HMD Praxis der Wirtschaftsinformatik (2024) 61:27–42
https://doi.org/10.1365/s40702-023-01032-5

SCHWERPUNKT

# Ok, gegen Cupids Pfeil hilft keine Firewall – Sichere(s) Daten durch ganzheitlichen Kompetenzaufbau

**Rebecca Finster · Thomas Kronschläger · Linda Grogorick · Susanne Robra-Bissantz**

Eingegangen: 1. September 2023 / Angenommen: 6. Dezember 2023 / Online publiziert: 20. Dezember 2023


**Zusammenfassung** In einer ständig präsenten digitalen Umgebung, die Technologie als zentrales Angebot nutzt, gewinnt Online-Dating immer mehr an Popularität. Ein Großteil der jüngeren Bevölkerung hat Erfahrung damit. Doch diese Entwicklung bringt neue Herausforderungen in Bezug auf Datenschutz und Informationssicherheit mit sich. Online-Dating-Plattformen (z. B. *OkCupid*) und -Apps (z. B. *Tinder*) führen zur Entstehung von Cyberintimität und eröffnen Risiken, wie Social Engineering, bei denen Menschen beeinflusst werden, um vertrauliche Informationen preiszugeben. Diese Bedrohungen könnten nicht nur persönliche Leben beeinträchtigen, sondern auch die Sicherheit von Unternehmen gefährden. Opfer von Social Engineering könnten in der vermeintlich privaten Online-Dating-Umgebung unbeabsichtigt sensible Informationen enthüllen und dadurch Unternehmensnetzwerke gefährden. Daher ist es von großer Bedeutung, digitale Fähigkeiten in Kompetenzbereichen wie Information Security Awareness und Kommunikation zu stärken und

✉ Rebecca Finster · Linda Grogorick · Susanne Robra-Bissantz
Institut für Wirtschaftsinformatik – Service-Informationssysteme, Technische Universität Braunschweig, Braunschweig, Deutschland
E-Mail: r.finster@tu-bs.de

Linda Grogorick
E-Mail: l.grogorick@tu-bs.de

Susanne Robra-Bissantz
E-Mail: s.robra-bissantz@tu-bs.de

Thomas Kronschläger
Institut für Germanistik – Didaktik der deutschen Sprache und Literatur, Technische Universität Braunschweig, Braunschweig, Deutschland
E-Mail: t.kronschlaeger@tu-bs.de

eine kritische Herangehensweise an online geteilte Informationen zu entwickeln. Diese Untersuchung analysiert die Verbindung zwischen Informationssicherheit und Online-Dating durch eine interdisziplinäre hermeneutische Analyse. Dabei liegt der Fokus auf der Rolle von Kommunikation und anderen digitalen Kompetenzen im Kontext von Informationssicherheit und Social Engineering und verdeutlicht die Wichtigkeit von Informationssicherheit über das Berufsleben hinaus.

**Schlüsselwörter** Digitale Kompetenzen · Informationssicherheit · Social Engineering · Online-Dating · Aus- und Weiterbildung

## Ok, a firewall is no match for Cupid‘s arrow- Secure dat(a/ing) through holistic competence development

**Abstract** In an ever-present digital environment that revolves around technology, online dating is gaining significant popularity. A large portion of the younger population has experience in this area. However, this trend brings with it new data privacy and information security challenges. Online dating platforms (e.g. *OKCupid*) and apps (e.g. *Tinder*) contribute to the emergence of cyber intimacy and introduce risks such as social engineering, where individuals are manipulated to gain confidential information. These threats can affect not only personal lives, but also the security of businesses. Victims of social engineering may inadvertently reveal sensitive information in supposedly private online dating situations, putting corporate networks at risk. As a result, it is critical to improve digital skills in competence areas such as information security awareness and communication, while adopting a critical approach to information shared online. A study explores the nexus between information security and online dating through an interdisciplinary hermeneutic analysis. Special emphasis is placed on the role of language, data protection, and other digital competences in the context of information security and social engineering and emphasizes the importance of information security beyond professional life.

**Keywords** Digital Competences · Information Security · Social Engineering · Online-Dating · Professional Training

## 1 Einleitung: Kim will Luka daten, aber Luka will nur Kims Daten

Kim entdeckt Lukas Profil auf einer Dating-App und ist sofort begeistert – ein Superlike folgt. Als Luka antwortet und das Gespräch beginnt, ahnt Kim nicht, dass Luka eigentlich Maxi heißt und ein erfundenes Profil verwendet, um Daten zu sammeln. Maxi flicht scheinbar unschuldige Fragen wie „Wo bist du aufgewachsen?“ oder „Hattest du Haustiere?“ in den Gesprächsverlauf, die dazu dienen können, Passwort-Wiederherstellungsfragen zu beantworten. Ohne Kims Wissen oder Zustimmung sammelt Maxi diese Informationen, um später Zugriff auf Kims E-Mail und andere digitale Dienste zu erhalten.

Wie Kim könnte es den etwa neun Millionen Nutzys von Online-Dating-Plattformen allein in Deutschland ebenfalls ergehen (Statista 2023). Weltweit betrachtet nutzen sogar eine halbe Milliarde Menschen Online-Dating-Services, die potenzielle Opfer von solchen Aktivitäten sein können (Statista 2023). Neben der gezielten Manipulation, um im direkten Gesprächsverlauf persönliche Informationen zu erhalten, stellen andere Datenlecks, die z. B. durch Hacker-Angriffe entstehen, ebenfalls ein Sicherheitsrisiko dar (Phan et al. 2021). In regelmäßigen Abständen werden solche Datenlecks entdeckt; so wurden zum Beispiel persönliche Daten wie Wohnort, Familienstand oder Angaben zum eigenen Körper von 2,28 Mio. Nutzys der Dating-Website *MeetMindful* (Cimpanu 2021) und mehr als eine Millionen Profile von Nutzys verschiedener Dating-Apps aus den USA, Südkorea und Japan veröffentlicht (BÎZGĂ 2020, 2023).

Bei der Erstellung eines Profils auf einer Online-Dating-Plattform müssen persönliche Informationen, wie zum Beispiel Geburtsdatum, Alter oder sexuelle Vorlieben angegeben werden, damit passende Vorschläge generiert werden können (Buthelezi 2021). Obwohl durchgeführte Interviews mit Nutzys von Online-Dating-Plattformen gezeigt haben, dass die Mehrheit nicht darauf vertraut, dass die Angaben in den Profilen korrekt sind, wird eher von kleineren Flunkereien ausgegangen. Beispielsweise betrifft dies ältere Nutzys, die sich darum sorgen, dass Profile falsche Angaben zum Alter oder Beziehungsstatus beinhalten oder jüngere Nutzys, die vermuten, dass Profilbilder veraltet oder aus einem besonders schmeichelhaften Blickwinkel aufgenommen sind (Norcie et al. 2013; Păduraru et al. 2022). Die Angst vor einer gezielten Manipulation wie in unserem Einstiegsbeispiel, bei dem Kim dazu gebracht wird, vertrauliche Informationen preiszugeben bzw. eine bestimmte Handlung auszuführen, ist im Online-Dating scheinbar noch nicht weit verbreitet, wohingegen solch ein Vorgehen bereits von über 60 % der befragten Unternehmen als eher oder sogar sehr bedrohlich für die IT-Sicherheit angesehen wird (Bitkom 2022). Social Engineering (SE) wird also als wachsende Bedrohung wahrgenommen und es besteht die Wahrscheinlichkeit hoher Dunkelziffern, da Nutzys dies aus Scham ungern offenlegen möchten (Haucke und Pokoyski 2018). Dass die Dunkelziffer bei Dating-App-relevanten Betrügereien (Scams) besonders hoch ist, ist anzunehmen. Gerade im Online-Dating gibt es aber nicht nur zusätzliche mögliche Angriffsvektoren, sondern auch frappierende Überschneidungen mit SE-Methoden, insbesondere, wenn es um die Manipulation von Kommunikation und Informationen geht (Hopkins 2016).

Vor diesem Hintergrund ist es heute wichtiger denn je, digitale Kompetenzbereiche wie Information Security Awareness und Kommunikation zu stärken und eine kritische Haltung gegenüber Informationen und Narrativen zu entwickeln, die wir online teilen und konsumieren (Wijaya et al. 2022). Dazu bedarf es einer Betrachtung der Vermischung der Sphären privat und beruflich, die zu unbewussten Sicherheitslücken führen können. In unserer Untersuchung führen wir daher eine interdisziplinäre hermeneutische Analyse (Scheuermann und Kroeze 2017; Capurro 2010) von wissenschaftlichen Quellen und Erfahrungsberichten aus den Bereichen Informationssicherheit und Online-Dating durch. Besonderes Augenmerk legen wir auf die Rolle von Sprache im Kontext von Informationssicherheit und SE. Dabei rücken insbesondere Aspekte wie Kommunikation und Vertrauen im Online-Dating in den Vordergrund (Haucke und Pokoyski 2018; Phan et al. 2021). Auch die aktive

bewusste Zustimmung, vulgo Consent, in Abgrenzung zu der in der Informationssicherheit weit verbreiteten Compliance, ist eine wichtige Teilkompetenz, die immer mehr in Datenschutz und Informationssicherheit aber auch als Zustimmung zur Kommunikation an sich und vor allem bei bestimmten Kommunikationsformaten und -inhalten eine Rolle spielt.

Dieser Beitrag leistet einen Beitrag, zur Schärfung des Bewusstseins für die Risiken von Online-Dating in Bezug auf Informationssicherheit und Datenschutz und beleuchtet die potenziellen Auswirkungen auf persönliche Leben und Unternehmenssicherheit. Er erweitert unser Verständnis für die komplexe Beziehung zwischen Informationssicherheit und Online-Dating und betont die Notwendigkeit von digitalen Kompetenzen wie Information Security Bewusstsein und effektiver Kommunikation in diesem Zusammenhang.

Der vorliegende Beitrag ist in vier Abschnitte gegliedert: wir betrachten zunächst die Schnittstellen zwischen Online-Dating und SE, untersuchen anschließend in einer hermeneutischen Analyse spezifische Risiken und Betrugsmöglichkeiten im Online Dating, ehe wir die Ergebnisse unter Berücksichtigung interdisziplinärer digitaler Kompetenzen als Schutzschild diskutieren. Im Fazit gehen wir neben einer Zusammenfassung und Limitationen unserer Untersuchung auch auf zukünftige Forschungsbedarfe ein.

## 2 Theoretische Grundlagen: Erfolgreich im Informationsaustausch

Wir reden mit, durch und über Technik – so gut wie immer und überall, in einem digitalen Raum, der immer neue Abenteuer und Gefahren mit sich bringt. Online-Dating erfreut sich dabei großer Beliebtheit. Rund 77 % der 16–29-Jährigen haben damit bereits Erfahrung und von den 30–49-Jährigen immerhin zwei Drittel (Bitkom 2022). Im Zuge dessen werfen Online-Dating-Plattformen und -Apps, sowie die Etablierung von Cyberintimität neue Herausforderungen in Bezug auf Informationssicherheit und Datenschutz auf (Aretz et al. 2017; Farvid 2015; Gibbs et al. 2011; Phan et al. 2021). Insbesondere Praktiken wie SE, also Handlungen Anderer, die eine Person dazu beeinflussen, eine Aktion auszuführen, die möglicherweise nicht in ihrem besten Interesse liegt (Hadnagy 2011), stellen in diesem Kontext eine wachsende Bedrohung dar, da sie nicht nur das persönliche Leben der Menschen, sondern auch die Sicherheit von Unternehmen gefährden können. Mitarbeitys, die Opfer von SE werden, könnten gerade und besonders im ‚privaten halböffentlichen Raum' des Online-Datings unbewusst sensible Informationen preisgeben und damit Unternehmensnetzwerke gefährden (Buthelezi 2021; Hopkins 2016).

In diesem Kapitel betrachten wir anhand theoretischer Grundlagen, wo Social Engineering ansetzen kann und welche Betrugsmaschen im Online Dating durch SE besonders ermöglicht werden.

### 2.1 Kommunikationskonzepte

Hadnagy (2011) hebt im Kontext SE die besondere Bedeutung von Kommunikationskompetenzen hervor: für erfolgreiches SE sei ‚Meisterschaft in der Kommunika-

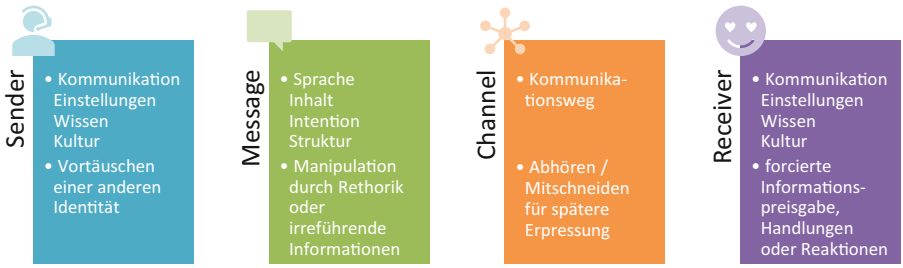


**Abb. 1** SMCR-Modell mit Manipulationsoptionen (nach Hadnagy 2011)

tion' nötig. Das spricht auch für eine genaue Betrachtung der Kommunikationssituation im Online-Dating per Chat: Ein passendes theoretisches Fundament dafür bietet das Berlo-Modell der Kommunikation (SMCR), das Sender, Message, Channel und Receiver als Kernelemente der Kommunikation beschreibt und den Kommunikationsprozess und die verschiedenen Faktoren erklärt, die ihn beeinflussen. Diese Elemente sind auch in der Dynamik des Online-Datings präsent und können manipuliert werden. Hier ein kurzer Überblick über die vier Hauptkomponenten und mögliche Manipulationen (Hadnagy 2011; Abb. 1):

- **Sender:** Die Person oder Einheit, die die Nachricht initiiert. In der Rolle des Sendys ist es wichtig, dass die Nachricht klar und verständlich formuliert ist. Das Vortäuschen einer anderen Identität, um Vertrauen aufzubauen, ist hier eine Option der Manipulation.
- **Message**: Die tatsächliche Nachricht, die übermittelt wird. Sie kann bei Online-Dating in Form von Text, Ton, Bild und Video erfolgen. Durch gezielte Rhetorik oder die Verwendung von irreführenden Informationen kann die Nachricht selbst manipuliert werden, um eine bestimmte Reaktion des Empfängys zu provozieren.
- **Channel**: Der Kommunikationsweg, durch den die Nachricht gesendet wird, z. B. ein Telefonat, eine E-Mail, eine Chatnachricht etc. Hier kommen technische Manipulationen wie Abhörmechanismen zum Tragen.
- **Receiver**: Die Person oder Einheit, die die Nachricht empfängt und interpretiert. Durch Social Engineering-Techniken kann das Empfängy manipuliert werden, bestimmte Informationen preiszugeben oder eine bestimmte Handlung auszuführen.

Ein weiteres Vorgehen ist Elicitation, welches vom FBI als das subtile Extrahieren von Informationen während eines scheinbar normalen und unschuldigen Gesprächs definiert wird (Federal Bureau of Investigation 2016). Dieses Konzept ist sowohl in SE als auch im Online-Dating relevant, da Menschen aus verschiedenen Gründen anfällig für Elicitation sind. Sie möchten als höflich, gut informiert und gebildet angesehen werden, reagieren positiv auf Lob und zeigen sich freundlich, wenn ihnen gegenüber Interesse oder Sorge gezeigt wird. Die Kunst der Konversation in SE, wie Hadnagy (2011) es formuliert, umfasst das Stellen der richtigen Menge an Fragen, natürliches Auftreten, ausreichende Vorbereitung auf das Gespräch und das richtige Maß an Aufmerksamkeit, wie z. B. aktives Zuhören. Diese Faktoren sind ebenso entscheidend im Kontext von Online-Dating, wo das Ziel häufig ist, eine persönliche Bindung herzustellen. Verschiedene Einflussfaktoren wie Reziprozität,

Verantwortung, künstliche Knappheit („playing hard to get“), Autorität, Verbindlichkeit und Konsens spielen ebenfalls eine Rolle für den erfolgreichen Austausch in beiden Kontexten. SE und Online Dating basieren also auf denselben Mechanismen, nur die Intentionen unterscheiden sich (Hadnagy 2011).

## 2.2 Scams

Bei Scams handelt es sich laut den Oxford Learners Dictonaries um „clevere und unehrliche Pläne zum Geldverdienen“ (Oxford University Press, 2023a) oder auch „Betrugsmaschen, um etwas, insbesondere Geld, von jemandem zu bekommen“ (Oxford University Press, 2023b). Eine einheitliche Taxonomie von Online-Scamming-Methoden konnte in einer Literatursuche einschlägiger Datenbanken (*Scopus, Google Scholar*) nicht gefunden werden, deshalb gehen wir hier auf Betrugsmaschen ein, die für unsere Untersuchung besonders relevant sind. Die Sicherheitsanbieter Kaspersky (2023) und Imam (2023) unterscheiden dabei folgende Varianten als häufige Formen des Online-Dating-Scams. In allen Fällen kann von einer Manipulation der Sendys ausgegangen werden, da diese sich meist als jemand anderes ausgeben, als sie sind. Darüber hinaus weist aber jede Form Besonderheiten der Manipulation auf.

### *2.2.1 Romance Scams*

Hierzu zählen insbesondere Military Romance Scams, bei denen Tätys Namen und Bilder echter Soldatys verwenden und nach einer Vertrauensbildung um finanzielle Unterstützung bitten. Oft werden keine direkten persönlichen Informationen abgefragt, sondern emotionaler Druck aufgebaut, um finanzielle Unterstützung zu erhalten. Besonders in den USA ist dieses Phänomen verbreitet und hat sogar zur Veröffentlichung einer Richtlinie durch die US-Armee geführt (Lange 2019). Sugar Daddy/Sugar Mommy Scams funktionieren ähnlich, wobei hier die Betrügys die Sehnsucht nach finanzieller Sicherheit, Gesellschaft und Luxus ausnutzen. Ein weiterer Unterbereich der Romance Scams sind die sogenannten Underage Scams. In diesen Fällen geben sich die Betrügys zunächst als volljährig aus, um eine virtuelle romantische oder sexuelle Beziehung zu initiieren. Nachdem intime Fotos oder Nachrichten ausgetauscht wurden, behaupten sie, minderjährig zu sein und drohen damit, die Kommunikation an die Öffentlichkeit oder die Behörden zu melden, falls nicht eine finanzielle ‚Entschädigung‘ geleistet wird. Bei dieser Form von Scam werden vor allem Empfängys manipuliert, um bestimmte Handlungen zu forcieren, dazu werden auch die Nachrichten so verfasst, dass emotionaler Druck aufgebaut wird (Imam 2023; Kaspersky 2023).

### *2.2.2 Intime Aktivitätsszenarien/Sextortion*

Diese Betrugsform führt dazu, dass Personen im Rahmen einer Videokonferenz intime Handlungen vornehmen, die später als Erpressungsmaterial dienen. Für diese Form des Scams wird der reale Name oder ein Social Media-Nickname benötigt und es werden Nacktbilder oder intime Momente aufgezeichnet. Die Initialisierung

erfolgt oft auf Plattformen, die auch von seriösen Nutzys frequentiert werden, allerdings sind auch spezifische, weniger vertrauenswürdige Apps und Websites im Umlauf. Ein markantes Element dieser Betrugsform ist, dass die Erpressung häufig über soziale Netzwerke erfolgt. Die Betrügys drohen damit, die aufgezeichneten Materialien an Freundys, Familie oder sogar Arbeitgebys der betroffenen Person zu senden, um sie zu zwingen, eine Zahlung zu leisten oder weitere Forderungen zu erfüllen. Durch die gezielte Nutzung von sozialen Netzwerken wird der psychische Druck auf die Opfer erhöht. Die Gefahr der sozialen Ächtung und des Reputationsverlusts lässt die Opfer den Forderungen der Betrügys wahrscheinlicher nachkommen. Bei Sextortion ist die Besonderheit die Kanalmanipulation durch das Abhören/Mitschneiden des Austausches (Imam 2023; Kaspersky 2023).

### *2.2.3 Investment- und Krypto-Betrug*

Diese Kategorie umfasst Betrugsformen, die sich über längere Zeiträume erstrecken und bei denen die Tätys eine emotionale Verbindung zu ihrem Opfer aufbauen. Nach dem Aufbau dieser emotionalen Verbindung werden vermeintlich lukrative ‚Investitionsmöglichkeiten' vorgestellt. In diesem Kontext werden häufig sensible Finanzinformationen wie Bankverbindungen, Kreditkarteninformationen, oder Informationen zu Kryptowallets abgefragt. Die Betrügys setzen hier oft auf komplizierten professionell klingenden Finanzjargon, um ihre Opfer zu täuschen. Sie versprechen hohe Renditen und nutzen den emotionalen Einfluss, um die Opfer zur Teilnahme an scheinbaren Investments oder Transaktionen zu bewegen. Manchmal werden sogar gefälschte Websites oder Apps erstellt, um die Legitimität der ‚Investitionsmöglichkeit' weiter zu untermauern. In einigen Fällen wird das Opfer dazu ermutigt, kleinere Summen zu investieren, die dann scheinbar hohe Renditen erzielen. Dies dient dazu, das Vertrauen des Opfers zu gewinnen und sie zur Investition größerer Summen zu motivieren, was schließlich zum Totalverlust der investierten Gelder führt. Aufgrund der zunehmenden Popularität von Kryptowährungen sind Betrugsformen in diesem Bereich besonders anfällig für Variationen und Anpassungen, was die Identifikation und Strafverfolgung erschweren. Die hohe Anonymität und die Unumkehrbarkeit von Kryptotransaktionen machen diese Betrugsform besonders riskant. Durch die Verwendung eines bestimmten Jargons werden die Nachrichten manipuliert, um schlussendlich langfristig das Empfängy zu bestimmten Handlungen zu überreden. Der Einsatz von Fake-Investions-Apps könnte auch als eine Kanalmanipulation betrachtet werden (Imam 2023; Kaspersky 2023).

### *2.2.4 Catfishing, Phishing, Malware und Identitätsdiebstahl*

In dem komplexen Spektrum von Online-Dating-Betrug nimmt das sogenannte ‚Catfishing' eine besondere Rolle ein. Dabei erstellen Betrügys gefälschte Profile, um eine emotionale Bindung zu ihren Opfern aufzubauen und deren Vertrauen zu gewinnen. Im fortgeschrittenen Stadium dieses Betrugsphänomens kann es vorkommen, dass Tätys die Herausgabe von Kontaktinformationen oder Zugang zu sozialen Medienprofilen fordern. Neben Catfishing gibt es sogar auf renommierten Online-Dating-Plattformen eine signifikante Prävalenz von Phishing-Attacken. Diese zie-

len darauf ab, sensible Login-Informationen durch gefälschte E-Mail- oder Code-Verifizierungsanfragen zu extrahieren. Darüber hinaus besteht das Risiko der Malware-Verbreitung durch betrügerische Links, die, obwohl sie normalerweise keine direkten persönlichen Informationen abfragen, dazu dienen, schädliche Software auf den Geräten der Opfer zu installieren. In Fällen von Identitätsdiebstahl erfragen Betrügys explizite persönliche Informationen unter dem Vorwand der Identitätsverifizierung, um die erlangten Daten für weitere betrügerische Aktivitäten zu nutzen. Hierbei werden insbesondere Name, Adresse, soziale Medienprofile und Kreditkarteninformationen abgefragt. Auch in diesen Fällen geht es um eine Kombination aus Empfängy- und Nachrichtenmanipulation um Informationen zu erhalten oder Handlungen zu provozieren (Imam 2023; Kaspersky 2023).

## 3 Hermeneutische Analyse: Dive into anything – oder besser nicht?

In diesem Kapitel stellen wir unsere hermeneutische Analyse vor, mit der wir die Verbindung zwischen Informationssicherheit und Online-Dating untersucht haben. Zunächst stellen wir die Methodik vor und gehen dann auf die Quellenauswahl und Analyse ein.

### 3.1 Methodik

In dieser Studie nutzen wir die hermeneutische Analyse als qualitative Forschungsmethode, um tiefgehendes Verständnis aus Texten zu gewinnen und ihre Bedeutungen zu interpretieren. Insbesondere bei Fragen zur Motivation und den Fähigkeiten der Tätys und Opfer im Zusammenhang mit Informationssicherheit und Online-Dating sind Erfahrungsberichte von unschätzbarem Wert. Diese persönlichen Einblicke können dazu beitragen, ein tieferes Verständnis für die zwischenmenschlichen Komponenten und Kompetenzen in diesem Kontext zu entwickeln, die oft von Statistiken und wirtschaftlichen Daten allein nicht erfasst werden. Somit trägt die hermeneutische Analyse dazu bei, die Lücke zwischen quantitativen Informationen und den tatsächlichen Erfahrungen und Beweggründen der Beteiligten zu schließen. Der Analyseprozess durchläuft mehrere Phasen. Zunächst erfolgt die Auswahl von wissenschaftlichen Quellen und Erfahrungsberichten aus den Bereichen Informationssicherheit und Online-Dating. Anschließend werden die ausgewählten Texte analysiert, um Schlüsselbegriffe, Muster und Zusammenhänge zu identifizieren. Die eigentliche Interpretation zielt darauf ab, über die Textoberläche hinauszugehen und tiefere Bedeutungen zu erschließen, wobei implizite Botschaften und Wertvorstellungen erkannt werden. Die gewonnenen Erkenntnisse werden dann in den sozialen, kulturellen und historischen Kontext eingebettet, um ein umfassendes Verständnis zu ermöglichen (Knassmüller und Vettori 2009).

### 3.2 Quellenauswahl

Auf der Suche nach geeigneten Erfahrungsberichten haben wir Beiträge auf Social-Media-Plattformen wie *Reddit, Twitter/X* oder *LinkedIn* in Betracht gezogen, da wir

die individuelle menschliche Ebene und Perspektive untersuchen möchten. Dabei erwies sich Reddit als besonders ergiebig, während andere Plattformen nur Einzelbeiträge (*Linkedin*) oder eher fragmentarische Diskussionen (*Twitter/X*) boten. Bei einer ersten allgemeinen Suche auf *Reddit* stellten sich die Subreddits */r/dating* (2023) und */r/Scams* (2023) als ergebnisreich heraus und wurden daraufhin gezielt durchsucht. Für */r/dating* wurden die Suchbegriffe „Social Engineering", „risks" und „scam" und für*/r/Scams* „Online Dating" verwendet. Unter den hunderten von Blogbeiträgen konnten wir eine sich wiederholende Art von Themen und Beitragsstrukturen identifizieren, so dass wir uns für 15 repräsentative und von *Reddit* als relevant gerankte Beiträge aus den letzten drei Jahren entschieden. In einer hermeneutischen Analyse wurden diese Blogbeiträge untersucht, zehn stammten aus dem Subreddit */r/Scams* und fünf aus dem Subreddit */r/dating*.

### 3.3 Analyse

Die Analyse konzentrierte sich auf verschiedene Aspekte der Beiträge, darunter Inhalt, Intention, Perspektive, Art des Scams und die Art der preisgegebenen Informationen. Die Beiträge wiesen unterschiedliche Inhalte auf: Acht Selbstberichte aus der Sicht der Betroffenen, ein Bericht aus der Perspektive einer „Täterin", zwei Meinungsstücke, ein Leitfaden und zwei Artikel, die sich auf Abwehrstrategien fokussieren. Folgende Schreibintentionen konnten identifiziert werden: Manche wollten Betrugsvorgänge öffentlich machen; dies geschah zum Teil aus kathartischen Gründen, aber sie sollten auch zur Warnung und Abschreckung dienen. Andere wiederum bündeln mehrere Erfahrungen, die in eine Guideline für sicheres Online-Dating konvergieren. Bedeutsam hervorzuheben ist aber auch, dass nicht alle Erfahrungsberichte eindeutig formuliert sind. Wie bei *Reddit* üblich, werden die Posts oft auch in Form von Fragen formuliert: Die Online-Community wird um Einschätzung gebeten, ob es sich bei dem geschilderten Fall um Scamming oder um echtes Dating handelt. Besonders aus letzteren Beiträgen spricht die Sehnsucht nach echter Verbindung, aber auch die Hoffnung, dass das, was zu gut um wahr zu sein scheint, doch vielleicht in diesem einen Fall wahr sein könnte. Abstrahiert betrachtet, erkennen wir hier eine große Unsicherheit im Umgang mit Chatsprache, was ein wichtiger Ansatzpunkt für entsprechende Weiterbildung in diesem Bereich sein könnte, aber auch ein grundlegendes Bewusstsein für die Risiken des Online-Datings. Ein besonderer Ausreißer war ein Erfahrungsbericht aus Täterinnenperspektive, der von einer kurzfristigen Tätigkeit im Romance Scamming erzählt und Einblicke in die Existenz von Fake-Profilen gibt, die von den Plattformbetreibys selbst bespielt werden, um mehr Umsatz zu generieren. Weitere Berichte aus Täty-Perspektive wären gerade für die Entwicklung von Abwehrstrategien sicherlich hilfreich, allerdings sind dazu bislang nur wenige (öffentlich) verfügbar.

Neben Romance-Scams wurden vor allem Investment- und Underage-Scams beschrieben. An Informationen wurden neben privaten Kontaktdaten und Fotos vor allem Finanzinformationen und in einem Fall sogar Passdaten weitergegeben. Positiv zu erwähnen ist das grundsätzliche Bewusstsein, dass es im Online-Dating Gefahren gibt und die Bereitschaft, Erlebtes als Warnung zu teilen oder sich abzusichern, ehe man Risiken eingeht. Allerdings ist bei einer Community-Plattform wie

*Reddit* davon auszugehen, dass die 57 Mio. Reddit-Usys eine erhöhte Bereitschaft zeigen, ihre Meinungen und Erfahrungen zu teilen und weniger online-involvierte Menschen hier angreifbarer sind. Die Altersgruppe der 18–49-Jährigen sollte aber auch hier einen Hauptteil der Nutzys ausmachen (Reddit 2023). Gleichzeitig ist *Reddit* ein anonymes Forum; ein Bekenntnis zum Opfer eines Scams geworden zu sein, fällt sicherlich gerade innerhalb eines Unternehmens weniger leicht.

## 4 Diskussion: Mit digitalen Kompetenzen Bewusstsein für die eigenen Schwächen schaffen

Im Kontext digitaler Interaktionen zeigen diese verschiedene Betrugsmethoden ein zunehmend komplexes und nuanciertes Risikoprofil für Einzelpersonen und ihre Arbeitgebys. Romance Scams, etwa in Form von Military Romance oder Sugar Daddy/Mommy Scams, resultieren primär in finanziellen und emotionalen Risiken für die Betroffenen. Diese Scams könnten, abgesehen von den offensichtlichen finanziellen Verlusten, psychologischen Stress erzeugen, der sich negativ auf die Arbeitsleistung auswirkt. Organisationen könnten insofern indirekt betroffen sein, da der emotional belastete Zustand der Mitarbeitys zu einer reduzierten Produktivität oder erhöhten Anfälligkeit für andere Sicherheitsrisiken führt. Im Bereich der Sextortion oder der intimen Aktivitätsszenarien liegt das Risiko nicht nur in der direkten finanziellen Erpressung, sondern auch in der potenziellen sozialen Ächtung und dem Reputationsverlust, der durch die Veröffentlichung kompromittierender Materialien entstehen kann. Organisationen sind hier ebenfalls gefährdet, insbesondere wenn kompromittierende Inhalte in einem Kontext veröffentlicht werden, der den professionellen Ruf der Organisation beeinträchtigen könnte oder die Betroffenen eine sensible Position in der Organisation innehaben. Bei Investment- und Krypto-Betrug gehen die Risiken weit über finanzielle Verluste hinaus. Die psychologischen Auswirkungen des Betrugs und des damit verbundenen Vertrauensverlustes könnten die Arbeitsleistung negativ beeinflussen. In extremen Fällen, in denen Mitarbeitys Zugang zu Unternehmensfinanzen haben, könnten Betrügys sogar versuchen, diesen Zugang für illegale Transaktionen zu nutzen. Schließlich verändern Catfishing, Phishing, Malware und Identitätsdiebstahl die Risikolandschaft sowohl für Einzelpersonen als auch für Organisationen: Neben dem offensichtlichen Risiko des Identitätsdiebstahls oder dem Verlust sensibler Informationen können schädliche Software und Phishing-Angriffe die Cyber-Sicherheitsinfrastruktur einer Organisation kompromittieren, insbesondere wenn Mitarbeitys berufliche Geräte für persönliche Zwecke nutzen (Phan et al. 2021).

Besonders im LGBTQIA+-Bereich, der lesbische, schwule, bisexuelle, trans, queere, inter, asexuelle und weitere Identitäten umfasst, gibt es spezifische zusätzliche Risiken, wie beispielsweise Fremdouting als Erpressungsfaktor. Eine Falschnachricht, die mehrfach von Zeitungen aufgegriffen wurde, ist die Überlegung, dass die App *Grindr*, die für die Anbahnung (auch) spontaner sexueller Kontakte schwuler Menschen konzipiert ist, all jene Legislatorys outen könnte, die bei der Schaffung homophober Gesetze mitstimmen würden. Dass dies, obwohl das nie so geschehen ist, dennoch so ein gewaltiges Medienecho hervorgerufen

hat, verdeutlicht die besondere Relevanz der Folgen des Fremdoutings (Czopek 2023). Standortbasierte Dating-Apps wie *Grindr* oder *GayRomeo* werden manchmal auch zum Aufspüren nicht-heterosexueller Menschen verwendet, um sie gezielt attackieren oder enttarnen zu können (Kelleher 2023).

Die heutige digitale Ära ist geprägt durch das rasante Zusammenwachsen von privaten und beruflichen Sphären. Diese Veränderung ermöglicht eine Fülle neuer Kommunikationsmöglichkeiten, zieht aber gleichzeitig besonders in der Wechselbeziehung zwischen Individuen und Organisationen komplexe Risiken nach sich. Beispielsweise können Aktivitäten auf Online-Dating-Plattformen wie *OKCupid, Grindr, Tinder* oder *Parship*, wenn nicht sorgfältig gehandhabt, unerwünschte Konsequenzen für das Image und die Sicherheit einer Organisation haben. Einmal geteilte Daten könnten von versierten Akteurys als Hebel gegen Organisationen genutzt werden, indem sie beispielsweise Verknüpfungen zwischen dem Privatleben eines Mitarbeitys und internen Unternehmensdaten herstellen (Nandwani und Kaushal 2018; Norcie et al. 2013). Es zeigt sich, dass SE und Online-Dating auf bedenkliche Weise interagieren können, insbesondere, wenn die Kommunikation manipuliert wird, um persönliche Informationen zu extrahieren.

Um sich in diesem komplexen digitalen Ökosystem effektiv bewegen zu können, reicht technisches Wissen alleine also nicht mehr aus. Ein tieferes Verständnis der Dynamiken und Einflussfaktoren dieser Interaktion ist daher für präventive Maßnahmen unerlässlich, nicht nur Kommunikation und kritisches Denken und Problemlösungsvermögen sind als Kompetenz gefragt.

Hier kommt Information Security Awareness (ISA) ins Spiel, ISA fokussiert die Erkennung und Reaktion auf potenzielle Sicherheitsbedrohungen, wie Phishing oder Datenlecks, und schult Individuen darin, stets wachsam und vorsichtig zu sein (Hänsch und Benenson 2014). In diesem Zusammenhang ist das kritische reflektierte Denken, unterstützt durch ausgeprägte Sprach- und Kommunikationskompetenzen, ein unerlässlicher Pfeiler der digitalen Sicherheit, um die Authentizität in Online-Interaktionen ständig zu hinterfragen (Gibbs et al. 2011). Dabei geht es uns hier um einen ganzheitlichen digitalen Kompetenzbegriff. Neben Wissen und Fähigkeiten sind auch individuelle Werte und Einstellungen von großer Bedeutung (Binkley et al. 2012; Vuorikari et al. 2022). Dazu gehört das Entwickeln eines ausgeprägten persönlichen Sicherheitsbewusstseins und eines Verständnisses für die Bedeutung der Informationen, die preisgegeben werden. Hadnagy (2011) betont, dass bei der Angriffserkennung und dem Entwickeln von Skripten, Verhaltensweisen und Prozessen, die das Risiko minimieren „jede Person engagiert sein muss“: Wir brauchen Consent und nicht nur Compliance. Consent bedeutet aktive Zustimmung und vereinigt innere Einstellung mit äußerem Handeln im Gegensatz zur Compliance, dem bloßen Einhaltung von Regeln. Dies gewinnt besonders im Online-Dating an Bedeutung, wo persönliche und berufliche Informationen in Beziehung stehen können. Die Berücksichtigung von Consent hat daher weitreichende Implikationen für Datenschutz und Kommunikation. Ein Fokus auf Zustimmung stärkt Privatsphäre und Vertrauen, beeinflusst Kommunikation positiv und schafft eine Basis für transparente, vertrauensvolle Interaktionen – gerade, wenn persönliche und berufliche Sphären ineinander übergehen (Aretz et al. 2017; Hadnagy 2011; Haucke und Pokoyski 2018). Diese Aspekte sind nicht nur für Individuen, sondern auch für die Wider-

standsfähigkeit oder Resilienz in einem breiteren Kontext von Bedeutung. Resilienz in der digitalen Welt heißt, sich effektiv an Veränderungen und Herausforderungen anzupassen, Risiken zu minimieren und aus Erfahrungen zu lernen und ist damit eine Folge des erfolgreichen Erwerbs digitaler Kompetenzen.

In der digitalen Welt erfordert das sichere Navigieren somit den Aufbau interdisziplinärer Kompetenzen, insbesondere ISA, kritisches Denkvermögen sowie Sprach- und Kommunikationskompetenzen (Finster et al. 2023). Daraus ergibt sich für uns ein ganzheitliches digitales Kompetenzprofil, in dessen Mittelpunkt ISA steht, die als zentraler Schutzwall gegen digitale Bedrohungen fungiert. Verstärkt wird dieser Schutzwall durch eine Reihe von Schlüsselkomponenten, die zusammen ein umfassendes und wirksames System bilden. Zunächst bildet ein fundiertes technologisches Verständnis die Basis. Dies umfasst nicht nur Kenntnisse über aktuelle Technologien und Sicherheitsprotokolle, sondern auch ein Verständnis für die Funktionsweise digitaler Systeme und die damit verbundenen Risiken (Kirchherr et al. 2018). Ergänzt wird dieses technische Fundament durch kritisches Denken. Es ermöglicht Individuen, Informationen und Situationen sorgfältig zu analysieren, potenzielle Risiken zu erkennen, fundierte, reflektierte Entscheidungen zu treffen und die direkten als auch die indirekten Konsequenzen ihres Handelns im digitalen Raum zu berücksichtigen (Vuorikari et al. 2022). Eine weitere Komponente ist die Kommunikationsfähigkeit, um sich klar und effektiv ausdrücken zu können. Eng verbunden mit kritischem Denken und der Kommunikation ist das Problemlösungsvermögen. In einer Welt, die ständig neuen digitalen Herausforderungen gegenübersteht, ist die Fähigkeit, Probleme systematisch zu identifizieren, zu analysieren und Lösungen zu entwickeln, von großer Bedeutung. Dies umfasst nicht nur technische Lösungen, sondern auch strategische Ansätze, um digitale Risiken zu minimieren und die Resilienz zu stärken (Vuorikari et al. 2022). Abgerundet wird das Profil durch Consent und (Selbst-)Vertrauen, die vor allem in der Wertedimension unseres Kompetenzverständnisses vertreten sind.

Digitale Kompetenzen fungieren hier also nicht nur als ein wesentlicher Schutzwall gegen digitale Risiken wie Datenverlust und Scams, sondern sind auch ein integraler Bestandteil der individuellen und organisationalen Resilienz. Für die Förderung dieser Kompetenzen, wie ISA, Kommunikationsfähigkeit und kritischem Denk- und Problemlösungsvermögen, ist ein mehrdimensionaler Ansatz notwendig, der neben informellem Lernen auch berufliche Weiterbildung und individuelle Motivation erfordert. Strategien wie Gamification oder projektbasiertes Lernen können dazu beitragen, die Motivation und das Engagement für den Erwerb digitaler Fähigkeiten zu erhöhen (Grogorick et al. 2019; Haucke und Pokoyski 2018; Hessler 2018).

## 5 Fazit und Ausblick

Im Rahmen dieses Beitrags wurde der ganzheitliche Kompetenzaufbau als entscheidende Maßnahme für sichere(s) Daten in der digitalen Welt, insbesondere im Kontext von Online-Dating, beleuchtet. Dabei wurde deutlich, dass technische Sicherheitsmaßnahmen wie Firewalls allein unzureichend sind, um gegen ‚Cupids Pfeile' – die


**Abb. 2** Kernerkenntnisse des Beitrags

vielfältigen menschenzentrierten Risiken wie SE – geschützt zu sein. Interessanterweise zeigen sich klare Parallelen zwischen den Herausforderungen des Online-Datings und denen von SE. In beiden Szenarien kann die Glaubwürdigkeit des Gegenübers ein erhebliches Risiko darstellen, das nur durch ausgeprägte kognitive und kommunikative Fähigkeiten gemildert werden kann.

Obwohl diese Studie wertvolle Einblicke in die Themen Informationssicherheit und Online-Dating bietet, ist es wichtig zu beachten, dass die Ergebnisse aufgrund der subjektiven Natur der untersuchten Texte, als auch der angewandten Methodik, der begrenzten Auswahl qualitativer Texte und der damit verbundenen begrenzten Generalisierbarkeit auf andere Online-Dating-Kontexte und Populationen interpretiert werden sollten.

Wir argumentieren, dass ein ganzheitlicher Ansatz erforderlich ist, der sowohl ISA als auch kritische Denk- und Kommunikationsfähigkeiten umfasst und in den individuellen und organisatorischen Lernprozess integriert werden sollte. Sowohl in der Forschung als auch in der Praxis sind die Entwicklung von geeigneten Lerneinheiten von hoher Relevanz. Dabei könnten folgende Themen betrachtet werden: Online-Kommunikation mit Best Practices für die Authentifizierung von Gesprächspartnern, gängige SE-Taktiken und die Vermeidung von Oversharing persönlicher oder geschäftskritischer Informationen. Ebenso Methoden zur Identifizierung und Abwehr von betrügerischen Aktivitäten, wie die Analyse von Verhaltensmustern, die auf Scamming oder Catfishing hindeuten könnten, sowie die Sensibilisierung für gängige Betrugsmaschen wie den Romance Scam (Kaspersky 2023; Koegler 2017). Der Ansatz interaktiver Formate, wie Fallstudien, Rollenspiele oder Simulationen, um das Erlernte zu vertiefen und die Teilnehmys aktiv im Lernprozess zu involvieren sollte ebenfalls weiterhin untersucht werden.

Während bisher viel Forschung darauf ausgerichtet ist, „wie“ digitale Systeme und Daten gesichert werden können, sollte zukünftige Forschung mehr Gewicht auf das „Warum“ legen, insbesondere im Kontext von Consent. Anstatt sich nur auf die Einhaltung von Regeln zu konzentrieren (Compliance), könnte zukünftige Forschung untersuchen, wie ein tiefergehendes Verständnis für die Bedeutung von aktiver Zustimmung (Consent) in der digitalen Interaktion eingebaut werden kann. Dafür sollten wir auch die Frage stellen: „Warum ist Sicherheit für mich überhaupt

von solch grundlegender Bedeutung?“ Das könnte weitreichende Implikationen für Resilienz und Vertrauen in der digitalen Welt haben.

Zusammenfassend macht dieser Beitrag deutlich, dass für effektive Sicherheit in der digitalen Welt ein umfassender, menschenzentrierter Ansatz erforderlich ist. Es hebt hervor, dass interdisziplinäre Kompetenzen – weit über technische Fähigkeiten hinaus – unabdingbar sind, um sich gegen die komplexen und vielschichtigen Herausforderungen des digitalen Zeitalters zu wappnen. In Abb. 2 haben wir unsere Kernerkenntnisse der verschiedenen Kapitel nochmal zusammengefasst. Nur durch diese ganzheitliche Betrachtung können wir hoffen, sowohl individuell als auch organisational gegen die Risiken des digitalen Zeitalters gerüstet zu sein. Ein bewusster Umgang mit digitalen Gefahren ist wie die richtige Verhütung: Nicht nur sicher, sondern macht Daten auch vertrauensvoller und facettenreicher.

**Funding** Open Access funding enabled and organized by Projekt DEAL.



## Literatur

/r/dating (2023) Reddit [Reddit Post]. https://www.reddit.com/r/dating/. Zugegriffen: 30. Aug. 2023

/r/scams (2023) Reddit [Reddit Post]. https://www.reddit.com/r/scams/. Zugegriffen: 30. Aug. 2023

Aretz W, Gansen-Ammann D-N, Ehrenberg K, Musiol A (2017) Date me if you can: Ein systematischer Überblick über den aktuellen Forschungsstand von Online-Dating. Z Sex-Forsch 30:7–34. https://doi.org/10.1055/s-0043-101465

Binkley M, Erstad O, Herman J, Raizen S, Ripley M, Miller-Ricci M, Rumble M (2012) Defining twenty-first century skills. In: Griffin P, McGaw B, Care E (Hrsg) Assessment and teaching of 21st century skills. Springer Netherlands, Dordrecht, S 17–66 https://doi.org/10.1007/978-94-007-2324-5_2

Bitkom (2022) Zukünftige Bedrohungen für die IT-Sicherheit in der deutschen Industrie 2022. https://de.statista.com/statistik/daten/studie/1014570/umfrage/umfrage-zu-den-zukuenftigen-bedrohungen-fuer-die-it-sicherheit-in-deutschland/. Zugegriffen: 25. Aug. 2023

BÎZGĂ A (2020) 5 Dating Apps Leak More than 1 Million User Profiles and Sensitive Information. https://www.bitdefender.com/blog/hotforsecurity/5-dating-apps-leak-more-than-1-million-user-profiles-and-sensitive-information/. Zugegriffen: 10. Aug. 2023 (Bitdefender Website)

BÎZGĂ A (2023) Unprotected dating database exposes data of 2.3 million users. https://www.bitdefender.com/blog/hotforsecurity/unprotected-dating-database-exposes-data-of-2-3-million-users/. Zugegriffen: 25. Aug. 2023 (Bitdefender Website)

Buthelezi P (2021) Living, loving and learning online: raising awareness of the new normal and its security considerations. In: 2021 International Conference on Computational Science and Computational Intelligence (CSCI), S 1444–1448 https://doi.org/10.1109/CSCI54926.2021.00287

Capurro R (2010) Digital hermeneutics: an outline. Ai Soc 25(1):35–42. https://doi.org/10.1007/s00146-009-0255-9
Cimpanu C (2021) Hacker leaks data of 2.28 million dating site users. https://www.zdnet.com/article/hacker-leaks-data-of-2-28-million-dating-site-users/. Zugegriffen: 10. Aug. 2023 (ZDNET Website)
Czopek M (2023) Grindr didn't threaten to identify Republican politicians who use its app. https://www.politifact.com/factchecks/2023/mar/28/instagram-posts/grindr-didnt-threaten-to-identify-republican-polit/. Zugegriffen: 31. Aug. 2023
Farvid P (2015) Cyber intimacies. In: The Wiley-Blackwell encyclopedia of gender and sexuality studies https://doi.org/10.1002/9781118663219.wbegss159
Federal Bureau of Investigation (2016) Elicitation techniques. U.S. Department of justice. https://www.fbi.gov/file-repository/elicitation-brochure.pdf/view
Finster R, Grogorick L, Kronschläger T, Robra-Bissantz S (2023) Information Security Awareness: Die kompetente Essenz für eine gesicherte digitale Zukunft. GeNeMe 2023.
Gibbs J, Ellison N, Lai C-H (2011) First comes love, then comes Google: an investigation of uncertainty reduction strategies and self-disclosure in online dating. Communic Res. https://doi.org/10.1177/0093650210377091
Grogorick L, Finster R, Robra-Bissantz S (2019) Digitales Lernen fesselnd gestalten: Motivation beim Lösen verschiedener Aufgabentypen, S 282–291
Hadnagy C (2011) Social engineering: the art of human hacking. Wiley, Indianapolis
Hänsch N, Benenson Z (2014) Specifying IT security awareness. In: 2014 25th International workshop on database and expert systems applications. IEEE, S 326–330 https://doi.org/10.1109/DEXA.2014.71
Haucke A, Pokoyski D (2018) „Ich bin der Fehler"—Schuld, Scham, Viktimisierung bei Social Engineering. Take Aware 01:20–24
Hessler S (2018) „Bei IT-Security Themen höre ich immer weg."—Sensibilisierung durch Linguistic Awareness. Take Aware 01:20–24
Hopkins T (2016) Online dating: a social engineer's playground. https://www.linkedin.com/pulse/online-dating-social-engineers-playground-hopkins-cissp-ceh-ccna-/. Zugegriffen: 10. Aug. 2023
Imam S Grindr scams that you should be aware of. https://www.purevpn.com/blog/grindr-scams/ (Erstellt: 22. Mai 2023). Zugegriffen: 10. Aug. 2023
Kaspersky Online dating scams and how to avoid them. https://www.kaspersky.com/resource-center/threats/beware-online-dating-scams (Erstellt: 24. Apr. 2023). Zugegriffen: 10. Aug. 2023
Kelleher P Police using apps to lure, arrest and abuse LGBTQ+ people, report finds. https://www.thepinknews.com/2023/02/22/police-grindr-apps-middle-east-africa-lgbtq/ (Erstellt: 22. Febr. 2023). Zugegriffen: 31. Aug. 2023 (von PinkNews | Latest lesbian, gay, bi and trans news | LGBTQ+ news website)
Kirchherr J, Klier J, Lehmann-Brauns C, Winde M (2018) Future Skills: Welche Kompetenzen in Deutschland fehlen, S 11
Knassmüller M, Vettori O (2009) Hermeneutische Verfahren. In: Buber R, Holzmüller HH (Hrsg) Qualitative Marktforschung: Konzepte – Methoden – Analysen. Gabler, Wiesbaden, S 299–317 https://doi.org/10.1007/978-3-8349-9441-7_19
Koegler S Learn to love online dating security. https://securityintelligence.com/learn-to-love-online-dating-security/ (Erstellt: 14. Febr. 2017). Zugegriffen: 24. Aug. 2023 (Security Intelligence Website)
Lange K (2019) These social media scams affect the military. https://www.defense.gov/News/News-Stories/Article/article/1921988/these-social-media-scams-affect-the-military/. Zugegriffen: 1. Dez. 2023 (U.S. Department of Defense website)
Nandwani M, Kaushal R (2018) Evaluating user vulnerability to privacy disclosures over Online dating platforms. In: Barolli L, Enokido T (Hrsg) Innovative mobile and Internet services in ubiquitous computing. Springer, Cham, S 342–353 https://doi.org/10.1007/978-3-319-61542-4_32
Norcie G, De Cristofaro E, Bellotti V (2013) Bootstrapping trust in online dating: social verification of online dating profiles. In: Adams AA, Brenner M, Smith M (Hrsg) Financial cryptography and data security. Springer, Berlin, Heidelberg, S 149–163 https://doi.org/10.1007/978-3-642-41320-9_10
Oxford University (2023a) scam_1 noun—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com. In: Oxford Learner's Dictionaries. Oxford University Press, (https://www.oxfordlearnersdictionaries.com/definition/english/scam_1)
Oxford University (2023b) scam_2 verb—Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com. In: Oxford Learner's Dictionaries. Oxford University Press, (https://www.oxfordlearnersdictionaries.com/definition/english/scam_2)

Păduraru R, Moraru A-V, Barbu V-A (2022) Online dating dynamics during COVID-19. Rev Rom Sociol 33(3/4):205–223
Phan A, Seigfried-Spellar K, Choo K-KR (2021) Threaten me softly: a review of potential dating app risks. Comput Hum Behav Rep 3:100055. https://doi.org/10.1016/j.chbr.2021.100055
Reddit (2023) Reddit—about. https://www.redditinc.com/. Zugegriffen: 31. Aug. 2023
Scheuermann L, Kroeze JHH (2017) Digital humanities and information systems: innovating two research traditions. Twenty-third Americas Conference on Information Systems.
Statista (2023) Dating Services—Anzahl der Online-Nutzer in Deutschland 2030. https://de.statista.com/prognosen/642366/dating-services-anzahl-der-online-nutzer-in-deutschland. Zugegriffen: 25. Aug. 2023
Vuorikari R, Kluzer S, Punie Y (2022) DigComp 2.2: the digital competence framework for citizens—with new examples of knowledge, skills and attitudes https://doi.org/10.2760/115376
Wijaya L, Taiwanella EU, Afrianto RA, Kuncoro A, Hidayat Z (2022) Harmless cyberstalking, case of onlinedaters. J Theor Appl Inf Technol 100(20):6233–6244