Co-funded by
the European Union

KAMPF GEGEN LIEBESBETRUG

2023-1-DE02-KA210-VET-000151265

Abstrakt

Fight Against Love Scam (FALS) ist eine europäische Initiative zum Schutz und zur Stärkung von Erwachsenen ab 50 Jahren vor Online-Liebesbetrug. Das Projekt vereint Partner aus Deutschland, den Niederlanden und Italien, um das Bewusstsein für dieses Thema zu schärfen und Erwachsenenbildner, Senioren und ihre Familien mit dem nötigen Wissen und den erforderlichen Werkzeugen auszustatten, um Liebesbetrug zu erkennen, zu verhindern und angemessen darauf zu reagieren.

Durch die Erstellung eines digitalen Leitfadens, praktischer Tests und eines Online-Kurses fördert FALS Online-Sicherheit, emotionales Wohlbefinden und aktives Altern. Das Projekt regt zudem die Zusammenarbeit zwischen Pädagogen, Sozialarbeitern und Gemeinden an, um stärkere Unterstützungsstrukturen für ältere Menschen aufzubauen.
Durch die Kombination von Aufklärung, Prävention und Empathie strebt FALS danach, die digitale Welt zu einem sichereren Ort für alle zu machen.

Projektpartner

EUTH WONDERS E.V

IGOR VITALE INTERNATIONAL

ECREC

Co-funded by the European Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen jedoch ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.

Inhaltsverzeichnis

Co-funded by
the European Union

Eine Nachricht der Projektpartner

Liebe Leserin, lieber Leser,

Wir heißen Sie herzlich willkommen zu diesem Leitfaden, der aus unserem gemeinsamen Engagement in Deutschland, den Niederlanden und Italien entstanden ist, einen der schutzbedürftigsten Bereiche unserer Gesellschaft zu unterstützen und zu stärken: ältere Erwachsene, die sich in der digitalen Welt zurechtfinden müssen.

Fight Against Love Scam (FALS) entstand aus einem einfachen, aber dringenden Bedürfnis: den emotionalen und finanziellen Schaden durch Liebesbetrug zu verhindern und Erwachsenenbildnern, Familien und Senioren selbst das nötige Wissen für mehr Sicherheit im Internet zu vermitteln. Zu viele Menschen sind im Stillen betroffen, und wir glauben, es ist an der Zeit, Wissen, Fürsorge und Gemeinschaft in den Vordergrund zu rücken.

Diese Broschüre ist mehr als nur eine Informationsquelle; sie ist ein Zeichen der Solidarität und des Respekts. Sie bietet Einblicke, praktische Anleitungen und Erfahrungsberichte, um Warnsignale zu erkennen, die digitale Resilienz zu stärken und sich gegenseitig im Umgang mit Online-Beziehungen zu unterstützen.

Wir hoffen, dass Sie auf diesen Seiten Trost, Klarheit und Zuversicht finden.

Herzliche Grüße,

Das FALS-Team
EUW(**Deutschland**)
ECREC (**Niederlande**)
IVI (**Italien**)

Co-funded by
the European Union

Handbuchübersicht

Inhalt des Handbuchs

Das Handbuch enthält 3 Kapitel, die den Inhalt des Methodenhandbuchs formulieren:

1. Hinter der Maske: Liebesbetrug verstehen.
2. Unterstützung durch Fürsorge: Bewährte Praktiken für Pädagogen.
3. Verteidigung: Grundlagen der Cybersicherheit für Anfänger.
4. Wissen & Wachstum: Selbsteinschätzung und -bewertung.

Wesentliche Elemente der Kapitel

Kapitel 1: Ein Überblick darüber, was Liebesbetrug ist, wie er abläuft und wie man ihn erkennt und verhindern kann.

Kapitel 2: Praktische Hinweise für Erwachsenenbildner zur Unterstützung älterer Menschen, zum Erkennen psychischer Verletzlichkeit und zum Umgang mit Betrugsfällen.

Kapitel 3: Einführung in die Online-Sicherheit, Phishing-Erkennung und Plattformbewusstsein für technisch nicht versierte Nutzer.

Kapitel 4: Eine Reihe kurzer Tests zur Überprüfung des Verständnisses von Liebesbetrug, emotionaler Intelligenz und digitaler Sicherheit. Enthält eine Analyse auf Basis von Infografiken.

Co-funded by
the European Union

Über FALS

Co-funded by
the European Union

Einführung

Die digitale Welt hat unzählige Möglichkeiten zur Kontaktaufnahme eröffnet, doch mit diesen Möglichkeiten gehen auch neue Risiken einher. Eine der emotional belastendsten Gefahren für ältere Menschen ist heute der sogenannte „Liebesbetrug“, eine Form des Online-Betrugs, die Verletzlichkeit und Vertrauen ausnutzt.

Das Projekt „Kampf gegen Liebesbetrug“ (FALS) ist eine europäische Kooperation zwischen Partnern in Deutschland, den Niederlanden und Italien mit dem gemeinsamen Ziel, Menschen ab 50 Jahren und ihre Bezugspersonen zu schützen, zu informieren und zu stärken. Mit diesem Handbuch möchten wir Erwachsenenbildnern das Wissen und die Werkzeuge vermitteln, die sie benötigen, um Anzeichen von Online-Liebesbetrug zu erkennen, psychologische und soziale Unterstützung anzubieten und grundlegende Cybersicherheitspraktiken auf verständliche und einfühlsame Weise zu vermitteln.

Dieser Leitfaden ist mehr als nur eine Anleitung; er ist ein Aufruf zum Handeln. Indem wir das Bewusstsein schärfen und die Kompetenzen von Pädagogen und Pflegekräften stärken, können wir Schäden verhindern, die Genesung unterstützen und Würde und Sicherheit älterer Menschen in digitalen Räumen fördern.

Wir laden Sie ein, die folgenden Kapitel zu erkunden, die Ihnen alle dabei helfen sollen, ein besserer Fürsprecher, Beschützer und Aufklärer im Kampf gegen Liebesbetrug zu werden.

FALS-ZIELE

- **Sensibilisierung älterer Erwachsener (50+)** für die Risiken und Taktiken von Online-Liebesbetrug, um ihnen zu helfen, Warnsignale zu erkennen und emotionalen und finanziellen Schaden zu vermeiden.

- **Wir möchten Erwachsenenbildner stärken**, indem wir ihnen Wissen, Werkzeuge und Methoden an die Hand geben, um Senioren in digitalen Räumen zu unterstützen und frühe Anzeichen psychischer Verletzlichkeit zu erkennen.

- **Wir unterstützen Familien und Pflegepersonen**, indem wir ihnen praktische Anleitungen geben, damit sie Warnsignale erkennen, mit ihren Angehörigen kommunizieren und angemessen auf vermutete Betrugsversuche reagieren können.

- **Förderung der digitalen Sicherheit** durch die Vermittlung von Grundlagen der Cybersicherheit, die Senioren helfen, sich sicherer auf Online-Plattformen zu bewegen und risikoreiche Interaktionen zu vermeiden.

- **Ein nachhaltiges Bildungsinstrument** soll durch die Entwicklung eines umfassenden Leitfadens, von Selbstbewertungstests und eines digitalen Videokurses geschaffen werden, der von Erwachsenenbildungszentren, Sozialarbeitern und Familienmitgliedern in ganz Europa genutzt werden kann.

- **Förderung von aktivem Altern und Resilienz** durch die Stärkung digitaler Kompetenzen und des emotionalen Wohlbefindens, damit ältere Erwachsene in ihren Online-Interaktionen engagiert, unabhängig und sicher bleiben können.

Zielgruppe

01 Primäre Zielgruppe: Ältere Erwachsene (ab 50 Jahren):

- Die Hauptnutzer des Projekts sind Menschen mit einer zunehmenden Online-Aktivität, denen es jedoch oft an digitaler Kompetenz und emotionaler Unterstützung mangelt, um sich vor Liebesbetrug und ähnlichen Online-Aktivitäten zu schützen. Das Projekt zielt speziell darauf ab, ihr Bewusstsein, ihre Widerstandsfähigkeit und ihre digitale Sicherheit zu stärken.

02 Erwachsenenbildner und Ausbilder

- Fachkräfte aus der Erwachsenenbildung, Gemeindezentren oder Programmen zur digitalen Kompetenzentwicklung werden geschult und mit Werkzeugen ausgestattet, um Liebesbetrug bei älteren Lernenden zu erkennen, zu verhindern und zu bekämpfen.

03 Familienmitglieder und Pflegekräfte

- Verwandte und enge Kontaktpersonen von Senioren, die oft als Erste Verhaltensänderungen bemerken und im Falle eines vermuteten Betrugs emotionale oder logistische Unterstützung anbieten können.

04 Gesundheitswesen, Sozialarbeiter, Gemeindezentren, Nichtregierungsorganisationen und Einrichtungen der Erwachsenenbildung

- Fachkräfte, die mit Senioren arbeiten, die aufgrund von Betrug oder Anfälligkeit für Online-Manipulation unter psychischen Belastungen leiden.
- Organisationen, die das von FALS entwickelte Handbuch, die Schulungsmaterialien und den digitalen Kurs in ihre Bildungs- oder Sensibilisierungsaktivitäten einbeziehen können.

Hinter der Maske: Liebesbetrug verstehen

Co-funded by
the European Union

Agnese Federica Gobbi

Agnese Federica Gobbi, geboren in Slowenien, besitzt einen Bachelor-Abschluss in Psychologie und absolviert derzeit ein Masterstudium in Psychologie an der Universität Guglielmo Marconi in Rom. Seit 2022 ist sie eine geschätzte Mitarbeiterin bei Igor Vitale International s.r.l., wo sie sich auf Audio- und Videoproduktion, Fotografie, Texterstellung und Webseitengestaltung spezialisiert hat. Agnese hat aktiv an über 15 Projekten in verschiedenen Bereichen wie Gastgewerbe, Kunsthandwerk, Ökologie und Psychologie mitgewirkt. Ihre Arbeit führte sie in verschiedene Teile Europas, die Karibik, Französisch-Polynesien, Grönland sowie Regionen Süd- und Ostasiens und unterstreicht ihre globale Perspektive und ihr multidisziplinäres Fachwissen.

Co-funded by
the European Union

1 EINFÜHRUNG IN DEN LIEBESBETRUG

Liebesbetrug, auch bekannt als Romanzenbetrug, ist eine Form des Online-Betrugs, bei der Betrüger emotionale Bindungen ausnutzen, um Menschen finanziell zu schädigen. Seine Wurzeln liegen in historischen Betrugstaktiken, wie dem „spanischen Gefangenenbetrug“ des 16. Jahrhunderts. Auch heute noch manipulieren moderne Liebesbetrüger ihre Opfer, indem sie falsche Beziehungen und idealisierte Persönlichkeiten erschaffen. Die Verbreitung digitaler Kommunikationsplattformen bietet diesen Maschen ideale Bedingungen, da Betrüger anonym agieren und ihre Reichweite global ausdehnen können. Opfer werden oft durch sorgfältig gestaltete Profile und überzeugende Geschichten geködert, was zu erheblichem emotionalem und finanziellem Schaden führt (Cemmi, o. J.; Coluccia et al., 2020; Europol, 2023). In den letzten Jahren sind Liebesbetrügereien raffinierter geworden. Betrüger setzen verschiedene psychologische Taktiken ein, um die Kontrolle über ihre Opfer zu erlangen und deren Kooperation zu erzwingen. Das Verständnis der Mechanismen und Auswirkungen von Liebesbetrug sowie das Erkennen von Frühwarnzeichen sind für die Bekämpfung dieser betrügerischen Aktivitäten unerlässlich.

1.1 Was ist ein Liebesbetrug?

Der Liebesbetrug, international auch als Romance Scam bekannt, ist eine Form des Online-Betrugs, bei dem Betrüger ihre Opfer manipulieren, um über das Internet an Geld zu gelangen. Dies geschieht durch falsche Liebesversprechen. Laut einem Urteil des italienischen Kassationsgerichtshofs (Nr. 25165/2019) sind Personen, die romantisches Interesse vortäuschen, um sich wirtschaftliche oder materielle Vorteile zu verschaffen, gemäß Artikel 640 des italienischen Strafgesetzbuches strafbar (Coluccia et al., 2020 in Cemmi, o. J.). Die weitverbreitete Nutzung von Technologie hat die Zunahme und Weiterentwicklung dieser Betrugsmasche begünstigt. Eine Studie in Italien ergab, dass 3 % der Bevölkerung Opfer von Liebesbetrug geworden sind, wobei Frauen zwischen 40 und 60 Jahren häufiger betroffen sind. Diese Altersgruppe neigt dazu, Beziehungen zu idealisieren und intensive Gefühle zu suchen, was sie anfälliger macht. Doch auch beruflich erfolgreiche Menschen wie Führungskräfte und Pädagogen können Opfer werden (Cemmi, o. J.; Commissariato di PS, o. J.). Obwohl Liebesbetrug heutzutage hauptsächlich über digitale Plattformen stattfindet, hat er uralte Wurzeln. Ein frühes Beispiel ist der „spanische Gefangenenbetrug“ aus dem 16. Jahrhundert, der es auf wohlhabende Personen abgesehen hatte. Dabei gab sich der Betrüger als zu Unrecht inhaftierter spanischer Adliger mit einem versteckten Vermögen aus. Er spielte Verzweiflung vor und bat um Geld für seine Freilassung, im Gegenzug versprach er einen Teil seines Vermögens.

Um die Masche attraktiver zu gestalten, erwähnte der Betrüger eine schöne, unverheiratete Tochter und nutzte romantische und familiäre Appelle, um Empathie und emotionale Beteiligung bei seinen Opfern zu wecken (Beek, 2016 in Cunha, o. J.; Gillespie, 2017 in Cunha, o. J.). Die Analyse des spanischen Gefangenenbetrugs liefert Einblicke in die Grundlagen des modernen Liebesbetrugs. Trotz der vergangenen Jahrhunderte beruht der Kern des Betrugs nach wie vor auf emotionaler Manipulation. Während sich Methoden und Technologien weiterentwickelt haben, ist das Schema im Kern unverändert geblieben: Der Betrüger baut eine vertrauensvolle Beziehung auf, indem er Liebesversprechen und ein gemeinsames Leben verspricht und das Opfer so dazu bringt, Geld und Vermögenswerte preiszugeben (Cunha, o. J.). Dieser Betrug, einer der raffiniertesten und erfolgreichsten seiner Zeit, erforderte die Koordination verschiedener Länder, was die Identifizierung und Festnahme der Betrüger erschwerte. Die Zusammenarbeit zwischen verschiedenen Gerichtsbarkeiten und die logistische Komplexität ermöglichten es diesen Betrügern, mit einem gewissen Maß an Straflosigkeit zu agieren, indem sie die begrenzten Kommunikations- und Strafverfolgungsmöglichkeiten der damaligen Zeit ausnutzten (Gregory & Nikiforova, 2012 in Cunha, o. J.).

Online-Betrug, einschließlich Liebesbetrug, umfasst ein breites Spektrum illegaler Aktivitäten und nutzt digitale Technologien wie soziale Medien und Dating-Apps, um Opfer anzulocken und zu täuschen. Betrüger verwenden digitale Werkzeuge wie VPNs und RATs, um anonym zu bleiben und auf persönliche und finanzielle Daten ihrer Opfer zuzugreifen. Ziel ist es, eine emotionale Abhängigkeit zu erzeugen und fortwährend Geld zu fordern (EUROPOL, 2023; Wang, 2022).

Romance Scams folgen typischerweise einem Muster, bei dem der Betrüger durch idealisierte Profile und tragische Geschichten eine emotionale Bindung zum Opfer aufbaut. Dieser Prozess kann sich über Monate hinziehen und dazu führen, dass das Opfer eine starke emotionale Bindung zum virtuellen Betrüger entwickelt. Diese Dynamik verursacht neben finanziellen Verlusten auch erheblichen psychischen Schaden (Whitty, 2015, 2012, 2018, 2013 in Wang, 2022; Dodge, 2016 in Wang, 2022).

1.2 Wie man die Warnsignale erkennt und ihnen vorbeugt

Liebesbetrug nutzt ausgeklügelte psychologische Manipulationstaktiken, um emotionale und finanzielle Kontrolle über die Opfer zu erlangen. Obwohl Liebesbetrug eine relativ moderne Form der Cyberkriminalität darstellt, basiert er auf einer Reihe gut erforschter Taktiken, die darauf abzielen, emotionale Schwächen zum finanziellen Vorteil auszunutzen.

Studien haben wiederkehrende Strategien identifiziert, die Einzelpersonen helfen können, Liebesbetrug zu erkennen und ihm nicht zum Opfer zu fallen. Ein bemerkenswertes Modell, das diese Phasen beschreibt, wurde von Whitty (in Cemmi, o. J.) entwickelt. Er beschrieb, wie sich Liebesbetrug typischerweise in fünf Phasen entwickelt. Diese Phasen – Profiling, Vorbereitung, Ausbeutung, sexueller Missbrauch und Aufdeckung – verdeutlichen die systematische Vorgehensweise und die manipulative Macht, die Liebesbetrug zugrunde liegen.

Die erste Phase (Profilierungsphase) eines Liebesbetrugs besteht darin, eine falsche Identität zu erstellen, die direkt auf das Opfer zugeschnitten ist. Dieser Prozess beginnt oft damit, dass der Betrüger persönliche Daten aus den Social-Media-Profilen und der Online-Präsenz des Opfers sammelt, darunter Hobbys, Interessen, Lebensziele und persönliche Werte.
Anhand dieser Informationen erstellen Betrüger Profile, die die Persönlichkeit und die Ziele ihres Opfers widerspiegeln. Dadurch erzeugen sie den Eindruck von Kompatibilität und gemeinsamen Interessen, was sie schnell für das Opfer sympathisch macht. Betrüger behaupten mitunter auch, in der Nähe zu wohnen, können sich aber aus beruflichen Gründen vorübergehend nicht treffen. Oftmals geben sie Berufe an, die internationale Reisen erfordern, wie beispielsweise Wehrdienst oder hochrangige Positionen in der Wirtschaft. Diese vorgetäuschte, aber nachvollziehbare Nähe schafft Vertrauen und ein Gefühl der Gemeinsamkeit. So kann der Betrüger die Beziehung zum Opfer vertiefen und gleichzeitig eine bequeme Ausrede für seine Abwesenheit liefern (Whitty, 2015, in Wang, 2022).

Sobald der erste Kontakt hergestellt ist, beginnt für den Betrüger die Phase der emotionalen Vertiefung (Vorbereitungsphase). Diese geht über oberflächliche Gespräche hinaus; der Betrüger versucht, eine scheinbar sehr liebevolle und aufrichtige Beziehung zum Opfer aufzubauen. Dabei bedient er sich der Taktik des sogenannten „Love Bombing“, bei der er das Opfer mit Komplimenten, Liebesbekundungen, Versprechungen einer gemeinsamen Zukunft und ständiger Aufmerksamkeit überschüttet. Diese Taktik ist äußerst effektiv, da sie das menschliche Bedürfnis nach Verbundenheit und Zugehörigkeit anspricht. Betrüger versenden mitunter manipulierte Fotos, romantische Nachrichten und sogar Gedichte, um die emotionale Bindung zu stärken. Mit der Zeit gewinnen sie Einblicke in die Persönlichkeit des Opfers und identifizieren emotionale Schwächen, die sie ausnutzen können. So kann sich beispielsweise ein Opfer, das sich unterbewertet fühlt, durch die Bewunderung des Betrügers geschmeichelt fühlen, während ein einsames Opfer schnell von der ständigen Aufmerksamkeit abhängig werden kann.

Indem der Betrüger diese emotionalen Schwächen seines Opfers nach und nach ausnutzt, positioniert er sich als Lösung für dessen unerfüllte Bedürfnisse und schafft so eine Abhängigkeit, die schwer zu durchbrechen ist. Diese Phase kann sich über Wochen oder sogar Monate erstrecken. In dieser Zeit baut der Betrüger eine emotionale Bindung auf und sorgt dafür, dass sich das Opfer in die Beziehung involviert fühlt. Das Endziel ist die Erzeugung emotionaler Abhängigkeit, wodurch das Opfer eine tiefe Bindung zum Betrüger entwickelt und zunehmend bereit ist, dessen Wünsche zu erfüllen, da es glaubt, diese seien für das Wohlbefinden des anderen unerlässlich (Commissariato di PS, o. J.).

Der Betrüger geht nun von der Vertrauensbildung zur Ausbeutungsphase über. Nachdem er bereits eine starke emotionale Bindung aufgebaut hat, tastet er sich vorsichtig heran, indem er kleine Gefälligkeiten verlangt, die oft als dringende Bedürfnisse getarnt sind. Die ersten Bitten wirken trivial oder vernünftig, wie etwa die Übernahme einer kleineren Notfallausgabe, und werden so formuliert, dass sie die Empathie des Opfers gegenüber einer ihm nahestehenden Person ansprechen. Diese Technik wird als „Fuß in der Tür“ bezeichnet, bei der kleine Bitten schrittweise zu größeren finanziellen Forderungen führen. Sobald der Betrüger erfolgreich Geld erhalten hat, steigert er seine Forderungen weiter. In manchen Fällen inszenieren Betrüger eine ausgeklügelte „Krise“, wie etwa einen plötzlichen Gesundheitsnotfall oder den Betrug durch einen Geschäftspartner, der einen erheblichen Geldbetrag erfordert. Eine andere Taktik, die sogenannte „Tür-ins-Gesicht“-Taktik, besteht darin, zunächst eine hohe, unrealistische Summe zu fordern und diese dann auf einen kleineren Betrag zu reduzieren.

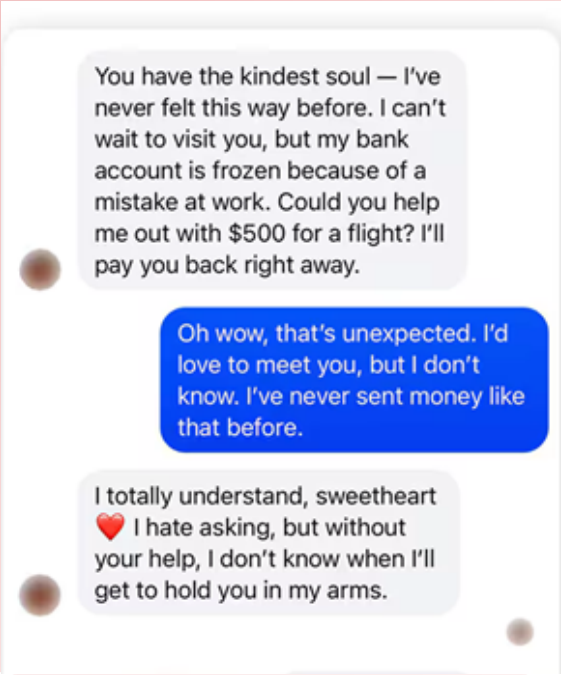
Diese Vorgehensweise nutzt die menschliche Neigung aus, einer Bitte zuzustimmen, nachdem man eine anspruchsvollere abgelehnt hat. Betrüger fordern häufig auch regelmäßig kleinere Beträge für alltägliche Ausgaben, was besonders bei männlichen Opfern vorkommt. Dabei bittet der Betrüger unter dem Vorwand von Routinekosten wie Stromrechnungen oder Miete fortwährend um kleinere Beträge und erweckt so den Eindruck einer Beziehung, die in einem realen Treffen münden soll (Cemmi, o. J.; Whitty & Buchanan, 2012 in Wang, 2022).

Obwohl nicht in allen Fällen, gehen manche Betrüger bei der Manipulation noch einen Schritt weiter und bringen ein sexuelles Element ein. Sobald ein beträchtlicher Geldbetrag erlangt wurde, drängt der Betrüger das Opfer dazu, sexuelle Handlungen per Webcam vorzunehmen, die oft ohne Wissen des Opfers aufgezeichnet werden.

Der Betrüger kann diese Aufnahmen dann zur Erpressung des Opfers nutzen und drohen, sie zu veröffentlichen, falls nicht mehr Geld gezahlt wird. Diese Taktik verursacht psychische Belastung und Demütigung und verschlimmert den emotionalen Schaden, der durch die finanzielle Ausbeutung entstanden ist. Sie zeigt auch, wie weit Betrüger gehen, um Kontrolle über ihre Opfer zu erlangen und ihren finanziellen Gewinn zu maximieren (Whitty & Buchanan, 2012 in Wang, 2022). Sobald der Betrüger der Meinung ist, maximal aus der Beziehung herausgeholt zu haben, bricht er abrupt jeglichen Kontakt zum Opfer ab und versetzt dieses oft in einen Zustand von Schock und Verwirrung (Phase der Enthüllung und des Verlassenwerdens). Dieser plötzliche Bruch zwingt das Opfer, sich der schmerzhaften Realität des Betrugs zu stellen. Der Verlust ist nicht nur finanzieller, sondern auch tiefgreifender emotionaler Natur, da viele Opfer das Gefühl haben, eine echte Beziehung verloren zu haben. Die Folgen sind oft von Gefühlen der Scham, Demütigung und des Verrats begleitet. Die Opfer durchlaufen einen Trauerprozess, der dem Verlust eines geliebten Menschen ähnelt, und die psychischen Folgen können gravierend sein, darunter Depressionen, Angstzustände und Vertrauensprobleme. Die Erkenntnis, dass die Beziehung auf Manipulation beruhte, lässt viele Opfer ihr Urteilsvermögen und ihren Selbstwert infrage stellen, was die emotionale Belastung durch den Betrug noch verstärkt (Whitty & Buchanan, 2012 in Wang, 2022).

Beispiele für Chatdialoge im Zusammenhang mit Liebesbetrug

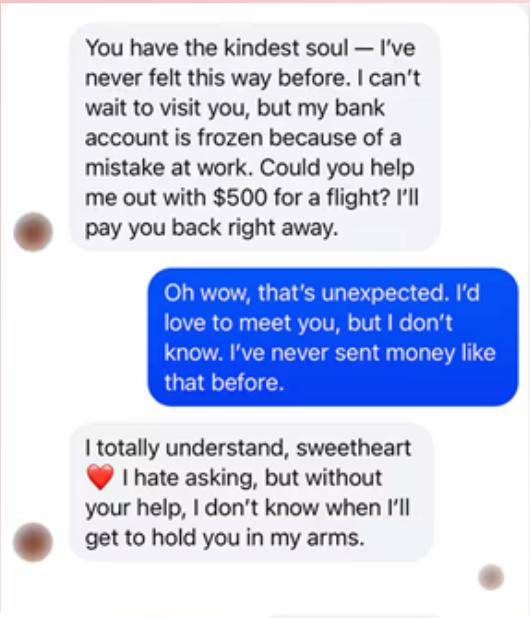
1. Militärbetrug



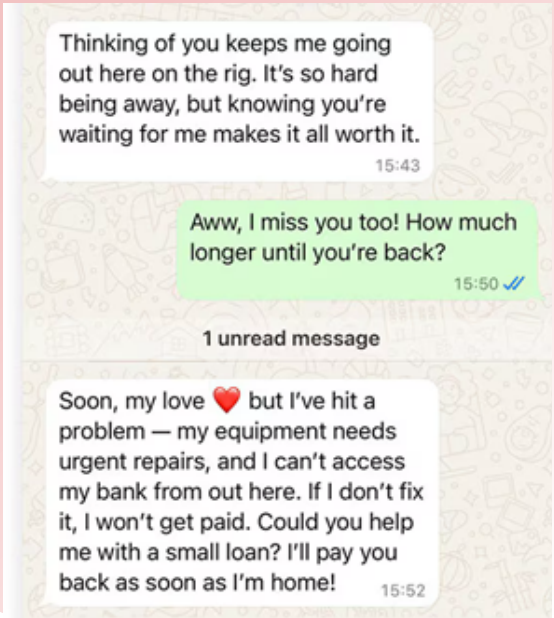
2. Nigerianischer Betrug

3. Krypto-Romantikbetrug

4. Facebook-Romance-Betrug

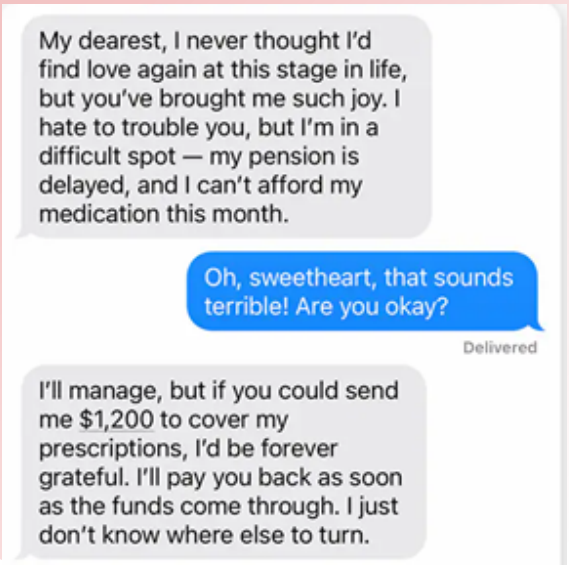


5. Betrug auf Ölplattformen

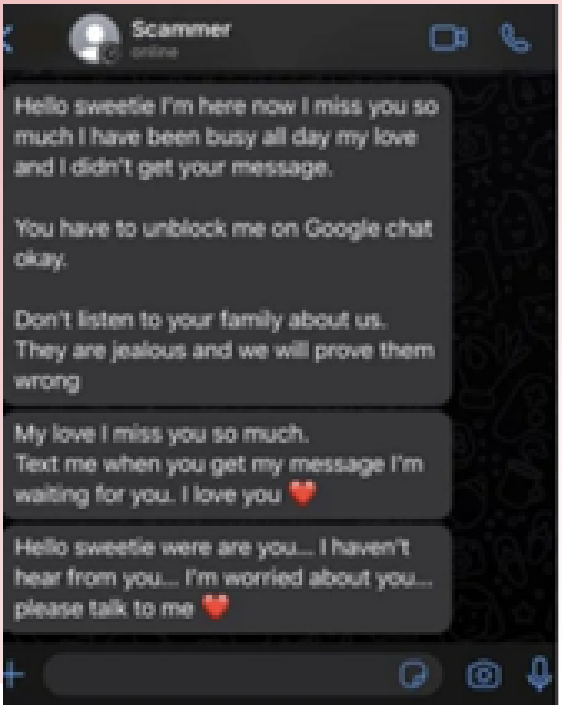


6. Promi-Romanzen

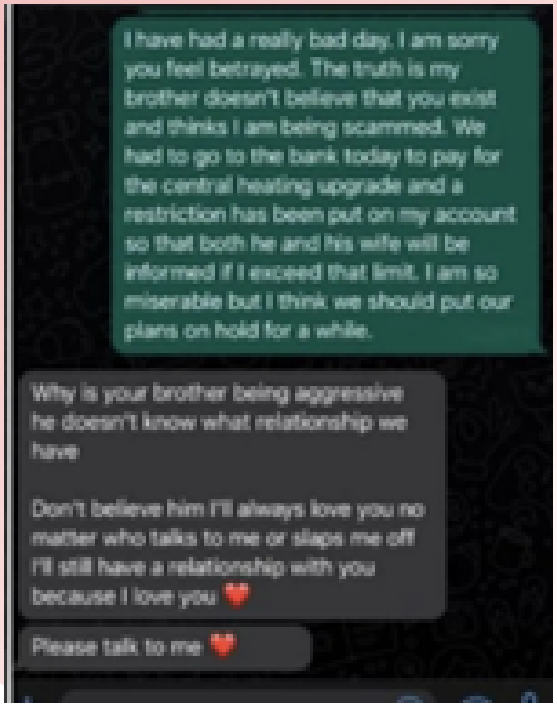
7. Liebesbetrug mit älteren Menschen



8. Beispiel eines Betrügers



9. Beispiel eines Betrügers



1.2.1 Was ist „Sextortion“ und wie erkennt man sie?

Sextortion ist eine Form der sexuellen Erpressung, ein Cyberverbrechen, bei dem Täter drohen, intime Bilder oder Videos zu verbreiten, falls das Opfer ihren Forderungen nicht nachkommt (Interpol, 2022; National Crime Agency, 2021 [NCA]; U.S. Immigration and Customs Enforcement [ICE], 2025). Bei diesen Maschen nutzen die Täter häufig romantische Beziehungen oder Online-Intimität aus, um kompromittierendes Material zu erlangen und dieses später für Geld, sexuelle Gefälligkeiten oder weitere Ausbeutung einzusetzen (Wang, 2024).

Bei Liebesbetrugsfällen beginnt die Erpressung typischerweise, nachdem online Vertrauen aufgebaut wurde: Betrüger erstellen falsche Identitäten auf Dating-Plattformen oder in sozialen Medien, bauen eine emotionale Bindung auf und drängen dann zum Teilen von Nacktbildern oder sexuellen Webcam-Interaktionen, die sie mitunter heimlich aufzeichnen (Kloess et al., 2014). Sobald diese Materialien erlangt sind, dienen sie als Druckmittel. Die Betrüger drohen damit, sie an Familie, Freunde oder Arbeitgeber zu senden, falls ihre Forderungen nicht erfüllt werden (Europol, 2017). In manchen Fällen nutzen die Täter die Drohung mit der Veröffentlichung als „implizite Erpressung“, um die Kontrolle über ihre Opfer zu behalten (Whitty & Buchanan, 2012).

Warnsignale sind unter anderem:

• rasche Eskalation hin zu sexuellen Gesprächen oder Forderungen (Europol, 2017);
• Weigerung, normale Videoanrufe zu tätigen, während gleichzeitig auf dem Erhalt von explizitem Material bestanden wird (Patchin & Hinduja, 2020);
• Profile mit gestohlenen oder inkonsistenten Fotos (Interpol, 2022);
• emotionale Manipulation oder Drohungen mit Selbstverletzung (Wang, 2024);
• und forderte die Opfer auf, schnell von öffentlichen Plattformen auf private Kanäle zu wechseln (NCA, 2021).

Psychologisch gesehen wenden Täter Manipulationsstrategien an, oft durch „Love Bombing“ oder übermäßige Schmeicheleien, um die Abwehrkräfte der Opfer zu schwächen (Coluccia et al., 2020). Sie recherchieren ihre Opfer unter Umständen auch in sozialen Medien, um die Bedrohungen zu verstärken und die unmittelbar bevorstehende Entlarvung vorzutäuschen (Patchin & Hinduja, 2020). Sextortion profitiert maßgeblich von der Scham und dem Schweigen der Opfer; Forschungsergebnisse zeigen, dass Sextortion ein weit verbreitetes Verbrechen ist.

Studien zeigen, dass viele Menschen aus Angst vor Stigmatisierung zögern, Anzeige zu erstatten (Cross, 2014; Pietilä & Korhonen, 2024). Das frühzeitige Erkennen der Anzeichen kann Betroffene dazu befähigen, den Kontakt abzubrechen und professionelle Hilfe oder Unterstützung bei der Polizei in Anspruch zu nehmen.

1.2.2 Fallstudien über Opfer von Liebesbetrug

Liebesbetrug hat sich von einfachen Online-Betrügereien zu komplexen kriminellen Netzwerken mit globaler Reichweite entwickelt, wie mehrere eindrucksvolle Fälle belegen. Diese Beispiele verdeutlichen, wie Liebesbetrug emotional verheerend und finanziell ruinös sein kann, indem er schutzbedürftige Menschen mit emotional manipulativen Taktiken ins Visier nimmt.

Fallstudie 1

In Italien hatte ein hochorganisiertes Netzwerk für Liebesbetrug vor allem ältere Männer, hauptsächlich in Kalabrien, ins Visier genommen. Das Netzwerk bestand aus rumänischen Staatsangehörigen, die junge Frauen einsetzten, um persönliche, oft auch körperliche Beziehungen zu ihren Opfern aufzubauen. Durch den Aufbau einer tiefen emotionalen Bindung brachten diese Frauen die älteren Männer dazu, ihnen hohe Geldbeträge zu überweisen, angeblich für familiäre oder gesundheitliche Notfälle. Dieser Fall zeigt, wie Liebesbetrug über den Online-Bereich hinausgeht und persönliche Begegnungen einbezieht, die die Auswirkungen des Betrugs auf die Opfer verstärken. Das international tätige Netzwerk wandte ausgeklügelte Geldwäschepraktiken an und verteilte das von den Opfern erlangte Geld über verschiedene Finanzkanäle, um nicht entdeckt zu werden. Diese Operation generierte über eine Million Euro und verdeutlicht die beträchtlichen Gewinne, die organisierter Liebesbetrug erzielen kann. Die multinationale Reichweite und die strukturierte Vorgehensweise dieses Betrugs zeigen die Herausforderungen auf, vor denen die Behörden bei der Untersuchung und Verfolgung solcher Fälle stehen, insbesondere da diese Netzwerke häufig grenzüberschreitend operieren (EUROPOL, 2022).

Fallstudie 2

Ein 53-jähriger Mann, der nach seiner Scheidung in einer schwierigen Lage war, wurde Opfer eines Liebesbetrugs, als er auf einer Dating-Website neue Kontakte knüpfen wollte. Er wurde von einer Frau kontaktiert, die behauptete, aus Spanien zu stammen, aber in den USA zu leben. Die Frau schickte ihm Fotos, vermied jedoch jeglichen persönlichen Kontakt oder Videoanruf und hielt die Kommunikation über Telefon, Skype und E-Mail aufrecht. Nachdem sich eine gewisse Beziehung aufgebaut hatte, bat sie ihn um finanzielle Unterstützung. Zunächst gab sie an, sich kein Essen leisten zu können, später behauptete sie, einen Reisepass zu benötigen, um ihn besuchen zu können. Im Laufe der Zeit überwies das Opfer seiner vermeintlichen Partnerin über 15.000 Pfund.

Nach dem Eingreifen der Polizei und der Unterstützung durch Opferhilfsorganisationen stellte der Mann die Geldzahlungen ein und erhielt stattdessen emotionale und praktische Hilfe. Dieser Fall verdeutlicht, wie Betrüger verletzliche Lebenssituationen, wie beispielsweise eine Scheidung, ausnutzen und ihre Forderungen schrittweise steigern, indem sie durch regelmäßigen, aber oberflächlichen Kontakt Vertrauen aufbauen (Polizei Surrey, o. J.).

Fallstudie 3

Eine 65-jährige Witwe wurde Opfer eines Liebesbetrugs, nachdem sie über Facebook Kontakt zu einem Mann aufgenommen hatte, der sich als Offizier ausgab. Einsam nach dem Tod ihres Mannes suchte sie Gesellschaft und war schnell von den aufrichtigen Absichten des Mannes überzeugt. Der Betrüger, der ausschließlich über Facebook und Telefon mit ihr kommunizierte, behauptete, er benötige Geld, um die Armee zu verlassen und seinen kranken Sohn zu versorgen. Die Witwe, die ihm helfen wollte, überwies 7.500 Pfund. Kurz darauf forderte der Betrüger weitere 3.500 Pfund für die medizinischen Kosten seines Sohnes. Die Bank schritt jedoch vor der Transaktion ein, löste gemäß ihren internen Richtlinien eine Warnung aus und verhinderte so weiteren Schaden. Dieses Eingreifen und die anschließende Beratung durch die Polizei halfen der Witwe zu erkennen, dass es sich um einen Betrug handelte. Dieser Fall unterstreicht die Bedeutung von Bankrichtlinien und familiären Unterstützungssystemen für den Schutz gefährdeter Personen vor Betrug (Surrey Police, o. J.).

Fallstudie 4

Ein 66-jähriger, geschiedener Mann, der allein lebte, wurde nach seiner Anmeldung auf verschiedenen Online-Dating-Plattformen Opfer mehrerer Liebesbetrüger. Er hielt per E-Mail, SMS und Telefon Kontakt zu mehreren Frauen und wurde in dem Glauben gelassen, deren Lebenshaltungskosten, einschließlich Miete und Nebenkosten, zu decken und sogar Flüge für Besuche zu bezahlen, die nie stattfanden. Innerhalb von fünf Jahren überwies er über 100.000 Pfund an verschiedene Betrüger. Seine Tochter wandte sich schließlich an die Polizei, die daraufhin eingriff. Finanzinstitute sperrten den Mann anschließend für Geldtransferdienste, um weitere Verluste zu verhindern. Dieser Fall verdeutlicht, wie langwierige Betrügereien die finanzielle Sicherheit untergraben können und unterstreicht die Bedeutung der Einbindung der Familie und der Finanzkontrolle, um solche Betrügereien zu erkennen und zu stoppen (Polizei Surrey, o. J.).

Fallstudie 5

Eine Untersuchung von Liebesbetrugsfällen aus Nigeria enthüllte eine detaillierte „Anleitung“, mit der Betrüger ihre Opfer täuschen. Diese Anleitung enthält eine Schritt-für-Schritt-Anleitung.

Anleitungen zum Aufbau von Vertrauen, zur Manipulation von Gefühlen und zur schrittweisen Steigerung der finanziellen Forderungen. Betrüger in Nigeria zielen häufig auf Frauen mittleren oder höheren Alters ab, die alleinstehend oder kürzlich verwitwet sind, und nutzen deren Einsamkeit und Sehnsucht nach Nähe aus. In der Anfangsphase erstellen die Betrüger Profile, die kultiviert und charmant wirken, mit schmeichelhaften Fotos und scheinbar bedeutungsvollen Gesprächen. Die Anleitung beschreibt Taktiken zum Aufbau einer „stürmischen Romanze", einer Strategie, die die in den Medien oft dargestellten idealisierten Beziehungen nachahmen soll. Mit der Zeit manipulieren die Betrüger das Opfer, sodass es an eine gemeinsame Zukunft glaubt, während sie gleichzeitig immer höhere finanzielle Forderungen stellen. Diese Anleitung verdeutlicht die systematische Vorgehensweise dieser Betrüger und die kalkulierten Schritte beim Liebesbetrug und unterstreicht den professionellen Charakter des Liebesbetrugs als kriminelles Geschäft (DocumentCloud, o. J.).

Angesichts der anhaltenden Probleme mit Liebesbetrug stehen verschiedene technische Hilfsmittel zur Verfügung, um betrügerische Profile zu erkennen. Swindlerbuster Face Search ermöglicht beispielsweise die umgekehrte Bildersuche von Fotos, die in Dating-Profilen verwendet werden. Indem festgestellt wird, ob ein Bild mit mehreren Namen oder Orten verknüpft ist, können Nutzer die Echtheit von Online-Profilen besser überprüfen.

1.3 Statistiken

Die italienische Post- und Kommunikationspolizei überwacht das Internet täglich aktiv. Spezialisierte Mitarbeiter überwachen Online-Bereiche, insbesondere soziale Medien, um kriminelles Verhalten zu verhindern und zu bekämpfen. Diese Spezialeinheit arbeitet national und international koordiniert zusammen und nutzt Büros im ganzen Land, um Fälle von Cyberkriminalität zu bearbeiten und zu untersuchen. Zu den behandelten Problemen gehört der Liebesbetrug, der 2021 im Vergleich zu 2020 einen dramatischen Anstieg von 118 % verzeichnete. Obwohl Männer im Allgemeinen weniger betroffen sind, wurden zahlreiche italienische Männer von Tätern getäuscht, die sich in sozialen Medien als ausländische Frauen ausgaben und mit freizügigen Bildern posierten, oft als Models oder wohlhabende Erbinnen. Diese Betrügereien können zu erheblichen finanziellen Verlusten führen, die sich in Einzelfällen auf Hunderttausende von Euro belaufen. Allein im Jahr 2021...

Rund 4,5 Millionen Euro gingen durch diese Betrugsmaschen verloren (Commissariato di Pubblica Sicurezza Online, o. J.). In Europa sind 1 bis 3 % der Bevölkerung von Liebesbetrug betroffen, wobei die Verluste in verschiedenen Ländern erhebliche finanzielle Auswirkungen haben. So verzeichneten beispielsweise finnische Polizeiberichte aus dem Jahr 2020 210 Fälle mit einem Gesamtschaden von 6,1 Millionen Euro, der bis 2023 auf 10,4 Millionen Euro anstieg und die zunehmende Verbreitung dieser Straftaten widerspiegelt (Pietilä & Korhonen, 2024). Die finanziellen Folgen von Liebesbetrug sind europaweit spürbar, und die in diesen Fällen beobachteten Betrugsmuster unterstreichen die Bedeutung von Aufklärung und digitaler Kompetenz in der Öffentlichkeit im Kampf gegen Online-Betrug.

Die Plattform CybSafe berichtet, dass etwa 20 % der Bevölkerung Opfer von Liebesbetrug werden, wobei Millennials (18 %) und die Generation Z (15 %) am stärksten betroffen sind. Trotz der hohen Opferzahlen melden nur 55 % der Betroffenen diese Betrugsfälle, und von diesen wenden sich lediglich 36 % an die Behörden. Diese Statistiken verdeutlichen sowohl generationsbedingte Unterschiede in der Anfälligkeit für Betrug als auch im Meldeverhalten und legen nahe, dass gezielte Präventionsstrategien und eine verstärkte Unterstützung für alle Bevölkerungsgruppen erforderlich sind (CybSafe, 2023).

1.4 Opferforschung zum Liebesbetrug

1.4.1 Psychologische Folgen für Opfer von Liebesbetrug

Opfer von Cyberkriminalität wie Liebesbetrug, Cyberstalking oder Betrug werden Opfer von Cyberkriminalität, die tiefgreifende psychologische Folgen haben, welche denen vergleichbarer Straftaten im realen Leben ähneln. Betroffene erleben eine Reihe emotionaler, sozialer und physiologischer Auswirkungen. Studien zeigen beispielsweise, dass Opfer von Cybermobbing ähnliche Folgen wie Opfer von traditionellem Mobbing erleiden, darunter soziale Ängste, Depressionen und ein vermindertes Sicherheitsgefühl (Smith et al., 2008, in Open University, 2024).

Die durch Cyberstalking verursachte Belastung ähnelt derjenigen von Stalking im realen Leben und führt bei den Opfern zu starker Angst, Hypervigilanz und Stress (Dreßing et al., 2014, in Open University, 2024).Obwohl die Auswirkungen von Trolling weniger erforscht sind, deuten erste Erkenntnisse darauf hin, dass auch dieses zu erheblichen psychischen Schäden beitragen kann, was die Notwendigkeit unterstreicht, die Auswirkungen auf die Opfer weitergehend zu untersuchen und zu erforschen.

Insbesondere Liebesbetrug hat aufgrund der Vielschichtigkeit des Schadens einzigartige und weitreichende psychologische Folgen. Studien zeigen, dass Opfer von Liebesbetrug einen sogenannten „Doppelschlag“ erleiden (Button et al., 2014): den finanziellen Verlust und die emotionale Zerstörung durch den vermeintlichen Zusammenbruch einer echten Beziehung. Untersuchungen heben hervor, dass dieser emotionale Verrat den finanziellen Schaden oft übertrumpfen und bei den Opfern tiefes Leid verursachen kann. Button et al. (2014) stellen fest, dass die Kombination aus finanziellem Verlust und emotionalem Verrat bei diesen Betrügereien viele Opfer zu schweren emotionalen Traumata führt. Die Arbeiten von Whitty und Buchanan (2012; 2016) bestätigen dies und zeigen, dass Opfer häufig mit Scham, Schuldgefühlen und Selbstvorwürfen zu kämpfen haben, was sie oft davon abhält, Hilfe zu suchen. Solche verinnerlichten Schamgefühle können durch Urteile von außen noch verstärkt werden, da die Opfer von anderen manchmal als „naiv“ oder „leichtgläubig“ bezeichnet werden (Buchanan & Whitty, 2014, in Open University, 2024).

Die psychologischen Folgen von Cyberkriminalität sind weitreichend und oft lang anhaltend. Viele Betroffene berichten von Depressionen, sozialem Rückzug, PTSD-ähnlichen Symptomen, zwanghaftem Verhalten, geringem Selbstwertgefühl und einem tiefsitzenden Misstrauen gegenüber anderen (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012; Bates, 2017, in Open University, 2024). Häufig berichten Betroffene auch von körperlichen Symptomen wie anhaltenden Kopfschmerzen, Verdauungsproblemen und Schlafstörungen, die ihre emotionale Belastung zusätzlich verstärken und die Genesung erschweren. Die Bewältigungsstrategien neigen zunächst zu ungesunden Mechanismen wie Substanzkonsum und Vermeidungsverhalten, bevor die Betroffenen positivere Methoden wie Beratung oder die Teilnahme an Hilfsangeboten in Anspruch nehmen können. Die Genesung wird jedoch oft durch gesellschaftliche Einstellungen behindert, insbesondere durch die weit verbreitete Täter-Opfer-Umkehr. Diese stellt ein erhebliches Hindernis im Genesungsprozess dar, insbesondere für Opfer von Cyberkriminalität. Die Viktimologie, deren Ursprünge bis zu Mendelsohns frühen Typologien aus den 1930er Jahren zurückreichen, legte nahe, dass Opfer eine Mitschuld an ihrer Viktimisierung tragen könnten. Die moderne Viktimologie hingegen sieht die Täter in der Regel zur Rechenschaft, da sie anerkennt, dass Faktoren außerhalb der Kontrolle des Opfers häufig zu dessen Ausbeutung beitragen. Trotzdem werden Opfer von Cyberkriminalität oft mit dem Vorwurf einer Teilschuld konfrontiert, häufig aufgrund tief verwurzelter Vorstellungen von einer gerechten Welt (Lerner, 1980, in Open University, 2024). Dieses Glaubenssystem suggeriert, dass die Welt nach dem Prinzip der Fairness funktioniert, was Menschen dazu veranlasst zu glauben, dass Opfer etwas getan haben müssen, um Schaden herbeizuführen.

Diese Denkweise, die häufig bei Liebesbetrug angewendet wird, impliziert, dass die Opfer aus Gier oder Leichtgläubigkeit handelten und die Straftat hätten vermeiden können, indem sie auf Online-Interaktionen oder die Nutzung sozialer Medien verzichtet hätten (Cross, 2015, in Open University, 2024).

Diese Art der Opferbeschuldigung kann die psychischen Folgen für Opfer von Liebesbetrug, die ohnehin schon mit Gefühlen des Verrats und der Scham zu kämpfen haben, noch verschlimmern. Viele Opfer berichten, dass der schmerzhafteste Aspekt ihrer Erfahrung die Verurteilung und der Mangel an Empathie seitens Familie und Freunden ist, die sie möglicherweise als Mittäter sehen. Opferbeschuldigung kann zudem die Selbstvorwürfe verstärken und es den Opfern erschweren, Unterstützung zu suchen oder offen über ihre Erfahrungen zu sprechen. Dieser Mangel an Unterstützung behindert nicht nur die emotionale Heilung, sondern kann dazu führen, dass sich die Opfer noch isolierter und unverstandener fühlen, was langfristig zu schwerwiegenderen psychischen Folgen führt (Wang, 2022). Liebesbetrug verursacht oft neben dem finanziellen Verlust auch tiefgreifende emotionale Belastungen und hinterlässt bei den Opfern Gefühle von Scham, Schuld und sozialer Isolation. Viele Opfer machen sich selbst Vorwürfe oder schämen sich zu sehr, den Betrug anzuzeigen, während einige mit schwerwiegenden finanziellen Konsequenzen konfrontiert werden, ihre Ersparnisse verlieren oder sich verschulden. Opfer, die eine emotionale Bindung zum Betrüger aufbauen, können ein Stockholm-Syndrom entwickeln und dem Täter auch nach Aufdeckung des Betrugs noch Mitgefühl oder Zuneigung entgegenbringen. Diese Bindung erschwert es ihnen, sich zu befreien oder den Betrug anzuzeigen (The Debt Advisor, 2023).

1.4.2 Opferprofil

Forschungen zur Opferschaft von Online-Liebesbetrug zeigen spezifische demografische und psychologische Merkmale auf, die die Anfälligkeit für solche Maschen erhöhen. Studien von Wang (2022) deuten darauf hin, dass Frauen, Menschen mittleren Alters und gut ausgebildete Personen ein höheres Risiko tragen, Opfer von Liebesbetrug zu werden. Demografische Daten legen nahe, dass 60 % der Opfer von Liebesbetrug Frauen und 40 % Männer sind. Unter den Opfern sind 63 % mittleren Alters, gefolgt von 21 % jungen Erwachsenen und 16 % älteren Menschen. Menschen mittleren Alters werden aufgrund ihrer finanziellen Stabilität und ihrer höheren Wahrscheinlichkeit, Online-Dating-Plattformen zu nutzen, häufig gezielt angesprochen. Dies gilt insbesondere nach einschneidenden Lebensereignissen wie Scheidung oder dem Verlust des Partners, wodurch sie anfälliger für die Versprechungen von Betrügern werden können.

Auch Persönlichkeitsmerkmale spielen eine Rolle; besonders gefährdet sind Menschen mit hohem Vertrauen, starker Impulsivität und geringerer Selbstkontrolle. Betrüger nutzen diese Eigenschaften aus und locken ihre Opfer mithilfe geschickt konstruierter Geschichten in vorgetäuschte Liebesbeziehungen. Diese Geschichten wecken Empathie, Mitgefühl und oft auch eine tiefe emotionale Bindung (Wang, 2022). Die psychologischen Folgen von Liebesbetrug sind gravierend und oft durch einen sogenannten „Doppelschlag" gekennzeichnet (Button et al., 2014): finanzieller Verlust gepaart mit der emotionalen Belastung durch einen vermeintlichen Beziehungsbruch.

Opfer leiden typischerweise unter schwerem emotionalem Stress, einschließlich Scham, Schuldgefühlen und einem verminderten Selbstwertgefühl. Studien von Whitty und Buchanan (2012, 2016) zeigen, dass diese emotionalen Folgen oft den mit finanziellen Verlusten verbundenen Stress übertreffen können, da die Opfer den Verrat einer Beziehung verarbeiten müssen, die sie für aufrichtig hielten. Viele Opfer zögern, Hilfe zu suchen oder die Straftat anzuzeigen, aus Angst vor Kritik oder Schuldzuweisungen von Familie und Freunden, die sie als „naiv" oder „leichtgläubig" abstempeln könnten (Buchanan & Whitty, 2014 in Open University, 2024). Cross et al. (2016) untersuchten die Dynamik von Liebesbetrug aus der Perspektive der Theorie häuslicher Gewalt und erforschten, wie Betrüger psychologische Manipulation einsetzen, um Kontrolle über ihre Opfer zu erlangen. Ihren Ergebnissen zufolge zeigen Opfer von Liebesbetrug in Online-Interaktionen oft ein hohes Maß an Vertrauen und Verletzlichkeit, was sie anfälliger für emotionale Manipulation macht. Betrüger nutzen dieses Vertrauen aus, indem sie Zuneigung vortäuschen und das Opfer so von der Echtheit der Beziehung überzeugen. Diese Vorgehensweise ähnelt den Taktiken emotionaler Manipulation bei häuslicher Gewalt, wo Täter Abhängigkeit erzeugen und die Opfer von ihrem sozialen Umfeld isolieren. Isolation ist ein typisches Merkmal von Liebesbetrug, da Betrüger die Opfer davon abhalten, Details ihrer Beziehung mit Freunden oder Familie zu teilen. Diese Taktik verstärkt die emotionale Bindung und Abhängigkeit des Opfers vom Betrüger und macht es ihm zunehmend schwerer, den Betrug zu erkennen oder sich daraus zu befreien (Cross et al., 2016).

Die finanziellen Folgen für Opfer von Liebesbetrug sind oft gravierend. Viele geben erhebliche Ersparnisse auf oder verkaufen persönliches Eigentum, um die Forderungen der Betrüger zu erfüllen. Diese finanzielle Belastung, verstärkt durch emotionalen Stress, kann zu einem Gefühl der Hoffnungslosigkeit und Ohnmacht führen. Für manche beeinträchtigen die Verluste die finanzielle Stabilität über Jahre hinweg und verschärfen die psychischen Probleme, mit denen sie zu kämpfen haben. Cross et al. (2016) weisen darauf hin, dass finanzielle Ausbeutung zu tiefen Scham- und

Schuldgefühlen bei den Opfern führen kann, da diese mit der Erkenntnis ihrer Manipulation durch Betrugsmaschen ringen. Neben den finanziellen und emotionalen Folgen berichten Opfer von Liebesbetrug von verschiedenen körperlichen und psychischen Symptomen, die mit einem Trauma einhergehen. Studien zeigen, dass Opfer häufig Symptome einer posttraumatischen Belastungsstörung (PTBS), Depressionen, sozialen Rückzug, zwanghaftes Verhalten und ein überwältigendes Misstrauen gegenüber anderen entwickeln. Körperliche Symptome wie Kopfschmerzen, Verdauungsprobleme und Schlafstörungen treten ebenfalls häufig auf und verschlimmern oft die emotionalen Folgen des Betrugs. Anfangs greifen die Opfer möglicherweise zu ungesunden Bewältigungsstrategien wie Substanzkonsum oder Vermeidungsverhalten, bevor sie schließlich konstruktivere Unterstützung durch Beratung oder Hilfsangebote suchen. Die Genesung wird jedoch häufig durch gesellschaftliche Täter-Opfer-Umkehr behindert, die bei Cyberkriminalität weit verbreitet ist.

Die Täter-Opfer-Umkehr, ein erhebliches Hindernis für die Genesung, wurzelt in gesellschaftlichen Einstellungen und Wahrnehmungen gegenüber Cyberkriminalität. Frühe viktimologische Theorien, wie Mendelsohns Typologien aus den 1930er Jahren, gingen davon aus, dass Opfer eine Mitschuld an ihrer Viktimisierung tragen. Obwohl moderne Ansätze die Täter in der Regel zur Rechenschaft ziehen, sind Opfer von Cyberkriminalität weiterhin gesellschaftlichen Vorurteilen ausgesetzt, insbesondere bei Liebesbetrug. Diese Vorurteile basieren oft auf dem Glauben an eine gerechte Welt, die besagt, dass die Welt nach Prinzipien der Fairness funktioniert; daher müssen Opfer etwas getan haben, um Schaden zu erleiden (Lerner, 1980 in Open University, 2024). Angewendet auf Liebesbetrug impliziert diese Denkweise, dass Opfer den Betrug hätten vermeiden können, indem sie offline geblieben oder vorsichtiger gewesen wären, wodurch ihre Erfahrungen stigmatisiert werden (Cross, 2015 in Open University, 2024).

1.4.3 Psychologische Rehabilitation des Opfers eines Liebesbetrugs

Liebesbetrug hinterlässt schwerwiegende psychische und emotionale Schäden. Die Opfer erleiden oft ein doppeltes Trauma: finanziellen Verlust und den Zusammenbruch einer vermeintlich echten Beziehung (Cross, 2014; Cross et al., 2018). Studien zeigen, dass fast zwei Drittel der Betrugsopfer über gesundheitliche oder psychische Schäden berichten, die noch lange nach dem Betrug anhalten (Button et al., 2014).

Zu den psychologischen Folgen gehören akute Stress- und Traumareaktionen, wobei einige Betroffene PTSD-Symptome wie intrusive Erinnerungen, Flashbacks, Albträume und Hypervigilanz entwickeln (Coluccia et al., 2020). Depressionen, Scham und Selbstvorwürfe sind häufig.

Opfer fragen sich oft, wie sie „so naiv sein konnten“ (Whitty, 2018). Viele entwickeln zudem dauerhafte Vertrauensprobleme, zweifeln an ihrem eigenen Urteilsvermögen und haben Schwierigkeiten, neue Beziehungen aufzubauen (Rege, 2019 in Pietilä & Korhonen, 2024). Häufig ziehen sich Opfer sozial zurück und erleben Gefühle der Isolation und Demütigung (Whitty & Buchanan, 2012). Der lange Weg der Genesung erfordert vielschichtige Unterstützung.

- Trauma-informierte Beratung, insbesondere kognitiv-verhaltenstherapeutische und trauerorientierte Ansätze, hat sich als wirksam erwiesen, um Opfern zu helfen, ihre Erfahrungen neu zu bewerten und Selbstvorwürfe zu reduzieren (Against Scams, 2024).
- Selbsthilfegruppen bieten Überlebenden einen geschützten Raum, um Erfahrungen auszutauschen, Gefühle zu bestätigen und ihre Resilienz wieder aufzubauen (AARP, 2021). Online-Communities wirken ebenfalls der Isolation entgegen und bieten Vernetzung und Normalisierung (AARP, o. J.).
- Das Verständnis der Beziehungs- und Manipulationstaktiken, die von Betrügern eingesetzt werden, hilft den Opfern, die Schuld von sich zu nehmen und ihr Selbstvertrauen wiederzuerlangen (Coluccia et al., 2020).
- Soziale, finanzielle und gemeinschaftliche Dienstleistungen, von Rechtsberatung bis hin zu Schulungen zur digitalen Sicherheit, tragen zur Genesung bei, indem sie die Kontrolle und Handlungsfähigkeit wiederherstellen (Pietilä & Korhonen, 2024).

Obwohl die Genesung schrittweise erfolgt, berichten Betroffene häufig von einem posttraumatischen Wachstum, sobald die Scham thematisiert und unterstützende Netzwerke aufgebaut sind (Cross et al., 2018; Whitty, 2018).

Unterstützung mit Sorgfalt: Gute Praktiken für Pädagogen

Co-funded by
the European Union

Salma Alaaelden

Salma ist Projektassistentin und Forscherin bei EUth Wonders e. V. und verfügt über fundierte wirtschaftswissenschaftliche Kenntnisse sowie mehr als sechs Jahre Erfahrung in der Jugendarbeit und im Projektmanagement. Sie hat weltweit mit Organisationen zusammengearbeitet und zu Initiativen beigetragen, die junge Menschen stärken und den interkulturellen Dialog fördern. Salma hat an zahlreichen Forschungsarbeiten zum Thema psychische Gesundheit mitgewirkt und im Rahmen ihrer Projektbeteiligungen Workshops zum Thema psychisches Wohlbefinden durchgeführt. Bei EUth Wonders e. V. spielt sie eine Schlüsselrolle bei der Konzeption, Koordination und Durchführung von Erasmus+-Projekten und anderen internationalen Projekten. Sie begleitet den gesamten Projektzyklus und stellt sicher, dass die Aktivitäten sinnvoll, inklusiv und im Einklang mit unserer Mission stehen, junge Menschen über Grenzen hinweg zu vernetzen und ihre Kompetenzen und Chancen zu verbessern.

Co-funded by
the European Union

2 GUTE PRAXIS FÜR PÄDAGOGEN

2.1 Inhalt dieses Kapitels

Da Liebesbetrug, der sich gegen ältere Erwachsene richtet, eine schnell wachsende Form der Cyberkriminalität in Europa darstellt und zu enormen sozialen und finanziellen Verlusten sowie psychologischen Folgen wie sozialer Isolation, Ausnutzung emotionaler Schwächen und finanziellen Einbußen führt, kommt Erziehern und Jugendarbeitern eine entscheidende Rolle beim Schutz älterer Menschen vor Liebesbetrug zu, indem sie soziale Unterstützung bieten, psychische Schwächen bewältigen und klare Wege zu diesen Senioren aufzeigen.

In Anbetracht der Bedeutung der Rolle von Jugendarbeitern und Pädagogen liefert dieses umfassende Kapitel die notwendigen Informationen, um die psychologischen Schwachstellen zu verstehen, die Opfer anfällig für Betrug machen, die emotionalen und psychologischen Folgen von Liebesbetrug und stattet Pädagogen mit dem Wissen und den Werkzeugen aus, wie sie Senioren, die anfällig für Liebesbetrug sind, durch präventive und reaktive Maßnahmen sozial und psychologisch unterstützen und ihnen im Falle eines Liebesbetrugs nützliche Ressourcen anbieten können, sowie Unterstützungsnetzwerke aufbauen können, um ein sicheres und vertrauensvolles Umfeld für Senioren zu fördern.

2.1.1 Hauptziele und Vorgehensweisen dieses Kapitels:

Dieses Kapitel konzentriert sich auf mehrere zentrale Ziele, die Senioren und ihre Unterstützungsnetzwerke befähigen sollen, Betrugsversuche zu erkennen, darauf zu reagieren und sie zu verhindern. Die Ziele sind:

1. **Psychologische, soziale und situative Schwachstellen erkennen:** Das Verständnis der Faktoren, die Senioren besonders anfällig für Betrugsmaschen machen, einschließlich psychologischer, sozialer und situativer Elemente, hilft dabei, Risikofaktoren zu erkennen und präventive Maßnahmen zu ergreifen.
2. **Untersuchung der psychologischen und emotionalen Auswirkungen von Liebesbetrug auf die Opfer:** Die Analyse der psychologischen Auswirkungen und der psychischen Gesundheitsprobleme bei Opfern von Liebesbetrug wird uns als Pädagogen helfen zu verstehen und zu erkennen, wie wir die Opfer nach dem Betrug effizienter unterstützen können.
3. **Fallstudien aus der Praxis zu Liebesbetrugsfällen:** Um einen umfassenderen Einblick in Präventions- und Reaktionsmethoden gegen Liebesbetrug zu geben, werden einige Fallstudien erläutert und analysiert.

4. Die wichtige Rolle von Jugendarbeitern und Pädagogen verstehen: In diesem Abschnitt werden die verschiedenen Faktoren erläutert, die die Notwendigkeit von Pädagogen bei der Unterstützung älterer Menschen unterstreichen, die anfällig für Liebesbetrug sind.

5. Bereitstellung von Leitlinien für Pädagogen zu Präventivmaßnahmen zum Schutz älterer Menschen vor Liebesbetrug: Identifizierung der verschiedenen Präventivmaßnahmen, die Pädagogen ergreifen können, um ältere Menschen aufzuklären und sie davor zu bewahren, möglicherweise Opfer von Liebesbetrug zu werden.

5. Hinweise für Pädagogen zur Erkennung laufender Betrugsversuche: In diesem Abschnitt wird erläutert, wie man laufende Betrugsversuche anhand von Verhaltensindikatoren und Anzeichen bei den Opfern erkennt und wie man ältere Opfer in solchen Fällen unterstützen kann.

6. Bereitstellung einer Schritt-für-Schritt-Anleitung für den Umgang mit Betrugsfällen: Bereitstellung eines klaren, umsetzbaren Prozesses für Senioren und Pflegekräfte, den sie befolgen können, wenn sie mit einem Betrug konfrontiert werden, um sicherzustellen, dass sie wissen, wie sie die Situation effektiv melden und bewältigen können.

7. Aufbau langfristiger Unterstützungsnetzwerke: Schaffung und Stärkung fortlaufender Unterstützungssysteme, die Senioren helfen können, künftigen Betrügereien vorzubeugen, durch Förderung von Aufklärung, Wachsamkeit und Gemeinschaftskontakten.

8. Vernetzung von Pädagogen und Senioren mit wichtigen Ressourcen: Bereitstellung der notwendigen Ressourcen und Instrumente für Pädagogen, Senioren und ihre Betreuer zur Genesung und zum Schutz, um sicherzustellen, dass sie Zugang zu Informationen und Unterstützung haben, um sich vor Betrug zu schützen.

9. Praktische Fallstudien: Dieser Teil dient als praktische Übung mit verschiedenen hypothetischen Fallstudien, anhand derer Pädagogen analysieren und erläutern können, wie sie in den jeweiligen Situationen handeln sollten, um ältere Opfer zu unterstützen.

Diese Ziele sollen Senioren dabei helfen, informiert, geschützt und widerstandsfähig gegen Betrugsmaschen zu bleiben und so sowohl kurz- als auch langfristig Sicherheit zu gewährleisten.

2.1.2 Ansätze

Der pädagogische Schwerpunkt dieses Kapitels liegt auf einem zweigleisigen Ansatz zum Schutz älterer Menschen vor Liebesbetrug. Erstens konzentrieren sich die Präventionsmaßnahmen darauf, ältere Erwachsene und ihre Betreuer über gängige Betrugsmethoden aufzuklären und ihnen die nötigen digitalen Kompetenzen und soziale Unterstützung zu vermitteln, damit sie betrügerische Angebote erkennen und vermeiden können.

Zweitens bieten die Maßnahmen zur Reaktion klare Protokolle für Intervention und Unterstützung im Falle eines Betrugs und führen die Pädagogen durch jeden Schritt – von der ersten Dokumentation und Meldung bis hin zu Ressourcen für die emotionale und finanzielle Erholung.

2.2 Erkennen psychologischer und sozialer Verletzlichkeit

Ältere Opfer erhalten vor, während und nach dem Betrugsprozess nur wenig Hilfe und Unterstützung. Dies erschwert es ihnen nicht nur, nach Online-Betrugsfällen rechtzeitig professionelle Hilfe zu erhalten, sondern birgt auch das Risiko, erneut Opfer eines Liebesbetrugs zu werden, wodurch sich der soziale, psychologische und finanzielle Schaden vervielfacht.

Bevor wir auf die verschiedenen Maßnahmen zur Prävention und Unterstützung von Betrugsopfern unter Senioren im Bildungsbereich eingehen und deren Notwendigkeit erläutern, ist es wichtig, zunächst die Risikofaktoren zu verstehen, die Senioren anfälliger für Betrug machen. Dies ist für Pädagogen, Pflegekräfte und Gemeindevertreter von entscheidender Bedeutung, da die Kenntnis dieser Faktoren ein frühzeitiges und wirksames Eingreifen ermöglicht und die Chance bietet, präventive Maßnahmen zu ergreifen, bevor Senioren Opfer von Betrug werden.

Eine Vielzahl psychologischer, sozialer und situativer Faktoren trägt zur Verwundbarkeit älterer Menschen bei, die Betrüger häufig ausnutzen. Zu diesen Faktoren zählen unter anderem soziale Isolation, kognitiver Abbau und emotionale Bedürfnisse.

✦ Soziale Isolation:

Einer der Hauptfaktoren, der Senioren anfälliger für Betrug macht, ist soziale Isolation. Viele ältere Menschen leiden unter einem Mangel an regelmäßigen sozialen Kontakten, was zu Einsamkeit und Langeweile führen kann. In manchen Fällen suchen Senioren deshalb online nach Gesellschaft oder emotionaler Nähe. Betrüger nutzen dieses Bedürfnis aus und gaukeln Online-Beziehungen vor, um diese Menschen zu manipulieren. Sie bauen Vertrauen und emotionale Bindungen auf und bringen die Opfer so dazu, Geld zu überweisen oder persönliche Daten preiszugeben. Um solche Ausbeutung zu verhindern, ist es daher unerlässlich, regelmäßige soziale Kontakte zu fördern und unterstützende soziale Netzwerke aufzubauen.

Kognitiver Abbau und Anfälligkeit für Betrug:

Mit zunehmendem Alter kann es zu kognitiven Beeinträchtigungen kommen, die sich in Gedächtnislücken, Schwierigkeiten bei der Verarbeitung neuer Informationen und einer verminderten Fähigkeit zu vernünftigen Urteilen äußern. Diese kognitiven Einschränkungen können es Senioren erschweren, Warnsignale für Betrugsversuche wie unerwünschte Anrufe, Phishing-E-Mails oder betrügerische Anlageangebote zu erkennen. Auch die Fähigkeit älterer Menschen, die Folgen der Weitergabe persönlicher oder finanzieller Informationen an Fremde zu verstehen, kann durch kognitive Beeinträchtigungen beeinträchtigt sein. Daher ist es wichtig, dass Erzieher und Pflegekräfte die kognitive Gesundheit älterer Menschen im Blick behalten und Strategien zur Erkennung von Warnsignalen und zur Vermeidung riskanter Situationen anbieten. Regelmäßige geistige Übungen, regelmäßige Gespräche und die Nutzung vertrauenswürdiger Technologien können dazu beitragen, die kognitiven Funktionen zu erhalten und Betrug vorzubeugen.

Emotionales Bedürfnis:

Emotionale Verletzlichkeit ist ein weiterer wichtiger Faktor, den Betrüger ausnutzen. Senioren können mit verschiedenen emotionalen Belastungen konfrontiert sein, wie Trauer, dem Verlust des Partners oder Einsamkeit. Diese Gefühle können dazu führen, dass sie aktiv nach neuen Beziehungen oder Bestätigung suchen – eine ideale Angriffsfläche für Betrüger, die diese emotionale Bedürftigkeit ausnutzen. Betrüger geben sich als potenzielle Partner aus und versprechen Zuneigung, Gesellschaft oder ein Gefühl der Zugehörigkeit. Leider können diese Betrügereien zu finanziellen Verlusten führen, da Senioren manipuliert werden können, Geld zu überweisen oder andere Formen der Unterstützung anzubieten. Das Verständnis für den emotionalen Zustand von Senioren und das Angebot emotionaler und sozialer Unterstützung sind entscheidend, um diese Betrugsmaschen einzudämmen. Der Zugang zu Trauerberatung, Selbsthilfegruppen und anderen sozialen Ressourcen kann dazu beitragen, die emotionale Verletzlichkeit zu verringern, die Betrüger ausnutzen.

Vertrauen in die Natur (Leichtgläubigkeit):

Mehrere Studien belegen, dass Menschen mit einem hohen Maß an Vertrauen häufiger Opfer von Liebesbetrug werden. Viele Senioren, insbesondere jene, die Zeiten des Vertrauens und der Stabilität erlebt haben, neigen zu einer gutgläubigen Natur, die von Betrügern ausgenutzt werden kann. Betrüger appellieren oft an den Wunsch älterer Menschen, freundlich und hilfsbereit zu sein, sei es im Rahmen einer vermeintlichen Wohltätigkeitsaktion oder eines vorgeblichen finanziellen Bedarfs. Senioren hinterfragen die Absichten ihres Gesprächspartners möglicherweise nicht und werden dadurch zu leichten Zielen für Finanzbetrug. Daher ist es ratsam, ein gesundes Maß an Skepsis zu fördern und Senioren zu raten, Anfragen nach Geld oder persönlichen Informationen stets zu überprüfen, selbst wenn diese von Bekannten oder Verwandten stammen, da das

Erkennen scheinbar vertrauter Quellen eine wichtige Präventivmaßnahme darstellt.

Zusammenfassend lässt sich sagen, dass die oben genannten Faktoren dazu beitragen, dass Senioren anfälliger für Betrug werden. Es ist wichtig zu beachten, dass Betrug in der Regel nicht nur auf einer einzigen Schwachstelle beruht, sondern vielmehr auf einem Zusammenspiel psychologischer, kognitiver und sozialer Schwächen. Diese schaffen Bedingungen für Ausbeutung, die schwerwiegend sind und die Wahrscheinlichkeit erhöhen, ins Visier genommen und manipuliert zu werden.

2.3 Die psychologischen Auswirkungen von Liebesbetrug auf die Opfer

Liebesbetrug verursacht weit mehr als nur finanzielle Verluste. Er führt häufig zu tiefem emotionalem Leid, langfristigen psychischen Problemen und sozialem Rückzug. Studien belegen immer wieder, dass diese Betrugsart zu den schädlichsten und schwerwiegendsten Formen des Betrugs zählt, insbesondere für ältere Erwachsene. Die Opfer können die psychischen Folgen wie Scham, Unsicherheit und Trauma noch bis zu zehn Jahre nach dem Vorfall spüren.

Nachfolgend werden die verschiedenen psychologischen Auswirkungen und andere Folgen aufgeführt, denen Senioren im Falle eines Liebesbetrugs ausgesetzt sind.

✦ Doppeltrauma: Emotionaler und finanzieller Verlust

Liebesbetrug besteht typischerweise aus einem doppelten Schaden: dem emotionalen Verrat in einer vermeintlich intimen Beziehung, gepaart mit finanzieller Ausbeutung. Diese Betrügereien erstrecken sich oft über Monate, in denen der Täter eine überzeugende emotionale Geschichte aufbaut und das Vertrauen des Opfers gewinnt. Die Folgen des Betrugs beschränken sich daher nicht nur auf den finanziellen Verlust, sondern umfassen auch tiefgreifende psychische Schäden. Die Opfer erleben ein starkes Gefühl der Verlassenheit, Manipulation und Identitätskrise, was zu einem emotionalen Trauma führt, das verheerender ist als der finanzielle Schaden.

Empirische Befunde zeigen, dass Opfer von Finanzbetrug deutlich stärkere emotionale Belastungen angeben als Opfer anderer Betrugsformen. Liebesbetrug ist die Betrugsart mit der höchsten emotionalen Belastung, und viele Opfer erleben emotionalen Missbrauch, insbesondere wenn die Manipulation über einen längeren Zeitraum erfolgte und tiefes Vertrauen auf dem Spiel stand. In diesen Fällen führt der plötzliche Verlust der vermeintlichen Beziehung häufig zu **Symptomen einer Anpassungsstörung oder zu traumabedingten Erkrankungen.**

Scham und Schuld

Nach einem Betrug geben sich ältere Opfer häufig selbst die Schuld an der Täuschung und betrachten den Betrug oft als persönliches Versagen. Scham stellt eine große Hürde dar, selbst im engsten Umfeld Hilfe zu suchen. Laut einer Studie vermeiden viele Opfer es, Familie, Freunde oder Fachleute anzusprechen, aus Angst vor Ablehnung oder Spott. Diese Reaktion kann Gefühle der Wertlosigkeit verstärken und die emotionale Genesung verzögern. Hier kommt der Pädagogen eine wichtige Rolle zu: Sie können die Opfer beruhigen, ihr Vertrauen gewinnen, ihnen das Gefühl geben, gesehen zu werden, und sie darin unterstützen, gegen den Betrug vorzugehen.

Depression und Angstzustände

Viele Betroffene berichten von Symptomen einer klinischen Depression, darunter Hoffnungslosigkeit, Schlafstörungen und Antriebslosigkeit. Häufig treten auch Angstzustände auf, insbesondere in Bezug auf Finanzen, Privatsphäre oder öffentliche Bloßstellung. Diese Auswirkungen verstärken sich, wenn die Betroffenen bereits emotional belastet sind, beispielsweise durch Trauer oder Einsamkeit. Die Symptome sind nicht vorübergehend, da Studien auf langfristige psychische Schäden und einen erhöhten Bedarf an psychosozialer Unterstützung hinweisen.

Sozialer Rückzug

Nach der Offenlegung des Betrugs ziehen sich ältere Opfer aus Scham oft von Gleichaltrigen und der Gemeinschaft zurück. Manche brechen den Kontakt zu Personen ab, die die Beziehung hinterfragt oder vor ihr gewarnt hatten, als sie von der vorgetäuschten „Beziehung“ wussten. Diese Isolation und der Vertrauensverlust erstrecken sich sowohl auf persönliche als auch auf institutionelle Beziehungen und tragen zu tieferer Einsamkeit und einem erhöhten Risiko einer erneuten Viktimisierung bei.

Emotionale Bindung und Trauer

Opfer entwickeln oft eine starke psychologische Bindung zu der erfundenen Identität des Betrügers, basierend auf der Beziehung, die sie vor dem Betrug online zu ihm aufgebaut haben. Wenn der Betrug auffliegt, erleben viele eine Trauer, die mit dem Verlust eines Partners vergleichbar ist. Die Opfer beschreiben den Betrüger dann als ihren „idealen Partner“ oder ihre „emotionale Stütze“ – selbst wenn die Beziehung ausschließlich online stattfand. Manche Opfer berichten von einem stärkeren Gefühl der Trauer als vom eigentlichen finanziellen Verlust. Dies liegt an dem sogenannten „Love Bombing“, den falschen Heiratsversprechen und der ständigen emotionalen Verstärkung, die während der Anbahnungsphase eingesetzt wurden.

Verlust des Selbstwertgefühls und des Selbstvertrauens

Viele Opfer berichten nach dem Betrug von einem verminderten Gefühl von Selbstwirksamkeit und Würde. Der erlittene Vertrauensverlust untergräbt oft ihr Vertrauen in ihre Entscheidungsfähigkeit und verstärkt ihre Abhängigkeit von anderen. Diese Ohnmacht kann zu langfristiger emotionaler Instabilität und einer Abneigung gegen neue Beziehungen oder Weiterbildungsangebote führen und Zweifel an ihrer Identität und ihren sozialen Rollen hervorrufen.

Angst vor Verurteilung und Vermeidung von Offenbarungen

Aufgrund gesellschaftlicher Stigmatisierung zögern Betroffene oft, den Betrug anzuzeigen oder emotionale Unterstützung zu suchen. Diejenigen, die sich dennoch offenbaren, berichten häufig von ablehnenden Reaktionen, die Schuld- und Schamgefühle verstärken. Diese ablehnenden Reaktionen führen zu weiterer Isolation, was wiederum die Dunkelziffer erhöht und den Zugang zu Hilfsangeboten erschwert. Daher ist die Sensibilität und die Rolle von Pädagogen entscheidend, um ein vorurteilsfreies Umfeld zu schaffen, das die Offenlegung von Betrugsfällen und frühzeitiges Eingreifen fördert.

Risiko einer erneuten Viktimisierung

Opfer, die den Betrug nicht erkennen oder darauf hereinfallen, insbesondere jene, die Warnungen aufgrund ihrer Gutgläubigkeit ignorieren, laufen Gefahr, erneut Opfer zu werden. Diese wiederholte Viktimisierung hängt mit emotionaler Verleugnung und dem fortwährenden Glauben an die Aufrichtigkeit der Absichten des Betrügers zusammen.

Dies wird noch verschlimmert, wenn die Opfer Warnungen Dritter ignorieren. Deshalb müssen Pädagogen in der Lage sein, diese Überzeugungen behutsam anzusprechen und gleichzeitig Vertrauen und Unterstützung zu wahren.

Verschlechterung der körperlichen und geistigen Gesundheit

In schweren Fällen äußert sich psychischer Stress auch körperlich. Betroffene berichten von Kopfschmerzen, Schlafstörungen, Panikattacken oder der Verschlimmerung chronischer Erkrankungen. Manche entwickeln Suizidgedanken, insbesondere diejenigen, die sich nicht in einem unterstützenden Umfeld befinden, von ihrem Umfeld mit Scham und Schuldgefühlen konfrontiert werden und sich deshalb selbst isolieren.

Finanzieller Schaden und Abhängigkeit

Opfer von Liebesbetrug meldeten finanzielle Verluste zwischen 50 € und über 800.000 €.

Die durchschnittlichen Verluste liegen zwischen 1.000 und 10.000 Euro pro Fall. Viele Betroffene leiden daher unter langfristiger wirtschaftlicher Unsicherheit, eingeschränktem Zugang zu Grundbedürfnissen und sind in manchen Fällen auf familiäre oder staatliche Unterstützung angewiesen. Einige verlieren sogar ihr Zuhause, ihre Altersvorsorge oder Erbschaften, was ihre Lebensqualität dauerhaft beeinträchtigen kann.

Psychologische Langzeitwirkungen

Auch lange nach dem Liebesbetrug zeigte sich, dass die Opfer noch bis zu zehn Jahre nach dem Vorfall unter anhaltender Trauer und einem Trauma des Verrats, Vermeidung von Online-Kommunikation, Misstrauen gegenüber anderen, beeinträchtigten zwischenmenschlichen Beziehungen sowie anhaltender finanzieller und emotionaler Unsicherheit, geringem Selbstwertgefühl und Angstzuständen leiden konnten.

2.4 Fallstudien aus dem realen Leben zu Liebesbetrugsfällen:

Nachdem die Auswirkungen von Liebesbetrug und die Verhaltens- und sozialen Schwachstellen älterer Opfer, die potenziell Opfer von Liebesbetrug werden können, erläutert wurden, werden in diesem Abschnitt einige Fallstudien aus der Praxis vorgestellt. Diese verdeutlichen nicht nur die Taktiken der Betrüger, sondern auch die emotionalen, finanziellen und psychischen Folgen für die Opfer. Die Fallbeispiele dienen Pädagogen als wichtige Lernhilfe, indem sie die Dynamik von Betrugsfällen veranschaulichen, das Erkennen von Warnsignalen in realen Situationen erleichtern und das komplexe Zusammenspiel von Verletzlichkeit, Vertrauen und Täuschung aufzeigen. Die folgenden Fallstudien basieren auf dokumentierten Vorfällen aus Europa und Australien und legen den Schwerpunkt auf deren Relevanz für die in den vorherigen Abschnitten erörterten Verhaltens-, emotionalen und systemischen Aspekte.

2.4.1 Fallbeispiel 1: Das französische Opfer eines Promi-Imitationsbetrugs

Einer der bekanntesten Fälle von Liebesbetrug der letzten Jahre betraf die 53-jährige Französin Anne, die von einem Betrüger, der sich als Schauspieler Brad Pitt ausgab, um rund 830.000 Euro betrogen wurde. Laut Medienberichten und Interviews von Euronews und Le Monde begann der Betrug damit, dass Anne über soziale Medien von einer Person kontaktiert wurde, die behauptete, Pitts Mutter zu sein. Aus dieser ersten Kontaktaufnahme entwickelte sich eine direkte Online-Kommunikation mit einem falschen „Brad Pitt“, unterstützt durch KI-generierte Fotos, gefälschte Wohltätigkeitsveranstaltungen und Bilder aus dem Krankenhaus.

Im Laufe von mehr als einem Jahr vertiefte sich die Beziehung, Anne isolierte sich sozial und misstraute zunehmend Freunden und Familie, die die Legitimität der Beziehung in Frage stellten.

Die Frau nutzte die Romanze aus und überwies Geld, um vermeintlich dringende finanzielle Bedürfnisse im Zusammenhang mit Arztrechnungen und eingefrorenen Bankkonten während Pitts Scheidung zu decken. Der Betrug bediente sich sowohl emotionaler Manipulation als auch technischer Täuschung, darunter KI-generierte Bilder und simulierte Videochats.

Nachdem Anna erkannte, dass sie betrogen worden war, litt sie unter schweren psychischen Belastungen wie Demütigung, emotionaler Verletzung und Depression. Nachdem der Betrug öffentlich bekannt wurde, wurde sie im Internet gemobbt und verspottet, was ihren psychischen Zustand weiter verschlechterte.

2.4.2 Fallbeispiel 1: Das französische Opfer eines Promi-Imitationsbetrugs

Im Jahr 2024 deckten die spanischen Behörden einen transnationalen Betrüger auf, der sich ebenfalls als Brad Pitt ausgab und mehrere ältere Frauen über soziale Medien betrog, wobei er auf der Grundlage psychologischer Profile gezielt vorging.

In diesem Fall schuf der Betrüger falsche Identitäten und erfand überzeugende Geschichten über Liebesbeziehungen und Geschäftsvorhaben. Die Opfer wurden dazu gebracht, in fiktive Filmprojekte oder angeblich von Pitt geleitete humanitäre Projekte zu investieren. Insgesamt wurden die Frauen um über 325.000 € betrogen. Die Ermittler verfolgten die Gelder über ein komplexes Geldwäschenetzwerk mit mehreren Strohmannkonten. Die Behörden beschlagnahmten diverse digitale Geräte, Dokumente und Mobilgeräte, die zur Erstellung und Aufrechterhaltung des Betrugs verwendet wurden.

Dieser Fall verdeutlicht zwei wichtige Erkenntnisse für die Pädagogik. Erstens: Liebesbetrug wird zunehmend von organisierten kriminellen Netzwerken mit transnationaler Reichweite und digitalen Kompetenzen begangen. Zweitens: Opfer hegen oft eine tiefe emotionale Bindung zu der vorgetäuschten Beziehung, die ihr Urteilsvermögen selbst bei wachsendem Misstrauen beeinträchtigen kann. Dies unterstreicht die Notwendigkeit, dass Pädagogen in Präventionsprogrammen gegen Betrug sowohl die kognitiven als auch die emotionalen Aspekte berücksichtigen.

2.4.3 Fallstudie 3: Veronica Watson und die Folgen von Vertrauen

Veronica Watson, eine 59-jährige australische Großmutter, erlangte internationale Bekanntheit, nachdem sie 2013 in Brasilien wegen unwissentlichen Kokainschmuggels verhaftet worden war. Der Betrug begann mit einem Mann, den sie online kennengelernt hatte und der vorgab, Hilfe bei der Zustellung von Investitionsdokumenten zu benötigen. Nachdem er monatelang ihr Vertrauen gewonnen und sie manipuliert hatte, überzeugte er sie schließlich dazu, Kokain zu schmuggeln.

Veronica schmuggelte einen Koffer mit 5 kg Kokain nach Brasilien. Daraufhin wurde sie am internationalen Flughafen von São Paulo festgenommen und verbrachte über zwei Jahre im Gefängnis, bevor sie freigesprochen wurde. Das Gericht nahmte an, dass sie Opfer eines Betrugs geworden war. Die psychischen Folgen waren jedoch irreparabel; sie litt unter anhaltenden Angstzuständen, sozialer Stigmatisierung und einem Verlust des Vertrauens in ihre Fähigkeiten.

Fallstudie 4: Der Liebesbetrugsfall von Annette Ford

Dieser Fall verdeutlicht die Überschneidungen zwischen Liebesbetrug und anderen Formen krimineller Ausbeutung, darunter Drogenhandel und Geldwäsche. Er zeigt auch, wie die Manipulation von Opfern nicht nur zu finanziellen Verlusten, sondern auch zu lebensverändernden rechtlichen Konsequenzen führen kann. Aus pädagogischer Sicht verdeutlicht er, wie wichtig es ist, ältere Erwachsene nicht nur über Finanzbetrug, sondern auch über „Romance- und Liebesbetrug“ im Zusammenhang mit kriminellen Aktivitäten aufzuklären.

2.4.4

Annette Ford, eine 57-jährige Frau aus Perth, Australien, wurde auf zwei verschiedenen Dating-Plattformen Opfer von Liebesbetrug. Insgesamt verlor sie rund 780.000 Dollar – ihre gesamten Ersparnisse. Die Betrügereien ereigneten sich nach ihrer Scheidung, in einer Zeit emotionaler Verletzlichkeit. In beiden Fällen zeigten die Männer, die sie online kennengelernt hatte, zunächst große Zuneigung und überhäuften sie mit Liebesbekundungen. Anschließend gaben sie sich als Akademiker aus, die aufgrund von Komplikationen im Ausland vorübergehende finanzielle Schwierigkeiten hatten.

Annette verkaufte ihr Haus, löste ihre Rentenversicherung auf und lieh sich Geld, um es den Betrügern zu schicken. Sie entfremdete sich ihrer Familie, die mit ihren Entscheidungen nicht einverstanden war. Nach dem Betrug wurde Annette obdachlos und war auf staatliche Unterstützung angewiesen. Zu den psychischen Folgen gehörten Depressionen, Schlaflosigkeit und Panikattacken.

Ihr Fall umfasst langfristige Folgen wie wirtschaftliche Benachteiligung, soziale Isolation und schwere psychische Belastung. Er zeigt auch, wie ein vorausgegangenes Trauma durch eine Scheidung in Kombination mit Betrugserfahrungen die emotionale Verletzlichkeit verstärken kann. Für Pädagogen verdeutlicht dies die Notwendigkeit traumasensibler Präventionsstrategien, die die vielschichtigen Kontexte berücksichtigen, in denen Betrugsfälle auftreten.

2.4.5 Mann aus Nordirland um über 200.000 Pfund betrogen

Ein weiterer Fall betrifft einen Mann aus Nordirland, der ebenfalls mehr als 200.000 Pfund verlor, nachdem er eine vermeintliche romantische Beziehung eingegangen war, die über eine Dating-App begann und von 2020 bis 2025 andauerte.

Er glaubte, mit einer Frau, die er online kennengelernt hatte, in einer Beziehung zu sein, und über zwei Jahre hinweg überwies er ihr große Geldbeträge als Reaktion auf dringend klingende Anfragen: Anwaltskosten im Zusammenhang mit dem Testament eines Verwandten; Arztrechnungen nach einem Autounfall; und einen manipulierten gefälschten Online-Banking-Link.

Dieser Betrug nutzte sowohl emotionale Abhängigkeit als auch technische Manipulation aus. Das Opfer berichtete, dass der Betrug so groß war, dass er sein Leben beinahe zerstörte und ihn emotional und finanziell ruinierte. Schließlich wandte er sich an die Polizei von Nordirland (PSNI), die ihm bei der Rückgewinnung der Gelder half.

2.4.6 Mann aus Wrexham um 25.000 Pfund betrogen

Anfang 2024 wurde ein 65-jähriger Mann aus Wrexham (Großbritannien) um etwa 25.000 Pfund betrogen, nachdem er sich im März 2023 aufgrund von Einsamkeit und familiärer Entfremdung bei einer Online-Dating-Plattform angemeldet hatte. Er nahm über die Plattform Kontakt zu einer Person auf, die das Gespräch auf WhatsApp verlagerte und ihn täglich kontaktierte.

Kurz darauf forderte der Betrüger Geld für eine Anzahlung, um gemeinsam ein Haus zu kaufen, und wies das Opfer an, Geld, Apple-Geschenkgutscheine, Schmuck und ein iPhone über mehrere Adressen zu senden.

Dies dauerte bis Januar 2021 an, als der Mann die Person bei der Polizei anzeigte. Er war tief betroffen, da das emotionale Versprechen einer „gemeinsamen Zukunft“ eine zentrale Rolle in seiner Beziehung und seinem Verlust gespielt hatte. Ihm wurden Beratungsgespräche mit Opferhilfsorganisationen angeboten, um ihm zu helfen, das Erlebte zu verarbeiten.

2.4.7 Schlussfolgerungen aus den obigen Fallstudien und pädagogische Implikationen

Diese Fallstudien verdeutlichen sowohl die Vielfalt der Betrugstaktiken als auch die gemeinsamen emotionalen Aspekte und kognitiven Muster, die Betrüger ausnutzen.

Daraus lässt sich schließen, dass die Opfer zwar aus unterschiedlichen sozioökonomischen Schichten und Ländern stammen, aber durch psychologische Themen wie Trauer, Isolation und idealisierte romantische Vorstellungen verbunden sind. Hier kommt die Rolle von Pädagogen und Jugendarbeitern ins Spiel: Sie müssen die Tiefe der emotionalen Bindung, die die Opfer entwickeln, die Raffinesse der Betrugsmethoden und die Komplexität der Bewältigung nach einer Viktimisierung erkennen. Diese umfasst nicht nur finanzielle Schäden, sondern auch psychische Beeinträchtigungen und soziale Stigmatisierung.

2.5 Fallstudien aus dem realen Leben zu Liebesbetrugsfällen:

Aus den zuvor erläuterten Informationen zu den psychischen Belastungen der Opfer, den Auswirkungen und den Erkenntnissen aus den oben genannten Fallstudien wird deutlich, dass die zunehmende und rasante Bedrohung durch Liebesbetrug unter älteren Erwachsenen ein koordiniertes und proaktives Vorgehen erfordert. Als Akteure an vorderster Front in der Gemeinde, im Bildungsbereich und in sozialen Einrichtungen spielen Pädagogen und Jugendarbeiter eine zentrale Rolle. Sie sind in einer einzigartigen Position, Frühwarnzeichen zu erkennen, präventive Maßnahmen umzusetzen und Betroffenen bei der Bewältigung ihrer Probleme zu helfen. Aufgrund dieser wichtigen Rolle ist es daher entscheidend, besser zu verstehen, warum Pädagogen und Jugendarbeiter – und nicht nur die Strafverfolgungsbehörden oder die Gemeinde – einbezogen werden müssen.

2.5.1 Pädagogen als Wächter über Betrugsaufklärung und Betrugsprävention

Pädagogen, die mit älteren Erwachsenen arbeiten, insbesondere in Gemeindezentren und Erwachsenenbildungsprogrammen, besitzen ein hohes Gespür für frühe Anzeichen von Betrug. Sie sind oft die erste verlässliche Anlaufstelle für ältere Menschen außerhalb des familiären Umfelds, da sie Verhaltensänderungen objektiv beobachten, einfühlsame Gespräche führen und strukturierte Lernumgebungen schaffen können, die eine frühzeitige Erkennung ermöglichen.

Einer Studie zufolge neigen ältere Erwachsene eher dazu, Betrugserfahrungen gegenüber Pädagogen als gegenüber Behörden oder Familienangehörigen anzuvertrauen, insbesondere wenn ein vorurteilsfreies, unterstützendes Verhältnis besteht. Dieses Vertrauen versetzt Pädagogen in eine ideale Position, um präventive Gespräche anzustoßen, auf geeignete Beratungsstellen zu verweisen und das Thema Betrugserfahrungen zu enttabuisieren.

Darüber hinaus ergaben experimentelle Studien, dass Bildungsangebote wie Betrugspräventionsspiele und -workshops das Bewusstsein älterer Menschen für Betrugsmaschen deutlich schärfen, ihre Anfälligkeit verringern und ihre Selbstwirksamkeit beim Erkennen von Betrugstaktiken sowie ihre digitale Kompetenz stärken. Dadurch wird ihre Abhängigkeit von gefälschten Online-Interaktionen reduziert. Diese Bildungsstrategie gilt zudem als die effektivste Methode zur frühzeitigen Prävention von finanzieller Ausbeutung. Darüber hinaus können Pädagogen insbesondere für Menschen mit beginnenden kognitiven Beeinträchtigungen als kognitive Stützen fungieren, indem sie durch regelmäßige Aktivitäten Gedächtnis, Urteilsvermögen und kritisches Denken fördern. Dies unterstreicht das Potenzial von Bildungsformaten und Pädagogen, sowohl das Verhalten als auch die Denkweise älterer Lernender positiv zu beeinflussen.

2.5.2 Jugendbetreuer als Brückenbauer zu digitaler Sicherheit und Empathie

Jugendarbeiter spielen eine entscheidende Rolle beim generationsübergreifenden Lernen. Älteren Erwachsenen mangelt es häufig an digitalen Kompetenzen, einem wichtigen Risikofaktor für Liebesbetrug. Durch Mentoring können Pädagogen älteren Erwachsenen beibringen, wie sie gefälschte Profile erkennen, verdächtige Nachrichten melden und ihre Online-Datenschutzeinstellungen verwalten. Wichtig ist auch, dass dieser Austausch die emotionale Widerstandsfähigkeit durch soziale Integration und gemeinsame Ziele stärkt – beides verringert die Anfälligkeit für Betrug.

Die Forschung betonte zudem, dass Präventionsmaßnahmen auf die besonderen Bedürfnisse älterer Menschen zugeschnittene Lehrpläne umfassen müssen. Dazu gehört die wichtige Aufgabe, Lehrkräfte darin zu schulen, nicht nur Wissenslücken zu schließen, sondern auch emotionale Traumata und kognitive Dissonanzen im Zusammenhang mit Betrugserfahrungen zu bewältigen.

2.5.3 Professionelles Vertrauen und systemischer Zugang

Pädagogen genießen oft ein hohes Vertrauen und können Opfern so helfen, sensible Informationen preiszugeben, die sie sonst vor Familie oder Behörden verheimlichen würden, ohne sich schämen oder schuldig fühlen zu müssen. Dadurch sind Pädagogen in einer einflussreichen Position, nachdem sie ein sicheres Netzwerk aufgebaut haben, um Opfer bei der Anzeigeerstattung zu unterstützen, mit Strafverfolgungsbehörden und Rechtsbeiständen zusammenzuarbeiten und Hilfsangebote für psychische Gesundheit und finanzielle Erholung zu vermitteln.

Die Pädagogen verfügen zudem über institutionelle Reichweite durch Partnerschaften mit Bibliotheken, Gesundheitszentren, Kirchen und Seniorenclubs, die mobilisiert werden können, um ältere Menschen zu erreichen und sie bei solchen Betrügereien durch präventive und reaktive Maßnahmen zu unterstützen.

2.5.4 Jugendarbeiter als Akteure der generationenübergreifenden Stärkung

Jugendarbeiter werden in Diskussionen über den Schutz älterer Menschen oft übersehen, obwohl ihre Rolle grundlegend für die Förderung digitaler Sicherheit und sozialer Kontakte ist. Als Pädagogen konzentrieren sie sich in erster Linie darauf, Entwicklung und Veränderung zu unterstützen. Dies entspricht den Bedürfnissen älterer Erwachsener, die sich in der ungewohnten Welt der Online-Beziehungen zurechtfinden müssen. Studien haben zudem gezeigt, dass generationsübergreifende Programme, die ältere Erwachsene mit jüngeren digitalen Mentoren zusammenbringen, vielversprechende Ergebnisse erzielen: Sie erhöhen die Betrugserkennungsrate, stärken das Vertrauen in Online-Tools und reduzieren soziale Isolation – einen der größten Risikofaktoren für Liebesbetrug. Jugendarbeiter begleiten diese Begegnungen und vermitteln gleichzeitig gesunde digitale Grenzen und die Fähigkeit zur kritischen Auseinandersetzung mit Online-Identitäten.

2.5.5 Bedeutung von Schulung und struktureller Unterstützung

Pädagogen und Jugendbetreuer verfügen über Instrumente und Schulungen, die für eine angemessene Unterstützung älterer Menschen hilfreich sind. Dazu gehören:

Kenntnisse über Betrugstypen, Anbahnungstaktiken und Verhaltensmerkmale

Zugang zu Checklisten, digitalen Hygieneleitfäden und Überweisungsvorlagen

Partnerschaften mit Strafverfolgungsbehörden, Anbietern von Leistungen im Bereich der psychischen Gesundheit und Organisationen zum finanziellen Schutz älterer Menschen.

Instrumente für anonyme Meldungen und Weiterleitungswege.

Aus den oben genannten Punkten geht hervor, dass in unserer schnelllebigen Welt die Rolle der Erzieher bei der Unterstützung von Opfern oder potenziellen Opfern von Liebes- und Romantikbetrug nicht nur wichtig, sondern auch notwendig ist, da sie einen großen Einfluss auf die Anwendung der verschiedenen Präventions- und Reaktionsmaßnahmen haben, wie in diesem Kapitel näher erläutert wird.

2.6 Präventive Maßnahmen zum Schutz von Senioren vor Betrügern

Um Senioren wirksam vor Liebesbetrug zu schützen, ist es unerlässlich, präventive Maßnahmen zu ergreifen, die das Risiko, Opfer von Liebesbetrug zu werden, verringern. Indem wir Senioren die nötigen Werkzeuge und Kenntnisse vermitteln, um Betrug zu erkennen und zu vermeiden, ein unterstützendes soziales Umfeld fördern und die Kompetenzen der Betroffenen stärken, können wir ihr Risiko, Opfer zu werden, deutlich reduzieren. Zu diesen Maßnahmen gehören die Förderung digitaler Kompetenzen und die Stärkung sozialer Kontakte. Beides spielt eine entscheidende Rolle, um Senioren zu helfen, sich in einer zunehmend technologie- und netzwerkorientierten Welt zurechtzufinden.

2.6.1 Bewusstsein für digitale Kompetenz

Eine der wichtigsten Präventionsmaßnahmen für Senioren ist die Verbesserung ihrer digitalen Kompetenzen. Da sich die Technologie ständig weiterentwickelt, passen Betrüger ihre Methoden fortwährend an und erstellen Rollenspiele mit realitätsnahen Szenarien. Hier können Lehrkräfte beobachten, wie Senioren gefälschte Profile erkennen, Datenschutzeinstellungen verstehen, Warnsignale im Internet wahrnehmen und umgekehrte Bildersuchen durchführen. Anschließend können sie die gewonnenen Erkenntnisse in anregenden Gesprächen mit den Senioren reflektieren. Indem sie die Senioren in realitätsnahe Situationen bringen, können sie das Gelernte im Alltag anwenden.

✦ Workshops zu gängigen Betrugstaktiken:

Gezielte Workshops sind eine effektive Methode, Senioren über die häufigsten Online-Betrugsmaschen aufzuklären. Diese Workshops sollten die Grundlagen zur Erkennung von Phishing-E-Mails, gefälschten Profilen in sozialen Medien oder auf Dating-Plattformen, KI-Betrug und anderen Betrugsmaschen wie gefälschten Anrufen von angeblichem technischen Support behandeln. Die Kursleiter sollten anhand praktischer Beispiele aufzeigen, wie Betrüger oft mit Dringlichkeitsfloskeln, Belohnungsversprechen oder emotionalen Appellen ihre Opfer manipulieren. Außerdem sollten sie den Einsatz von KI thematisieren und erklären, wie man von KI-Tools erstellte Bilder oder Texte vergleicht und analysiert. Ziel dieser Workshops ist es, Senioren in die Lage zu versetzen, Warnsignale zu erkennen und potenzielle Betrugsversuche sicher zu durchschauen.

✦ Praxisorientiertes Training:

Digitale Kompetenz geht weit über das bloße Wissen um Betrugsmaschen hinaus – sie vermittelt Senioren die Fähigkeiten, Technologie sicher zu nutzen. In praktischen Schulungen lernen sie, soziale Medien sicher zu nutzen, beispielsweise durch das Anpassen von Datenschutzeinstellungen, die Überprüfung der Identität von Online-Kontakten, das Erkennen verdächtiger Links oder Anfragen nach persönlichen Daten sowie das Erkennen typischer Gesprächsmuster von Betrügern. So lernen sie beispielsweise, Phishing-E-Mails zu erkennen, indem sie die Absenderadresse prüfen, auf Rechtschreibfehler achten oder verdächtige Anhänge identifizieren. Schulungsleiter können ihnen außerdem beibringen, wie man sichere Websites (mit „https://“ in der URL) nutzt und wie man das Herunterladen von Dateien aus unbekannten Quellen vermeidet. Senioren sollten zudem lernen, wie sie verdächtige Aktivitäten melden, sei es eine betrügerische E-Mail, ein betrügerischer Anruf oder ein fragwürdiges Online-Profil. Um diese Schulungen effektiver zu gestalten, empfiehlt es sich, Übungen und Anwendungsaufgaben in die Schulungen zu integrieren, beispielsweise Rollenspiele mit realitätsnahen Szenarien, in denen die Schulungsleiter mögliche Gefahren erkennen können.

Die Senioren lernen, gefälschte Profile zu erkennen, Datenschutzeinstellungen zu verstehen, Warnsignale im Internet zu erkennen und umgekehrte Bildersuchen durchzuführen. Anschließend werden die Ergebnisse in anregenden Gesprächen reflektiert. Indem die Senioren in realitätsnahe Situationen versetzt werden, können sie das Gelernte in der Praxis anwenden.

Bürgerbeteiligungsveranstaltungen:

- Es sollten auch Informationsveranstaltungen angeboten werden, die über die Rolle von Strafverfolgungsbehörden, Banken und Finanzsicherheitsverfahren, Cybersicherheit und das richtige Verhalten bei Liebesbetrug aufklären. Experten sollten zu diesen regelmäßigen Veranstaltungen eingeladen werden. Darüber hinaus sollten Vorlagen für die Meldung verschiedener Fälle bereitgestellt werden. All dies kann auch in gedruckten Handouts und visuellen Hilfsmitteln enthalten sein, um als Erinnerung zu dienen und Senioren Sicherheit hinsichtlich der nächsten Schritte im Betrugsfall zu geben.

2.6.2 Förderung sozialer Kontakte

- Eine weitere wichtige Präventionsmaßnahme ist die Förderung sozialer Kontakte. Viele Betrüger nutzen die Isolation und Einsamkeit älterer Menschen aus. Ein Gemeinschaftsgefühl und die Förderung sozialer Interaktion helfen Senioren nicht nur, in Kontakt zu bleiben, sondern bieten ihnen auch die Unterstützung und Ressourcen, die sie benötigen, um zu erkennen, wenn etwas nicht stimmt. Dies kann durch Gruppengespräche, Treffen zur gegenseitigen Unterstützung und Patenschaftsprogramme geschehen.

A. Gruppenaktivitäten und Buddy-System

Gruppenaktivitäten:

Die Teilnahme älterer Menschen an Gruppenaktivitäten kann deren Isolationsgefühl, das oft zu Verletzlichkeit führt, deutlich verringern. Peer-to-Peer-Clubs, Hobbygruppen und virtuelle Treffen sind hervorragende Möglichkeiten, Senioren zusammenzubringen, damit sie gemeinsame Interessen teilen und wertvolle Beziehungen aufbauen können. Durch den regelmäßigen Kontakt mit anderen sind Senioren weniger anfällig dafür, Betrügern zum Opfer zu fallen, die ihre emotionalen oder sozialen Bedürfnisse ausnutzen wollen. Gruppenaktivitäten bieten zudem einen geschützten Raum, um verdächtige Begegnungen zu besprechen, Rat von Gleichaltrigen zu erhalten und sich über mögliche Betrugsmaschen in der Gemeinde zu informieren. Beispielsweise kann ein Buchclub oder eine Bastelgruppe eine wertvolle Möglichkeit sein, Senioren in ein soziales Umfeld einzubinden und so sowohl die geistige Anregung als auch das soziale Wohlbefinden zu fördern.

Buddy-Systeme:

Eine weitere wirksame Methode, soziale Kontakte zu fördern und Isolation zu verringern, ist die Einrichtung von Patensystemen. Wenn Senioren sich regelmäßig treffen, Erfahrungen austauschen und sich gegenseitig unterstützen, entsteht ein Gefühl der Zusammengehörigkeit. Fühlen sich Senioren stärker mit anderen verbunden, sind sie weniger anfällig für Betrug, da sie in verdächtigen Situationen eine vertrauenswürdige Person haben, an die sie sich wenden können. Ein Patensystem ermöglicht es Senioren außerdem, sich über potenzielle Betrugsmaschen zu informieren, indem sie Informationen über aktuelle Fälle oder Warnsignale austauschen. Darüber hinaus kann die emotionale Unterstützung durch einen Paten Senioren mehr Sicherheit geben und die Wahrscheinlichkeit verringern, dass sie sich an potenziell betrügerische Personen wenden.

B. Ausweitung der sozialen und emotionalen Unterstützung

- Neben Gruppenaktivitäten und Patenschaften ist der Aufbau eines breiteren Unterstützungsnetzwerks unerlässlich. Lokale Gemeindezentren, Seniorenorganisationen und Online-Gruppen mit spezifischen Interessen können Senioren dabei helfen, ein aktives Sozialleben zu führen und so das Risiko von Isolation und emotionaler Verletzlichkeit zu verringern. Mit einem starken sozialen Netzwerk sind Senioren besser gerüstet, um Situationen zu bewältigen, in denen sie sich manipuliert oder unter Druck gesetzt fühlen, da sie sich auf die Unterstützung vertrauter Freunde oder Familienmitglieder verlassen können.

- Darüber hinaus kann die emotionale Unterstützung von Senioren, die trauern, unter Einsamkeit leiden oder mit anderen emotionalen Belastungen zu kämpfen haben, dazu beitragen, dass Betrüger diese Schwächen nicht ausnutzen. Trauerberatung, Therapiegruppen und Mentoring-Programme können wesentlich dazu beitragen, dass Senioren ihr emotionales Wohlbefinden bewahren und somit weniger anfällig für die Machenschaften von Betrügern werden, die nach leichten Opfern suchen.

Durch die Kombination von Maßnahmen zur Förderung digitaler Kompetenzen mit Strategien zur Stärkung sozialer Kontakte können Senioren besser vor Betrug und Täuschung geschützt werden. Pädagogen, Pflegekräfte und Gemeindevertreter spielen eine entscheidende Rolle bei der Umsetzung dieser Präventionsmaßnahmen. Ob durch Workshops zur digitalen Sicherheit oder durch soziale Programme gegen soziale Isolation – diese Initiativen helfen Senioren, ihre Unabhängigkeit und Sicherheit in einer zunehmend von Technologie und sozialen Interaktionen geprägten Welt zu bewahren. Gemeinsam bilden diese Präventionsmaßnahmen eine solide Grundlage, um Senioren vor der stetig wachsenden Bedrohung durch Betrug zu schützen.

2.7 Liebesbetrug frühzeitig verhindern durch Verhaltensindikatoren für Betrugsfälle:

- Nachdem wir die Maßnahmen kennengelernt haben, die Pädagogen ergreifen können, um Senioren künftig vor Betrug zu schützen, sollten wir auch überlegen, wie sie reagieren können, wenn sie einen laufenden Liebesbetrug bei älteren Opfern bemerken. Um dem entgegenzuwirken, werden Verhaltensindikatoren – einige davon aus den oben genannten Fallstudien – erläutert, um Pädagogen, Jugendarbeiter und Betreuer bei der Früherkennung von Liebesbetrug zu unterstützen. Anschließend werden verschiedene Instrumente und Maßnahmen zur Beurteilung vorgestellt, damit Pädagogen wissen, wie sie im Falle eines laufenden Liebesbetrugs handeln können.

2.7.1 Verhaltenswarnzeichen bei älteren Opfern

- Um Schäden durch Liebesbetrug zu verhindern, ist nicht nur allgemeine Aufklärung wichtig, sondern auch die frühzeitige Erkennung von Verhaltens- und emotionalen Warnsignalen, die darauf hindeuten, dass eine Person in einen Liebesbetrug verwickelt sein könnte. Zahlreiche Studien bestätigen, dass Liebesbetrug typischerweise einem strukturierten Ablauf folgt: von der ersten Kontaktaufnahme über die emotionale Manipulation und die finanzielle Anbahnung bis hin zur sozialen Isolation. Jede dieser Phasen ist durch spezifische Verhaltensänderungen gekennzeichnet, die, richtig interpretiert, auf die Notwendigkeit eines zeitnahen und gezielten Eingreifens hinweisen können. Zu diesen Warnsignalen gehören unter anderem die folgenden:

Geheimhaltung bei neuen Online-Beziehungen:

- Oftmals verbergen Opfer ihre Kommunikation mit dem Betrüger aus Angst vor Verurteilung oder dem vermeintlichen Verrat ihres Online-„Partners“. Dies deckt sich mit den Ergebnissen von Forschungsstudien, die festgestellt haben, dass Opfer eine Offenlegung bewusst vermeiden, insbesondere wenn sie emotional involviert sind.

Plötzlicher übermäßiger Telefon- oder Internetgebrauch:

- Die Opfer neigen dazu, sich zwanghaft in der digitalen Kommunikation zu engagieren und wirken oft emotional abhängig von Messaging-Apps oder Videochats.

Sozialer Rückzug:

- Mit zunehmender Intensität der Anbahnungsversuche meiden die Opfer möglicherweise Gemeinschaftsveranstaltungen und Treffen mit Gleichaltrigen.

- und sogar familiäre Interaktionen. Sie reagieren möglicherweise auch defensiv auf Online-Aktivitäten. Eine Studie ergab, dass Betrüger davon profitieren, ihre Opfer von anderen Einflussquellen zu isolieren.

Erhöhte emotionale Zustände:

- Opfer können zwischen Euphorie (beim Erhalt von Nachrichten des Betrügers) und Angst oder Traurigkeit (wenn der Betrüger nicht erreichbar ist oder Geld verlangt) schwanken. Auch plötzliche Stimmungs- oder Verhaltensänderungen sind möglich. Diese emotionalen Schwankungen sollten nicht als allgemeine Stimmungsschwankungen abgetan, sondern im Kontext neu entstandener sozialer Kontakte betrachtet werden.

Unerklärte Finanzaktivitäten:

- Lehrkräfte und Familienangehörige bemerken möglicherweise Geldabhebungen an Geldautomaten, plötzliche Überweisungen oder Anfragen nach Hilfe bei internationalen Bankgeschäften. Eine Studie erklärt, dass solchen Transaktionen oft eine verminderte kognitive Kontrolle und ein eingeschränktes Finanzverständnis vorausgehen.

2.7.2. Die Rolle der Pädagogen bei der Aufdeckung eines laufenden Betrugs und der Unterstützung älterer Menschen

- Pädagogen und Jugendarbeiter sind in einer einzigartigen Position, diese frühen Anzeichen zu erkennen. Anders als Familienmitglieder, denen möglicherweise der objektive Einblick in den emotionalen Zustand des Einzelnen fehlt, sind Pädagogen oft in strukturierte Gruppenumgebungen eingebunden, in denen sie Veränderungen im Laufe der Zeit objektiv beobachten können. Beispielsweise können Senioren, die sich ungewöhnlich enthusiastisch für eine neue Online-Bekanntschaft interessieren, häufig von einer idealisierten Beziehung sprechen oder sich, wie bereits erwähnt, von Gemeinschaftsveranstaltungen zurückziehen.

Pädagogische Fachkräfte sollten über ein ausgeprägtes Beobachtungsvermögen verfügen und in der Lage sein, Verhaltensweisen von allgemeinen Alterserscheinungen oder Stimmungsschwankungen zu unterscheiden. Sie können kurze, unaufdringliche Screening-Instrumente in Gruppensitzungen oder Einzelgesprächen einsetzen. Bei Unsicherheiten können sie das Einzelgespräch mit neutralen, offenen Fragen einleiten, um Konfrontationen und Schamgefühle zu vermeiden, wie zum Beispiel: „Haben Sie sich bei Ihren Online-Interaktionen sicher und respektiert gefühlt?“, „Sind Ihnen ungewöhnliche Anfragen oder Gespräche online aufgefallen?“, „Haben Sie in letzter Zeit jemanden online kennengelernt?“ oder „Wurden Sie nach finanziellen Informationen gefragt?“

- „Wollen Sie etwas verschweigen oder etwas geheim halten?“ Diese Fragen ermöglichen es älteren Erwachsenen, ohne Abwehrhaltung zu reflektieren. So fördern Pädagogen eine vertrauensvolle Atmosphäre statt aufdringlicher Berührung. Sollte die betroffene Person nicht sehr reaktionsfreudig auf die Fragen reagieren, können simulierte Szenario-Diskussionen anhand anonymisierter Geschichten oder hypothetischer Charaktere durchgeführt werden. Dabei können Pädagogen die Risiken erörtern und aufklären, ohne die Person direkt zu konfrontieren. Diese Methode reduziert nachweislich Schamgefühle und fördert das reflektierende Denken.

- Sobald Verhaltensmerkmale erkannt und der Verdacht auf einen Betrug bei Senioren bestätigt wird, sollten Fachkräfte ein sanftes Vorgehen wählen: Kontaktaufnahme, Aufklärung und Beurteilung. In der Kontaktaufnahmephase steht das Zuhören und das Zeigen von Anteilnahme im Vordergrund, während gleichzeitig ein wertfreies Umfeld geschaffen wird. Die Aufklärungsphase umfasst die Bereitstellung allgemeiner Informationen über Online-Liebesbetrug, idealerweise in neutralen Formaten wie Broschüren, Videos oder anonymisierten Fallbesprechungen. Diese indirekte Methode ermöglicht es den Betroffenen, sich mit den beschriebenen Mustern zu identifizieren, ohne sich beschuldigt zu fühlen. Die Beurteilungsphase, die oft informell erfolgt, dient der Einschätzung, ob die betroffene Person für weitere Gespräche oder Unterstützung offen ist oder ob eine Weitervermittlung an externe Stellen erforderlich sein könnte.

Darüber hinaus verbessern indirekte, gruppenbasierte Ansätze die Früherkennung. Wenn Aufklärung über Betrugsmaschen in reguläre Programme integriert wird, erkennen ältere Erwachsene Manipulationen eher in ihren eigenen oder den Erfahrungen anderer. Sie fühlen sich gesehen und nicht allein, wodurch sie sich weniger schämen und offener für Hilfe sind. Gruppenangebote und die Wiedereinbindung in verschiedene Aktivitäten tragen außerdem dazu bei, dass sie sich wieder stärker mit der Gemeinschaft verbunden fühlen und sich weniger an den Betrüger binden, was letztendlich dazu führt, dass sie sich von ihm lösen.

Zusammenfassend lässt sich sagen, dass Pädagogen frühe Verhaltensindikatoren nicht als isolierte Beobachtungen, sondern als potenzielle Unterstützer betrachten müssen. Durch die Entwicklung von Beobachtungsgabe, den Einsatz informierter Kommunikation und die Vermittlung von Kenntnissen zur Betrugserkennung können sie Liebesbetrug frühzeitig erkennen und unterbinden, bevor finanzieller oder psychischer Schaden entsteht.

2.8 Reaktionsmaßnahmen im Falle eines Liebesbetrugs

- Nachdem wir untersucht haben, welche Maßnahmen zur Prävention von Liebesbetrug ergriffen werden sollten und wie Pädagogen ältere Menschen frühzeitig erkennen und vor Betrug schützen können, analysiert dieser Abschnitt die notwendigen Reaktionen, falls ein älterer Mensch bereits Opfer eines Liebesbetrugs geworden ist. In diesem Fall ist ein behutsames, einfühlsames und strukturiertes Vorgehen unerlässlich. Diese Betrugsmaschen sind besonders schädlich, da sie die emotionale Verletzlichkeit älterer Menschen ausnutzen und häufig zu erheblichem seelischem Leid und finanziellen Verlusten führen. Es ist wichtig, schnell zu reagieren und sicherzustellen, dass sich der betroffene Senior unterstützt und befähigt fühlt, die notwendigen Schritte zur Bewältigung des Betrugs einzuleiten. Im Folgenden werden die Maßnahmen beschrieben, die im fortgeschrittenen Stadium eines Betrugs ergriffen werden sollten:

A. Zuhören und beruhigen

- Der erste Schritt im Umgang mit Liebesbetrug ist, den Betroffenen unvoreingenommen zuzuhören. Viele Senioren, die Opfer von Liebesbetrug werden, schämen sich oder fühlen sich sogar gedemütigt. Sie haben möglicherweise nicht nur Geld, sondern auch viel emotionale Energie in eine Beziehung investiert, die sie für echt hielten. Es ist entscheidend, ihre Gefühle zu bestätigen und ihnen zu versichern, dass sie keine Schuld trifft. Daher müssen Fachkräfte strukturiert und traumasensibel vorgehen und die Würde und psychische Stabilität der Opfer berücksichtigen. Ein unsachgemäßer Umgang mit dem Moment der Offenbarung kann zu Retraumatisierung oder weiterem Schweigen führen, insbesondere bei Senioren, die möglicherweise bereits mit digitaler Ausgrenzung und generationsbedingtem Misstrauen gegenüber Autoritäten zu kämpfen haben.

- Betrüger sind geschickt darin, Emotionen zu manipulieren und ein falsches Gefühl von Vertrautheit zu erzeugen, wodurch Senioren leicht ausgenutzt werden können. Daher ist es wichtig, dass Pädagogen die Erfahrungen der Betroffenen anerkennen und ihnen einfühlsam erklären, dass sie nicht allein sind und viele andere ähnlichen Betrügereien zum Opfer gefallen sind. Versichern Sie ihnen, dass diese Täter Kriminelle sind und ihre emotionalen und finanziellen Verluste eine direkte Folge betrügerischer Handlungen und nicht ihres eigenen Fehlverhaltens sind.

Empathie und Verständnis können dazu beitragen, Schuld- oder Schamgefühle abzubauen, die ein Hindernis für die Meldung des Vorfalls und die Suche nach Hilfe darstellen können. Teilen Sie der älteren Person mit, dass

- Sie haben Ihre volle Unterstützung und eine Genesung ist möglich. Machen Sie ihnen keine Vorwürfe, verhören Sie sie nicht und bagatellisieren Sie ihre Erfahrungen nicht, da dies zu einem sehr tiefen emotionalen Schaden führen und sie anfällig dafür machen würde, in Zukunft immer wieder Betrügereien zum Opfer zu fallen.

B. Dokumentieren Sie den Vorfall

Sobald sich die ältere Person unterstützt fühlt, besteht der nächste Schritt darin, ihr zu helfen, die Details des Betrugs zu dokumentieren. Die Aufzeichnung wichtiger Informationen wird Strafverfolgungs- und Verbraucherschutzbehörden bei ihren Ermittlungen unterstützen. Ermutigen Sie die ältere Person, die folgenden Details aufzuschreiben:

- **Datum/Datum:** Notieren Sie, wann der Betrug begann, wann Zahlungen erfolgten und alle anderen wichtigen Interaktionen.
- **Vom Betrüger verwendete Namen:** Die vom Betrüger verwendeten Namen, auch wenn sie nur angenommen oder erfunden sind. Dies kann den Behörden helfen, den Betrüger zu ermitteln.
- **Gesendete Beträge:** Notieren Sie den an den Betrüger gesendeten Geldbetrag sowie alle anderen Finanztransaktionen und seine Kontoinformationen.
- **Kommunikationskanäle:** Dokumentieren Sie, wie der Betrüger mit dem Senior kommuniziert hat (z. B. per E-Mail, Telefon, über soziale Medien oder Dating-Websites).

Diese Dokumentation ist unerlässlich, da sie den Betrug klar dokumentiert und als Beweismittel für Ermittlungen dienen kann. Sie hilft auch bei der Erstattung von Anzeigen bei den zuständigen Behörden.

C. Melden Sie sich umgehend

Der nächste entscheidende Schritt ist die Meldung des Betrugs. Schnelles Handeln ist unerlässlich, um weiteren finanziellen Schaden zu begrenzen und die Ermittlungen zu unterstützen. Helfen Sie der betroffenen Person, den Betrug den zuständigen Behörden zu melden, z. B. der örtlichen Polizei, Verbraucherschutzorganisationen oder der nationalen Betrugshotline. Wichtige Anlaufstellen für die Meldung von Liebesbetrug sind unter anderem:

- **Örtliche Polizei:** Erstatten Sie so schnell wie möglich Anzeige bei der Polizei. Bei erheblichen finanziellen Verlusten kann die örtliche Polizei Ermittlungen einleiten oder das Opfer an die zuständige Behörde weiterleiten.

- **Die Federal Trade Commission (FTC)** ist die US-amerikanische Regierungsbehörde, die für den Verbraucherschutz zuständig ist. Senioren können Betrugsfälle über die Website ReportFraud.ftc.gov melden. Die FTC bietet außerdem hilfreiche Informationen zum Schutz vor zukünftigen Betrugsversuchen.

- **Internet Crime Complaint Center (IC3):** Senioren, die Opfer von Betrügern auf Online-Plattformen (wie Dating-Websites oder sozialen Medien) geworden sind, können den Betrug dem IC3 melden. Das IC3 ist eine gemeinsame Einrichtung des FBI und des National White Collar Crime Center. Weitere Informationen finden Sie unter IC3.gov.

- **Nationale Betrugshotline:** Viele Länder verfügen über Meldestellen für Betrugsfälle, die den Behörden bei der Untersuchung und Verfolgung von Betrügern helfen. In Großbritannien können sich Senioren beispielsweise an Action Fraud unter ActionFraud.police.uk wenden, um Unterstützung zu erhalten.

- **Verbraucherschutzbehörden:** Viele Bundesländer oder Kommunen verfügen über Verbraucherschutzbehörden, die sich mit Betrugsfällen befassen. Die Schulungsleitung sollte die zuständige Behörde im jeweiligen Land ermitteln und das Opfer an diese verweisen. In Deutschland können sich Senioren beispielsweise an die Verbraucherzentrale Bundesverband (VZBV) wenden. Die VZBV ist die zentrale deutsche Verbraucherschutzbehörde und bietet umfassende Unterstützung für Betrugsopfer, darunter Rechtsvorlagen, Beratungsgespräche und Hinweise zur digitalen Sicherheit. Auf europäischer Ebene können Opfer grenzüberschreitenden Internetbetrug über das Europäische Verbraucherzentrumsnetz (ECC-Net) melden oder transnationale Beschwerden über die EUROPOL-Schnittstelle zur Meldung von Internetkriminalität einreichen.

- **Finanzinstitute und Banken:** Melden Sie den Betrug unbedingt der Bank, von der das Opfer das Geld an den Betrüger überwiesen hat. Dies hilft, die Überweisung nachzuverfolgen und gegebenenfalls eine Anzeige zu erstatten, um dem Opfer sein Geld zurückzuholen.

- **Psychologische Beratungsstellen:** Opfer sollten auch an Organisationen verwiesen werden, die psychologische Beratung, Opferhilfe und Begleitung vor Gericht anbieten. In Deutschland können sie sich beispielsweise an den Weißen Ring wenden, Deutschlands größte Organisation für Kriminalitätsopfer, die kostenlose psychologische Unterstützung anbietet. Darüber hinaus können grenzüberschreitende Fälle mit internationalen Betrügern an das OLAF (Europäisches Amt für Betrugsbekämpfung) eskaliert oder über Europols Europäisches Zentrum für Wirtschaftskriminalität (EFECC) zur potenziellen internationalen Rückverfolgung gemeldet werden.

Durch die umgehende Meldung des Betrugs schützen Senioren sich nicht nur selbst vor weiteren Verlusten, sondern helfen auch den Strafverfolgungsbehörden, Betrüger aufzuspüren und andere davor zu bewahren, ähnlichen Betrügereien zum Opfer zu fallen.

2.9 Aufbau langfristiger Unterstützungsnetzwerke:

- Nachdem ältere Opfer bei der Anzeige der Betrüger unterstützt wurden, ist es entscheidend, sie auch in den Wochen und Monaten nach der Anzeige weiterhin zu betreuen. Studien zeigen, dass viele Senioren sekundäre Viktimisierung erfahren, darunter Ablehnung, Unglaube oder Spott seitens Familie oder der Gemeinschaft. Dies kann das Trauma verstärken und zu anhaltender Isolation, erneuter Viktimisierung oder posttraumatischen Belastungssymptomen führen. Daher sind langfristige emotionale Rehabilitation, soziale Wiedereingliederung und Stärkung der Selbstbestimmung von großer Bedeutung. Pädagogen und Jugendarbeiter spielen in dieser Phase eine entscheidende Rolle, indem sie den Kontakt aufrechterhalten und die Wiedereingliederung in die Gemeinschaft sowie die emotionale Rehabilitation ermöglichen.

Um dies zu ermöglichen, sollten Jugendbetreuer und Pädagogen Betroffene zunächst ermutigen, an Selbsthilfegruppen oder von Gleichaltrigen geleiteten Genesungskreisen teilzunehmen, in denen Überlebende ihre Erfahrungen vertraulich und ohne Vorurteile austauschen können. Diese Gruppen können von Volkshochschulen, an denen die Betroffenen arbeiten, oder von altersgerechten Vereinen angeboten werden. Dies verringert ihre Isolation und fördert die soziale Integration, denn Studien haben gezeigt, dass ältere Erwachsene, die nach einem Betrug an strukturierten Selbsthilfegruppen teilnehmen, eine deutlich verbesserte psychische Widerstandsfähigkeit aufweisen und weniger anfällig für Rückfälle sind.

Ein weiterer entscheidender Aspekt ist die Nachbetreuung durch Pädagogen, beispielsweise durch regelmäßige Treffen und kontinuierliche pädagogische Unterstützung. Dies hilft ihnen, die Bedürfnisse der Betroffenen zu verstehen und ihnen das Gefühl zu geben, unterstützt zu werden. So können sie sich emotional erholen und wieder soziale Kontakte knüpfen. Wichtig ist auch, dass in allen Phasen der Reaktion die Autonomie und Würde der Betroffenen gewahrt bleiben. Pädagogen agieren dabei nicht als Ermittler oder Berater, sondern als vertrauenswürdige Partner auf dem Weg der Genesung, an dem gegebenenfalls mehrere Fachkräfte beteiligt sind. Ihre Aufgabe ist es, die Erfahrungen der Betroffenen zu bestätigen, ihnen ihre Handlungsfähigkeit zurückzugeben und sicherzustellen, dass sie die Folgen des Traumas nicht isoliert bewältigen müssen.

Darüber hinaus können Pädagogen Betroffene ermutigen, an **Gruppentherapien**, traumasensibler Beratung und Übungen zur narrativen Rekonstruktion teilzunehmen, da diese nachweislich zur Wiederherstellung der Identität und Selbstwirksamkeit beitragen. In Deutschland können Überlebende beispielsweise über die örtlichen gesetzlichen Krankenkassen (z. B. AOK, TK) oder Organisationen wie den Weißen Ring, die spezialisierte Beratung für traumatisierte Menschen anbieten, solche Angebote in Anspruch nehmen. Auch städtische Seniorenzentren und Gesundheitsnetzwerke können als Anlaufstellen für nicht-stigmatisierende psychologische Beratung dienen.

Die **digitale Wiedereingliederung** ist ein weiterer Schlüsselfaktor für die langfristige Genesung. Viele Betroffene haben Angst, digitale Werkzeuge wieder zu nutzen, was ihre Isolation verstärkt. Pädagogen und Jugendarbeiter können dazu beitragen, das Vertrauen wiederherzustellen, indem sie Workshops zur digitalen Wiedereingliederung anbieten. Diese Workshops vermitteln Online-Sicherheit, Datenschutzeinstellungen, Betrugserkennung und Kommunikationsgrenzen. Dies ist besonders wirksam, um Senioren einen sicheren und unterstützenden Wiedereinstieg in die digitale Welt zu ermöglichen.

Ein weiterer entscheidender Punkt ist **die Bereitstellung von Leitfäden und Informationsmaterialien sowie Workshops für die Familien und Freunde** der Opfer. Darin werden ein offener Dialog gefördert und Informationen vermittelt, wie man auf die älteren Menschen reagieren und sie unterstützen kann, um ihren Heilungsprozess zu fördern. Auch die Bewältigung schwieriger Gespräche wird thematisiert. So wird ein Umfeld geschaffen, in dem die Opfer nicht beschuldigt oder beschämt, sondern unterstützt werden.

Schließlich muss die Wiedereingliederung auch **Möglichkeiten zur Selbstermächtigung** umfassen, in denen Betroffene ermutigt werden, über ihre Erfahrungen zu sprechen, da ihnen das Vertrauen ihrer Mitmenschen größer ist. Opfer, die sich zu Aufklärern, Fürsprechern oder Peer-Beratern entwickeln, berichten oft von einem stärkeren Gefühl der Kontrolle und Heilung. Gemeinschaftsplattformen sollten es Überlebenden zudem ermöglichen, ihre Geschichten anonym in Newslettern, öffentlichen Foren oder Aufklärungskampagnen zu teilen und so persönlichen Schaden in gemeinschaftlichen Schutz umzuwandeln. Diese partizipative Genesung kommt nicht nur dem Einzelnen zugute, sondern stärkt auch die kollektive Wachsamkeit gegenüber Betrug.

Zusammenfassend lässt sich sagen, dass die selbstständige Genesung kein linearer, sondern ein zyklischer Prozess ist, der kontinuierliche emotionale Unterstützung, strukturierte digitale Rehabilitation, eine enge institutionelle Koordination und eine sinnvolle soziale Teilhabe erfordert.

Die Rolle der Lehrkraft auf diesem Weg ist sowohl unterstützend als auch wiederherstellend, indem sie den Opfern hilft, den Betrug nicht nur zu überwinden, sondern zu einer stärkeren, widerstandsfähigeren Person zu werden.

2.10 Praktische Fallstudien

Aufbauend auf den vorangegangenen Abschnitten zu Betrugserkennung, psychologischen Auswirkungen, der Rolle der Lehrkräfte und Interventionsstrategien werden im Folgenden praxisnahe Szenarien vorgestellt, die Lehrkräften und Jugendarbeitern helfen sollen, die wichtigsten Lernergebnisse anzuwenden. Jeder Fall stellt eine typische Situation aus dem Alltag dar und wird von Reflexionsfragen begleitet, die das Urteilsvermögen, die Kommunikationsstrategien und die ethische Sensibilität überprüfen.

2.10.1 Fallstudie 1:

Anna, 71, ist in den letzten Monaten sehr aktiv auf Facebook geworden. Während einer Kaffeepause in Ihrem Gemeindezentrum erzählt sie begeistert, dass sie einen „wunderbaren Witwer" kennengelernt hat. „Er versteht mich wirklich", sagt sie, „es ist, als wüsste er genau, wie ich mich fühle." Sie fügt hinzu, dass er sie vielleicht bald besuchen kommt, und in letzter Zeit stellt sie Fragen zum internationalen Bankwesen.

Reflexionsfragen:

- Welche Anzeichen deuten darauf hin, dass Anna gefährdet sein könnte?
- Welche konkreten Anzeichen deuten darauf hin, dass Anna anfällig für einen Liebesbetrug sein könnte?
- Wie würden Sie ein nicht-konfrontatives, vertrauensbildendes Gespräch führen, um mehr über den Betrüger zu erfahren, ohne Schamgefühle hervorzurufen?
- Welche pädagogischen Instrumente oder Strategien für den Austausch mit Gleichaltrigen könnten Sie einsetzen, um Anna dabei zu helfen, ihre Situation kritisch zu reflektieren?
- Wenn Anna weiterhin unnachgiebig bleibt, wie könnte man dann ein Sicherheitsnetz aufbauen, ohne ihr die Autonomie zu nehmen?

2.10.2 Fallstudie 2:

Walter, 78, fehlt seit Kurzem immer öfter in Ihrer Seniorengruppe. Wenn er doch mal kommt, sitzt er still da und vermeidet Augenkontakt. Ihnen fällt auf, dass er viel Zeit mit Texten verbringt und sichtlich unruhig ist. Eines Tages hören Sie zufällig, wie er erwähnt, dass er Geld schickt, um einem „Freund", den er online kennengelernt hat, einen Pass zu besorgen, damit dieser zu ihm nach Deutschland ziehen kann.

Reflexionsfragen:

- Welche Verhaltensauffälligkeiten bei Walter stimmen mit bekannten Indikatoren für eine Beteiligung an einem Betrug überein?
- Wie würden Sie einen Dialog eröffnen, der respektvoll und traumasensibel ist und keine Abwehrreaktionen auslöst?
- Welche Unterstützungsangebote oder Partnerschaften könnten Sie aktivieren (z. B. Rechtshilfe, Betrugs-Hotlines)?
- Wie kann man Walters Würde und Autonomie wahren und gleichzeitig schützende Maßnahmen fördern?

2.10.3 Fallstudie 3:

Sie erhalten einen Anruf von Lara, der Tochter von Maria, einer Ihrer langjährigen Teilnehmerinnen. Lara ist aufgebracht und besorgt: „Meine Mutter hat gerade 5.000 € an einen Mann überwiesen, den sie noch nie getroffen hat! Er sagt, er sei beim Militär und im Ausland gestrandet. Sie glaubt, die beiden seien verliebt – das ist doch Wahnsinn!“ Lara ist wütend und besteht darauf, dass ihre Mutter sich dumm verhält. Sie möchte, dass Sie Maria zur Rede stellen und sie überzeugen, damit aufzuhören.

Reflexionsfragen:

- Wie würden Sie Maria ansprechen, um ihr Vertrauen zu bewahren und gleichzeitig Bedenken behutsam anzusprechen?
- Welche Strategien aus dem Bereich der traumasensiblen Betreuung könnten Sie anwenden, um Schamgefühle abzubauen und einen sicheren Raum für Offenbarungen zu schaffen?
- Wie würden Sie Lara auf eine unterstützende, nicht-zwanghafte Weise einbeziehen, um ihr die emotionalen Dimensionen solcher Betrügereien zu verdeutlichen?
- Welche Rolle können Sie dabei spielen, beiden Parteien zu helfen, eine gemeinsame Basis für die Erholung und den künftigen Schutz zu finden?

Digitale Verteidigung: Grundlagen der Cybersicherheit für Einsteiger

Co-funded by
the European Union

Jim Boelhouwer

Ich bin ein erfahrener Projektmanager und IT-Experte mit Leidenschaft für kontinuierliches Lernen und herausragende Ergebnisse. Dank meiner fundierten Erfahrung im Management komplexer Projekte und meines tiefen Verständnisses von IT-Systemen bringt Jim in jedes Projekt, das er übernimmt, umfassende Expertise ein.

Ich verfüge über eine beeindruckende Erfolgsbilanz in der Leitung und Durchführung anspruchsvoller IT-Projekte. Meine umfassende Erfahrung erstreckt sich über verschiedene Bereiche, darunter Softwareentwicklung, Infrastrukturimplementierung und Systemintegration. Meine Fähigkeit, interdisziplinäre Teams effektiv zu führen und Projektziele mit den Unternehmenszielen in Einklang zu bringen, hat stets zu termingerechten und budgetkonformen Projektabschlüssen geführt.

3 Grundlagen der Cybersicherheit für Anfänger

3.1 Wichtige Komponenten des Sicherheitsbewusstseins

Im vorangegangenen Kapitel wird erläutert, welche Taktiken und Methoden Kriminelle anwenden, um an schutzbedürftige ältere Menschen heranzukommen und sie finanziell auszurauben.

Eine Möglichkeit, diese Taktiken und Methoden auszunutzen, besteht in der Nutzung digitaler Kommunikation. Wir sind durch die Digitalisierung zunehmend miteinander vernetzt. Das bedeutet, dass besonders gefährdete ältere Menschen sich der damit verbundenen Risiken bewusst sein müssen. Der Empfang von E-Mails oder der Beginn von Chat-Konversationen kann der Auftakt zu finanziellem Betrug sein.

Sicherheitsbewusstsein bezeichnet das Verständnis und die Erkennung potenzieller Cybersicherheitsbedrohungen sowie bewährter Verfahren zum Schutz sensibler Informationen und Systeme. Es umfasst die Aufklärung von Menschen über verschiedene Aspekte der Cybersicherheit, um das Risiko von Sicherheitsverletzungen und Datenverlusten zu verringern. Die wichtigsten Komponenten des Sicherheitsbewusstseins sind:

a) Phishing-Angriffe und wie man sie erkennt
b) Passwortsicherheit und starke Authentifizierung
c) Sichere Verwendung von Wechseldatenträgern
d) Social-Engineering-Taktiken
e) Richtige Nutzung von sozialen Medien und E-Mails
f) Best Practices für Cloud-Sicherheit

3.2 Phishing-Angriffe und wie man sie erkennt

Phishing-Angriffe sind betrügerische Versuche, sensible Informationen wie Benutzernamen, Passwörter, Kreditkartendaten oder andere persönliche Daten zu erlangen, indem sich Angreifer als vertrauenswürdige Institution ausgeben. Typischerweise nutzen sie irreführende E-Mails, SMS oder Webseiten, die legitim erscheinen, um Empfänger zur Preisgabe ihrer Daten oder zum Anklicken schädlicher Links zu verleiten, die zur Installation von Malware führen. Hier finden Sie eine Übersicht über gängige Arten von Phishing-Angriffen und wie Sie diese erkennen können.

A. Phishing-Angriffe

Arten von Phishing-Angriffen:

- **E-Mail-Phishing:** Dies ist eine der am weitesten verbreiteten Formen des Phishings. Angreifer nutzen E-Mails, um sich als vertrauenswürdige Organisationen oder Einzelpersonen auszugeben und die Empfänger dazu zu verleiten, sensible Daten preiszugeben oder auf schädliche Links zu klicken.

- **Spear-Phishing:** Eine gezieltere Form des Phishings, bei der E-Mails auf bestimmte Personen oder Organisationen zugeschnitten werden.

- **Smishing (SMS-Phishing):** Angreifer verwenden Textnachrichten, die schädliche Links oder Telefonnummern enthalten, um persönliche Informationen zu sammeln oder Geräte mit Schadsoftware zu infizieren.

- **Vishing (Sprach-Phishing):** Hierbei handelt es sich um Telefonanrufe, bei denen sich die Anrufer als vertrauenswürdige Personen ausgeben. Mithilfe KI-gestützter Stimmreplikation können diese Anrufe täuschend echt klingen.

- **Clone-Phishing:** Angreifer erstellen Kopien von legitimen E-Mails und ersetzen die ursprünglichen Links durch schädliche Links.

- **Pop-Up-Phishing:** Bösartige Pop-ups auf Webseiten, die das Herunterladen von Schadsoftware auslösen oder Benutzer auf gefälschte Webseiten umleiten können.

- **Evil Twin Phishing:** Angreifer erstellen gefälschte WLAN-Hotspots, um Daten von Benutzern abzufangen, die sich damit verbinden.

B. Wie man Phishing-Angriffe erkennt

Um sie zu erkennen, achten Sie auf ungewöhnliche Absenderinformationen, dringliche oder bedrohliche Formulierungen, Anfragen nach persönlichen Daten, verdächtige Links und Anhänge sowie allgemeine Begrüßungen. Seien Sie besonders vorsichtig bei E-Mails, die zu gut klingen, um wahr zu sein, wie beispielsweise Angebote für kostenlose Produkte oder Dienstleistungen.

Merkmale verdächtiger E-Mails:

- Anfragen nach sensiblen Informationen (z. B. Passwörter, Kreditkartendaten)
- Dringende oder alarmierende Meldungen, die ein Gefühl der Panik auslösen
- Unbekannte oder leicht veränderte Absender-E-Mail-Adressen

- Rechtschreib- und Grammatikfehler
- Allgemeine Begrüßungen statt personalisierter

Warnsignale für Links und Anhänge:

- Verkürzte oder maskierte URLs, die das eigentliche Ziel verbergen
- Linktext und tatsächliche URL stimmen nicht überein (zum Überprüfen mit der Maus bewegen)
- Unaufgeforderte Anhänge, insbesondere von unbekannten Absendern

Inhaltswarnzeichen:

- Angebote, die zu gut erscheinen, um wahr zu sein (z. B. kostenlose Geschenkgutscheine)
- Unerwartete Benachrichtigungen oder Probleme im Zusammenhang mit Ihrem Konto
- Anfragen zur Überprüfung oder Aktualisierung von Kontoinformationen per E-Mail

Technische Vorsichtsmaßnahmen:

- Prüfen Sie, ob Website-URLs HTTPS enthalten, insbesondere bei sensiblen Transaktionen.
- Seien Sie vorsichtig mit doppelten WLAN-Hotspots an öffentlichen Orten.
- Verwenden Sie Pop-up-Blocker und seien Sie vorsichtig bei Browserbenachrichtigungsanfragen.

Durch Wachsamkeit und das Befolgen dieser Richtlinien können Sie das Risiko, Opfer von Phishing-Angriffen zu werden, deutlich verringern. Denken Sie daran: Seriöse Organisationen werden Sie niemals per E-Mail oder Nachricht nach sensiblen Daten fragen.

3.3 Passwortsicherheit und starke Authentifizierung

Passwortsicherheit und starke Authentifizierung sind in der heutigen digitalen Welt entscheidende Bestandteile der Cybersicherheit. Um Online-Konten und sensible Daten zu schützen, ist die Implementierung robuster Sicherheitsmaßnahmen unerlässlich.

3.3.1 Sichere Passwörter

Die Erstellung sicherer Passwörter ist die erste Verteidigungslinie gegen unbefugten Zugriff. Ein sicheres Passwort sollte:

- Mindestens 10 Zeichen lang sein
- Verwenden Sie eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Symbolen.

- Vermeiden Sie gebräuchliche Wörter oder leicht zu erratende Wortfolgen.

Um aus einem Satz ein sicheres Passwort zu erstellen, können Sie verschiedene Techniken anwenden. Eine gängige Methode besteht darin, den Anfangsbuchstaben jedes Wortes des Satzes zu verwenden, gegebenenfalls Zahlen oder Symbole hinzuzufügen und sicherzustellen, dass das Passwort ausreichend lang ist.

Hier ist eine Übersicht der Methoden:

1. Abkürzungen:
- Nimm den Anfangsbuchstaben jedes Wortes in deinem gewählten Satz.
- Zum Beispiel könnte der Satz „Meine Lieblingsfarbe ist blau“ zu „Mfcib“ werden.
- Erwägen Sie, Zahlen oder Symbole hinzuzufügen, um es aussagekräftiger zu machen, wie zum Beispiel „Mfcib12!“.

2. Substitution:
- Ersetzen Sie Buchstaben durch ähnlich aussehende Zahlen oder Symbole (z. B. „a“ durch „@“, „e“ durch „3“).
- Zum Beispiel könnte der Satz „Ich liebe Katzen“ zu „1 l0v3 c@ts“ werden.

3. Rechtschreibfehler und Groß-/Kleinschreibung:
- Schreiben Sie Wörter in Ihrem Satz absichtlich falsch oder schreiben Sie einige Buchstaben groß, um eine einzigartige Kombination zu erzeugen.
- Zum Beispiel könnte „The quick brown fox“ zu „Th3 q!ck br0wn f0x“ oder „The quick br0wn Fox“ werden.

- 4. Techniken kombinieren:
- Sie können Akronyme, Ersetzungen, Rechtschreibfehler und Großschreibung kombinieren, um ein noch stärkeres Passwort zu erstellen.
- Zum Beispiel könnte die Formulierung "This is a test" zu "T!s!s@t3s7t" werden.

3.3.2 Bewährte Verfahren für die Passwortverwaltung

Zu den bewährten Methoden für eine sichere Passwortrichtlinie gehören die Festlegung einer Mindestlänge für Passwörter, die Anforderung einer Kombination aus Großbuchstaben, Kleinbuchstaben, Zahlen und Symbolen sowie die Empfehlung zur Verwendung von Passphrasen oder Passwortmanagern. Zur Verbesserung der Passwortsicherheit:

- Verwenden Sie für jedes Konto ein individuelles Passwort.
- Ändern Sie Ihre Passwörter regelmäßig, idealerweise alle 3 Monate.
- Erwägen Sie die Verwendung eines Passwort-Managers zum sicheren Speichern und Generieren komplexer Passwörter.
- Vermeiden Sie die Weitergabe von Passwörtern oder die Verwendung leicht zu erratender Informationen.

3.3.3 Multi-Faktor-Authentifizierung (MFA)

Starke Authentifizierung geht über Passwörter hinaus und implementiert Multi-Faktor-Authentifizierung (MFA). MFA erfordert mindestens zwei Identitätskomponenten zur Überprüfung der Benutzeridentität. Diese Komponenten umfassen typischerweise:

1. Etwas, das der Benutzer weiß (z. B. Passwort oder PIN).
2. Etwas, das der Benutzer besitzt (z. B. ein Smartphone oder ein Hardware-Token).
3. Etwas, das den Benutzer ausmacht (z. B. biometrische Daten wie Fingerabdrücke oder Gesichtserkennung)

Die Aktivierung der Multi-Faktor-Authentifizierung (MFA) auf allen Konten, wo immer möglich, erhöht die Sicherheit erheblich, da eine zusätzliche Schutzebene hinzugefügt wird.

3.3.4 Starke Authentifizierungstechniken

Starke Authentifizierung zielt darauf ab, die Identität von Nutzern zuverlässig zu überprüfen und unberechtigten Zugriff zu verhindern. Zu den wichtigsten Aspekten starker Authentifizierung gehören:

- Sich nicht ausschließlich auf gemeinsame Geheimnisse oder symmetrische Schlüssel verlassen
- Abwehr von Phishing-Angriffen und Identitätsdiebstahl
- Für ein Höchstmaß an Sicherheit werden hardwarebasierte kryptografische Token wie FIDO-Schlüssel oder Smartcards verwendet.

3.3.5 Vorteile einer starken Authentifizierung

Die Implementierung starker Authentifizierungsverfahren bietet mehrere Vorteile:

- Verbesserter Schutz vor Zugangsdatendiebstahl und unberechtigtem Zugriff

- Reduziertes Risiko erfolgreicher Phishing-Angriffe
- Verbesserte Einhaltung regulatorischer Anforderungen
- Erhöhtes Vertrauen in die Identität der Benutzer und die allgemeine Systemsicherheit

Durch die Kombination von starken Passwörtern mit Multi-Faktor-Authentifizierung und der Einhaltung bewährter Verfahren können Sie Ihre Cybersicherheitslage deutlich verbessern und sensible Informationen vor potenziellen Bedrohungen schützen.

3.4 Sichere Verwendung von Wechseldatenträgern

Die Verwendung von Wechseldatenträgern wie USB-Sticks, externen Festplatten, SD-Karten usw. hat aufgrund ihrer kompakten Größe und hohen Speicherkapazität stark zugenommen. Doch genau diese Eigenschaften, die sie so benutzerfreundlich machen, machen sie auch zu attraktiven Zielen für Cyberkriminelle, die sensible Daten stehlen wollen.

Einer Studie von IBM Security zufolge waren menschliche Fehler für über 90 % der Sicherheitsvorfälle im Zusammenhang mit Wechseldatenträgern verantwortlich. Häufige Fehler wie das Verlegen oder Verlieren dieser Geräte können zu unbefugtem Zugriff oder Diebstahl vertraulicher Daten führen.

Darüber hinaus werden bösartige Angriffe wie Malware-Infektionen über infizierte USB-Sticks immer häufiger.

Laut Astra Security und DeepStrike werden täglich etwa 560.000 neue Schadprogramme entdeckt. Diese Zahl stellt ein beträchtliches Volumen dar und erhöht die bereits bestehende Anzahl von Schadprogrammen auf über eine Milliarde.

Um die sichere Verwendung von Wechseldatenträgern zu gewährleisten, befolgen Sie bitte diese bewährten Vorgehensweisen:

1. Verwenden Sie nur vertrauenswürdige Geräte:
- Schließen Sie niemals gefundene oder unbekannte Wechseldatenträger an Ihren Computer an.
2. Sicherheitsmaßnahmen implementieren:
- Installieren und pflegen Sie stets aktuelle Antivirensoftware, die angeschlossene Wechseldatenträger aktiv scannt.

- Deaktivieren Sie die Autostart- und Autoplay-Funktionen auf Ihrem Computer, um die automatische Ausführung von Schadcode zu verhindern.
- Verschlüsseln Sie alle Wechseldatenträger, um die Daten im Falle von Verlust oder Diebstahl zu schützen.
- Weisen Sie Wechseldatenträger mit starken Passwörtern ab.

3. Daten ordnungsgemäß verarbeiten:
- Trennen Sie private und geschäftliche Daten.
- Sensible Daten können nach Gebrauch sicher von Wechseldatenträgern gelöscht werden.
- Die Verwendung von Wechseldatenträgern ist nur dann zulässig, wenn dies notwendig und genehmigt ist.

4. Physische Sicherheit gewährleisten:
- Lassen Sie Wechseldatenträger niemals unbeaufsichtigt und bewahren Sie sie sicher auf, wenn Sie sie nicht benutzen.
- Deaktivieren Sie unnötige drahtlose Dienste wie Bluetooth und WLAN auf den Geräten.

5. Regelmäßige Wartung:
- Führen Sie regelmäßige Scans von Wechseldatenträgern auf Schadsoftware durch.
- Führen Sie regelmäßige Prüfungen durch und überwachen Sie die Nutzung von Wechseldatenträgern, um verdächtige Aktivitäten aufzudecken.

Durch die Einhaltung dieser Richtlinien können Sie die mit der Verwendung von Wechseldatenträgern verbundenen Risiken deutlich reduzieren und gleichzeitig von deren Komfort und Portabilität profitieren.

3.5 Social-Engineering-Taktiken

Social Engineering bezeichnet die psychologische Manipulation von Menschen, um Zugang zu vertraulichen Informationen zu erlangen oder sie zu Handlungen zu bewegen, die möglicherweise nicht in ihrem besten Interesse liegen. Neben den bereits erwähnten Phishing-Taktiken gibt es auch die folgenden:

Ködern: etwas Verlockendes anbieten (wie kostenlose Software), das beim Zugriff Schadsoftware enthält oder die Sicherheit gefährdet.
Quid pro quo: das Versprechen eines Vorteils im Austausch für Informationen oder eine Handlung, wie zum Beispiel das Anbieten von kostenlosem IT-Support, der Schadsoftware installiert.
Scareware: Einsatz von Angsttaktiken, um Opfer zum Handeln zu manipulieren, beispielsweise durch gefälschte Virenwarnungen.
Watering-Hole-Angriffe: Kompromittierung von Webseiten, die vom Ziel häufig besucht werden, um Schadsoftware einzuschleusen.

In den nächsten beiden Absätzen werden wir genauer auf zwei bekannte Arten von Social Engineering eingehen: den Romance Scam und den Pig Metchering Scam.

3.5.1 Liebesbetrug

Ein Liebesbetrug ist eine Masche, bei der romantische Absichten vorgetäuscht werden, um das Vertrauen des Opfers zu gewinnen und dieses dann auszunutzen, um das Opfer unter falschen Versprechungen zur Geldüberweisung zu bewegen oder Betrug zu begehen. Betrügerische Handlungen können den Zugriff auf Geld, Bankkonten, Kreditkarten, Pässe, E-Mail-Konten oder Personalausweisnummern des Opfers umfassen oder das Opfer zwingen, in seinem Namen Finanzbetrug zu begehen. Diese Betrügereien werden oft von organisierten kriminellen Banden verübt, die zusammenarbeiten, um mehrere Opfer gleichzeitig zu erbeuten. Schweineschlachtbetrug (auch bekannt als Schweineschlachtbetrug) ist eine zunehmend verbreitete Form des Liebesbetrugs, die häufig mit Betrugsfällen im Zusammenhang mit Hochzinsanlagen (HYIPs) einhergeht. Wir werden diese Betrugsart in einem separaten Abschnitt behandeln.

Gestohlene Bilder

Liebesbetrüger erstellen Profile mit gestohlenen Fotos attraktiver Personen, um andere zur Kontaktaufnahme zu bewegen. Diese Masche wird oft als Catfishing bezeichnet. Häufig werden Fotos unbekannter Schauspielerinnen oder Models verwendet, um das Opfer in dem Glauben zu wiegen, mit dieser Person zu kommunizieren. Auch US-Militärangehörige werden imitiert, da der vorgebliche Militärdienst erklärt, warum der Betrüger nicht für ein persönliches Treffen zur Verfügung steht.

Da die Betrüger den Fotos, die sie ihren Opfern schicken, oft überhaupt nicht ähneln, treffen sie sich selten persönlich oder gar per Videoanruf mit ihren Opfern. Sie täuschen ihre potenziellen Opfer mit plausibel klingenden Ausreden, warum sie ihr Gesicht nicht zeigen wollen, beispielsweise indem sie behaupten, vorübergehend verreist zu sein oder eine defekte Webcam zu haben.

Das Opfer austricksen

Betrüger sind sehr geschickt darin, ihre Opfer zu manipulieren – sie verschicken Liebesgedichte, spielen sexuelle Anspielungen in E-Mails und bauen eine vermeintliche Liebesbeziehung mit dem Versprechen auf, eines Tages zu heiraten. Betrüger stellen ihren Opfern viele Fragen, geben aber selbst kaum etwas von sich preis.

Sie überschütten die Opfer oft mit Komplimenten.

Die Kommunikation zwischen Betrüger und Opfer erstreckt sich über einen Zeitraum von manchmal Monaten oder sogar einem ganzen Jahr, bis der Betrüger das Gefühl hat, genügend Vertrauen zum Opfer aufgebaut zu haben, um Geld zu fordern. Betrüger nutzen das falsche Vertrauensverhältnis ihrer Opfer aus, um sie zur Geldüberweisung zu verleiten.

Diese Bitten können sich auf Benzingeld, Bus- oder Flugtickets für einen Besuch beim Opfer oder auf medizinische oder Ausbildungskosten beziehen. Meistens wird versprochen, dass der Betrüger das Opfer eines Tages zu Hause besuchen wird.

Die Opfer werden möglicherweise eingeladen, in das Land des Betrügers zu reisen; in einigen Fällen reisen die Opfer mit dem erbetenen Geld für Familienangehörige oder mit Bestechungsgeldern von korrupten Beamten an, nur um dann geschlagen, ausgeraubt oder ermordet zu werden.

Der Betrug endet meist, wenn das Opfer merkt, dass es betrogen wurde, oder keine Gelder mehr überweist. Oftmals fällt es den Betroffenen jedoch schwer, die Realität zu akzeptieren, und die Scham, auf einen solchen Betrug hereingefallen zu sein, kann sie davon abhalten, Anzeige bei der Polizei zu erstatten. Viele Opfer können selbst bei erdrückenden Beweisen nicht glauben, dass die Person, die in den Textnachrichten so liebevoll wirkt, in Wirklichkeit ein krimineller Betrüger ist. Sie reagieren unter Umständen wütend oder gar gewalttätig auf jeden, der Einwände erhebt. Banken können das Geld des Opfers sperren, insbesondere bei Verdacht auf finanziellen Missbrauch älterer Menschen.

Kriminelle Gruppen

Kriminelle Netzwerke betrügen einsame Menschen weltweit mit falschen Liebesversprechen. Betrüger erstellen Profile auf Dating-Websites, in sozialen Medien (die nicht der Partnersuche dienen), auf Kleinanzeigenportalen und sogar in Online-Foren, um neue Opfer zu finden. Sie versuchen in der Regel, eine privatere Kommunikationsmöglichkeit wie E-Mail-Adresse oder Telefonnummer zu erlangen, um Vertrauen aufzubauen.

Da die Betrüger in Gruppen arbeiten, kann jederzeit jemand aus der Gruppe online sein und dem Opfer E-Mails oder SMS senden. Der Wechsel zwischen verschiedenen Betrügern, die sich alle als dieselbe Person ausgeben, ist in textbasierten Systemen schwer zu erkennen.

Nachrichten, wohingegen es offensichtlich wäre, wenn bei einem persönlichen Treffen oder einem Video- oder Telefongespräch eine andere Person erscheinen würde.

3.5.2 Betrug bei der Schweineschlachtung:

Die Masche des sogenannten „Schweineschlachtens“ entstand 2016 oder früher als regionaler Betrug in China. Die Opfer wurden zunächst auf Dating-Plattformen für gleichgeschlechtliche Paare gefunden, bevor sich die Masche auch auf heterosexuelle Plattformen ausweitete. Der Begriff „Schweineschlachten“ leitet sich von der Analogie ab, die das anfängliche Vertrauensgewinnen mit dem Masten von Schweinen vor der Schlachtung vergleicht.

Diese Vorgehensweise verbreitete sich später auf dem Höhepunkt der COVID-19-Pandemie in ganz Südostasien. In Kambodscha, einst eine blühende Glücksspielstadt, wandelten viele lokale Glücksspielbanden Casinos in Betrugszentren um und verübten Schweineschlachtungen. Dies war vermutlich eine Folge der pandemiebedingten Besucherrückgänge in den Casinos und des harten Vorgehens der kambodschanischen Regierung gegen das kommerzielle Glücksspiel. Viele Operationen werden auch von Gebieten in Myanmar aus gesteuert, die aufgrund des Bürgerkriegs außerhalb der Kontrolle der Zentralregierung liegen. Ein wichtiger Knotenpunkt ist die Stadt Myawaddy nahe der thailändischen Grenze. Laut UNHR wurden Hunderttausende Menschen verschleppt und sind in Betrugszentren in Kambodscha und Myanmar gefangen. Weitere Operationen werden von Laos, den Philippinen und Thailand aus geleitet. Viele der Gruppen, die Schweineschlachtungen verüben, sind chinesische Verbrechersyndikate mit Sitz in Südostasien. Sie verschleppen Angehörige der ethnischen Minderheiten, darunter auch andere, in Betrugsfabriken und zwingen sie zur Begehung der Betrügereien.

Betrugsmaschen mit vorgetäuschter Schweineschlachtung gewannen durch die Ausnutzung von Online-Dating-Apps und sozialen Medien international an Bedeutung. Die Betrüger erstellten aufwendige falsche Identitäten, um romantische oder emotionale Beziehungen zu ihren Opfern aufzubauen. Dies unterschied sich von herkömmlichen Finanzbetrügereien durch den Einsatz psychologischer Manipulation. In dieser frühen Phase richteten sich diese Betrügereien vorwiegend gegen die lokale Bevölkerung, breiteten sich aber mit zunehmender digitaler Vernetzung rasch aus.

Die Betrugsmaschen entwickelten sich durch den Einsatz ausgefeilter Techniken deutlich weiter, darunter die Erstellung gefälschter Online-Investitionsplattformen und der Einsatz von Social Engineering.

Durch die zunehmende Nutzung von Plattformen wie WhatsApp und Telegram können zufällige Personen allein durch den Beginn einer zufälligen Konversation ins Visier genommen werden. Ein Schlüsselaspekt dieser Entwicklung war die Verwendung von Kryptowährungen für Transaktionen, die aufgrund ihrer Schwierigkeit, diese nachzuverfolgen und zurückzuerlangen, für Betrüger attraktiv waren. Die Globalisierung dieser Betrugsmaschen lässt sich auf die zunehmende Allgegenwärtigkeit digitaler Interaktionen und die steigende Popularität von Kryptowährungen zurückführen, die Betrügern weltweit neue Möglichkeiten eröffneten.

Kriminelle Gruppen

Bei Betrugsmaschen, die auf der Ausbeutung von Opfern durch die Schlachtung von Schweinen basieren, handelt es sich um eine Reihe sorgfältig geplanter Schritte, um die Opfer zu täuschen und auszubeuten. Der Schwerpunkt liegt dabei typischerweise auf Betrugsfällen im Zusammenhang mit Kryptowährungsinvestitionen.

Vertrauensbildung: Betrugsmaschen beginnen oft mit unverbindlichen Gesprächen, die vom Betrüger initiiert werden. Dieser gibt vor, die Kontaktdaten des Opfers zufällig oder über einen gemeinsamen Bekannten erhalten zu haben. Diese ersten Kontakte dienen dem Vertrauensaufbau und können die Verwendung ansprechender Profilbilder beinhalten, um Opfer anzulocken.
Einführung in die Investition: Sobald Vertrauen aufgebaut ist, stellt der Betrüger dem Opfer ein betrügerisches Anlageprogramm vor und verspricht hohe Renditen innerhalb kurzer Zeit. Die Betrüger nutzen überzeugende Taktiken und gefälschte Anlageportfolios, um die Opfer von der Seriosität des Programms zu überzeugen.
Geldeintreibung: Nachdem die Betrüger das Opfer zur Investition überredet haben, treiben sie die Gelder ein, oft über digitale Zahlungsplattformen oder Kryptowährungen, um die Nachverfolgung der Transaktionen zu erschweren.
Verschwinden des Betrügers: Sobald ein beträchtlicher Betrag eingesammelt wurde oder die Opfer versuchen, Gelder abzuheben, sind die Betrüger nicht mehr erreichbar, löschen ihre Online-Präsenz oder erstellen neue Identitäten, sodass die Opfer keine Möglichkeit haben, ihr Geld zurückzuerhalten.

Darüber hinaus entwickeln die Betrüger gefälschte Broker-Websites und mobile Anwendungen, um ihrem Betrug Legitimität zu verleihen, was es den Opfern erschwert, diese von echten Plattformen zu unterscheiden.

3.6 Richtige Nutzung von sozialen Medien und E-Mails

Soziale Medien sind natürlich alles andere als schlecht. Ihre Nutzung bringt oft handfeste Vorteile mit sich. Viele von uns nutzen sie, um ein Zugehörigkeitsgefühl zu entwickeln, sich auszudrücken, ihrer Neugier nachzugehen oder Kontakte zu knüpfen. Apps wie Facebook, Instagram, WhatsApp, Telegram und Twitter ermöglichen es uns, mit weit verstreuten Familienmitgliedern und Freunden in Kontakt zu bleiben, uns mit Gleichgesinnten über unsere Interessen auszutauschen und uns in Online-Communities für Herzensangelegenheiten einzusetzen.

Wir alle müssen unsere eigenen Entscheidungen bezüglich der Nutzung sozialer Medien treffen, basierend auf unseren persönlichen Erfahrungen. Die Auseinandersetzung mit Forschungsergebnissen hilft uns dabei, Vor- und Nachteile abzuwägen und fundierte Entscheidungen zu treffen. Auch wenn die Entwicklung sozialer Medien nicht mehr aufzuhalten ist, werden wir, wie Shakya und Christakis es ausdrücken, feststellen, dass „Online-Interaktionen kein Ersatz für reale Begegnungen sind“ und dass persönliche, gesunde Beziehungen für die Gesellschaft und unser individuelles Wohlbefinden unerlässlich sind. Wir täten gut daran, uns diese Wahrheit vor Augen zu halten und nicht alles auf die Karte „Soziale Medien“ zu setzen.

✦ Allgemeine Richtlinien:

Schützen Sie Ihre Privatsphäre, indem Sie die Einstellungen regelmäßig überprüfen.
Überlegen Sie gut, bevor Sie etwas veröffentlichen – Inhalte können unbegrenzt online bleiben.
Seien Sie in allen Interaktionen respektvoll und rücksichtsvoll.
Überprüfen Sie Informationen, bevor Sie sie weitergeben, um die Verbreitung von Fehlinformationen zu vermeiden.
Denken Sie daran, dass Ihr digitaler Fußabdruck Ihre persönliche und berufliche Reputation beeinflusst.

✦ Sicherheitsbewusstsein:

Seien Sie vorsichtig mit Links und Anhängen.
Überprüfen Sie die Absenderadressen, bevor Sie auf verdächtige E-Mails antworten.
Geben Sie niemals sensible Informationen weiter, es sei denn, Sie sind sich der Sicherheit absolut sicher.
Verwenden Sie Verschlüsselung für sensible Kommunikationen

- Verwenden Sie starke, einzigartige Passwörter und aktivieren Sie die Zwei-Faktor-Authentifizierung.

3.7 Die Einführung von Künstlicher Intelligenz (KI)

Künstliche Intelligenz (KI) bezeichnet die Entwicklung von Computersystemen, die Aufgaben ausführen können, die typischerweise menschliche Intelligenz erfordern. Zu diesen Aufgaben gehören Lernen,

Problemlösung, Entscheidungsfindung und das Verstehen natürlicher Sprache. Künstliche Intelligenz umfasst ein breites Spektrum an Techniken und Ansätzen, von einfachen regelbasierten Systemen bis hin zu komplexen Modellen des maschinellen Lernens. Hier ein detaillierterer Blick auf die Kernkonzepte:

- **Nachahmung menschlicher Intelligenz:** Künstliche Intelligenz zielt darauf ab, Maschinen zu entwickeln, die Aufgaben ausführen können, die Menschen normalerweise mit ihrer Intelligenz erledigen.
- **Lernen und Problemlösen:** KI-Systeme können aus Daten lernen, Muster erkennen und auf der Grundlage dieser Erkenntnisse Entscheidungen treffen.
- **Vielfältige Anwendungsgebiete:** KI wird in verschiedenen Bereichen eingesetzt, darunter Gesundheitswesen, Finanzen, Bildung und Transportwesen.
- **Maschinelles Lernen:** Ein Kernbestandteil moderner KI, bei dem Algorithmen aus Daten lernen, ohne explizit programmiert zu werden.
- **Verarbeitung natürlicher Sprache:** Ermöglicht Maschinen, die menschliche Sprache zu verstehen und mit ihr zu interagieren.
- **Computer Vision:** Ermöglicht Maschinen, Bilder und Videos zu "sehen" und zu interpretieren.

Beispiele für den Einsatz von KI:

- **Sprachassistenten:** Wie Siri oder Alexa, die Sprachbefehle verstehen und darauf reagieren.
- **Empfehlungssysteme:** Werden von Online-Plattformen verwendet, um Produkte oder Inhalte basierend auf den Präferenzen der Nutzer vorzuschlagen.
- **Selbstfahrende Autos:** Einsatz von KI für Navigation und Entscheidungsfindung in autonomen Fahrzeugen.
- **Betrugserkennung:** Einsatz von KI zur Identifizierung verdächtiger Transaktionen in Finanzsystemen.

Künstliche Intelligenz (KI) ist ein sich rasant entwickelndes Feld mit dem Potenzial, verschiedene Aspekte unseres Lebens grundlegend zu verändern. Dieselben Prinzipien gelten auch für Liebesbetrug, bei dem KI-generierte Profile, die sich als Freunde, Familie oder Kollegen des Betrügers ausgeben, mit dem Opfer interagieren, um die Beziehung zu bestätigen und dessen Zweifel zu zerstreuen. Diese Interaktionen simulieren soziale Beweise und erschweren es den Opfern, Ungereimtheiten zu hinterfragen.

3.7.1 Erstkontakt

Die Glaubwürdigkeit eines Betrügerprofils ist in der Frühphase von Liebesbetrug entscheidend, da sie mitentscheidend dafür ist, ob ein Opfer auf eine gefälschte Identität hereinfällt. Während Betrüger traditionell Bilder von echten Nutzern stahlen, konnten umgekehrte Bildersuchen und forensische Bildanalysen diese Täuschungen aufdecken. Durch die Integration von LLMs und Deepfake-Bildgenerierung können Betrüger nun jedoch problemlos synthetische Profile in Massenproduktion herstellen, die echten Nutzern täuschend ähnlich sehen. Diese Profile sind darauf ausgelegt, Erkennungsmechanismen in sozialen Medien, Dating-Plattformen und beruflichen Netzwerken zu umgehen und Opfer effektiv zu täuschen.

Das Ausmaß der KI-gestützten Profilerstellung ist enorm. So entfernte Meta beispielsweise im Jahr 2024 Berichten zufolge Milliarden gefälschter Konten (darunter alle Konten, die nach Ansicht des Unternehmens in böswilliger Absicht oder für nicht-menschliche Organisationen erstellt worden waren). Der sprunghafte Anstieg KI-generierter betrügerischer Profile zwang die Dating-Plattform Tinder im Jahr 2024, ihr Programm zur Identitätsprüfung auszuweiten und in den USA und Großbritannien verstärkte Maßnahmen einzuführen. Diese Maßnahmen verpflichten Nutzer zur Vorlage amtlicher Ausweisdokumente und selbstaufgenommener Videos. Angesichts der zunehmenden Komplexität generativer KI reichen diese Maßnahmen jedoch möglicherweise nicht aus, da die Technologie KYC-Prüfungen und andere Identitätsprüfungsverfahren vor Herausforderungen stellt.

KI-generierte Profile funktionieren nicht isoliert. Betrüger können synthetische Profile mit automatisierter Kontaktaufnahme kombinieren und so leistungsstarke Systeme erstellen, in denen Tausende realistischer Profile gleichzeitig LLM-generierte Nachrichten versenden. Wie bereits im vorherigen Abschnitt erläutert, nutzen Betrüger LLMs wahrscheinlich eher bei der ersten Kontaktaufnahme als in späteren Interaktionen. Dies liegt daran, dass:

- Die erste Nachricht erfordert nur eine minimale Personalisierung, wodurch sie sich leicht in großem Umfang generieren lässt.
- Das Versenden von Begrüßungsnachrichten ist eine sehr repetitive Arbeit, weshalb die Automatisierung für Betrüger, die ihre Effizienz steigern wollen, höchste Priorität hat.
- LLMs erzielen die besten Ergebnisse in strukturierten Szenarien mit geringem Kontext, wodurch sie sich besonders für diese Phase eignen.

Das bedeutet, dass KI bereits gut positioniert ist, um die Skalierbarkeit von Liebesbetrugsfällen in der Frühphase zu verbessern.Betrüger können die Technologie auf verschiedenen Plattformen einsetzen und sich dabei auf automatisch generierte Nachrichten von LLMs (Large Language Models) verlassen, um effizient Gespräche zu initiieren.

Sobald ein Opfer darauf reagiert, können Betrüger dann zu manuellen Interventionen oder verfeinerten KI-gestützten Interaktionen übergehen, um die Täuschung aufrechtzuerhalten.

Da KI-generierte Profile und Kommunikationsstrategien immer ausgefeilter werden, können traditionelle Erkennungsmethoden wie die Profilverifizierung und die textbasierte Anomalieerkennung möglicherweise nicht mehr mithalten, sodass adaptive Gegenmaßnahmen erforderlich werden.

3.7.2 Beziehungsaufbau

Sobald Betrüger den Erstkontakt hergestellt haben, gehen sie in die Beziehungsaufbauphase über. In dieser Phase versuchen sie, eine tiefere emotionale Bindung aufzubauen und Vertrauen zu ihren Opfern zu gewinnen. KI-gestützte Tools haben die Möglichkeiten von Betrügern, Täuschungen auszuweiten und zu personalisieren, zwar verbessert, aber ihre Automatisierungskapazitäten für diese Phase sind begrenzt. Anders als die Erstansprache, die von generischen Skripten und großflächiger Automatisierung profitiert, erfordert der Beziehungsaufbau Anpassungsfähigkeit, emotionale Intelligenz und individuell zugeschnittene Reaktionen auf die Interaktionen des Opfers.

Ein wesentlicher Unterschied zwischen KI-gesteuerter und von Menschen gesteuerter Täuschung liegt in der Anpassungsfähigkeit. Menschliche Betrüger können ihre Erzählungen dynamisch an die Reaktionen ihrer Opfer anpassen und so sicherstellen, dass die Gespräche emotional ansprechend bleiben und auf finanzielle Ausbeutung abzielen. KI-gestützte Nachrichtensysteme (LLMs) können zwar verfahrenstechnisch korrekte Betrugsnachrichten generieren, haben aber Schwierigkeiten, Kontinuität und eine tiefgreifende Personalisierung über längere Interaktionen hinweg aufrechtzuerhalten. Ohne menschliche Aufsicht bergen KI-generierte Nachrichten das Risiko von Toninkonsistenzen, Widersprüchen und sich wiederholenden Formulierungen, was die Glaubwürdigkeit mit der Zeit schwächen kann. Das Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC)[29] berichtet, dass KI zwar bereits bei Cyberkriminalität eingesetzt wird, die meisten Betrugsmaschen jedoch weiterhin auf menschliche Aufsicht angewiesen sind, um Glaubwürdigkeit zu wahren und komplexe zwischenmenschliche Dynamiken zu bewältigen.

Künstliche Intelligenz kann diese Phase jedoch auf verschiedene Weise verbessern:

Optimierung von Betrugsskripten: Betrüger können LLMs verwenden, um Betrugsskripte zu verfeinern, indem sie verschiedene Formulierungen und emotionale Appelle testen, um die Interaktion zu maximieren.

- **Mehrsprachiger Chat-Support:** Die Übersetzungsfunktion ermöglicht es Betrügern, mit ihren Opfern in mehreren Sprachen flüssiger zu kommunizieren.
- **Automatisiertes Beziehungsmanagement:** KI-Tools können Betrügern helfen, mehrere Opfer gleichzeitig zu betreuen, indem sie Antwortvorschläge und Interaktionsstrategien bereitstellen und gleichzeitig Inkonsistenzen in den Gesprächen minimieren.

Während LLM-generierte Texte skalierbare und personalisierte Interaktionen ermöglichen, bieten Deepfake-Medien eine zusätzliche Ebene der Authentizität, wodurch betrügerische Profile überzeugender und immer schwerer zu verifizieren sind. KI-gestützte Stimmklonierungstools erlauben Betrügern, Inhalte zu erstellen, die Sprachmuster, Akzente und emotionale Nuancen imitieren und so den Bedarf an direkter menschlicher Interaktion reduzieren. Ebenso können Betrüger KI-generierte Videos nutzen, um visuelle Identitätsnachweise zu fälschen, wodurch sie Verifizierungsanfragen umgehen und das Vertrauen potenzieller Opfer stärken können. Obwohl vollständig autonome Deepfake-Interaktionen technisch noch eine Herausforderung darstellen, nutzen Betrüger bereits vorab aufgezeichnete synthetische Videoinhalte, um ihre Täuschung länger aufrechtzuerhalten.

Aktuelle, aufsehenerregende Fälle verdeutlichen die zunehmende Bedeutung von Deepfake-Betrug. Ein britisches Ingenieurbüro berichtete im Januar 2024, dass Kriminelle mithilfe eines Deepfake-Videos erfolgreich Führungskräfte imitierten und so einen Unternehmensbetrug in Höhe von 25 Millionen US-Dollar ermöglichten. Im Oktober 2024 nutzten Liebesbetrüger Deepfake-generierte Bilder, um ihre Opfer in dem Glauben zu wiegen, sich in echten Beziehungen zu befinden, und erbeuteten so letztendlich 46 Millionen US-Dollar. Obwohl sich neuere Fälle auf die Rolle von Deepfakes bei Liebesbetrug konzentrieren, breiten sich die zugrundeliegenden Taktiken auf andere Bereiche aus, darunter auch Anlagebetrug.

Fortschritte in der KI-gestützten Bildrekonstruktion, die generierte Inhalte nahtlos in bestehende Bilder oder Videos integriert, haben den Realismus dieser betrügerischen Materialien weiter erhöht und die Erkennung sowohl für Menschen als auch für automatisierte Systeme zunehmend erschwert. Mit der Entwicklung neuer KI-Fähigkeiten wird sich ihre Rolle beim Aufbau betrügerischer Beziehungen voraussichtlich verändern und automatisierte Täuschung mit strategischer menschlicher Kontrolle verbinden, um die Effektivität von Betrugsmaschen zu maximieren.

3.7.3 Körperpflege

Mit zunehmender Vertiefung einer Beziehung verlagern Betrüger ihren Fokus von allgemeinem Vertrauensaufbau hin zu gezielter psychologischer Manipulation. Diese Phase, oft als Grooming bezeichnet, beinhaltet die Steigerung der emotionalen Abhängigkeit und die Isolation des Opfers von äußeren Einflüssen, um dessen Anfälligkeit für finanzielle oder persönliche Ausbeutung zu erhöhen. Künstliche Intelligenz (KI) optimiert und personalisiert diesen Prozess, indem sie das Online-Verhalten des Opfers analysiert, dessen emotionalen Zustand überwacht und Kommunikationsmuster – potenziell in Echtzeit – anpasst. Durch die Automatisierung dieser Manipulationstechniken ermöglicht KI Betrügern, Täuschungen in großem Umfang zu optimieren und ihre Taktiken dadurch raffinierter, effizienter und schwerer erkennbar zu machen.

KI-gestützte Systeme können Daten aus verschiedenen Quellen, darunter soziale Medien und öffentliche Register, schnell erfassen und analysieren, um ein umfassendes psychologisches Profil potenzieller Opfer zu erstellen. Früher erforderte diese Profilerstellung einen hohen manuellen Aufwand, doch KI kann diesen Prozess innerhalb von Sekunden automatisieren und verfeinern. Dadurch können Betrüger besonders gefährdete Ziele identifizieren und priorisieren. KI-gestütztes Profiling ist im Bereich Social Engineering, insbesondere bei Spear-Phishing-Angriffen, gut dokumentiert. Diese Angriffe werden so angepasst, dass sie die Ängste, Wünsche oder Unsicherheiten von Einzelpersonen ausnutzen.

Betrüger können diese KI-gestützte Profilerstellung zu einer Echtzeit-Verhaltensanalyse ausweiten und so die Reaktionen, Interaktionsmuster und emotionalen Signale ihrer Opfer verfolgen. Durch die Auswertung laufender Gespräche kann die KI Betrügern helfen, Tonfall, Zeitpunkt und Botschaften dynamisch anzupassen, um den Eindruck echter Verbundenheit zu erwecken. Dies ermöglicht eine schrittweise, aber hochgradig kalkulierte Vertiefung der emotionalen Abhängigkeit von der erfundenen Identität des Betrügers.

Die Fähigkeit von KI, immersive Online-Umgebungen zu schaffen, verstärkt den Anbahnungsprozess, indem sie die erfundene Identität des Betrügers untermauert und die Skepsis der Opfer gegenüber dem Vorgehen verringert. Studien zur KI-gestützten politischen und Marketing-Beeinflussung haben gezeigt, dass Modelle Einzelpersonen mit maßgeschneiderten Botschaften gezielt ansprechen und so deren Engagement steigern und ihre Überzeugungen formen können. Dieselben Prinzipien gelten für Liebesbetrug, bei dem KI-generierte Profile, die sich als Freunde, Familie oder Kollegen des Betrügers ausgeben, mit dem Opfer interagieren, um die Beziehung zu bestätigen und dessen Zweifel zu zerstreuen. Diese Interaktionen simulieren soziale Beweise und erschweren es den Opfern, Ungereimtheiten zu hinterfragen.

Darüber hinaus ist die Art der KI-gestützten Inhaltserstellung und der botgesteuerten Verstärkung oft so, dass – wie bei politischen Einflusskampagnen beobachtet – Online-Plattformen mit sich verstärkenden Narrativen überschwemmt werden können. Dadurch wird sichergestellt, dass Opfer bei der Suche nach dem Namen ihres Partners auf gefälschte Erfahrungsberichte, Fake-Profile oder KI-generierte Artikel stoßen, die die Glaubwürdigkeit des Betrugs erhöhen. So wie Persönlichkeiten des öffentlichen Lebens KI nutzen können, um den öffentlichen Diskurs zu lenken und politische Narrative zu verstärken, können Betrüger sie einsetzen, um ein künstliches digitales Netzwerk zu erstellen, das das Opfer isoliert.

3.7.4 Ausführung

Mit zunehmendem Vertrauen gehen Betrüger von emotionaler Manipulation zur finanziellen Ausbeutung über und nutzen die Bindung des Opfers aus, um Zahlungsforderungen zu rechtfertigen. In dieser Phase werden oft Krisen vorgetäuscht, wie medizinische Notfälle, logistische Probleme oder rechtliche Schwierigkeiten. All dies dient dazu, Dringlichkeit zu erzeugen und das Opfer unter Druck zu setzen, Geld zu überweisen. Geschenkkarten sind nach wie vor eine gängige Methode, um Geld zu erpressen und kommen in 24 % der gemeldeten Fälle von Liebesbetrug vor. Kryptowährungen und Banküberweisungen führen jedoch zu deutlich höheren Verlusten pro Opfer. Berichten zufolge sind die Verluste durch Liebesbetrug in den letzten Jahren stark angestiegen und kosten die britische Bevölkerung jährlich über 80 Millionen Pfund. In Australien überstiegen die gemeldeten Verluste im Jahr 2024 23 Millionen australische Dollar, wobei künstliche Intelligenz maßgeblich zu diesem Anstieg beiträgt.

Neben Timing und Umfang hilft KI Betrügern, raffinierte Täuschungen durchzuführen, finanzielle Legitimität vorzutäuschen und Geldwäsche zu optimieren, wodurch die Erpressung von Finanzmitteln subtiler und effektiver wird. Eine besorgniserregende Entwicklung betrifft die Fähigkeit von KI, finanzielle Glaubwürdigkeit zu erzeugen. Wie viele andere Kriminelle nutzen auch Liebesbetrüger Scheinfirmen, um ihre illegalen Gewinne zu verbergen. Betrüger setzen generative KI ein, um überzeugende Finanzberichte, juristische Dokumente und synthetische Identitäten zu fälschen und so die Kontrollen von Finanzinstituten zu umgehen. Wie bereits erwähnt, verwenden Kriminelle zunehmend KI-generierte synthetische Identitäten, um die KYC-Prüfung zu umgehen. Dies ermöglicht ihnen, betrügerische Bankkonten zu eröffnen und Geldwäsche in großem Umfang zu betreiben. Ihre KI-generierten Identitäten können legitime Finanznetzwerke auf eine Weise infiltrieren, die herkömmliche Betrugsüberwachungssysteme zunehmend nicht mehr erkennen können.

Auch beim Anstieg von Betrugsfällen im Zusammenhang mit der Schweineschlachtung spielt KI eine entscheidende Rolle – eine der häufigsten Betrugsarten.

Lukrative Formen der finanziellen Ausbeutung sind bei Liebesbetrug weit verbreitet. Betrüger manipulieren ihre Opfer über Wochen oder Monate, bevor sie sie auf gefälschte Kryptowährungs- oder Investmentplattformen locken. Dort werden die Opfer dazu verleitet, immer höhere Beträge einzuzahlen. Die Betrüger erhöhen die Glaubwürdigkeit und den Realismus dieser gefälschten Investmentseiten, indem sie nicht nur Code von echten Plattformen kopieren, sondern auch KI zur Inhaltserstellung nutzen. Sie setzen zudem KI-gestützte Chatbots als vermeintliche Anlageberater ein, um die Opfer durch die Plattform zu führen und selbst skeptische Nutzer durch erfundene Markttrends und personalisierte Empfehlungen zu beruhigen. Diese Chatbots locken die Opfer weiter in die Falle, indem sie schädliche Links in ihre Kommunikation einbetten, sie zu anderen Betrugsmaschen führen und so ihre finanziellen Verluste vergrößern.

Die Einnahmen aus Kryptowährungsbetrug erreichten in den USA im Jahr 2024 schätzungsweise 12,4 Milliarden US-Dollar, wobei Betrugsfälle im Zusammenhang mit der Schlachtung von Schweinen einen erheblichen Anteil dieser Verluste ausmachten. Gleichzeitig haben KI-gestützte Programmierwerkzeuge die erforderlichen technischen Kenntnisse für die Erstellung gefälschter Anlageplattformen reduziert, sodass Betrüger mit minimalem Aufwand massenhaft betrügerische Websites produzieren können.

Da KI die Täuschung immer weiter automatisiert und Betrugsoperationen optimiert, vermischen sich Schweineschlachtbetrügereien zunehmend mit Liebesbetrug. Die Möglichkeit, hochgradig personalisierte, KI-gesteuerte Anlagebetrügereien zu erstellen, macht diese Maschen noch heimtückischer und schädigt die Opfer sowohl finanziell als auch psychisch.

3.7.5 Ausstieg oder Eskalation

Wenn Liebesbetrugsfälle in ihre Endphase eintreten, verschwinden die Betrüger entweder abrupt, nachdem sie Zahlungen von ihren Opfern erhalten haben, oder sie verschärfen ihre Täuschungsmanöver, um noch mehr Geld zu erpressen. Künstliche Intelligenz ermöglicht immer komplexere Ausstiegsstrategien und verlängert die Ausbeutung der Opfer durch Techniken wie Deepfake-Erpressung und Identitätsdiebstahl.

Wie die US-amerikanische Federal Trade Commission (FTC) kürzlich berichtete, nimmt eine Betrugsmasche zu, bei der KI-gestützte Täter sich als Strafverfolgungsbehörden oder Mitarbeiter von Finanzermittlungsdiensten ausgeben. Bei dieser Betrugsart kontaktieren die Täter ihre Opfer mit falschen Versprechungen auf finanzielle Entschädigung und geben sich als Polizisten, Finanzaufsichtsbeamte oder Ermittler aus, um gegen Gebühr zu behaupten, verlorene Gelder wiedererlangen zu können.

3.8 Fallstudie zum Liebesbetrug: Sarah Thompson

Hintergrund

Sarah Thompson, eine 58-jährige Witwe aus Portland, Oregon, verlor 2022 ihren Mann nach 30 Jahren Ehe an Krebs. Nach einem Jahr der Trauer ermutigten ihre erwachsenen Kinder sie, Online-Dating auszuprobieren, um wieder soziale Kontakte zu knüpfen. Da Sarah wenig Erfahrung mit Online-Dating hatte, erstellte sie im März 2023 ein Profil auf einer beliebten Dating-Plattform.

Erstkontakt

Innerhalb von zwei Wochen nach ihrer Anmeldung auf der Plattform erhielt Sarah eine Nachricht von „William Pierce“, der sich als 62-jähriger amerikanischer Bauingenieur ausgab, der in Malaysia im Rahmen eines Projekts arbeitete. Sein Profil zeigte Fotos eines attraktiven, silberhaarigen Mannes mit einem freundlichen Lächeln. William gab an, verwitwet zu sein und eine Partnerin zu suchen.

Ihre Gespräche verlagerten sich schnell von der Dating-Plattform auf E-Mail und WhatsApp, was eigentlich ein Warnsignal hätte sein sollen. William war aufmerksam, romantisch und schien sehr an Sarahs Leben interessiert zu sein. Sie kommunizierten täglich per Nachricht und gelegentlich auch telefonisch, wobei William immer Ausreden parat hatte, warum Videoanrufe nicht möglich waren – schlechte Internetverbindung, voller Terminkalender oder Zeitunterschiede.

Beziehungsentwicklung

In den folgenden zwei Monaten baute William eine emotionale Bindung zu Sarah auf durch:

- Tägliche Guten-Morgen- und Gute-Nacht-Nachrichten
- Er erzählte persönliche Geschichten über seine verstorbene Frau und seine Kinder.
- Sie besprachen Zukunftspläne, um sich zu treffen und möglicherweise ein gemeinsames Leben aufzubauen.
- Gelegentlich Geschenke (Blumen, Pralinen) an Sarahs Zuhause schicken.
- Tiefe romantische Gefühle relativ schnell zum Ausdruck bringen

Die Finanzanträge

Etwa drei Monate nach Beginn ihrer Beziehung begannen Williams finanzielle Forderungen:

1. **Ursprüngliche Anfrage:** William behauptete, sein Projekt verzögere sich aufgrund eines Geräteausfalls. Er benötige 3.000 US-Dollar für Ersatzteile und könne wegen „Bankproblemen im Ausland“ nicht auf sein Geld zugreifen. Sarah, besorgt um seine Situation, überwies ihm das Geld.
2. **Eskalation:** Nachdem William seine tiefe Dankbarkeit zum Ausdruck gebracht hatte, verkündete er, das Projekt sei fast abgeschlossen und er werde in wenigen Wochen in die USA zurückkehren. Dann behauptete er jedoch, einen medizinischen Notfall (Blinddarmentzündung) zu haben und benötige 7.500 Dollar für eine Operation, die nicht von seiner Versicherung übernommen werde. Sarah, die nun emotional involviert war, nahm einen Kredit auf ihre Altersvorsorge auf, um das Geld zu überweisen.
3. **Krisensituation:** Kurz vor seiner geplanten Rückkehr in die USA behauptete William, einen Arbeitsunfall gehabt zu haben. Er benötigte 15.000 Dollar für medizinische Kosten und um einen Rechtsstreit mit der Firma vor Ort beizulegen, damit sein Pass wieder freigegeben wurde. Er versprach, alles nach seiner Rückkehr zurückzuzahlen.

Warnsignale, die Sarah übersehen hat

Im Rückblick erkannte Sarah mehrere Warnsignale, die sie übersehen hatte:

Williams Abneigung gegen Videochats
Widersprüche in seinen Erzählungen über Familie und Arbeit
Seine Kenntnisse im Ingenieurwesen wirkten auf Nachfrage nach Details vage.
Auf den Fotos war er nie in Malaysia oder an Arbeitsplätzen zu sehen.
Alle Gespräche drehten sich um ihre Beziehung oder seine Probleme.
Seine Schriften enthielten grammatikalische Fehler, die nicht mit denen eines englischen Muttersprachlers vereinbar sind.
Die Gründe, warum er nicht auf sein beträchtliches Vermögen zugreifen konnte, wurden immer komplexer.

Der Wendepunkt

Sarah wurde misstrauisch, als Williams Forderungen zunahmen und seine Geschichten immer komplizierter wurden. Als sie vorschlug, ihn in Malaysia zu besuchen, riet er ihr entschieden davon ab. Ihre Tochter, besorgt um die finanzielle Lage ihrer Mutter, bestand darauf, Williams Kommunikation zu überprüfen und erkannte die Muster eines Liebesbetrugs.

Um ihren Verdacht zu bestätigen, führte Sarahs Tochter eine umgekehrte Bildersuche mit Williams Fotos durch und entdeckte, dass diese einem pensionierten Professor in Kanada gehörten, der keine Verbindung zum Betrüger hat.

Auflösung und Folgen

Sarah verlor letztendlich etwa 25.500 US-Dollar an den Betrüger, bevor sie den Kontakt abbrach. Als sie ihn zur Rede stellte, leugnete „William“ den Betrug zunächst, wurde dann aber aggressiv und verschwand schließlich spurlos. Sarah meldete den Betrug an:

- örtliche Polizei
- Das Internet Crime Complaint Center (IC3) des FBI
- Die Dating-Plattform, auf der sie sich kennengelernt haben
- Ihre Bank und Finanzinstitutionen

Obwohl sie die verlorenen Gelder nicht wiedererlangen konnte, führte die Erfahrung Sarah zu Folgendem:

- Schließen Sie sich einer Selbsthilfegruppe für Überlebende von Liebesbetrug an.
- Arbeiten Sie mit einem Finanzberater zusammen, um ihre Altersvorsorge wieder aufzubauen.
- Setzen Sie sich für die Aufklärung über Liebesbetrug in Seniorengemeinschaften ein.
- Entwickeln Sie gesündere Grenzen in Beziehungen

Psychologische Auswirkungen

Sarah erlitt durch den Betrug ein erhebliches emotionales Trauma:

- Tiefe Scham und Verlegenheit
- Vertrauensprobleme in neuen Beziehungen
- Depression und Angst
- Finanzielle Belastung durch die Verluste
- Trauer über die Beziehung, die sie zu haben glaubte

Wichtigste Erkenntnisse

Dieser Fall verdeutlicht mehrere wichtige Aspekte von Liebesbetrug:

1. Betrüger zielen auf schutzbedürftige Personen ab, insbesondere auf solche, die kürzlich einen Verlust erlitten haben.
2. Sie bauen emotionale Bindungen auf, bevor sie finanzielle Anfragen stellen.

3. Sie isolieren die Opfer von Unterstützungsnetzwerken, die den Betrug aufdecken könnten.
4. Sie erzeugen Dringlichkeit und emotionalen Druck in Bezug auf finanzielle Anfragen.
5. Sie haben plausible Erklärungen dafür, warum sie nicht per Videochat kommunizieren oder sich persönlich treffen können.

Präventionsstrategien

Aus Sarahs Erfahrung lassen sich mehrere Präventionsstrategien ableiten:

- Überweisen Sie niemals Geld an jemanden, den Sie nicht persönlich getroffen haben.
- Bestehen Sie in Online-Beziehungen frühzeitig auf Videoanrufen.
- Recherchieren Sie die Informationen und Fotos der Person.
- Besprechen Sie neue Beziehungen mit vertrauten Freunden oder der Familie.
- Seien Sie vorsichtig bei Beziehungen, die sich ungewöhnlich schnell entwickeln.
- Hinterfragen Sie, warum jemand mit angeblichen Ressourcen Ihre finanzielle Hilfe benötigt.
- Seien Sie skeptisch gegenüber wiederholten Notfällen und Krisen.

Abschluss

Sarahs Fall ist beispielhaft für Tausende von Liebesbetrügereien, die jährlich vorkommen. Obwohl sie viel Geld verlor, waren die emotionalen Folgen des Betrugs noch verheerender. Durch Therapie und Selbsthilfegruppen hat Sarah ihr Leben wieder aufgebaut und hilft nun anderen, die Warnzeichen von Liebesbetrug zu erkennen, bevor sie ihre Ersparnisse – oder gar ihr Herz – an geschickte Manipulatoren verlieren.

Erkennen & Wachsen: Selbsteinschätz-ung und -bewertung.

Co-funded by
the European Union

4 Selbsteinschätzung und -bewertung

4.1 Selbstbewertungstests zu Kapitel 1: Liebesbetrug verstehen

1. Was ist das Hauptziel eines Liebesbetrugs?

A) Um echte Liebespartner zu finden
B) Um emotionale Bindungen finanziell auszunutzen
C) Um gesunde Online-Beziehungen zu fördern
D) Um Dating-Tipps zu geben
Richtige Antwort: B

2. Auf welchem historischen Betrug soll der Liebesbetrug seine Wurzeln haben?
A) Schneeballsystem
B) Der „spanische Gefangenen"-Betrug
C) Pyramidensystem
D) Nigerianischer Prinzen-Betrug
Richtige Antwort: B

3. Was ist die erste Phase in Whittys Modell für die Phasen eines Liebesbetrugs?
A) Vorbereitungsphase
B) Profilierungsphase
C) Auswertungsphase
D) Aufdeckungsphase
Richtige Antwort: B

4. Bei Liebesbetrugsfällen wird die Taktik, das Opfer mit Zuneigung und Aufmerksamkeit zu überhäufen, als folgende bezeichnet:
A) Schuldgefühle erzeugen
B) Krisen herbeiführen
C) Liebesbombardement
D) Finanzielle Ausbeutung
Richtige Antwort: C

5. Welches der folgenden Anzeichen ist ein häufiges Warnsignal bei Liebesbetrug?
A) Aufforderung zu einem sofortigen persönlichen Treffen
B) Unklare oder vage persönliche Angaben im Profil des Betrügers
C) Klare und schlüssige Lebensgeschichten
D) Öffentliche Präsenz in sozialen Medien
Richtige Antwort: B

6. Welche Gruppe ist laut Studien eher davon betroffen, Opfer von Liebesbetrug zu werden?
A) Junge Erwachsene im Alter von 18 bis 25 Jahren
B) Ältere Männer über 70 Jahre
C) Frauen mittleren Alters im Alter von 40 bis 60 Jahren
D) Jugendliche
Richtige Antwort: C

7. Welche Zahlungsmethode wird von Betrügern bei Liebesbetrugsfällen am häufigsten verlangt?
A) Persönliche Schecks
B) Kryptowährung oder Geschenkkarten
C) Kreditkartenzahlungen
D) Direkteinzahlung auf ein Bankkonto
Richtige Antwort: B

8. Wie versuchen Betrüger häufig zu verhindern, dass ihre Opfer den Betrug erkennen?
A) Durch regelmäßige Treffen mit den Opfern
B) Ausschließlich per Videoanruf
C) Indem man die Opfer bittet, Details ihrer Beziehung nicht mit anderen zu teilen
D) Indem man die Opfer ermutigt, Anzeige zu erstatten
Richtige Antwort: C

10. Welche der folgenden Maßnahmen wird als Präventivmaßnahme gegen Liebesbetrug empfohlen?
A) Schnell Geld schicken, um die Beziehung nicht zu gefährden
B) Details geheim halten und Hintergrundüberprüfungen neuer Kontakte durchführen
C) Freundschaften und Beziehungen gänzlich vermeiden
D) Jegliches Misstrauen ignorieren
Richtige Antwort: B

9. Welche psychologischen Auswirkungen hat Liebesbetrug laut Button et al. (2014) häufig auf die Opfer?

A) Erleichterung und Zufriedenheit
B) Nur finanzieller Verlust ohne emotionale Auswirkungen
C) Schweres emotionales Trauma und finanzieller Verlust (Richtig)
D) Mehr Sicherheit
Richtige Antwort: C

4.2 Selbstbewertungstests zu Kapitel 2: Gute Praktiken für Pädagogen

1. Was ist einer der Hauptgründe, warum Betrüger sozial isolierte Senioren ins Visier nehmen?
A) Sie investieren eher in risikoreiche Aktien.
B) Sie sind daran interessiert, neue Technologien zu erlernen.
C) Sie sind in der Regel vermögend.
D) Sie sind emotional verletzlich und suchen nach sozialen Kontakten.
Richtige Antwort: D

2. Welche Faktoren tragen am häufigsten dazu bei, dass ältere Menschen anfällig für Liebesbetrug sind?
A) Hohes Einkommen und geringe Erfahrung mit sozialen Medien
B) Vertrauenswürdigkeit, kognitiver Abbau und emotionales Bedürfnis
C) Freizeit und gute familiäre Unterstützung
D) Sie sind in der Regel wohlhabend
Richtige Antwort: B

3. Welche Taktik wenden Betrüger häufig an, um ihre Opfer emotional zu manipulieren?
A) Strenge juristische Formulierungen
B) Versprechungen eines frühen Erbes
C) Übergriffige Liebesbekundungen und emotionale Verstärkung
D) Verhöhnung ihrer Einsamkeit
Richtige Antwort: C

4. Welches doppelte Trauma erleben Opfer von Liebesbetrug häufig?
A) Emotionaler Verrat und finanzieller Verlust
B) Rechtliche Probleme und gesundheitliche Verschlechterung
C) Familienkonflikte und Peinlichkeit
D) Missbrauch von Technologie und Arbeitsplatzverlust
Richtige Antwort: A

5. Welche Folge kann noch Jahre nach dem Betrug bestehen bleiben, wenn den Opfern keine angemessene Unterstützung angeboten wurde?
A) Verbesserte Urteilsfähigkeit
B) Langfristiges Trauma und Vermeidung von Beziehungen
C) Bessere Online-Gewohnheiten
D) Besseres Selbstwertgefühl
Richtige Antwort: A

6. Warum vermeiden Senioren es oft, Betrugsfälle zu melden?
A) Sie verstehen nicht, wie das Melden von Betrug funktioniert.
B) Sie sind emotional nicht betroffen.
C) Sie fürchten Scham, Spott oder Verurteilung.
D) Sie wollen den Betrüger schützen.
Richtige Antwort: C

7. Warum sind Pädagogen bei der frühzeitigen Erkennung von Betrugsfällen oft effektiver als die Familie?
A) Sie haben die rechtliche Befugnis, Ermittlungen durchzuführen.
B) Sie schränken die Online-Nutzung ein.
C) Senioren fühlen sich weniger verurteilt und können sich ihnen leichter anvertrauen.
D) Sie leben mit den Senioren zusammen.
Richtige Antwort: C

8. Welche Rolle können Jugendarbeiter bei der Verringerung der Anfälligkeit älterer Menschen für Betrugsfälle spielen?
A) Betrugsfälle im Namen von Senioren bei Banken melden
B) Generationenübergreifendes digitales Mentoring und Empathie anbieten
C) Senioren von Online-Plattformen entfernen
D) Dozenten in allen Workshops ersetzen
Richtige Antwort: B

9. Was ist der Hauptgrund dafür, dass digitale Kompetenz bei der Betrugsprävention so stark betont wird?
A) Um die Anfälligkeit für Online-Betrugsmaschen zu verringern.
B) Um Senioren zu mehr Online-Zeit zu animieren.
C) Um ihnen das Erstellen von Blogs beizubringen.
D) Um Polizeieinsätze zu vermeiden.
Richtige Antwort: A

10. Warum sind „Buddy-Systeme“ wirksam bei der Verhinderung von Betrug?
A) Sie reduzieren die Reisekosten für Lehrkräfte.
B) Sie begrenzen Telefonate.
C) Sie überwachen die Internetnutzung.
D) Sie bieten Senioren eine Vertrauensperson für verdächtige Aktivitäten.
Richtige Antwort: D

11. Was sollten Pädagogen bei der Konzeption von Workshops zur Betrugsprävention priorisieren?
A) Komplexe Fachsprache und lange Sitzungen
B) Schambasierte Warngeschichten
C) Zugängliche, interaktive Methoden zur Förderung emotionaler und digitaler Kompetenzen
D) Älteren Menschen raten, die Nutzung von Technologie einzustellen
Richtige Antwort: C

12. Welches Verhalten ist ein frühes Warnzeichen für einen laufenden Liebesbetrug?
A) Häufigeres ehrenamtliches Engagement
B) Mehr Familienbesuche
C) Teilnahme an Kursen zur digitalen Kompetenz
D) Plötzliche Geheimhaltung einer neuen Online-Beziehung (Richtig)
Richtige Antwort: D

13. Welche der folgenden Methoden ist NICHT als Nachweismethode zu empfehlen?
A) Direkte Konfrontation
B) Vertrauensbildende Gespräche
C) Emotionale Einbindung
D) Verhaltensbeobachtung
Richtige Antwort: A

14. Was versteht man unter „Triage“ in der Betrugsbekämpfungsstrategie?
A) Dem Opfer die Schuld geben
B) Bewerten, anklagen, melden
C) Ignorieren, beobachten, analysieren
D) Einbeziehen, aufklären, bewerten
Richtige Antwort: D

15. Wie sollten Pädagogen mit emotional involvierten Senioren umgehen, die in aktive Betrugsfälle verwickelt sind?
A) Angstmacherei anwenden
B) Anonymisierte Szenarien und gezielte Fragen verwenden
C) Darauf bestehen, dass sie den Betrug sofort melden
D) Ihre Familie ohne deren Zustimmung alarmieren
Richtige Antwort: B

16. Wie können Pädagogen dazu beitragen, die Isolation nach einem Betrugsfall zu verringern?
A) Geheimhaltung fördern
B) Opfer wieder mit sicheren sozialen Aktivitäten und Selbsthilfegruppen verbinden
C) Ihre sozialen Medien überwachen
D) Internetnutzung unterbinden
Richtige Antwort: B

17. Warum sollten Pädagogen die Familien der Opfer sensibel einbeziehen?
A) Um ihnen die Schuld zuzuschieben
B) Um den Druck zu erhöhen
C) Um die Verantwortung abzugeben
D) Um Unterstützung aufzubauen und die Scham der Opfer zu verringern
Richtige Antwort: D

18. Warum sind Partnerschaften mit Bibliotheken, Gesundheitszentren und Gemeindezentren so wichtig für die Betrugsprävention?
A) Sie reduzieren den Verwaltungsaufwand.
B) Sie ersetzen die Arbeit der Lehrkräfte.
C) Sie helfen, Senioren zu erreichen und ihnen ein vertrauensvolles Umfeld zu bieten.
D) Sie können rechtliche Schritte durchsetzen.
Richtige Antwort: C

4.3 Selbstbewertungstests zu Kapitel 3: Grundlagen der Cybersicherheit für Anfänger

1: Was ist das Hauptmerkmal eines Phishing-Angriffs?
a) Installation von Schadsoftware über USB-Geräte
b) Ausnutzung von Software-Schwachstellen
c) Personen durch betrügerische Kommunikation zur Preisgabe sensibler Informationen verleiten
d) Physisches Eindringen in Computersysteme
Richtige Antwort: C

2: Worin unterscheidet sich Spear-Phishing von regulärem Phishing?
a) Es nutzt Telefonanrufe statt E-Mails.
b) Es zielt mit personalisierten Angriffen auf bestimmte Personen oder Organisationen ab.
c) Es zielt ausschließlich auf Regierungsbehörden ab.
d) Es nutzt physische Post statt elektronischer Kommunikation.
Richtige Antwort: B

3: Was versteht man unter Pretexting im Social Engineering?
a) Massen-E-Mails an zufällige Empfänger versenden
b) Ein fingiertes Szenario erstellen, um Opfer zu manipulieren und Informationen zu stehlen
c) Technische Sicherheitslücken ausnutzen, um Systemzugriff zu erlangen
d) Keylogger auf Zielcomputern installieren
Richtige Antwort: B

4: Welches Szenario beschreibt am besten einen Köderangriff?
a) Infizierte USB-Sticks auf Parkplätzen auslegen, damit Mitarbeiter sie finden
b) Droh-E-Mails versenden, in denen Zahlungen gefordert werden
c) Telefonanrufe tätigen und sich als IT-Support ausgeben
d) Gefälschte Profile in sozialen Medien erstellen
Richtige Antwort: A

5: Was versteht man unter Tailgating im Kontext von Social Engineering?
a) Jemandes Online-Aktivitäten verfolgen
b) Netzwerkverkehr überwachen
c) Jemandem ohne entsprechende Berechtigung durch eine Sicherheitstür folgen
d) Jemandes Tastatureingaben kopieren
Richtige Antwort: C

6: Was versteht man unter „Vishing“?
a) Visuelles Phishing über gefälschte Websites
b) Virales Phishing über soziale Medien
c) Video-Phishing über gefälschte Videoanrufe
d) Sprach-Phishing per Telefonanruf
Richtige Antwort: D

7: Welches psychologische Prinzip nutzen Social Engineers üblicherweise aus?
a) Technische Komplexität
b) Netzwerkprotokolle
c) Autorität und Vertrauen
d) Verschlüsselungsalgorithmen
Richtige Antwort: C

8: Was ist ein Wasserlochangriff?
a) Vergiftung der tatsächlichen Wasserversorgung
b) Kompromittierung von Websites, die von Zielorganisationen häufig besucht werden
c) Angriffe auf Wasserversorgungsunternehmen
d) Verwendung von Phishing-E-Mails mit Bezug zu Wasser
Richtige Antwort: B

9: Was kennzeichnet einen Social-Engineering-Angriff mit dem Ziel einer Gegenleistung?
a) Anbieten von etwas im Austausch für Informationen oder Zugang
b) Drohen mit rechtlichen Schritten
c) Ausschließlich technische Methoden anwenden
d) Nur Führungskräfte ins Visier nehmen
Richtige Antwort: A

10: Was ist Reverse Social Engineering?
a) Social Engineering rückwärts nutzen
b) Angreifer geben sich als hilfsbereit aus und warten auf Kontaktaufnahme durch das Opfer
c) Die Auswirkungen von Social Engineering umkehren
d) Soziale Medien in umgekehrter chronologischer Reihenfolge nutzen
Richtige Antwort: B

11: Welches der folgenden Anzeichen ist ein Warnsignal, das auf einen Social-Engineering-Versuch hindeuten könnte?
a) Anfragen nach Software-Updates
b) Dringende Anfragen nach sensiblen Informationen mit Androhung von Konsequenzen
c) Regelmäßige private Kommunikation
d) Geplante Treffen mit bekannten Personen
Richtige Antwort: B

Quellen

AARP. (o. J.). Liebesbetrug. https://www.aarp.org/money/scams-fraud/

AARP. (2021). AARP VOA ReST-Programm: Heilung nach Betrug. AARP Fraud Watch Network. https://www.aarp.org/fraudwatchnetwork

AARP. (o. J.). Emotionale Unterstützung für Betrugsopfer. https://states.aarp.org/maryland/emotional-support-for-victims-of-fraud#

Against Scams. (2024). Die Bedeutung der Traumatherapie für Betrugsopfer. https://againstscams.org/importance-of-trauma-therapy-for-scam-victims-2024

Action Fraud. (o. J.). Liebesbetrug. https://www.actionfraud.police.uk/

Action Fraud. (30. Januar 2025). Unsere Forschung und Statistiken zu Liebesbetrug – Hinweise von Action Fraud zu Schadensfällen. https://www.actionfraud.org.uk/research-and-statistics-on-romance-scams-fraud/

Ayoobi, N., Shahriar, S. & Mukherjee, A. (5. September 2023). Die drohende Gefahr gefälschter und von LLM-Absolventen erstellter LinkedIn-Profile: Herausforderungen und Chancen für deren Erkennung und Prävention. arXiv. https://doi.org/10.1145/3603163.3609064

BBC News. (7. Mai 2024). Wie ein „Brad Pitt"-Betrug meiner Mutter das Herz brach. https://www.bbc.com/news/articles/ckgnz8rw1xgo

Berry, K. (24. November 2024). Betrugsmasche: „Ich wurde von einer Deepfake-Werbung von Martin Lewis getäuscht". BBC News. https://www.bbc.co.uk/news/articles/clyvj754d9lo

Boulat, P.-A., & Wake, P. (15. Mai 2024). Können KI-generierte Deepfakes die Kundenidentifizierung (KYC) gefährden? techUK. https://www.techuk.org/resource/can-ai-generated-deepfakes-compromise-know-your-customer-kyc-authentication.html

Quellen

Brady, S. (20. Februar 2024). Tinder verstärkt die Identitätsprüfung angesichts steigender KI-Betrugsfälle. Verdict. https://www.verdict.co.uk/tinder-bolsters-id-verification-amid-surge-in-ai-scams/?cf-view&cf-closed

Button, M., Nicholls, C. M., Kerr, J. & Owen, R. (2014). Online-Betrug: Erkenntnisse aus der Sicht von Opfern – Warum sie auf diese Betrugsmaschen hereinfallen. Australian & New Zealand Journal of Criminology, 47(3), 391–408. https://doi.org/10.1177/0004865814521224 (Originalveröffentlichung 2014)

Polizeistation (Anmerkung der Redaktion). Liebesbetrug. Staatspolizei. https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/truffe-romantiche-romance-scam/index.html

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A. & Gualtieri, G. (2020). Online-Romance-Scams: Beziehungsdynamiken und psychologische Merkmale der Opfer und Betrüger. Eine Übersichtsarbeit. Clin Pract Epidemiol Ment Health, 16. https://doi.org/10.2174/1745017902016010024

Cross, C. (2014). Liebe tut weh: Die kostspielige Realität des Online-Liebesbetrugs. The Conversation.

Cross, C., Dragiewicz, M. & Richards, K. (2016). Romance Fraud verstehen: Erkenntnisse aus der Theorie häuslicher Gewalt. Cyberpsychology, Behavior, and Social Networking, 19(7), 419–423. https://doi.org/10.1089/cyber.2016.0729

Cross, C., & Layt, R. (2021). „Ich vermute, die Bilder sind gestohlen“: Liebesbetrug, Identitätsdiebstahl und der Umgang mit Verdachtsfällen unauthentischer Identitäten. Social Science Computer Review, 40(4), 1043–1058. https://doi.org/10.1177/0894439321999311

Cross, C. (2022). Künstliche Intelligenz (KI) und Deepfakes zur Täuschung von Opfern: Die Notwendigkeit, die aktuelle Präventionsstrategie gegen Liebesbetrug zu überdenken. Crime Prevention and Community Safety, 24(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Quellen

Cunha, H. S. (o. J.). Warum sind Liebesbetrügereien so wirkungsvoll? https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf

CybSafe. (2023). Romance Scams: Die Statistiken und ihre Bedeutung für Ihr Unternehmen. https://www.cybsafe.com/blog/romance-scams-stats-for-organizations/

Daily Mail. (1. Juni 2024). Britische Großmutter in Brasilien wegen Kokainschmuggels verhaftet. https://www.dailymail.co.uk/news/article-14718249/Grandmother-Veronica-Watson-Brazil-drugs.html

Dellinger, A. J. (2019). Anatomie eines Betrugs: Nigerianischer Liebesbetrüger packt aus. Forbes. https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/

Dogma. Liebesbetrug: Die Anzeichen und wie Sie sich schützen können. https://www.dogma.it/it/news/truffe-sentimentali--i-segnali-e-come-difendersi

Eberhart, C. (26. Mai 2023). Wer beobachtet Sie? KI kann ahnungslose Opfer mit „Leichtigkeit und Präzision“ ausspionieren: Experten. Fox News. https://www.foxnews.com/us/who-is-watching-you-ai-can-stalk-unsuspecting-victims-ease-precision-experts

Europol. 13 Festnahmen in Italien wegen Betrugs an älteren Liebenden. https://www.europol.europa.eu/media-press/newsroom/news/13-arrested-in-italy-for-tricking-elderly-love

Europol. Wie man nicht auf den „Loverboy“-Betrug hereinfällt. Europol. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-not-to-fall-for-lover-boy-scam

Quellen

Europol. (2023). Spotlight-Bericht: Online-Betrugsmaschen. https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Europol. (2017). Sexuelle Nötigung und Erpressung im Internet als Straftat gegen Kinder. Agentur der Europäischen Union für die Zusammenarbeit der Strafverfolgungsbehörden. https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Federal Bureau of Investigation (FBI). (3. Dezember 2024). Kriminelle nutzen generative künstliche Intelligenz zur Erleichterung von Finanzbetrug. https://www.ic3.gov/PSA/2024/PSA241203

Federal Trade Commission. (2023). Die beliebtesten Lügen von Liebesbetrügern aufgedeckt. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

Bundeshandelskommission (FTC). Betrug melden. https://reportfraud.ftc.gov/

Bundeshandelskommission (FTC). So vermeiden Sie Liebesbetrug im Internet. https://www.consumer.ftc.gov

Finney, G. (2023). Project Zero Trust. Cybersecurity Insights. https://www.cybersecurityinsights.com/project-zero-trust

Fintech Global. (13. Februar 2025). Banken sehen sich aufgrund des Anstiegs von Liebesbetrug erhöhten Reputations- und Finanzrisiken ausgesetzt. https://fintech.global/2025/02/13/banks-face-heightened-reputational-and-financial-risks-as-romance-scams-surge/

Goodwin, L. (19. Dezember 2024). „KI-Deepfake-Romance-Betrug hat mich um 17.000 Pfund gebracht“. BBC News. https://www.bbc.co.uk/news/articles/cdr0g1em52go

Quellen

Gozzi, L. (15. Januar 2025). Französin von KI getäuscht – Brad Pitt wird im Internet verspottet. BBC News. https://www.bbc.co.uk/news/articles/ckgnz8rw1xgo

Howard, R. (2023). Cybersecurity First Principles: A Reboot of Strategy and Tactics. John Wiley & Sons. https://www.wiley.com/en-us/Cybersecurity%2BFirst%2BPrinciples%3A%2BA%2BReboot%2Bof%2BStrategy%2Band%2BTactics-p-9781394173099

Internet Crime Complaint Center (IC3). (o. J.). Romance Scams. https://www.ic3.gov/

Interpol. (2022). Interpol-Bericht zu Sextortion-Trends. Internationale Kriminalpolizeiliche Organisation. Abgerufen von https://www.interpol.int

Kollmorgen, A. (2025). KI-gesteuerte Liebesbetrügereien führen wahrscheinlich zu höheren Verlusten. Choice. https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/romance-scams-and-how-to-avoid-them

Kloess, J. A., Beech, A. R. & Harkins, L. (2014). Sexuelle Ausbeutung von Kindern im Internet: Prävalenz, Prozess und Tätermerkmale. Trauma, Violence & Abuse, 15(2), 126–139. https://doi.org/10.1177/1524838013511543

Lee, Y., & Gelman, B. (27. November 2023). Die Schattenseiten der KI: Groß angelegte Betrugskampagnen durch generative KI ermöglicht. Sophos News. https://news.sophos.com/en-us/2023/11/27/the-dark-side-of-ai-large-scale-scam-campaigns-made-possible-by-generative-ai/

Magramo, K. (17. Mai 2024). Britischer Technologiekonzern Arup Opfer eines Deepfake-Betrugs in Höhe von 25 Millionen US-Dollar. CNN. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

Quellen

Mattackal, L. P. (14. Februar 2025). Kryptobetrugsfälle erreichen 2024 dank KI-Unterstützung wahrscheinlich einen neuen Rekord, so Chainalysis. Reuters. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/

Narang, S. (14. Februar 2024). Schweineschlacht-Betrug: Wie Bitcoin-, Ethereum-, Litecoin- und Spot-Gold-Investitionen (XAUUSD) in Liebesbetrügereien genutzt werden, um Hunderte von Millionen zu stehlen. Tenable. https://www.tenable.com/blog/pig-butchering-scam-bitcoin-ethereum-litecoin-spot-gold-xauusd-romance-scam

Nationales Zentrum für Cybersicherheit. (24. Januar 2024). Die kurzfristigen Auswirkungen von KI auf die Cyberbedrohung. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

National Crime Agency [NCA]. (2021). Bericht über Sextortion-Bedrohung. NCA-Einheit für Cyberkriminalität. https://www.nationalcrimeagency.gov.uk

Newcastle University. (o. J.). Opfer von Online-Dating-Betrug: Psychologische Folgenanalyse. https://doi.org/10.54097/ehss.v4i.2740

Newman, L. H., & Burgess, M. (30. September 2024). Die Invasion der Schweineschlachtereien hat begonnen. Wired. https://www.wired.com/story/pig-butchering-scam-invasion/

Newman, L. H., & Burgess, M. (13. Februar 2025). Die Epidemie der Einsamkeit ist eine Sicherheitskrise. Wired. https://www.wired.com/story/loneliness-epidemic-romance-scams-security-crisis/

Nielson, S. J. (2023). Discovery cybersecurity: A technical introduction for the absolute beginner. Apress. https://doi.org/10.1007/978-1-4842-9560-1

Patchin, J. W., & Hinduja, S. (2020). Sextortion unter Jugendlichen: Ergebnisse einer nationalen Umfrage unter US-amerikanischen Jugendlichen. Sexual abuse: a journal of research and treatment, 32(1), 30–54. https://doi.org/10.1177/1079063218800469

Quellen

Patel, M. (2025). Cybersicherheit für Einsteiger: Praktische Fähigkeiten zur Abwehr von Cyberbedrohungen erlernen und sich auf Zertifizierungsprüfungen vorbereiten. Michael Patel. ISBN-13: 9798227516435.

University of Pennsylvania. (2024). Die Psychologie der Cyberkriminalität. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

Pietilä, E. & Korhonen, H. (5.06.2024). Die harte Realität von Liebesbetrug. https://nordicwelfare.org/popnad/en/artiklar/the-harsh-realities-of-romance-scams/

Policija.si. (o. J.). Romance Scams. Slowenische Polizei. https://www.policija.si/eng/prevention/internet-security/romance-scams

Rege, A. (2009). Verdorbene Liebe: Eine systematische Literaturübersicht zur Forschung über Online-Romance-Scams. Interacting with Computers, 21(5-6), 427–437. https://doi.org/10.1016/j.intcom.2009.06.006

Rogiers, A., et al. (11. November 2024). Überzeugung mit großen Sprachmodellen: Eine Übersicht. arXiv. https://doi.org/10.48550/arxiv.2411.06837

Sanction Scanner. (16. September 2024). Wie generative künstliche Intelligenz Geld wäscht. https://www.sanctionscanner.com/blog/ais-dark-side-how-generative-artificial-intelligence-launders-money-863

ScamWatch. (15. August 2024). Online-Dating- und Liebesbetrug. https://www.scamwatch.gov.au/types-of-scams/online-dating-and-romance-scams

SciSpace. (o. J.). Online-Liebesbetrug: Beziehungsdynamiken und psychologische Erkenntnisse. https://scispace.com/papers/online-romance-scams-relational-dynamics-and-psychological-5cckseevfj

Quellen

Shea, S., & Krishnan, A. (2024). Wie KI Phishing-Angriffe gefährlicher macht. TechTarget. https://www.techtarget.com/searchSecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

Shepardson, D. (2024). Berater wegen Verwendung von KI zur Fälschung von Bidens Stimme in automatisierten Anrufen zu einer Geldstrafe von 6 Millionen US-Dollar verurteilt. Reuters. https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/

Statista. (2025). Anzahl der von Facebook pro Quartal weltweit entfernten Fake-Accounts (Stand: 1. Quartal 2025). https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hall, J. & Kieran. (November 2024). KI-gestützte Einflussoperationen: Die Sicherung zukünftiger Wahlen. CETaS-Forschungsberichte.

Polizei Surrey. Liebesbetrug. Polizei Surrey. https://www.surrey.police.uk/romancefraud

Tech Report. Statistiken zu Liebesbetrug. https://techreport.com/statistics/cybersecurity/romance-scam-statistics/

The Debt Advisor. (2023). Liebesbetrug: Eine wachsende Bedrohung für Männer und Frauen. https://www.thedebtadvisor.co.uk/romance-scams/

The Guardian. (2024). Spanische Polizei verhaftet fünf Personen wegen Betrugs mit gefälschtem Brad Pitt. https://www.theguardian.com/film/2024/sep/23/spanish-police-arrest-five-people-over-fake-brad-pitt-scam

Quellen

Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung. (2024). Transnationale organisierte Kriminalität und die Konvergenz von Cyberbetrug, illegalem Bankwesen und technologischer Innovation in Südostasien: Eine sich wandelnde Bedrohungslandschaft. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

US-amerikanische Federal Reserve. (2024). Synthetischer Identitätsbetrug: Generatives KI-Toolkit zur Erkennung von Zahlungsbetrug. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

US-Einwanderungs- und Zollbehörde (ICE). (10.02.2025). Sextortion. https://www.ice.gov/features/sextortion#

Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung. (2024). Transnationale organisierte Kriminalität und die Konvergenz von Cyberbetrug, illegalem Bankwesen und technologischer Innovation in Südostasien: Eine sich wandelnde Bedrohungslandschaft. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

US-amerikanische Federal Reserve. (2024). Synthetischer Identitätsbetrug: Generatives KI-Toolkit zur Erkennung von Zahlungsbetrug. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

Wang, C. (2022). Psychologische Folgen von Online-Dating-Betrug: Eine Analyse. Journal of Education, Humanities and Social Sciences, 4, 149–154. https://doi.org/10.54097/ehss.v4i.2740

Wang, F. (2024). Das Schweigen brechen: Eine Untersuchung des Prozesses von Cybersextortion und der Bewältigungsstrategien von Opfern. International Review of Victimology, 31(1), 91–116. https://doi.org/10.1177/02697580241234331 (Originalveröffentlichung 2025)

Quellen

Whitty, M. T., & Buchanan, T. (2016). Liebst du mich? Psychologische Merkmale von Opfern von Liebesbetrug. Psychologische Merkmale von Opfern von Liebesbetrug – PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5297105/

Whitty, M. T., & Buchanan, T. (2016). Der Online-Dating-Romance-Scam: Ursachen und Folgen der Opferrolle [PDF]. Universität Warwick. https://wrap.warwick.ac.uk/id/eprint/81382/1/WRAP_whitty__buchananpsychological_impact_romance_scam_final_version.pdf

Whitty, M. & Buchanan, T. (2012). Online-Romance-Scam: Ein schweres Cyberverbrechen. Cyberpsychology, behavior and social networking. 15. 181-183. 10.1089/cyber.2011.0352.

Wrexham.com. (13. Februar 2024). Mann aus Wrexham um 25.000 Pfund durch Liebesbetrug betrogen. https://wrexham.com/news/warning-issued-after-wrexham-man-conned-out-of-25k-in-romance-scam-247088.html

Yeung, J. (15. Oktober 2024). Deepfake-Romance-Betrug brachte Männern in ganz Asien 46 Millionen Dollar ein, so die Polizei. CNN. https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk/index.html

Zhang, D., et al. (9. Februar 2024). IP-Adapter Inpainting: Kontrollierbares Inpainting mit IP-Adapter. arXiv. https://arxiv.org/html/2502.06593v1

Zvelo. (8. November 2023). Die Rolle der KI im Social Engineering. https://zvelo.com/the-role-of-ai-in-social-engineering

Zvelo. (8. November 2023). Die Rolle der KI im Social Engineering. U

Nehmen Sie Kontakt mit uns auf!

Dieses Handbuch wurde in Zusammenarbeit der FALS-Projektkoordinatoren EUW (Deutschland), ECREC (Niederlande) und IVI (Italien) entwickelt.

Um mit uns in Kontakt zu bleiben und falls Sie Fragen, Anmerkungen oder Vorschläge haben, können Sie uns gerne über die folgenden Kanäle kontaktieren.

ECREC (Niederlande)

Telefon
+31 70 200 2595

E-Mail
info@ecrec.eu

Webseite
https://ecrec.eu/

EUW (Deutschland)

Telefon
+49 176 55030502

E-Mail
projects@euthwonders.org

Webseite
www.euthwonders.org

IVI (Italien)

Telefon
+39 329 599 7585

E-Mail
igorvitaleinternational@gmail.com

Webseite
https://www.igorvitale.org/

Co-funded by the European Union