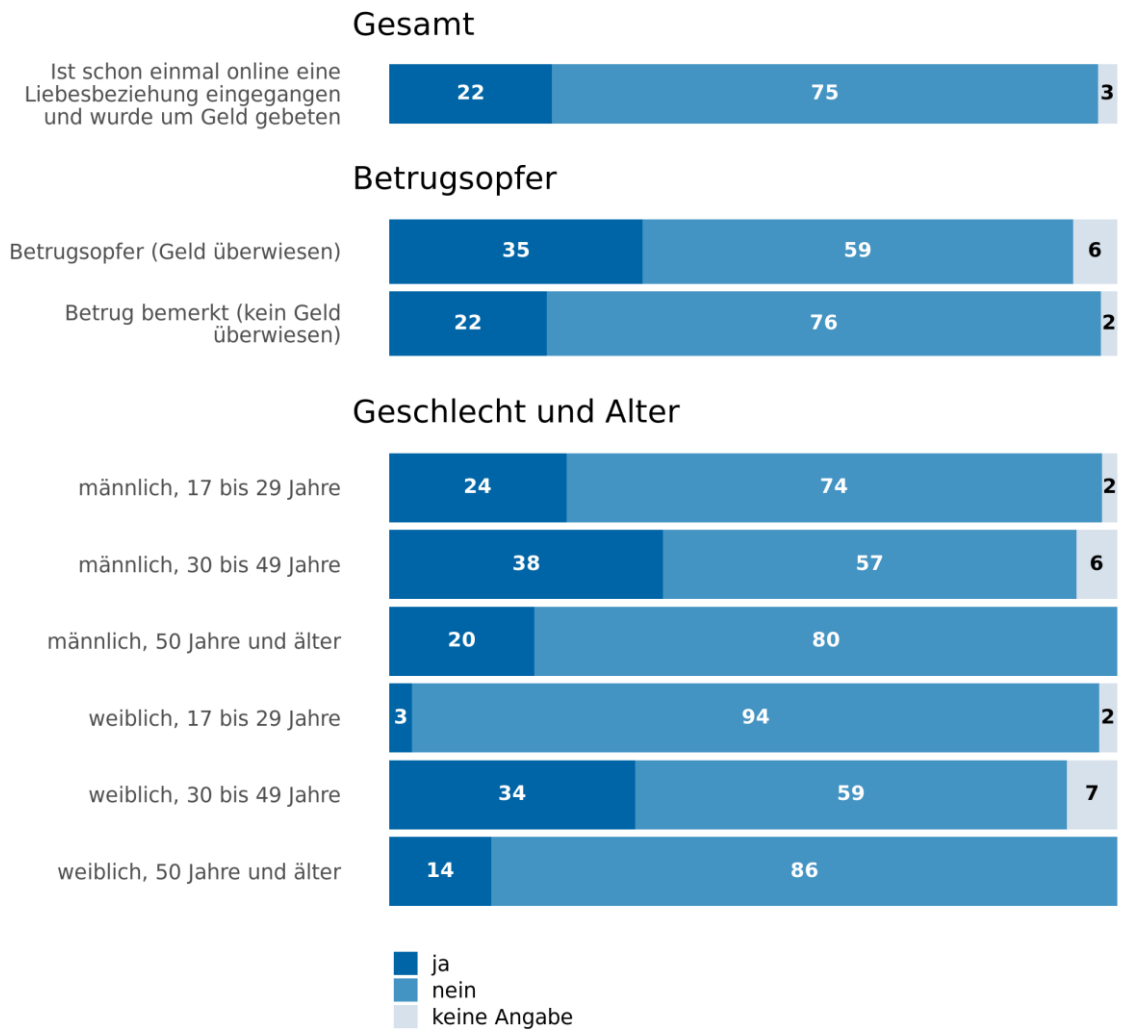


Abbildung 28: Aktiv auf Partnersuche

15 % hatten zudem das Gefühl, mit dem Täter in einer ernsthaften Beziehung zu stehen. Bei den Betroffenen, die Geld überwiesen haben, beläuft sich dieser Anteil auf 43 %. Insbesondere unter weiblichen Opfern mittleren Alters (30-49 Jahre) war der Prozentsatz jener, die von einem ernst zu nehmenden Verhältnis mit der Onlinebekanntschaft ausgingen, hoch (28 %). Im Gegensatz dazu hatten nur 13 % all jener Betroffenen, die den Betrug rechtzeitig bemerkten, das Gefühl, mit dem Täter in einem ehrlichen partnerschaftlichen Verhältnis zu sein.

Als Auslöser für das dem Täter entgegengebrachte Vertrauen wurden zumeist genannt:

- intensiver Kontakt, den man mit dem Täter pflegte
- das Gefühl von Liebe, Vertrautheit und Geborgenheit
- Schmeicheleien und Komplimente

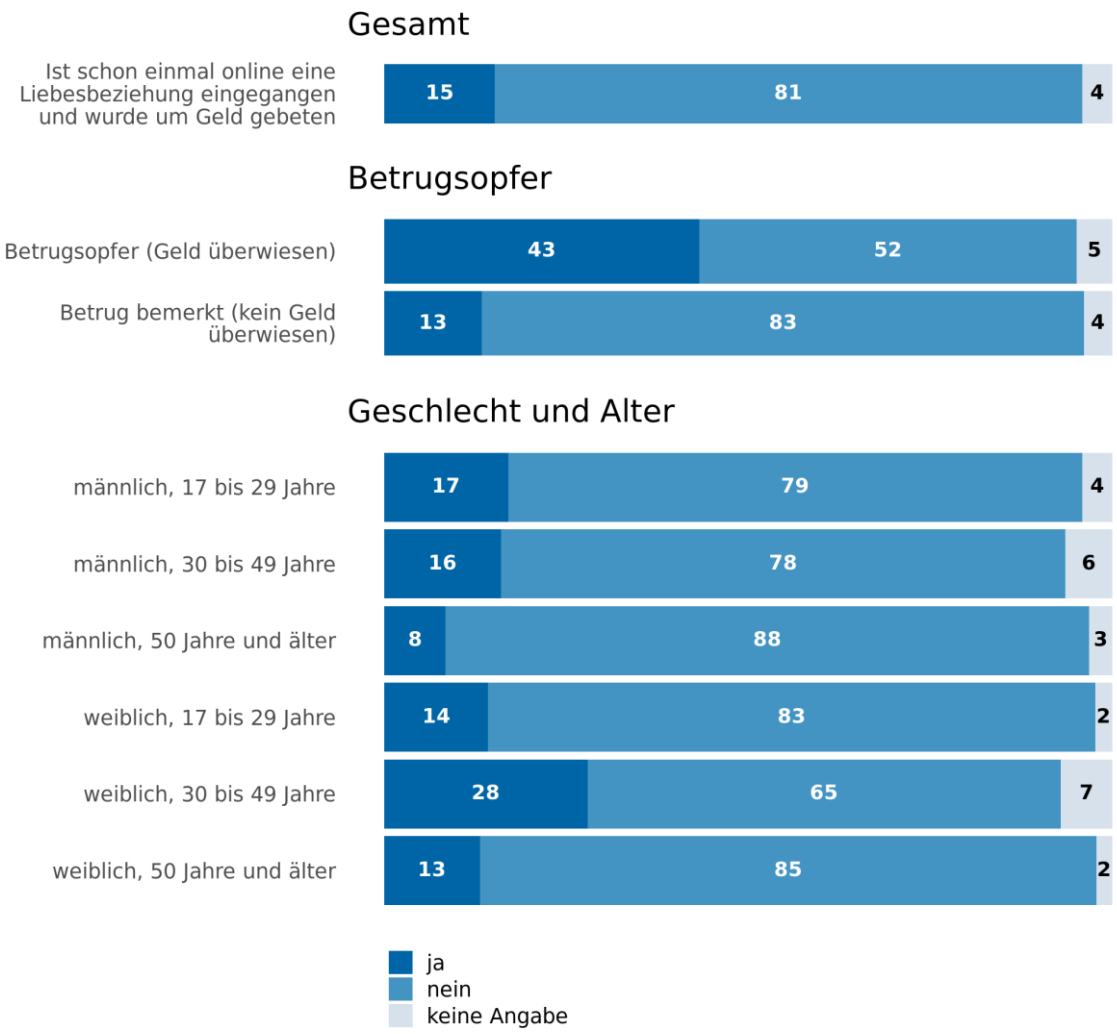


Abbildung 29: Gefühl der Ernsthaftigkeit der Beziehung

4.2.16. Andere Formen von Cybercrime

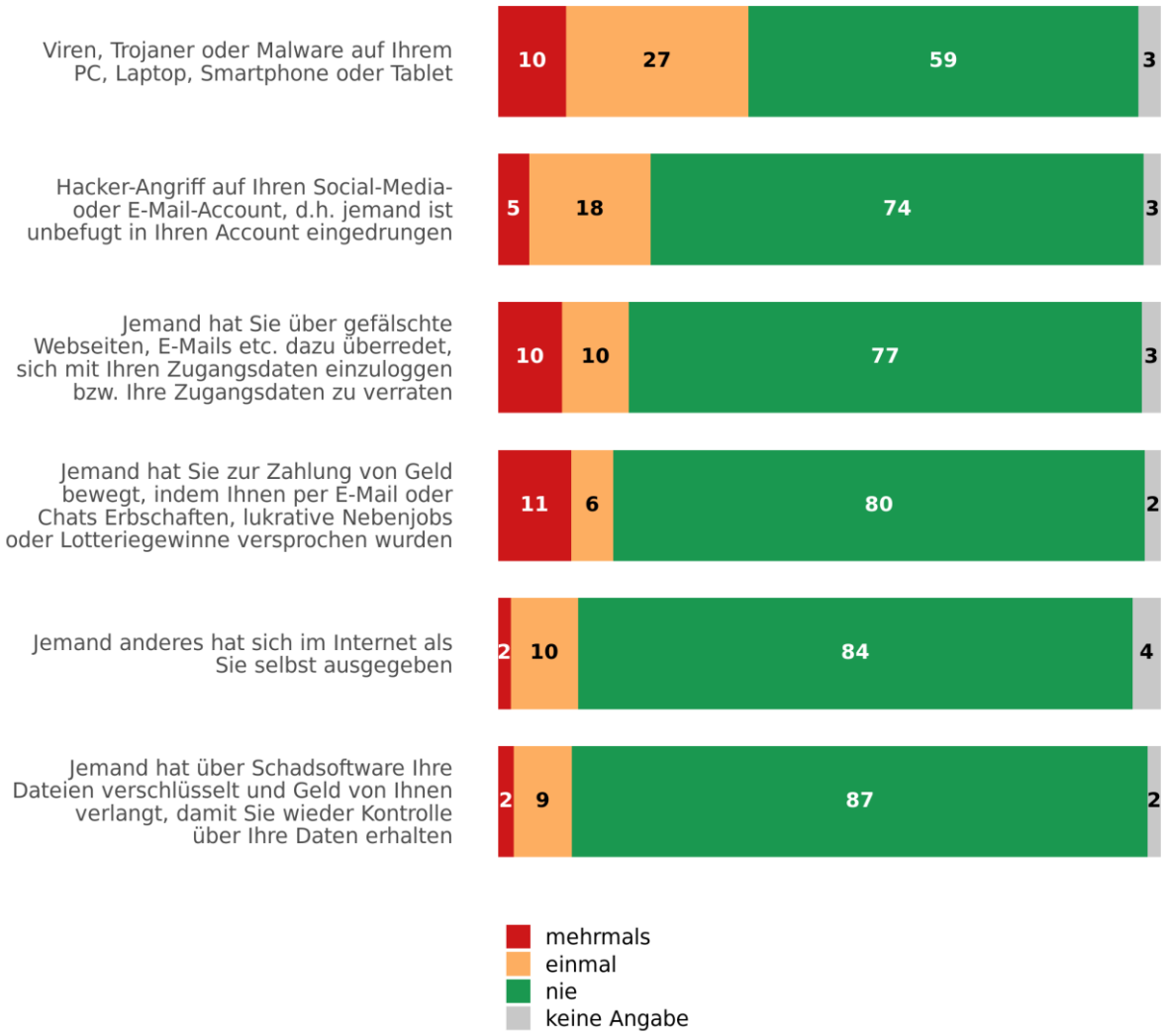


Abbildung 30: Von Internetbetrug betroffen – Teil 1

Am häufigsten wurden in diesem Zusammenhang E-Mails und Chats genannt, in denen mehrmals lukrative Nebenjobs, Erbschaften oder Lotteriegewinne versprochen wurden (11 %). Gefälschte Websites und E-Mails, über welche Zugangsdaten abgefragt wurden, sowie Trojaner und Malware wurden jeweils weiteren 10 % der Befragten schon des Öfteren zum Verhängnis. 27 % der im Rahmen der KFV-Studie befragten Personen fielen bereits Malware bzw. Trojanern zum Opfer, 23 % waren zumindest einmal einem Hacker-Angriff ausgesetzt. In 12 % der Fälle kam es zum Identitätsdiebstahl im Netz, außerdem wurden 11 % damit erpresst, dass eine Schadsoftware ihre Daten verschlüsselte und sie die Kontrolle verloren.

Abbildung 31: Von Internetbetrug betroffen – Teil 2

Online bestellte Waren oder Dienstleistungen haben rund ein Viertel (24 %) der Befragten schon einmal bezahlt oder angezahlt, aber nie erhalten, 15 % waren bereits mit einer Aufforderung zum Versenden von Nacktfotos konfrontiert, und weitere 15 % sahen Videos und Fotos von sich selbst im Internet, zu deren Veröffentlichung sie nie ihr Einverständnis gegeben hatten.

Von Cybermobbing waren 11 % der Interviewpartner*innen bereits persönlich betroffen, bei 9 % wurden die Bank- oder Kreditkartendaten über Phishing oder Skimming gestohlen, und 8 % wurden zur Zahlung eines Geldbetrags genötigt, um die Veröffentlichung von Nacktfotos zu verhindern.

4.3. Zusammenfassung der Ergebnisse

Mit ihren vielfältigen Nutzungsmöglichkeiten begleiten uns digitale Geräte im Alltag rund um die Uhr – sofern wir das wollen. Die österreichische Bevölkerung nutzt das Internet pro Tag im Durchschnitt drei Stunden lang für private Zwecke, wobei mit 77 % die Nutzung von Messenger-Diensten und mit 70 % der Einsatz von E-Mail-Korrespondenz an der Spitze der (fast) täglichen Anwendungen stehen. Vier von zehn Befragten (40 %) haben schon einmal Menschen über soziale Netzwerke kennengelernt, 23 % über Singlebörsen oder Dating-Apps. Am öftesten sind es junge Menschen, insbesondere Männer unter 30 Jahren, die Dating-Apps nutzen und im Allgemeinen häufiger Kontaktanfragen von Fremden annehmen. Knapp 6 von 10 Befragten kennen ihre Chatpartner*innen persönlich, nur bei jungen Leuten sind es weniger als die Hälfte (Männer 44 %, Frauen 47 %).

Die meisten Nutzer*innen scheinen sich der möglichen Risiken im Zusammenhang mit der Internetnutzung bewusst zu sein, wobei hier zumeist Delikte wie Hacking und Phishing genannt werden. Dies hat wohl auch damit zu tun, dass ebendiese Formen des Cybercrime zu den häufigsten zählen, die schon einmal persönlich erlebt wurden. Der Summenindex zu den Sicherheitsbedenken im Umgang mit persönlichen elektronischen Daten im Internet zeigt jedoch, dass knapp ein Drittel der Bevölkerung (30 %) geringe Bedenken hat, wobei sich insbesondere junge Männer und ältere Frauen am wenigsten besorgt zeigen.

Im Vergleich zu anderen Cybercrime-Delikten wird Romance Scam weniger stark als Gefahr wahrgenommen. Rund 9 von 10 Befragten ist das Phänomen bekannt. Dennoch hegen 4 von 10 Internetnutzenden wenige oder keinerlei Bedenken im Zusammenhang mit dieser Art der Täuschung im Onlinebereich: 21 % machen sich wenige Sorgen, und weitere 21 % zeigen sich ganz und gar unbekümmert.

Ein Fünftel der im Rahmen der KFV-Studie befragten Personen ist selbst schon Opfer eines Romance Scam geworden, hat aber den Betrugsversuch schon früh, d.h., als der Kontakt zustande kam, bemerkt. 11 % erkannten die Täuschung nach der ersten Geldforderung, und 5 % der Befragten haben sogar schon einmal Geld an eine vermeintliche Liebschaft im Internet überwiesen (Viktimisierung im engeren Sinn). Am häufigsten betroffen waren jüngere Personen, vor allem junge Männer unter 30 Jahren. In dieser Altersgruppe ist der Anteil der Betroffenen rund dreimal so hoch wie bei älteren Internetnutzenden. Weitere Erkenntnisse der Studie sind, dass Betroffene tendenziell öfter Kontaktanfragen von Fremden annehmen und dass die meisten Opfer ihre Schädiger über Apps für Freundschaften und gemeinsame Interessen kennenlernten (22 %).

Betreffend die Häufigkeit der Betrugsversuche kann man auf Basis der Interviews folgende Rückschlüsse ziehen: Ein Viertel der jungen Menschen unter 30 Jahren, die schon einmal in einer Online-Liebesbeziehung um Geld gebeten wurden, ist bereits dreimal oder öfter Opfer eines solchen Betrugsversuchs geworden. Demgegenüber sind mit 42 % (Männer) bzw. 44 % (Frauen) ältere Internetnutzende ab 50 Jahren stärker dafür anfällig, mehrmals Opfer eines derartigen Betrugsversuchs zu werden. Wenn also ältere Menschen von Romance Scam betroffen sind, so passiert ihnen dies in der Regel häufiger. Wurden hingegen Überweisungen im Rahmen einer vorgetäuschten Beziehung getätigt, war der Lerneffekt größer, und wiederholte Betrugsversuche

traten seltener auf. Während 21 % der jungen Opfer in den letzten 12 Monaten von Romance Scam betroffen waren, sind es bei den älteren mit 41 % doppelt so viele.

Überwiegend gingen die Forderungen von den Tätern aus: 51 % der Betroffenen wurden um Geld und 17 % um Sachgeschenke gebeten. Nur in 2 % der Fälle boten die Opfer eine finanzielle Zuwendung von sich aus an. Die von den Betrügern erhaltenen Beträge beliefen sich im Durchschnitt auf 400 Euro. Rund ein Viertel der zahlenden Betroffenen überwies nicht mehr als 100 Euro. Dennoch schickten immerhin 15 % der Betrugsopfer mehr als 1.500 Euro an ihre vermeintliche Liebe im Internet. Von den Opfern gingen 21 % zur Polizei, um den Vorfall zu melden, allerdings erstatteten nur 6 von 10 Personen, die den Betrug bzw. Betrugsversuch der Polizei meldeten, tatsächlich auch Anzeige. Mehr als ein Viertel aller Betroffenen machte den Betrug im Internet publik, und 16 % suchten Hilfe in einschlägigen Foren oder Facebook-Gruppen. Personen, die dem Täter Geld überwiesen hatten, zogen vergleichsweise häufiger Konsequenzen als jene, die dies nicht getan hatten.

Zum Zeitpunkt des Betrugs fühlten sich 3 von 10 Opfern einsam oder sehr einsam. In Sachen Einsamkeit zeigt sich ein Unterschied zwischen den Personen, die Geld überwiesen haben, und jenen, die den Betrug noch rechtzeitig bemerkten. Mehr als die Hälfte derjenigen, die eine Überweisung vornahmen, fühlten sich (sehr) einsam. Im Kontrast dazu waren unter den Internetnutzern, die keine finanzielle Zuwendung an den Betrüger boten, nur 29 % von Einsamkeit betroffen. Das Gefühl der Einsamkeit spielte diesbezüglich auch bei den jüngeren und mittleren Altersgruppen eine größere Rolle als bei anderen Kohorten.

Knapp ein Drittel der Getäuschten war zum Zeitpunkt des Romance Scam in einer glücklichen Beziehung. Alleinstehende überwiesen verhältnismäßig öfter Geld als andere Kohorten, und rund ein Viertel aller Betroffenen war aktiv auf Partnersuche. Letzteres trifft insbesondere auf Opfer im engeren Sinn sowie auf Personen der mittleren Altersgruppe (30-49 Jahre) zu. Außerdem hatten 15 % der Betroffenen das Gefühl, in einer echten Beziehung zum Täter zu stehen. Mehr als ein Viertel der weiblichen Opfer mittleren Alters und fast die Hälfte derjenigen, die eine Geldtransaktion vornahmen, gingen von einem ernst zu nehmenden partnerschaftlichen Verhältnis mit der vermeintlichen Online-Liebe aus. Hingegen hatten nur 13 % der Betroffenen, die den Betrug rechtzeitig bemerkten, das Gefühl, in einer ernsthaften Beziehung mit dem Romance Scammer zu stehen. Dieser Eindruck entstand vor allem durch den intensiven Kontakt zum Täter, das Gefühl von Liebe, Vertrautheit und Geborgenheit sowie durch Schmeicheleien und Komplimente (spontane Nennungen der Befragten).

Die vermehrte Verlagerung der Partnerschaftssuche in die digitale Welt bringt Möglichkeiten, aber auch Tücken mit sich. Romance Scam ist in Österreich angekommen und hat in den letzten 12 Monaten zugenommen. Vorsicht ist bei der Annahme fremder Kontaktanfragen geboten. Eine Identitätsrecherche im Internet kann schon einmal Abhilfe schaffen, doch ist es besser, eine Person von vornherein persönlich kennenzulernen, bevor man sich in ein Vertrauensverhältnis mit ihr begibt und finanzielle Unterstützung gewährt. Jedenfalls sollte man Skepsis walten lassen, wenn der Onlinepartner um finanzielle Zuwendungen bittet. Dies kann dabei helfen, letzten Endes einer leidvollen (Ent-)Täuschung vorzubeugen.

5. Fazit

Love Scam ist eine perfide Form des Betrugs, die meist schwerwiegende Auswirkungen auf die Opfer hat. Die emotionalen und psychologischen Folgen können verheerend sein, da die Betroffenen oft mit einem Gefühl des Verrats, der Scham und des Vertrauensverlusts konfrontiert werden. Sie haben möglicherweise eine tiefe Bindung zu einer fiktiven Person aufgebaut und sind dann mit der brutalen Realität konfrontiert, dass ihre Gefühle und Investitionen in eine Lüge geflossen sind.

Neben den schmerzlichen emotionalen Konsequenzen erleiden die Opfer in vielen Fällen auch erhebliche finanzielle Schäden. Betrüger*innen nutzen geschickt die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus und erschleichen sich Geld oder andere Wertgegenstände unter dem Vorwand von Notlagen oder gemeinsamen Zukunftsplänen. Die finanziellen Verluste können beträchtlich sein und die Geschädigten oft in eine schwierige finanzielle Lage bringen.

Eine der Herausforderungen für Betroffene von Love Scam ist es, ihre Situation anzuerkennen und sich anderen gegenüber zu öffnen. Die Scham und das demütigende Gefühl, auf den Betrug hereingefallen zu sein, können Opfer dazu bringen, ihre Erfahrungen geheim zu halten und keine Hilfe zu suchen. Es ist daher wichtig zu verstehen, dass Love Scam ein weit verbreitetes Problem ist, das jeden treffen kann, und dass das Opfer keine Schuld an dem Betrug trägt. Die Öffentlichkeit muss über dieses kriminelle Phänomen umfassend aufgeklärt werden, um das Stigma der Betroffenen zu reduzieren und diesen zutiefst enttäuschten und vielfach auch finanziell geschädigten Menschen eine Unterstützungsumgebung zu bieten.

Es ist von entscheidender Bedeutung, Anzeige bei den Strafverfolgungsbehörden zu erstatten, wenn man Opfer eines Love Scam geworden ist. Obwohl es schwierig sein kann, Beweise zu sammeln, ist es wichtig, den Betrug zu melden, um andere potenzielle Opfer zu schützen und den Behörden bei der Bekämpfung dieser Art von Kriminalität zu helfen. Durch die Meldung des Vorfalls können auch spezialisierte Einheiten und Organisationen auf das Ausmaß des Problems aufmerksam gemacht werden und Ressourcen zur Unterstützung der Opfer bereitgestellt werden.

Love Scam ist eine raffinierte Form der Internetkriminalität, die vermehrt in den Fokus öffentlicher Aufmerksamkeit rücken muss. Es ist wichtig, sich über die Taktiken und Warnzeichen von Love Scam zu informieren, um sich selbst und andere vor den verheerenden Folgen dieser Betrugsart zu schützen. Im Fall persönlicher Betroffenheit ist es ratsam, sich nicht im stillen Kämmerlein mit Scham und Selbstvorwürfen zu quälen, sondern aktiv Unterstützung zu suchen und Anzeige zu erstatten, um die Strafverfolgung zu erleichtern, das allgemeine Bewusstsein für dieses Problem zu schärfen und anderen zu helfen, sich vor ähnlichen Betrügereien zu schützen. Denn Tatsache ist: Wenn Liebe teuer wird, ist niemand mit diesem Problem allein. Der moderne Heiratsschwindel im Internet boomt – und diesem kriminellen Boom muss mit vereinten Kräften entgegengewirkt werden.

6. Präventionstipps

Um Love Scams zu erkennen und sich vor ihnen zu schützen, sind hier einige wichtige Tipps und Strategien genannt:

- Seien Sie skeptisch: Behalten Sie eine gesunde Skepsis bei, wenn Sie jemanden online kennenlernen. Nehmen Sie sich Zeit, um die Person besser kennenzulernen, und lassen Sie sich nicht zu schnell von romantischen Gesten oder Liebesbekundungen mitreißen.
- Überprüfen Sie die Identität: Untersuchen Sie sorgfältig das Online-Profil und die im Internet verfügbaren Daten der mit Ihnen in Kontakt stehenden Person. Suchen Sie in diesen Informationen nach Inkonsistenzen oder widersprüchlichen Angaben. Überprüfen Sie, ob die verwendeten Fotos nicht gestohlen sind, indem Sie eine umgekehrte Bildsuche durchführen.
- Achten Sie auf widersprüchliches Verhalten: Wenn die Person sich in widersprüchlichen Aussagen verstrickt oder plötzliche Verhaltensänderungen zeigt, sollten Sie wachsam sein. Betrüger*innen verwenden oft Ausreden und Lügen, um ihre Täuschung aufrechtzuerhalten.
- Seien Sie vorsichtig bei finanziellen Forderungen: Seien Sie misstrauisch, wenn die Person Geld oder finanzielle Unterstützung verlangt. Betrüger*innen nutzen oft finanzielle Notlagen als Vorwand, um ihre Opfer auszunutzen. Geben Sie niemals persönliche Bankdaten oder andere finanzielle Informationen an Unbekannte weiter.
- Bleiben Sie in Ihrem sozialen Netzwerk: Teilen Sie Informationen über Ihre Online-Beziehungen mit Freunden oder Familienmitgliedern. Das Einbeziehen anderer Menschen kann helfen, objektive Perspektiven und Ratschläge zu erhalten und Betrügereien frühzeitig zu erkennen.
- Seien Sie vorsichtig bei der Weitergabe persönlicher Informationen: Geben Sie nicht zu früh persönliche Informationen preis, wie Ihre Adresse, Ihre Telefonnummer oder Ihre Bankdaten. Schützen Sie Ihre Privatsphäre und geben Sie generell nur jenen Menschen derartige Informationen preis, denen Sie voll und ganz vertrauen können.
- Verwenden Sie sichere Kommunikationsmittel: Achten Sie darauf, dass Sie sichere Kommunikationsmittel verwenden, insbesondere wenn es um sensible Informationen geht. Verwenden Sie verschlüsselte Messaging-Apps oder sichere Online-Dating-Plattformen, um Ihre persönlichen Daten zu schützen.
- Vertrauen Sie Ihrem Bauchgefühl: Wenn Ihnen etwas an einer Online-Beziehung seltsam oder unangenehm erscheint, vertrauen Sie Ihrem Instinkt. Wenn etwas zu schön erscheint, um wahr zu sein, ist es möglicherweise nicht real. Hören Sie auf Ihre Intuition und brechen Sie den Kontakt ab, wenn Sie sich unsicher fühlen.

Es ist wichtig, sich dessen bewusst zu sein, dass Love Scams existieren und dass Betrüger*innen raffinierte Taktiken anwenden, um ihre Opfer zu täuschen. Durch eine Kombination von Vorsicht, gesundem Menschenverstand und der Aufrechterhaltung einer kritischen Denkweise können Sie dazu beitragen, sich vor Love Scams zu schützen.

Abbildungsverzeichnis

Literaturverzeichnis

Bundeskriminalamt, 2022. *Cybercrime Report 2021,* Wien: Bundesministerium für Inneres.

Dove, M., 2021. *The Psychology of Fraud, Persuasion and Scam Techniques.* London and New York: Routledge.

FBI, 2021. *FEDERAL BUREAU OF INVESTIGATION.* [Online] Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams [Zugriff am 08 03 2022].

Jakobsson, M., 2016. *Understanding Social Engineering Based Scams.* New York: Springer Science+Business Media.

Thiel, C., 2020. Liebesschwindel im Cyberspace. Aktuelle Forschungsergebnisse zum Phänomen des Romance Scam im Überblick. In: T. Rüdiger & P. S. Bayerl, Hrsg. *Cyberkriminologie. Kriminologie für das digitale Zeitalter.* Wiesbaden: Springer Fachmedien Wiesbaden GmbH, pp. 241-267.

Wikipedia, 2022. *Wikipedia.* [Online] Available at: https://de.wikipedia.org/wiki/Love_Bombing#cite_note-bzw-mag-1 [Zugriff am 25 08 2022].

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

Medieninhaber und Herausgeber: Kuratorium für Verkehrssicherheit
Verlagsort: Wien
Herstellung: Eigendruck

SAFETY FIRST!