Interacting with Computers, 2023, **00**, 1–16
https://doi.org/10.1093/iwc/iwad048
Article

Tainted Love: a Systematic Literature Review of Online Romance Scam Research

Alexander Bilz, Lynsay A. Shepherd* and Graham I. Johnson

School of Design and Informatics, Division of Cyber Security, Abertay University, Dundee DD1 1HG, United Kingdom
*Corresponding author: lynsay.shepherd@abertay.ac.uk

Abstract

Romance scams involve cybercriminals engineering a romantic relationship on online dating platforms for monetary gain. It is a cruel form of cybercrime whereby victims are left heartbroken, often facing financial ruin. We characterize the literary landscape on romance scams, advancing the understanding of researchers and practitioners by systematically reviewing and synthesizing contemporary qualitative and quantitative evidence. The systematic review establishes influencing factors of victimhood and explores countermeasures for mitigating romance scams. We searched 10 scholarly databases and websites using terms related to romance scams. The methodology followed the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) guidelines: a total of 279 papers were screened. One hundred seven papers were assessed for eligibility, and 53 were included in the final analysis. Three main contributions were identified: common profile features and techniques used by romance scammers, countermeasures for mitigating romance scams and factors predisposing an individual to become a scammer or a victim. Despite a growing corpus of literature, the total number of empirical or experimental examinations remained limited. The paper concludes with avenues for future research and victimhood intervention strategies for practitioners, law enforcement and the industry.

RESEARCH HIGHLIGHTS

- A systematic review of online romance scams was conducted using the PRISMA methodology (Page *et al.*, 2021).
- Studies exploring the socio-demographic and psychological factors associated with scammers and victims were limited.
- Few empirical studies focused on the interaction between scammers and victims on messaging platforms.
- Collaboration between researchers, online platform providers and law enforcement is needed to address the issue of romance scams in the future.

Keywords: romance fraud; romance scams; cybercrime; human–computer interaction; systematic review; online dating

1. INTRODUCTION AND BACKGROUND

Romance scams are a form of social engineering that emerged in the early 2000s. Scammers create fraudulent profiles on dating platforms and strike up a relationship with their potential victims, with the end goal of conning individuals out of money. The resulting damage to victims of romance scams can be devastating; in addition to monetary loss, there is a substantial emotional impact on users desperate for companionship. Romance scams have become a growing problem, exacerbated by the COVID-19 pandemic, alongside other cybercrimes (Kemp *et al.*, 2021; Lallie *et al.*, 2021).

The execution of a romance scam typically begins with the scammer creating an attractive profile on a dating site or social media platform that replicates a celebrity or figure of authority or portrays an entirely fictitious identity (Sorell and Whitty, 2019). Once the profile has been created, the scammer reaches out to potential victims and lures them into an online conversation (Rege, 2009). Soon after communication has been established, the conversation between the perpetrator and the target is moved to another channel, such as instant messaging, SMS or email, outside the dating platform's control (Whitty, 2013a). The grooming phase follows, establishing a strong, well-trusted, emotional relationship before the victim is asked for financial support to overcome a tragic or desperate situation (Whitty, 2013). Reasons for the monetary requests may include inheritance fees, plane tickets, visa fees, family emergencies or presents (Whitty, 2013a; Cross and Holt, 2021). The scam usually ends several months or years after the initial contact, when the victim runs out of money or realizes they have been targeted (Cross and Blackshaw, 2015; Cross, 2016a).

A key difference between romance scams and other financial dating scams lies in the *modus operandi*. Romance scammers, as opposed to gold diggers, never seek to establish a relationship, even temporarily, but merely use the perception of a relationship to take advantage of the victim (Whitty, 2013; Thompson, 2016). Victims of romance scams typically experience a 'double hit' because they simultaneously lose significant financial means and are emotionally wounded due to the loss of the relationship (Whitty and Buchanan, 2012). Even though individual financial losses can be substantial, with recent reports as high as £300 000 in one case (BBC, 2021), emotional consequences have

Received: March 1, 2023. **Revised:** September 12, 2023. **Accepted:** September 26, 2023

been estimated to be even more impactful than the perceived consequences of the financial loss (Modic and Anderson, 2015).

Despite the impact of romance scams on society and the damage caused to individuals, few in-depth reviews have been conducted to synthesize and reflect on the literature in the field. Lazarus *et al.* (2023) recently published work introducing a systematic review of romance fraud. However, the work is presented through an economic criminology lens and focuses on underpinning theories and proposed models, with limited consideration of technological advances concerning countermeasures to identify romance fraud and prevent further victimization.

The work presented in our paper is framed from a human-centred security perspective. It seeks to explore common ways romance scams are executed, the socio-demographic and psychological traits of those involved and countermeasures to reduce instances of such crime in the future. Therefore, the objective was to answer three research questions that are pertinent to understanding romance scams:

- RQ1: What is the state-of-the-art approach for profiling, describing and characterizing romance scams?
- RQ2: What underlying socio-demographic and psychological factors enable and foster the execution of a romance scam?
- RQ3: What countermeasures and mitigation techniques have been proposed to help identify romance scams, thus limiting the risk of victimization?

Our research starts by analysing existing literature based on meta-level information, such as the type of literature (journal articles, conference proceedings or theses), the main contributions in line with three research questions and authorship to establish an overview of the current literary landscape. Subsequently, the papers and their findings are presented, critically appraised and contrasted to identify commonalities and discrepancies. This paper closes with an extensive discussion of gaps in the current knowledge and directions for future research.

Although the terms ‘scam’ and ‘fraud’ are often used interchangeably in existing studies, we use ‘scam’ consistently throughout our paper, unless we are citing a term used by an author. Banking institutions such as HSBC (2023) state that a scam ‘*involves you making or authorizing the payment yourself*’, providing romance scams as a specific example. In contrast, they define fraud as ‘*suspicious activity on your account that you didn’t know about and didn’t authorize*’. Both Barclays (2023) and the Financial Ombudsman Service (2023) in the UK also refer to the term ‘romance scam’; therefore, we have adopted the same terminology.

2. METHODOLOGY

The following section presents the methodology for conducting this systematic review of romance scams.

2.1. Protocol

We adopted the Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) technique and protocol to search, collect and analyse relevant literature (Page *et al.*, 2021). PRISMA provides a well-structured approach for reporting the work conducted and the findings of systematic reviews. Our study aimed to provide a state-of-the-art view of the published literature on romance scams, including contributions from different fields; thus, advanced statistical data processing was not feasible. Therefore, the following sections present our adaption of the PRISMA technique while closely adhering to the relevant checklist’s items, such as the specification of the eligibility criteria, search strategy and data collection process.

2.2. Eligibility criteria

The primary inclusion criterion was that papers had to involve empirical research or experimental examinations that profiled romance scams (including demographics), characterize the psychological aspects involved or examine countermeasures and mitigations. In addition, literature considered acceptable were peer-reviewed journal articles and book chapters, conference proceedings, theses and dissertations. The choice to include grey literature (defined as electronic and print literature that institutions produce outside of the control of commercial publishers (Auger, 1998) was deliberate because it helped create a comprehensive picture of the current research on romance scams. The search was limited to English-language papers available through the University’s subscriptions.

Several articles were omitted because they featured unclear research methodologies or focused on other types of online dating scams (e.g. identity fraud or e-whoring), which lack the double-hit effect unique to romance scams. Also excluded were articles whose primary research was only weakly related to romance scams. In cases where the same findings were published twice (e.g. as a conference paper and journal article) as separately standing works, the less extensive paper was excluded.

2.3. Information sources

Existing romance scam research features contributions from several domains using varied research methods. To reflect the diverse and disparate nature of the contributions in this review, a wide range of information sources were searched for articles, including journal articles, conference proceedings, theses and dissertations and book chapters. The bibliographic search was conducted in October 2021 and updated with recently published articles in April 2023. It explored the following reputable and renowned publication databases: Scopus, PsycInfo, PsycArticles, Medline, Web of Science, ProQuest, ACM Digital Library, IEEE Digital Library, ScienceDirect and PubMed. Two additional sources were also used. Firstly, the reference lists of publications included in the full-text review were screened for relevant inclusions. Secondly, a Google Scholar alert was created to obtain recently published literature.

2.4. Search strategy and selection process

The first step consisted of constructing a search string and querying the information sources for articles capable of answering the research questions outlined in Section 1. Due to the research questions’ breadth and the methodology’s exploratory nature, the search query was designed to capture the largest possible body of relevant literature. Therefore, the search query included an extensive range of euphemisms and synonyms commonly associated with romance scams and refrained from using Boolean conditions to narrow down the number of articles at the time of the search. Although it is acknowledged that this can lead to a larger number of irrelevant articles being returned, it was considered preferable over prematurely excluding articles from the overall scarce corpus of literature. The construction of the search query also meant it could be used across all databases without considering the unique technical limitations of the individual database searches, such as processing of nested conditions and the number of supported search terms.

The final search query was as follows: *‘romance fraud’ OR ‘romance scam’ OR ‘sweetheart swindle’ OR ‘dating scam’ OR ‘love scam’ OR ‘relationship fraud’ OR ‘relationship scam’*.

Table 1. Data items collected from the selected studies.

Metadata	**Information on the article: title, year, literature type (e.g. journal, conference paper, thesis), venue (name of the journal and conference), research field (e.g. computer science, linguistics, psychology, criminology) and Google Scholar citations** **Information on the authors: full name, affiliation (typically the university or research institute), location (country) and profession (e.g. academic, law enforcement, industry professional** **Funding information** **Contribution type: exploring/proposing profiles, methodologies, countermeasures, legal aspects or discussion of open issues** **Study setup: study objectives, research methodology (e.g. qualitative study, quantitative study, mixed study design, experimental), sample size, sample characteristics, country of research and approaches for gathering data (e.g. interviews, questionnaires, online forums, social media sites)**
Findings	The perspective of the study (e.g. victims, scammers, website operators) Applied theories and frameworks Main findings: approaches for profiling romance scams and their progression, demographics and psychological characteristics of scammers and victims and countermeasures and mitigations Contributions of the article

The selection process was designed with scientific scrutiny and reproducibility in mind. Therefore, all process steps were distinguished into separate tasks, and all intermediates and outcomes were documented. At first, the publication databases were searched using the final search query. Identified articles were imported into Covidence (2022), where the two-staged study selection was performed. The article's title and abstracts were screened in the first stage according to the inclusion and exclusion criteria. Eligible articles were screened once more based on their full text.

2.5. Data collection process and data extraction

A custom data extraction template was created within Covidence to ensure consistent and reliable data extraction from selected articles. The data items assessed by the data extraction form can be grouped into two distinct categories: high-level metadata relevant for characterizing the field of the literature and in-depth findings that capture study-specific data pertinent to answering the research questions. All extracted data were validated a second time within Covidence to ensure the accuracy of the extraction. A complete list of all the variables captured by the data extraction process can be found in Table 1.

3. RESULTS

The following section presents the main findings of the systematic review. At first, the study selection and study characteristics are introduced. Afterwards, the main findings are presented, grouped by their primary research contribution.

3.1. Study selection

A total of 334 studies were identified across 10 databases and secondary sources (Table 2). Of these, 55 were removed as duplicates, and 172 were excluded based on the title and abstract screening because they did not meet the inclusion and exclusion criteria (Fig. 1). The remaining 107 were sought for retrieval.

Eighteen were excluded because they mentioned romance scams but did not provide an in-depth discussion on the topic. Nine articles had research methodologies outwith the scope of our study (i.e. the papers used non-empirical research methods such as literature reviews and scoping reviews). An additional nine were removed because their full texts were not in English, and 10 were not available in full text. Furthermore, five articles were excluded because they had unclear research methodologies and three duplicated findings of a study by the same author, leaving 53 studies to be included in this review (Table 3).

Table 2. Search results by source.

Search source	Number of items before deduplication
Scopus	85
PsycInfo	0
Psycarticle	0
Medline	0
Web of Science	61
ProQuest	54
ACM Digital Library	10
IEEE Digital Library	2
ScienceDirect	59
PubMed	25
Manually included	38
Total number of articles	**334**

3.2. Study characteristics

This section provides an overview of the descriptive characteristics derived from the included articles. The final selection comprised 39 journal articles, nine conference proceedings, four theses/dissertations and a single book chapter. All studies were published between 2009 and 2023, with a rise in publications from 2019–21 (Fig. 2).

The contributors were distributed across 13 countries based on the institutional affiliation listed (Fig. 3).

In our analysis of the type of contribution present in the articles, we identified that n = 29 contributed to the profiling of romance scams and their manifestations, n = 14 focused on the exploration of countermeasures for mitigating romance scams and n = 10 examined related factors of becoming a scammer or a victim. The studies included in this review used a range of different research designs. Most prevalent were qualitative studies (n = 27), commonly focusing on victim reports, followed by quantitative research (n = 20), frequently using online surveys.

3.3. Excluded work

Articles were excluded if duplicate records were found or there was no access to the full text. Papers were also excluded if they were not written in English or contained no relevance or

Table 3. Full list of articles included in the study.

Authors	Location	Research design	Methodology	Sample
Al-Rousan *et al.* (2020)	USA Saudi Arabia	Quantitative	Machine learning	Not mentioned
Anesa (2020)	Italy	Qualitative	Linguistic profiling	26 online messages and 43 template messages
Barnor *et al.* (2020)	Ghana	Qualitative	Semi-structured interviews	10 individuals engaged in romance scams
Buchanan and Whitty (2014)	UK	Quantitative	Questionnaire	Study 1: 853 members of an online dating site Study 2: 397 members of a website to support romance scam victims
Buil-Gil and Zeng (2021)	UK	Quantitative	ARIMA modelling	Average of 4166 respondents per month
Button *et al.* (2014)	UK	Qualitative	Interviews/focus groups	Study 1: 15 online fraud victims Study 2: 6 focus groups with a further 48 online fraud victims Study 3: 9 professional stakeholders.
Carter (2021)	UK	Qualitative	Discourse analysis	1 conversation between a scammer and the victim
Cross *et al.* (2018)	Australia	Qualitative	Semi-structured interviews	21 victims of romance fraud
Cross (2019)	Australia	Qualitative	Semi-structured interviews	First Round: 6 victims of romance fraud Second Round: 7 victims of romance fraud
Cross and Holt (2021)	Australia USA	Mixed	Content analysis	2478 complaints to Scamwatch
Cross and Layt (2021)	Australia	Qualitative	Content analysis	509 victim reports to Scamwatch
Cross *et al.* (2022)	Australia USA	Qualitative	Content analysis	258 victim reports to Scamwatch
Cross and Lee (2022)	Australia	Qualitative	Content analysis	3259 victim reports to Scamwatch
Cross and Holt (2023)	Australia USA	Mixed	Content analysis	2699 victim reports to Scamwatch
Cross *et al.*, 2023	Australia USA	Qualitative	Content analysis	253 victim reports to Scamwatch
De Jong (2019)	Netherlands	Quantitative	Machine learning	4154 profile images
Dickerson *et al.* (2020)	UK	Mixed	Pre-test and post-test experiment	12 participants who had used online dating platforms
Dickinson *et al.* (2023)	USA	Qualitative	Content analysis	94 email exchanges with scammers.
Dreijers and Rudziša (2020)	Latvia	Qualitative	Linguistic profiling	7 letter sets
Edwards *et al.* (2018)	UK	Quantitative	Geocoding of IP addresses	5194 profiles of known scammers
Garrett (2014)	USA	Quantitative	Questionnaire	110 internet users
Gould *et al.* (2022)	Australia	Quantitative	Questionnaire	Survey of 101 clinicians
Graham (2021)	UK	Quantitative	Reverse image search	240 ordinary profiles images and 240 scammer profiles
He *et al.* (2021)	China Germany	Quantitative	Machine learning	240 million posts, 320 million comments and 33 million user profiles
Huang *et al.* (2015)	UK	Mixed	Content analysis	500 000 profiles of known scammers
Koon and Yoong (2017)	Malaysia	Qualitative	Linguistic profiling	21 email conversations
Kopp *et al.* (2015)	Australia	Qualitative	Content analysis	37 profiles of known scammers
Kopp *et al.* (2016a)	Australia	Qualitative	Content analysis	17 reports on an internet help forum
Kopp *et al.* (2016b)	Australia	Descriptive	Theory/content analysis	No participants
Li *et al.* (2019)	Norway	Quantitative	Machine learning	45 participants
Luu *et al.* (2017)	Australia	Quantitative	Questionnaire	399 victims of romance fraud
Modic and Anderson (2015)	UK	Quantitative	Questionnaire	6609 individuals from the public
Obada-Obieh *et al.* (2017)	Canada	Qualitative	Semi-structured interviews	10 general online daters
Offei *et al.* (2020)	Ghana USA	Quantitative	Questionnaire	320 individuals engaged in romance fraud
Pan *et al.* (2010)	Australia	Mixed	Data mining	5481 profiles of known scammers
Pizzato *et al.* (2012)	Australia	Quantitative	Probabilistic modelling	2 000 000 expressions of interest from a dating site
Rege (2009)	USA	Qualitative	Document meta-analysis	170 documents
Saad *et al.* (2018)	Malaysia	Quantitative	Study 1: Questionnaire Study 2: Association learning	Study 1: 280 romance scam victims Study 2: 2274 victims reporting to CCID
Shaari *et al.* (2019)	Malaysia	Qualitative	Content analysis	60 online chats
Smeitink (2021)	Netherlands	Qualitative	Semi-structured interview	9 victims of romance fraud

(Continued)

Table 3. Continued.

Authors	Location	Research design	Methodology	Sample
Sorell and Whitty (2019)	Australia	Qualitative	Semi-structured interviews	3 romance scam victims
Suarez-Tangil *et al.* (2019)	UK USA Australia	Quantitative	Machine learning	14 720 ordinary profiles and 5402 scammer profiles
Tao (2022)	UK	Qualitative	Content analysis	16 interviews with dating platform users in China
Wang and Zhou (2022)	USA China	Qualitative	Content analysis	40 victim narratives from Zhihu
Wang and Topalli (2022)	USA	Qualitative	Content analysis	52 victim stories.
Webster and Drew (2017)	Australia	Qualitative	Semi-structured interviews	9 police officers
Whitty and Buchanan (2012)	UK	Quantitative	Questionnaire	2028 individuals from the general public
Whitty (2013a)	UK	Qualitative	Study 1: Content analysis Study 2 + 3: Semi-structured interview	Study 1: 200 posts from a public online support group; Study 2: 20 victims of romance fraud; Study 3: 1 SOCA officer
Whitty (2013)	UK	Qualitative	Semi-structured interview	20 victims of romance fraud
Whitty and Buchanan (2016)	UK	Qualitative	Semi-structured interviews	20 victims of romance scams or individuals who feel that they have been scammed
Whitty (2018)	Australia	Quantitative	Questionnaire	11 780 victims and non-victims
Whitty (2019)	UK	Quantitative	Questionnaire	261 dating site and social media users
Whitty (2020)	Australia	Quantitative	Questionnaire	Study 1: 11 780 participants (10 723 non-victims, 1057 victims) Study 2: 531 participants (sub-set of study 1)

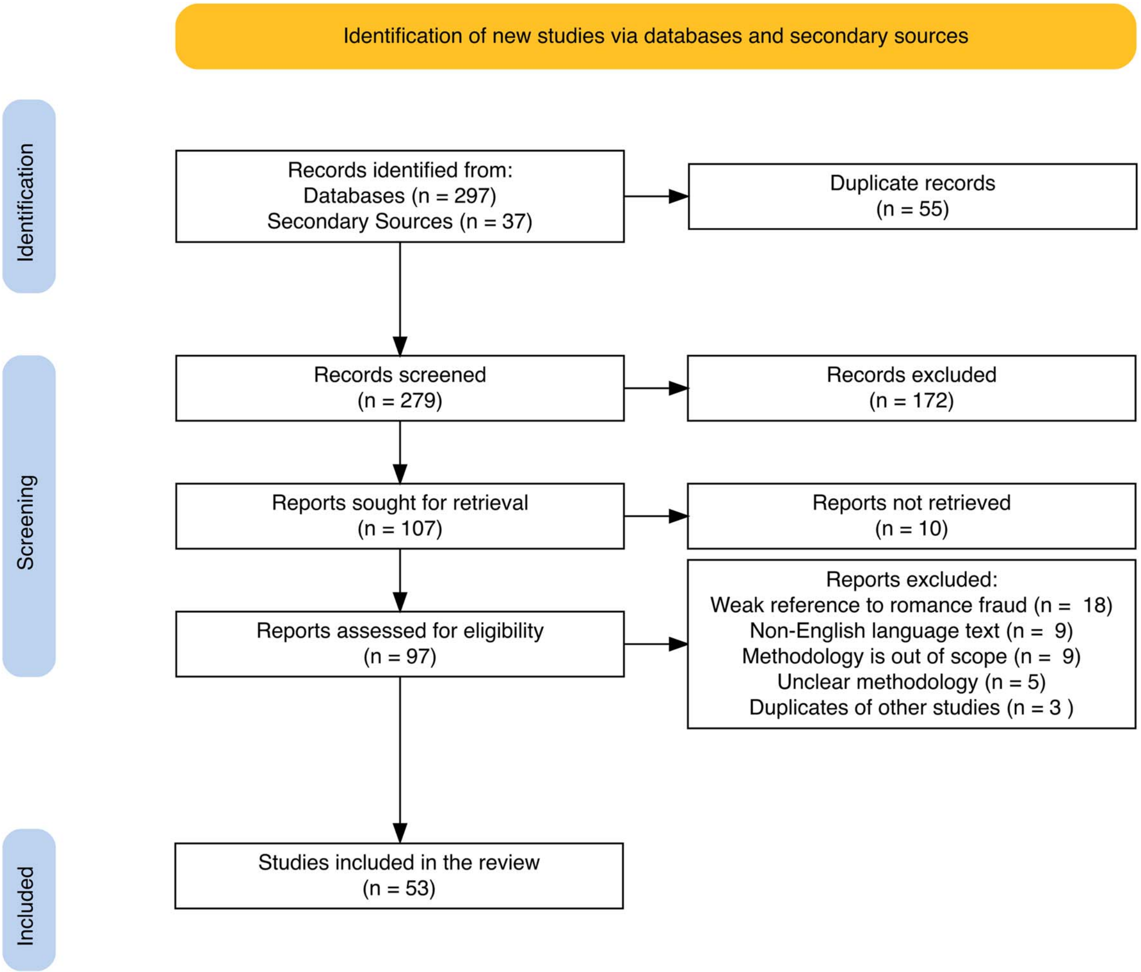
Identification of new studies via databases and secondary sources
Identification
Screening
Included
Records identified from:
Databases (n = 297)
Secondary Sources (n = 37)
Duplicate records
(n = 55)
Records screened
(n = 279)
Records excluded
(n = 172)
Reports sought for retrieval
(n = 107)
Reports not retrieved
(n = 10)
Reports assessed for eligibility
(n = 97)
Reports excluded:
Weak reference to romance fraud (n = 18)
Non-English language text (n = 9)
Methodology is out of scope (n = 9)
Unclear methodology (n = 5)
Duplicates of other studies (n = 3)
Studies included in the review
(n = 53)

FIGURE 1. PRISMA flow diagram for identifying articles related to romance scams.

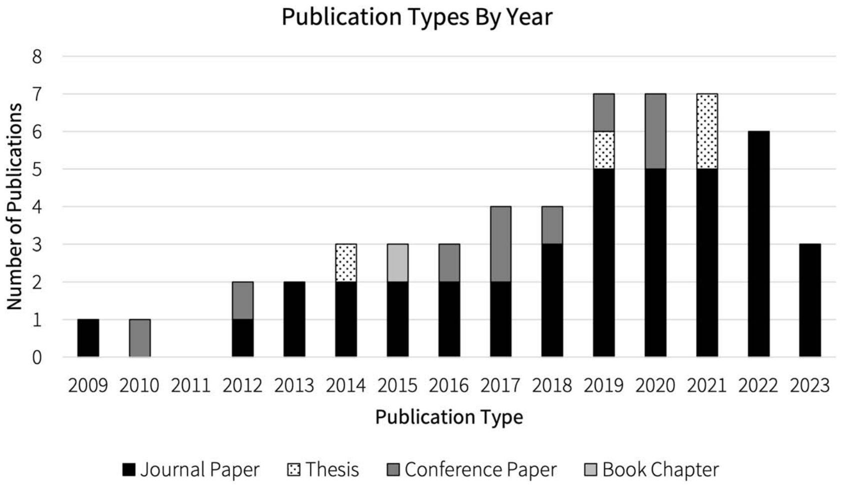

FIGURE 2. Types of publications each year.

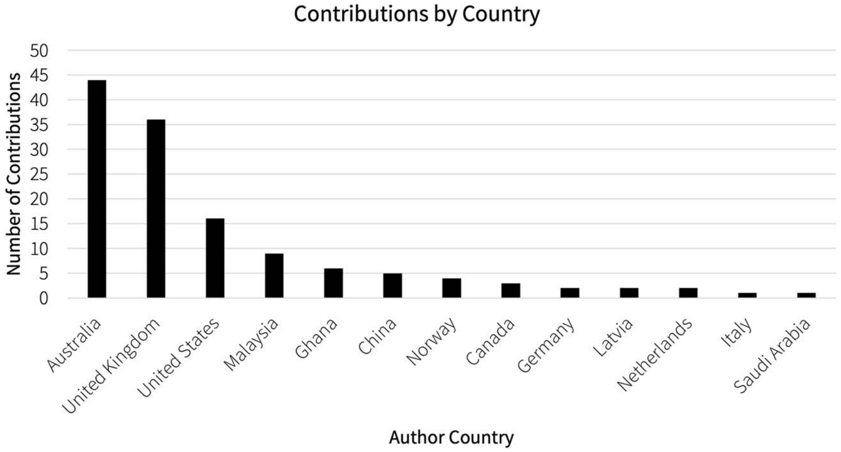

FIGURE 3. Contributions by country.

a weak link to romance scams. Furthermore, several papers were excluded if they did not feature a methodology of relevance to our review. This incorporated papers with limited detail in the methodology regarding participants and materials evaluated (Gregory and Nikiforova, 2012; Annadorai *et al.*, 2018; Jimoh and Stephen, 2018). Several papers were also position-like pieces, featuring no empirical research (Gillespie, 2017, 2021; Steyerl, 2011; M. Whitty *et al.*, 2017). Other papers featured a short review of existing literature, e.g. providing an overview of romance scams or linking to established theories (Rege, 2013; Cross, 2016b, 2020; Khader and Yun, 2017; Eseadi *et al.*, 2021). Coluccia *et al.* (2020) conducted a scoping review of romance scams' relational dynamics and psychological characteristics and identified 12 relevant studies. Although such reviews contribute to the basic understanding of romance scams, they do not deliver a detailed picture of the current body of literature on the subject.

3.4. Profiling romance scams: Models, characteristics and tactics

The following section presents the findings of studies that contributed to the profiling of romance scams through process models, taxonomies as well as discussions of characteristics and tactics prevalent in romance scams, which addresses RQ1: *'What is the state-of-the-art approach for profiling, describing and characterizing romance scams?'*

3.4.1. *Process models of romance scams*

Several researchers have sought to explain the progression of romance scams. An early examination by Rege (2009) is one of the most referenced articles on this topic and describes three distinct stages commonly found in romance scams. The scam begins with the creation of a fake profile and continues with the contact phase, which aims to establish trust and a strong bond between the scammer and the victim over a more extended period. The third and final stage entails one or multiple requests for money by describing a terrible or desperate situation.

The most frequently referenced model, however, was developed by Whitty (2013a), who identified five stages involved in the scam: being presented with an ideal profile, the grooming process (establishing the trust), the sting (request for money), sexual abuse and revelation. Subsequently, Whitty (2013) proposed the Scammers Persuasive Model, a refined and extended version of her initial model, adding the motivation to find an ideal partner and a re-victimization stage to the process flow, whereby victims refuse to believe the relationship is fake. Romance scams are often described as a unique crime due to the 'double hit' experienced by victims; the loss of money and a relationship. Not all those interviewed or who posted online experienced monetary loss; thus, this may have impacted the development of the model.

The work also acknowledges that not all victims experience all stages. In particular, the sexual abuse stage depends on the individual and the scam's setup and is no longer part of the immediate flow. Advancements in technology mean that photo and video sharing is easier than ever due to smartphone camera hardware developments. Thus, sextortion is now reported as an aspect of romance scams, more commonly among men (Cross *et al.*, 2022).

Others have argued that the crime's relationship aspect is separate from the monetary aspect, and these are considered two mutually supportive storylines (Kopp *et al.*, 2016b). Whereas the former aimed at establishing a romantic relationship to develop commitment and trust, the latter sought to engineer the victim into transferring funds to the perpetrator. In subsequent research, Kopp *et al.* (2016a) explained the transition between the storylines using the Transtheoretical Model's stages of change. However, the use of the Transtheoretical Model is not without criticism; it is often seen as prescriptive (Herzog, 2008) and may not be best suited for fully realizing the complexities of romance scams.

Few papers consider the aftermath of a romance scam and the devastation the victim experiences. Despite being based on a small number of interviews (nine) in the Netherlands, Smeitink (2021) references the aftermath in their model, noting that the recovery of the victim is a crucial step to reduce re-victimization. Similarly, Wang and Topalli (2022) have considered the aftermath as part of their model, which, although based on victim testimonials, also considers offender behaviour.

Romance scams continue evolving as fraudsters adapt to new and emerging technologies. Scams may not follow the 'typical' path outlined in existing models. Thus, future work should focus on incorporating flexibility within the models, with consideration as to how the victim recovers, preventing further victimization.

3.4.2. *Characteristics of romance scams*

Determining occurrences of romance scams is challenging due to the high likelihood of under-reporting, meaning it is also difficult to estimate the financial losses involved (Cross *et al.*, 2018). Based on survey data from 2028 British adults, 0.65% of all adults in the UK had already been scammed, and 2.28% know a victim (Whitty and Buchanan, 2012). Losses of between £50 and £800 000 and median financial damages of £1001 and £10 000 per victim have been cited (Whitty and Buchanan, 2012; Buchanan and Whitty, 2014). Similarly, Rege (2009) quotes losses of >$3000 for average victims.

Early qualitative research on romance scams suggested that most scams originate from western parts of Africa, such as Nigeria, which was infamous for running fraudulent schemes (Rege, 2009; Whitty, 2013a). Later research conducted by Pan *et al.* (2010) confirmed these findings by highlighting that scammer profiles were frequently associated with IP address blocks assigned to the Lagos Region. Subsequent research by Edwards *et al.* (2018), which decoded IP addresses on a country level, identified that scams originated from Nigeria (30%), Ghana (13%) and Malaysia (11%), followed by South Africa (9%).

3.4.3. *Persuasive tactics and tricks*

Researchers have explored various tactics scammers use to lure victims into the scam and keep them engaged. Studies have performed linguistic profiling (Koon and Yoong, 2017; Shaari *et al.*, 2019; Anesa, 2020; Dreijers and Rudzīša, 2020), researched persuasion and repression tactics (Whitty, 2013; Button *et al.*, 2014; Kopp *et al.*, 2015; Cross *et al.*, 2018; Carter, 2021; Wang and Zhou, 2022) and the usage of military identities to convey authority (Cross and Holt, 2021).

Linguistic profiling

Previous research has analysed written scam communications' structure and linguistic patterns and identified three distinct stages: initial, pre-attraction and hooked (Shaari *et al.*, 2019). During the initial stage, the relationship is established and is dominated by formal and polite communication, where scammers disclose details about their personality and successful career to gain the victim's trust. The prevalence of pseudo–self-disclosure evokes trust, empathy and sympathy by displaying the scammer as a successful, educated, affluent and elite individual (Koon and Yoong, 2017; Anesa, 2020).

The second stage (pre-attraction), according to Shaari *et al.* (2019), aims at strengthening the online relationship. Common phrases include discussions about religion, expressions of attraction and phrases that prioritize the victim, helping develop an emotional bond (Koon and Yoong, 2017; Anesa, 2020; Dreijers and Rudzīša, 2020). During this stage, scammers seek to change to an alternative communication channel, such as email or a third-party messaging platform, a necessary step for evading online dating platform detection algorithms.

The final phase (known as the hooked phase) occurs from the mid-stage of the relationship until the money is requested. Commonly identified expressions suggest feelings of indebtedness and gratitude for the received companionship (Koon and Yoong, 2017; Shaari *et al.*, 2019) and may give the impression that the victim has freedom of choice as to whether they respond to requests (Dickinson *et al.*, 2023). Messages may contain signs of aggression if the victim does not comply with monetary requests (Shaari *et al.*, 2019). If the victim offers a reward early on, the scammer may reveal less information about themselves because they have already achieved the end goal of extracting funds (Dickinson *et al.*, 2023).

Persuasion and repression tactics

There are many reasons why victims fall for a range of online scams, including romance scams (Button *et al.*, 2014), corroborated by Whitty (2013). In addition, Whitty identified appeals to urgency, reciprocation, norm activation, Cialdini's (2007) principles of commitment and consistency and love, liking and similarity and addictive relationships; these findings align with Kopp *et al.* (2015) and the concept of a tailored personal love story for individual victims.

Similarly, Carter (2021) establishes that scammers use stories of physical trauma and urgency to evoke the victim's visceral responses during monetary requests while keeping victims isolated from friends and family. The theme of isolation also draws comparisons with domestic violence research; scammers mistreat victims through economic abuse, degradation, psychological destabilization, emotional or interpersonal withdrawal and contingent expressions of love (Cross *et al.*, 2018). Furthermore, such persuasive techniques are also seen in China, where a variation of online romance scams termed '*Sha Zhu Pan* (杀猪盘)' or '*Pig Butchering*' is becoming common, whereby victims are lured into financial schemes, 'fattened up' and ultimately defrauded (Wang and Zhou, 2022).

3.4.4. *Military themes*

In recent years, personas involving a military context have frequently been mentioned as distinct themes used by scammers (Rege, 2009; Whitty and Buchanan, 2012; Whitty, 2013). In military-themed scams, the perpetrators use profile photos of army or peacekeeping personnel and use a military context to create a persona and storyline that projects authority (Anesa, 2020; Cross and Holt, 2021). Such contexts are commonly justified by the lack of access to personal financial means and the inability to communicate through voice or video for security and secrecy reasons (Cross and Holt, 2021).

Based on the victims' reports from the Australian Consumer and Competition Commission's Scamwatch, Cross and Holt (2021) identified significant predictors for reporting being targeted by a military-themed scam: being female, younger in age, being a primary English speaker, and living outwith Australia. Their work also identified that military scams typically start on social media platforms and are likely to involve the loss of personal details. However, it was found that these types of scams typically did not show signs of abuse (e.g. threats or blackmail). These variables, however, were not significant for indicating financial losses in the scam. Instead, males and victims who already faced financial hardship were more at risk of monetary loss.

3.4.5. *Fraudulent online dating profiles*

Online dating profiles play a vital role in romance scams. It is typically the first point of contact that lures a victim into the scam and plays a crucial role in successfully executing the subsequent scam stages (Whitty, 2013a; Kopp *et al.*, 2016a). Thus, the profiles and self-presentation of scammers have been subject to extensive research. Pan *et al.* (2010) highlight that most (61%) scammer profiles misrepresent their origin by claiming to be from the USA. Follow-up studies confirm this, e.g. Edwards *et al.* (2018) notes that most scammers claimed to be from the USA (63%), the UK (11%) or Germany (3%) because these are typically also the countries where their victims are located and are some of the biggest users of online dating platforms (Buchholz, 2023).

Differences between male and female scammer profiles have been characterized by average age and profession. Whitty (2013a) states that female profiles targeting heterosexual male victims in their later years typically portray themselves as aged no older than 30 years and working in low-paying or non-professional jobs. For profiles targeting heterosexual females, the profiles typically claimed to be as old as 50 but mostly younger than the victim. Occupations include professional jobs, entrepreneurial activities or army ranks. For fake male homosexual profiles, Whitty (2013a) elaborates that these incorporate age ranges generally younger than 30 years and claim mixed professional status. Edwards *et al.* (2018) support these findings by indicating an average age of 30 for females and 50 for males. Similarly, Pan *et al.* (2010) identified that most females claimed to be between 20 and 29, and males stated ages between 40 and 49.

Disagreement exists on the prevalence of a particular gender linked to scammer profiles. Although Pan *et al.* (2010) argues the predominance of young females (64.93%), Huang et al.'s (2015) analysis of flagged profiles from a Chinese dating site presents most (close to 80%) romance swindlers as males. Similarly, Edwards *et al.* (2018) found that 64% of all profiles were males.

Different findings also exist for the marital status indicated by the profiles. Although Edwards *et al.* (2018) produce a convincing account for the existence (50%) of single status across all profiles, Huang *et al.* (2015) found a prevalence of widows (50%), followed by divorcees (33%), with single people only accounting for 15%. Whitty (2013a) indicates that the marital status is again dependent on the target characteristics, with male profiles typically posing as widowers with a child, whereas females commonly pose as singles. Edwards *et al.* (2018) extended these perspectives and reason that the gender, ethnicity, marital status and profession misrepresented in the profile can show unique characteristics based on the origin of the scam. Profiles originating from Nigeria, Malaysia and South Africa primarily posed as males, whereas profiles from the Philippines, Ukraine and Senegal presented themselves as females.

Kopp *et al.* (2015) performed a qualitative analysis of 37 fraudulent profile descriptions, and they identified that the profile descriptions typically consist of a self-presentation, explanations of hobbies, motivations and the ideal partner. The study argues that male profiles describe themselves as masculine, wealthy, humorous and God-fearing, while females portray confidence, financial independence and occasionally sexually provocative suggestions. Men also frequently included personal tragedies in the profile, such as the loss of a loved one, suggesting their need for a caring, sympathizing partner.

In addition, two rather curious findings about scammer profiles were reported by Pan *et al.* (2010), who postulated that the fraudulent profiles were frequently associated with Yahoo's email service and descriptions that suggested a bisexual sexual orientation. One aspect both female and male profiles have in common is their use of attractive profile pictures commonly stolen from social media sites or modelling agencies (Rege, 2009; Whitty, 2013; Cross & Layt, 2021).

3.4.6. *Consequences of romance scams*

Romance scams typically consist of a financial and emotional impact, which can be noted among victims (Rege, 2009; Whitty, 2013a). Buchanan and Whitty (2014) analysed the effects on the victim. They showed that financial victims report higher emotional impact than non-financial victims, with 40% signifying they were 'very distressed over a long period'. Modic and Anderson (2015) add support to their findings. They determined lonely heart swindles as the fraud category with the highest emotional impact on the victim, combined with reasonably high financial losses. Women were found to experience higher emotional impact and suffer higher financial losses than their male counterparts (Buchanan and Whitty, 2014).

The emotions that victims experience post-scam include shame, embarrassment, shock, anger, worry and stress (Whitty and Buchanan, 2016), and can be associated with subsequent mental health problems and homelessness (Cross, 2019). Feelings of fear have been found in romance scam reports (Cross and Lee, 2022), touching on physical and family safety but also linking to other consequences such as a diminished sense of self-worth and confidence, loss of trust in others and cutting social ties with former acquaintances (Whitty and Buchanan, 2016). In some cases, the victims' perceived loss of their 'ideal partner' weighed heavier than the financial loss; as a result, most victims struggle to cope with the experiences because they feel they cannot disclose to family, friends or work colleagues out of fear of rejection and anger (Whitty and Buchanan, 2016). This consequence leaves most victims in a stage of denial, where they are at particular risk of re-victimization. Those victims who disclosed to peers did not get the necessary support but experienced increased negative feelings of self-blame, which is common among romance scam victims, especially when victims cannot recognize the fraudulent nature of the relationship despite being warned by others (Sorell and Whitty, 2019).

3.4.7. *Summary*

Although there seem to be commonalities across many of the online romance scam models developed, most fail to consider the aftermath of the scam and the support required by the victims. Currently, romance scams are under-reported, partially owing to the embarrassment victims feel. Future developments in the field should focus on support and recovery; thus, it is plausible that more victims will feel they can come forward and report such crimes. It is also clear that a deeper understanding of scammer characteristics is needed, building on work by the likes of Rege (2009). With the advent of large-language models such as Chat-GPT becoming readily available to the public, alongside tools for creating deepfake videos and audio, scammer tactics are likely to evolve at a rapid pace, with the potential of creating realistic-looking 'synthetic' soulmates to lure potential victims.

3.5. Influential factors: Socio-demographic, experiential and dispositional characteristics of scammers and victims

In exploring answers to RQ2: '*What underlying socio-demographic and psychological factors enable and foster the execution of a romance scam?*' several articles focused on influential factors, such as experiential and dispositional characteristics, that may increase the likelihood of being involved in a romance scam, from both scammer and victim perspectives.

3.5.1. *Typology of victims*

Garrett (2014) indicates that active engagement in finding a partner yields a higher likelihood of falling for a romance scam. A potential reason is that these people simply encounter more profiles in general, thus, there is a higher likelihood of finding a scammer profile. Those who want a partner but do not actively engage in the search process showed higher monetary losses than other online daters. Another factor that significantly increases both the likelihood and severity is a focus on finding an international partner; this may be because it can be challenging to meet a long-distance partner in the early stages of a relationship to verify their identity.

Furthermore, the years of internet usage affect the probability and average losses. Garrett (2014) demonstrates that respondents with 1–5 years of internet experience were particularly exposed. This could be due to limited online fraud awareness (Saad *et al.*, 2018). Interestingly, Saad *et al.* (2018) used an Apriori algorithm and found that well-educated, married women of Chinese and Malay ethnicity between the ages of 25 and 45 have a high likelihood of victimization. The authors did not elaborate on their finding that married people were more likely to experience victimhood than individuals who were not in a relationship.

Regarding socio-demographic and psychological characteristics, Whitty (2018) suggests that well-educated women aged 35–54 are at particular risk of victimization because this group is most likely to engage in online dating and have higher levels of disposable income. More recently, there has been a growing number of romance scammers targeting younger lesbian and '*lala*' women (defined as '*a loose term referring to lesbian, bisexual and transgender women who are attracted by women*') in China (Tao, 2022). Dating platforms and forums for these individuals are rare; thus the presence of a few scammers may be perceived as disproportionately high in an already limited dating pool.

Although romance scam research historically reports that women are more likely to become victims, increasing numbers of young men are falling victim, with links to sextortion, potentially due to increased social media usage (Cross *et al.*, 2022; Cross *et al.*, 2023).

In addition, psychological characteristics, including impulsivity, lack of self-control, addiction disposition, trustworthiness and less kindness, were indicative of romance scam victimhood compared with other cyber scams (Whitty, 2020). Those with acquired brain injuries may be particularly vulnerable owing to impulsivity associated with their condition (Gould *et al.*, 2022). In assessing the effects of personality and psychological variables on the risk of being scammed and the emotional distress experienced after a scam, Buchanan and Whitty (2014) only identified idealization, a sub-element of romantic beliefs, as the only significant factor but in practice, a limited predictor for victimhood. Idealization is an individual's belief in the fulfilment of a perfect relationship. Other psychological characteristics, such as loneliness, personality and sensation, did not reach statistical significance.

3.5.2. *Typology of scammers*

In contrast to the well-studied influencing factors for victims, research on perpetrators is still scarce. This may be due to the international nature of romance scams, whereby law enforcement may find it difficult to track scammers owing to jurisdictional challenges. Furthermore, law enforcement agencies are limited in terms of the data they can share with researchers investigating the phenomenon. The following section presents studies that primarily analysed the psychometric aspects of individuals conducting online romance scams.

Work by Barnor *et al.* (2020) relies on the Motivation Opportunity Ability (MOA) framework and the Rationalization dimension of the Fraud Triangle Theory to explain male Ghanaian scammers' socio-economic drivers. They discovered that the main drivers of romance scams are peer recruitment, poverty, unemployment and low education and income. For the opportunity dimension, the conditions that allow or make it possible for people to engage in a behaviour, the study suggests that flaws in current legislation, its enforcement and lack of law enforcement capabilities are the primary enablers for committing romance scams. The third and final dimension of the MOA framework, ability, can be described as necessary skills and proficiencies for completing a set task.

Based on their qualitative interviews, Barnor *et al.* (2020) ascertained the need for social abilities, such as teamwork and interactional skills, and technology-related capabilities to remain anonymous, like knowing how to use VPNs (Virtual Private Networks). However, no formal IT training or higher education was present among the interviewees. Similarly, Rege (2009) lists basic computing skills as required technical skills and patience, social skills and the ability to follow routines as non-technical skills.

Most offenders interviewed by Barnor *et al.* (2020) rationalized their behaviour by stating that cybercrime is less severe than physical crimes like murder because their 'wealthy' victims are supposedly less affected by the loss of money. Others also justified their behaviour as retaliation for the harm caused to their forefathers during the colonization times.

In a similar study, Offei *et al.* (2020) analysed Ghanaian individuals' justifications for executing online romance scams using Neutralization and Denial of Risk Theory. They found that scammers only use the denial of victim aspect of the Neutralization Theory to justify their deviant behaviour. Scammers alleviate the sole responsibility for the deception by reasoning that their extensive investments contribute to a romantic relationship with mutual responsibilities. Findings for the denial of risk theory were consistent with Barnor *et al.*'s (2020) and Rege's (2009) findings on ability and rationalization.

3.5.3. *Summary*

To summarize, existing literature indicates that those most at risk of falling victim to romance scams are single, heterosexual women between the ages of 25 and 54 who have a disposable income and may have traits such as poor impulse control. This suggests that researchers, dating platforms and law enforcement should target mitigations toward this group to help reduce victimization. That said, anyone is potentially vulnerable to romance scams, as evidenced by the growing number of men providing reports.

Less is known about who the 'typical' scammer is due to the dearth of studies in this area. An interdisciplinary approach is needed to address this, requiring law enforcement and dating platforms to release pertinent information to researchers to help create a more robust profile. Ultimately, this will help drive targeted mitigations to protect platform users against scammers.

3.6. Countermeasures and mitigations

Two broad groups were covered by the research on countermeasures and mitigations: technology-centred and human-centred approaches, in the context of RQ3: *'What countermeasures and mitigation techniques have been proposed to help identify romance scams, thus limiting the risk of victimisation?'*. The technology-centred approaches can further be divided by whether a system seeks to detect fraudulent profiles actively or if the primary goal is to create a robust people recommender system. Similarly, the human-centred approaches can be grouped into two subfields. The first group entails research focusing on inherent safeguarding approaches, while the second group concentrates on externally provided intervention and coping strategies.

3.6.1. *Research on detection mechanisms*

Work focusing on detecting fraudulent online dating profiles and scammer behaviour using machine learning approaches can be grouped based on the input features used to distinguish between bogus and genuine profiles.

Several researchers have focused on image recognition and reverse search to compare and match the profile pictures used by romance scammers (De Jong, 2019). Using existing tools such as Amazon's Rekognition API (Amazon, 2023) and Google Vision API (Google, 2023), Al-Rousan *et al.* (2020) proposed a tool called Social-Guard to detect such images, using OkCupid (2023) profiles as a test bed. Others have drawn on image and text in profiles to create a browser add-on communicating with a client-side Python application that reverse searches Google (2023), Yandex (2023) and TinEye (2023), evaluating the identified web pages based on keywords in near real time (Graham, 2021).

Although machine learning is well suited to detect romance scams, there are particular challenges with accuracy. Given the nature of the crime and the embarrassment victims may feel, it is challenging to acquire reasonably large datasets used for training. Furthermore, the tactics scammers use continually evolve, meaning existing datasets may become quickly outdated. For example, in de Jong (2019), the proposed model is more likely to falsely classify a scammer's image as benign than a regular online dater as fraudulent. Similar issues were found in Graham's (2021) work; of 40 profiles investigated, 35 returned inconclusive results.

Despite these challenges, other researchers have achieved higher accuracy ratings. Suarez-Tangil *et al.* (2019) extended the number of factors and included static profile information such as demographical data and profile descriptions in their evaluation and used various machine learning classifiers based on the input variables and their completeness. Using a Naïve Bayes approach, LibShortText's (Yu *et al.*, 2013) implementation of an SVM (support vector machine) and an RBF (radial basis function) Ensemble Classifier, a prediction of whether a profile was a scam or benign was made by combining the votes of the classifiers. Overall, the authors proclaim an accuracy of 97% for the ensemble classifier.

More recently, He *et al.* (2021) extended the static profile features used by Suarez-Tangil *et al.* (2019). They used dynamic features, such as user behaviours, to detect fraudulent profiles on a Chinese social media and dating app called Momo (陌陌) (2023). Their proposed content-based attention network, dubbed 'DatingSec', consists of three layers: input, pattern extraction and prediction. The input layer takes five types of features: profile features, community features, behavioural features and topic distributions of posts and comments. The extraction layer uses an MLP (Multi-Level Perceptron) for processing static information and multiple Bilateral-*long short-term memory* (Bi-LSTM) processing dynamic information. He *et al.* (2021) indicated that their combined approach reached a precision of 90.5%, an F1 of 0.857 and an AUC (area under the curve) score of 0.940.

Another notable approach focused on message-based keystroke dynamics rather than dating profiles for verifying user identity (Li *et al.*, 2019). Four features were considered: the average thinking time, the ratio of key deletions, the average number of letters in a word and the average number of words within a message. Keystroke dynamics focused on the latency between keypresses and the duration of key presses. Using these six keystroke dynamics, a person's gender could be predicted via a 15-minute chat conversation with an accuracy of 72%. An evaluation based solely on the four stylometry features reached a prediction accuracy of 64%. A significant limitation of this work is that detecting key dynamics, such as the latency between releasing the first and pressing the second key, required the installation of a custom-developed keylogger called BeLT (Mondal *et al.*, 2017) because traditional chat clients do not record and transmit these. Therefore, these detection mechanisms must be integrated into applications where keystroke dynamics can be accurately recorded.

3.6.2. *Research on susceptibility of people recommenders to fraudulent profiles*

Pizzato *et al.* (2012) researched the sensitivity of recommender algorithms to scammer profiles. In an experiment, they assessed the recommendations of collaborative filtering, a hybrid (content-collaborative reciprocal plus content filter) and content-based 'RECON' recommender algorithms. They identified that collaborative filtering and hybrid recommenders more often recommend highly suspicious profiles, favouring popular and active profiles and candidates with high interaction and high 'reply to' rates. The limited research in this space indicates that researchers and online dating platforms must work closely together to ensure scammers do not 'poison' recommender systems.

3.6.3. *Research on intrinsically motivated safeguarding strategies*

Several pieces of literature on countermeasures and mitigation strategies focused on intrinsically motivated safeguarding approaches used by online daters and their effectiveness in detecting online deceit.

Cross and Layts' (2021) large-scale survey showed that the most common action taken in response to suspicious profiles was to conduct an internet search of the online persona. Most frequent were reverse image searches or online searches based on addresses, phone numbers, personal details and message content. In most cases, these created suspicion of communicating with a scammer due to warnings on scammer awareness sites, image reuse and identity mismatches. However, even in cases without search hits, participants were still suspicious due to the lack of a digital footprint, such as a social media profile.

In contrast, similar research by Obada-Obieh *et al.* (2017) indicated that only three of ten participants searched for online social media presence as a precautionary method. Most frequently (six of ten times), online daters looked for inconsistency in the dating profiles, overly attractive profiles or complete duplicates to identify scammers, followed by reliance on their 'gut feelings'. Interviewees were particularly suspicious of profiles with profile pictures that were 'too cute' and descriptions that seemed to be hoaxes. This discrepancy in safeguarding strategies can potentially be explained based on the characteristics of the sample groups and the data sources. Whereas Cross and Layt (2021) drew on reports from scam victims to Scamwatch (2023), Obada-Obieh *et al.* (2017) interviewed general online daters without the precondition of being involved in a scam; individuals who have previously been exposed to a scam may be more cautious (Whitty, 2019). That said, distinguishing fake from genuine profiles remains a nontrivial task; on average, participants only classified 13.51 of 40 profiles correctly.

Although the former research covered the safeguarding techniques used by individuals, Luu *et al.* (2017) examined the factors and processes influencing the adoption of protection mechanisms, such as checks of identities or reporting of users, using the Protection Motivation Theory (Rogers, 1983). They identified that adopting protection mechanisms was mainly influenced by an individual's coping appraisal, response efficacy and self-efficacy factors. In contrast, response cost played a minor role. The authors discovered that perceived vulnerability and perceived severity were most influential for the threat appraisal. In particular, thorough knowledge of the harm caused by romance scams motivated individuals to use protection mechanisms.

3.6.4. *Research on externally stimulated intervention and coping strategies*

The externally stimulated intervention and coping strategies can be distinguished based on the scam phase in which they intervene, either from the grooming phase onward or after the scam. Dickerson *et al.* (2020) proposed targeted and dynamic warning messages displayed to potential victims when a trigger situation, such as a request for money by a potential scammer, occurs. Their study identified that contextualized warning messages helped increase user awareness and decrease risky behaviour. Furthermore, warning messages contextualized advice on how to spot scammers made available by dating sites and public entities. Although none of the participants in the control group interacted with the educational information, all the participants in the experimental group engaged with the training material referenced by the warning messages.

Proactive policing strategies were another target of research. Webster and Drew (2017) explored the experiences of law enforcement officers involved in an early intervention model by the Queensland Police Service. They identified that proactive policing yielded the first promising results through qualitative interviews, particularly when victims were already questioning their relationship. This has the potential to be coupled with another strategy put forward by Cross and Holt (2023): discouraging potential victims from sharing sensitive information until a relationship is verified reduces the risk of financial and identity theft later down the line, ultimately reducing victimization.

Research by Cross (2019) examined the motivations, expectations and actual experiences of individuals who joined police-run peer support groups after being targeted by scammers. Significant reasons for joining a peer support group were the interactions with like-minded people, a sense of community, the expected release of the burden suffered by the victim, the prospect of giving and receiving help and the sheer absence of other means of support, such as family and friends. Unlike the motivations, which were largely optimistic, the actual experiences were mixed. Most participants valued sharing their own story with others and subsequent gain of solidarity and acknowledgement, the ability to learn how they have been victimized or build a friendship. However, others acknowledged diverse challenges, such as lack of engagement in the group, logistical problems, high participant fluctuation rates of the group members, expectation mismatches and perceived tension between financial and non-financial victims.

3.6.5. *Summary*

Owing to the scale and complexities involved with online romance scams, machine learning is ideal for analysing large-scale conversations, identifying patterns or verifying profile images. However, available datasets are scarce, and many researchers repeatedly use the same dataset, risking bias or producing findings that are not generalizable. Researchers require support from law enforcement and dating platforms to access robust datasets, harnessing the power of emerging technologies to develop cutting-edge mitigations against scammers. Furthermore, concepts derived from usable security and persuasion research can lead to the development of user interfaces with timely interventions if signs of a scam are detected in conversation. Lastly, although not a technical countermeasure, awareness campaigns as part of policing strategies still have a vital role to play, ensuring the public knows how to get help should they fall victim to a romance scam.

4. DISCUSSION

This section discusses the main findings and limitations of existing studies, and future research directions are presented.

4.1. Study characteristics

After applying the selection criteria, 53 studies were included in this review. Most primarily focused on profiling romance scams and their manifestations, followed by an exploration of countermeasures for mitigating them. Contributions used a wide range of research methodologies and frameworks, which made direct comparisons of individual findings challenging due to the limited homogeneity between these studies. Furthermore, many studies focused primarily on online crime research rather than romance scams, requiring caution when comparing and contrasting findings.

Evaluation of the research methodologies showed that qualitative methods were more prevalent than quantitative methods. Most qualitative studies contributed to profiling romance scams, whereas quantitative studies primarily shaped the understanding of countermeasures and influencing factors. Unsurprisingly, the sample size between both methods greatly varied.

Across all studies, the complexity of acquiring novel, accurate and complete primary data on the subject was acknowledged. Multiple authors from different fields voiced the challenge of collecting reliable data due to the under-reporting of the crime, ethical and legal challenges and the sensitive nature of the crime (e.g. Rege, 2009; de Jong, 2019). In particular, collecting of long-ranging dynamic information, such as complete chat logs covering all stages of the scam, from the message of interest on the dating site to the money transfer negotiated off-platform, was acknowledged as challenging (Carter, 2021). This challenge might also explain the frequent usage of questionnaires and surveys for collecting relevant data. In addition, multiple studies were based on the same data, e.g. research involving Cross frequently makes use of Scamwatch data because this is one of the few available data sources in the domain. In contrast, others did not fully disclose their data sources.

Even when datasets differed, commonalities could be identified based on the origin of the data. Multiple studies relied on data from datingnmore.com (2021), a self-proclaimed scammer-free online dating site, when analysing known genuine profiles. Others relied on data from scamdigger.com (2021) when examining scammer profiles (Pan *et al.*, 2010; Edwards *et al.*, 2018; de Jong, 2019 ; Suarez-Tangil *et al.*, 2019 ; Graham, 2021). Because both sites are publicly accessible and allow for easy access to a large pool of data, it is no surprise that three of five studies that incorporated machine learning used at least one of these sites (de Jong, 2019; Suarez-Tangil *et al.*, 2019; Graham, 2021). However, the firm reliance on these two data sources might lead to incorrect assumptions because datingnmore.com primarily caters to an older audience and might not represent the general dating population.

One way of furthering work on spotting scammers is through an extended collaboration between academics, online dating providers and law enforcement to identify legal and ethical ways to access the relevant data. Existing studies that use corporations with dating sites, such as those conducted by Huang *et al.* (2015) on an unnamed Chinese dating site and by He *et al.* (2021) on the Momo (2023) app, indicate promising findings.

4.2. RQ1—Profiling romance scams

Considerable research contributions have been made in characterizing the prevalence and impact of romance scams. In terms of experienced financial losses, studies have found losses between £50 and £800 000 and medians of £1001–£10 000 per victim (Buchanan and Whitty, 2014). Because these numbers are frequently based on reports to anti-fraud agencies such as Action Fraud (2023), the actual numbers are likely to be higher due to many unrecorded cases.

The origins of romance scams have also been explored in several papers. Studies by Pan *et al.* (2010) and Edwards *et al.* (2018) confirmed that most romance scams originate from the West African countries of Nigeria and Ghana. However, Edwards et al. also showed that a considerable number of scams also originate in Malaysia (11%), Turkey (3%), the Philippines (2%) and Russia (1.5%). Research on the scams from these parts of the world is still scarce, despite initial indications of differences in the scam's execution and the groups they target (Garrett, 2014; Edwards *et al.*, 2018). Thus, more research is needed that addresses romance scams by region to identify unique characteristics, commonalities and differences in the execution of the scam.

Studies concerned with the persuasive tactics used by scammers achieve a general consensus among those in this review. Scammers use a range of persuasive tactics and linguistic devices to evoke the desired emotion in a particular scam stage. Tactics include visceral appeals, the creation of urgency, fast-moving relationships, appeals to strong emotions and even isolation and monopolization. Anesa (2020) argued that most tactics are particularly effective because these scam victims into processing clues peripherally, according to the Elaboration Likelihood Model by Petty and Cacioppo (1984). An improved understanding of how individuals process messages from scammers could provide insights into why individuals fall for such deceit and how it can be prevented.

The literature on the creation of fraudulent profiles has once again identified similarities and discrepancies. Although the literature has supported the frequent use of high-quality, stolen photos, the prevalence of specific scammer profiles is under debate. Recent findings suggest that significant differences in the proclaimed demographics and personality traits exist based on the target population and the origin of the profile (Whitty, 2013a; Edwards *et al.*, 2018). On average, male profiles stated higher age ranges and more prestigious professions than their female counterparts.

Finally, research on the consequences experienced confirmed the preconceived idea of a double hit that affects victims financially and emotionally. Victims have reported feelings including shame, embarrassment, shock, anger, worry and physical and mental health problems (Whitty and Buchanan, 2016; Cross, 2019). Other victims also stated losing an 'ideal', almost therapeutic, relationship (Whitty and Buchanan, 2016). Common themes were the struggle to cope with their experiences due to a lack of support from peers and a strong notion of self-blame.

4.3. RQ2—Influencing factors

Despite a number of papers establishing influencing factors that increase the likelihood of becoming a victim, few factors are statistically significant (Garrett, 2014; Whitty, 2018). The indicative ones, such as gender, education, age, active engagement in online dating, desire to find an international partner, impulsivity, locus of control and neuroticism, are not free from contradiction. Gender has been highly controversial. Although the studies by Whitty (2018) and Shaari *et al.* (2019) suggest that women are more at risk, Rege (2009) reasons that a romance scam is gender-agnostic. However, Whitty (2020) later suggests that men are more prone to fall for romance scams than women.

A better understanding of the influencing factors is needed because it could help to tailor law enforcement efforts and improve intervention success (Webster and Drew, 2017). Hence, we suggest that future research disaggregates the available data by influencing factors to identify vulnerable groups to a particular scam type. Factors that should be considered are pre-dispositional factors, such as previous experiences in relationships, sexual orientation, physical and mental health problems and the financial situation before the scam. In addition, such high-level data means it can be difficult to establish links between victim characteristics and the type of scammer profile they find engaging.

Saad *et al.* (2018) conducted a study based on association rule learning, identifying four specific profile categories of victims in Malaysia. Despite these novel findings, the work has multiple shortcomings. Firstly, it is unclear why the type of fraud was defined as parcel scams in the associative learning rules, even though the document was concerned with romance scams. Secondly, the authors did not discuss their finding that married people are at particular risk of victimization, which is seemingly counterintuitive.

Regarding profiling fraudsters, commonalities in the motivation and neutralization techniques were identified because scammers are primarily driven by the prospect of financial gain and place blame on the victims (Barnor *et al.*, 2020; Offei *et al.*, 2020). However, beyond that, very little is known about the demographics and psychological insights of the offenders.

4.4. RQ3—Countermeasures and mitigations

Regarding technical countermeasures, six studies were identified. The features considered were: profile images (de Jong, 2019;

Suarez-Tangil *et al.*, 2019; Al-Rousan *et al.*, 2020; Graham, 2021), profile descriptions and demographics (Suarez-Tangil *et al.*, 2019; He *et al.*, 2021), keystroke patterns (Li *et al.*, 2019), as well as the behaviour showcased by a scammer (He *et al.*, 2021). Different datasets used in the study may influence the performance of the proposed countermeasure. A possible solution is the publication of a standardized dataset with known scammers and benign profiles. The publication of structured, machine-legible data could also enable a streamlined development of technical countermeasures because current research (Suarez-Tangil *et al.*, 2019; Graham, 2021) scraped unstructured and semi-structured data from websites like datingnmore.com and scamdigger.com. Publishing structured data on fraudulent profiles through an API, similar to existing solutions for managing phishing submissions, would also support the rapid integration into end-user–facing solutions, like browsers and chat clients.

It was noted that ensemble classifiers outperformed singular classifiers. Works by Suarez-Tangil *et al.* (2019) and He *et al.* (2021) independently confirmed the benefit of using an ensemble classifier that combines predictions of the single classifiers that comprise the fraud detection system.

One limitation that all studies had in common is that the countermeasures are rarely viable for end-users to use during online dating. The closest work to an integrated solution, a browser add-on proposed by Graham (2021), still required a locally running Python server to perform the reverse image search. Different applications that must run simultaneously might severely inhibit the adoption among online daters and would be most unsuitable for non-technical users; thus, a more usable solution is required.

The analysis surrounding intrinsically motivated safeguarding strategies by Luu *et al.* (2017) showed that an individual's coping appraisal and the factors of response efficacy and self-efficacy significantly influence the adoption of safeguarding techniques when online dating (even more than threat appraisal). Similarly, Whitty (2019) reported that previous experience in online dating deception improves the ability to spot deceit. Therefore, training and awareness resources must be well disseminated on online dating sites and strengthen the individuals' belief that they can protect themselves from financial losses and emotional harm. Current guidance around online dating often focuses on listing risky behaviours rather than persuading individuals to consider adverse outcomes associated with romance scams and the individual's ability to cope. Therefore, we endorse Whitty's (2019) call to develop interactive awareness and training material that teaches potential victims how to detect and prevent romance scams. Similar methods used to educate employees about phishing have indicated improved confidence levels among participants (Cj *et al.*, 2018).

Because romance scams are still a heavily stigmatized crime, few victims have been able to disclose their experiences and receive support (Whitty and Buchanan, 2016; Cross, 2019). Although the research concerned with externally stimulated intervention approaches, such as peer support groups and active policing, has displayed some success, more work is needed to support victims (Webster and Drew, 2017; Cross, 2019). Law enforcement plays a key role because they are typically the first point of contact after a victim realizes that they have been defrauded or even while victims are still caught in the scam in the case of active policing (Whitty and Buchanan, 2016; Webster and Drew, 2017). Hence, law enforcement personnel working with romance scam victims must be well trained in handling the traumatized, potentially disbelieving and vulnerable victims and inform victims about professional counselling and support.

4.5. Further considerations

When looking at the current proposed technical countermeasures, it is clear that these primarily target the dating platform. However, based on the profiling of romance scams and the analysis of persuasive tactics, we have explained that scammers swiftly move communication away from the first contact point to minimize their risk of getting blocked. This action, however, reduces the amount of behavioural data, such as exchange chat messages, that can be collected from the platform where the initial contact occurred. Therefore, we recommend that future research be conducted independent of changes in communication platforms.

Dating and relationships are highly delicate aspects of people's lives. Thus, we see a strong need for ethical and legal considerations when conducting research that might infringe on the privacy of unsuspicious online daters. For future work in this space, it will be necessary to establish stringent policies that govern the secure collection, handling, storage and deletion of data.

This review identified contributions from various backgrounds and disciplines, using various frameworks and approaches. To harness the full power of the different research fields, such as psychology, linguistics and computer science, more interdisciplinary work is required, as has already been called for by Sorell and Whitty (2019). In particular, the development of advanced technical countermeasures, such as machine learning models, needs to be well grounded in established theory. Factors that come into play are the characteristics and processes of romance scams, persuasive tactics, linguistic patterns and influencing and propensity factors of becoming a victim. This state-of-the-art review on romance scams has demonstrated that this field offers ample opportunity for nurturing interdisciplinary research.

Ultimately, improved countermeasures and mitigation strategies can help prevent romance scams. However, as Barnor *et al.* (2020) and Offei *et al.* (2020) reasoned, more effective law enforcement is also needed to apprehend perpetrators in countries where scams originate.

5. CONCLUSION

Romance scams constitute an ever-increasing challenge for online daters, dating platform providers and law enforcement. In particular, the COVID-19 pandemic, with its lockdown restrictions, may have contributed to increases in victimization. This systematic review has examined the major findings of studies in the field. It assessed the approaches for profiling romance scams, the socio-demographic and psychological factors of persons involved and countermeasures and mitigation techniques.

Our comprehensive analysis of the salient study characteristics showed that the field has received considerable interest, especially during the last 3 years; however, the total number of relevant studies remained small ($n = 53$). Most studies in our review contributed to profiling romance scams by establishing process models to describe the progression of the scam or analysing linguistic patterns and persuasion techniques used by the scammers when interacting with their victims. In addition, studies examined scammers' online dating profiles for commonalities, such as occupations, marital status and age. These findings can aid in developing improved detection and mitigation techniques and seed the development of practical training and awareness programmes.

Countermeasures and mitigation techniques have also received much attention. Various studies proposed that machine learning classifiers can detect fraudulent profiles on online dating sites by considering features such as profile characteristics, profile image and behaviour. However, as indicated in Section 4.4, the absence of common datasets for training and testing severely limits the deployment of machine learning techniques.

Less commonly found within the review were contributions on the socio-demographic and psychological factors, including age, gender and education of victims and scammers. Although diverse characteristics attributed to victimization have been considered, few were statistically significant. Because romance scams are still a relatively new and multifaceted research field, it is unsurprising that limited attention is given to the factors that increase the risk of victimization.

Although valuable contributions have already been made in the field, an additional cross-organizational collaboration between researchers, platform providers and law enforcement will be required to address current issues.

Romance scams will remain an arms race between cybercriminals and bona fide online daters. As new scam techniques emerge and existing ones evolve, future research must keep pace with scammers' ever-changing methods. New ways to detect and prevent romance scams must be developed in tandem with engaging training and awareness programmes.

Acknowledgements

The authors would like to thank the Scottish Funding Council and Abertay University's Graduate School for supporting the research.

Funding

This research was funded by the Scottish Funding Council.

Data availability

The data supporting this study are openly available on figshare at 10.6084/m9.figshare.21817587

Conflict of Interest

The authors report there are no competing interests to declare. The funders had no involvement in the study's design, data collection, analysis, interpretation, manuscript writing or publication of the findings.

References

Action Fraud (2023) Action Fraud - National Fraud and Cyber Crime Reporting Centre. *Action Fraud*. https://www.actionfraud.police.uk/ (accessed January 21, 2023).

Al-Rousan, S., Abuhussein, A., Alsubaei, F., Kahveci, O., Farra, H. and Shiva, S. (2020) Social-Guard: Detecting Scammers in Online Dating. In *2020 IEEE International Conference on Electro Information Technology (EIT)*, Chicago, IL, USA, 2020-July, pp. 416–422.

Amazon (2023) *Amazon Rekognition Documentation*. https://docs.aws.amazon.com/rekognition/ (accessed January 21, 2023).

Anesa, P. (2020) Lovextortion: persuasion strategies in romance cybercrime. *Discourse Context & Media*, **35**, 100398–100398.

Annadorai, K., Krish, P., Shaari, A. H. and Kamaluddin, M. R. (2018) Mapping computer mediated communication theories and persuasive strategies in analysing online dating romance scam. *Journal of Xi'an Shiyou Univ.* ISSN No, 1673, p.064X, **14**, 37–47.

Auger, P. (1998) *Information Sources in Grey Literature, Berlin*. De Gruyter Saur, Boston 1998.

Barclays (2023) *Romance Scams*. https://www.barclays.co.uk/fraud-and-scams/romance-scams/ (accessed September 10, 2023).

Barnor, J. N. B., Boateng, R., Kolog, E. A. and Afful-Dadzie, A. (2020) Rationalizing online romance fraud: in the eyes of the offender. *2020 Americas Conference on Information Systems. AMCIS 2020 Proceedings. 21*. 1–10.

BBC (2021) Romance fraud: 'I wish I hadn't given £300k to a man I met online. *BBC News*. https://www.bbc.com/news/newsbeat-59135689 (accessed January 21, 2023).

Buchanan, T. and Whitty, M. T. (2014) The online dating romance scam: causes and consequences of victimhood. *Psychol. Crime Law*, **20**, 261–283.

Buchholz, K. (2023) *How the World Dates Online [Digital image]*. https://www.statista.com/chart/24165/online-dating-penetration-rate-revenue-selected-countries/ (accessed June 18, 2023).

Buil-Gil, D. and Zeng, Y. (2021) Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*, **29**, 460–475.

Button, M., Nicholls, C. M., Kerr, J. and Owen, R. (2014) Online frauds: learning from victims why they fall for these scams. *Aust. N. Z. J. Criminol.*, **47**, 391–408.

Carter, E. (2021) Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. *The British Journal of Criminology*, **61**, 283–302.

Cialdini, R. B. (2007) *Influence: The Psychology of Persuasion*. HarperCollins, New York.

Cj, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V. and Lodha, S. (2018) PHISHY - a serious game to train enterprise users on phishing awareness. *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169–181. https://doi.org/10.1145/3270316.3273042.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A. and Gualtieri, G. (2020) Online romance scams: relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clin. Pract. Epidemiol. Ment. Health*, **16**, 24–35.

Covidence—Better systematic review management. (2022) *Covidence*. https://www.covidence.org/ (accessed December 21, 2022).

Cross, C. (2016a) 'They're very lonely': understanding the fraud victimisation of seniors. *Int. J. Crime Justice Soc. Democr.*, **5**, 60–75 Publicly Available Content Database.

Cross, C. (2016b) Using financial intelligence to target online fraud victimisation: applying a tertiary prevention perspective. *Crim. Justice Stud.*, **29**, 125–142.

Cross, C. (2019) "You're not alone": the use of peer support groups for fraud victims. *J. Hum. Behav. Soc. Environ.*, **29**, 672–691.

Cross, C. (2020) *Romance fraud*. The Palgrave handbook of international cybercrime and cyberdeviance, pp. 917–937.

Cross, C. and Blackshaw, D. (2015) Improving the police response to online fraud. *Policing*, **9**, 119–128.

Cross, C. and Holt, T. J. (2021) The use of military profiles in romance fraud schemes. *Vict. Offenders*, **16**, 385–406.

Cross, C. and Holt, T. J. (2023) More than money: examining the potential exposure of romance fraud victims to identity crime. *Global Crime*, **24**, 107–121.

Cross, C. and Layt, R. (2022) "I suspect that the pictures are stolen": romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Soc. Sci. Comput. Rev.*, **40**, 955–973.

Cross, C. and Lee, M. (2022) Exploring fear of crime for those targeted by romance fraud. *Vict. Offenders*, **17**, 735–755.

Cross, C., Dragiewicz, M. and Richards, K. (2018) Understanding romance fraud: insights from domestic violence research. *The British Journal of Criminology*, **58**, 1303–1322.

Cross, C., Holt, K. and O'Malley, R. L. (2022) "If U don't pay they will share the pics": exploring Sextortion in the context of romance fraud. *Vict. Offenders*, **1–22**, 1–22.

Cross, C., Holt, K. and Holt, T. J. (2023) To pay or not to pay: an exploratory analysis of sextortion in the context of romance fraud. *Criminol. Crim. Just.*, **1–16**, 174889582211495.

Dating 'n More. (2021) *Dating 'n More*. https://datingnmore.com/ (accessed December 2, 2021).

Dickerson, S., Apeh, E. and Ollis, G. (2020) Contextualised Cyber Security Awareness Approach for Online Romance Fraud. In *7th International Conference on Behavioural and Social Computing (BESC)*, pp. 1–6. IEEE.

Dickinson, T., Wang, F. and Maimon, D. (2023) What money can do: examining the effects of rewards on online romance fraudsters' deceptive strategies. *Deviant Behav.*, **44**, 1386–1400.

Dreijers, G. and Rudziša, V. (2020) Devices of textual illusion: victimization in romance scam e-letters. *Research in Language*, **18**, 1–13.

Edwards, M., Suarez-Tangil, G., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M. (2018) The geography of online dating fraud. *Workshop on Technology and Consumer Protection (ConPro)*, 1–7.

Eseadi, C., Ogbonna, C. S., Otu, M. S. and Ede, M. O. (2021) Hello Pretty, Hello Handsome!: Exploring the Menace of Online Dating and Romance Scam in Africa. In Oliver Chan, H. C., Adjorlolo, S. (eds), *Crime, Mental Health and the Criminal Justice System in Africa: A Psycho-Criminological Perspective*, pp. 63–87. Springer International Publishing, Switzerland.

Financial Ombudsman Service (2023) *Financial Ombudsman Service Warns of Increase in 'Hybrid' Scams*. https://www.financial-ombudsman.org.uk/news-events/financial-ombudsman-service-warns-increase-hybrid-scams (accessed September 10, 2023).

Garrett, E. V. (2014). *Exploring internet users' vulnerability to online dating fraud: Analysis of routine activities theory factors (1656449717)*. M.S., The University of Texas at Dallas, USA. http://hdl.handle.net/20.500.11990/2034.

Gillespie, A. A. (2017) The electronic Spanish prisoner: romance frauds on the internet. *The Journal of Criminal Law*, **81**, 217–231.

Gillespie, A. A. (2021) Just the money? Does the criminal law appropriately tackle romance frauds? *Journal of International and Comparative Law*, **8**, 1, 143–174.

Google Vision AI | Cloud Vision API | Google Cloud (2023) *Google. Google*. Available at: https://cloud.google.com/vision (accessed January 21, 2023).

Gould, K. R., Carolan, M. and Ponsford, J. L. (2023) Do we need to know about cyberscams in neurorehabilitation? A cross-sectional scoping survey of Australasian clinicians and service providers. *Brain Impairment*, **24**, 229–244.

Graham, A. (2021) *Automatic Detection of Fraudulent Dating Site Profiles Through Use of Reverse Image Searching*. M.S., University of Bristol, United Kingdom. http://xn--bta-yla.net/students/graham2021automatic.pdf

Gregory, D. and Nikiforova, B. (2012) A sweetheart of a deal: how people get hooked and reeled in by financial scams. *The Journal of Behavioural Finance and Economics*, **2**, 96–122.

He, X., Gong, Q., Chen, Y., Zhang, Y., Wang, X. and Fu, X. (2021) DatingSec: detecting malicious accounts in dating apps using a content-based attention network. *IEEE Transactions on Dependable and Secure Computing*, **1–16**, 1.

Herzog, T. A. (2008) Analyzing the transtheoretical model using the framework of Weinstein, Rothman, and Sutton (1998): the example of smoking cessation. *Health Psychol.*, **27**, 548–556.

HSBC. (2023) *What's the Difference Between Fraud and a Scam?*. https://www.hsbc.co.uk/help/security-centre/fraud-guide/difference-between-fraud-and-scams/ (accessed September 10, 2023).

Huang, J., Stringhini, G. and Yong, P. (2015) Quit Playing Games with My Heart: Understanding Online Dating Scams. In Almgren, M., Gulisano, V., Maggi, F. (eds), *Detection of Intrusions and Malware, and Vulnerability Assessment*Vol. 9148, pp. 216–236. Springer International Publishing, Switzerland.

Jimoh, I. and Stephen, K. (2018) Is this love? A study of deception in online romance in Nigeria. *Covenant Journal of Communication*, **5**, 40–61.

de Jong, K. (2019) *Detecting the Online Romance Scam: Recognising Images Used in Fraudulent Dating Profiles*. University of Twente, Netherlands.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F. and Díaz-Castaño, N. (2021) Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during COVID-19. *J. Contemp. Crim. Justice*, **37**, 480–501.

Khader, M. and Yun, P. S. (2017) *A Multidisciplinary Approach to Understanding Internet Love Scams: Implications for Law Enforcement*. In The Psychology of Criminal and Antisocial Behavior (pp. 523-548). Academic Press.

Koon, T. H. and Yoong, D. (2017) Preying on lonely hearts: a systematic deconstruction of an internet romance scammer's online lover persona. *Journal of Modern Languages*, **23**, 28–40.

Kopp, C., Layton, R., Sillitoe, J. and Gondal, I. (2015) The role of love stories in romance scams: a qualitative analysis of fraudulent profiles. *Int. J. Cyber Criminol.*, **9**, 205–217.

Kopp, C., Sillitoe, J., Gondal, I. and Layton, R. (2016a) Online romance scam: expensive e-living for romantic happiness. *BLED*, **2016**, 175–189.

Kopp, C., Sillitoe, J., Gondal, I. and Layton, R. (2016b) The online romance scam: a complex two-layer scam. *Journal of Psychological and Educational Research*, **24**, 144–161.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021) Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers and Security*, **105**, 102248–102221.

Lazarus, S., Whittaker, J. M., McGuire, M. R. and Platt, L. (2023) What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, **2**, 100013.

Li, G., Borj, P. R., Bergeron, L. and Bours, P. (2019) Exploring keystroke dynamics and stylometry features for gender prediction on chat data. *42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1049–1054. https://doi.org/10.23919/MIPRO.2019.8756740.

Luu, V., Land, L. and Chin, W. W. (2017) Safeguarding against romance scams – using protection motivation theory. *25th European Conference on Information Systems (ECIS)*, 2429–2444.

Modic, D. and Anderson, R. (2015) It's all over but the crying: the emotional and financial impact of internet fraud. *IEEE Secur. Priv.*, **13**, 99–103.

Momo (2023) *Momo*. Momo Technology Co., Ltd. Available at: https://www.immomo.com/ (accessed January 21, 2023).

Mondal, S., Bours, P., Johansen, L., Stenvi, R. and Øverbø, M. (2017) Importance of a Versatile Logging Tool for Behavioural Biometrics and Continuous Authentication Research. In *Developing Next-Generation Countermeasures for Homeland Security Threat Prevention*, pp. 282–305. IGI Global, Pennsylvania.

Obada-Obieh, B., Chiasson, S. and Somayaji, A. (2017) “Don’t break my heart!”: user security strategies for online dating. *Workshop on Usable Security (USEC)*, 1–6.

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W. and Asamoah, D. (2022) How do individuals justify and rationalize their criminal behaviors in online romance fraud? *Inf. Syst. Front.*, **24**, 475–491.

Okcupid (2023) OkCupid. *Match Group*. Available at: https://www.okcupid.com/ (accessed January 21, 2023).

Page, M. J. *et al.* (2021) The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, **372**, 1–9. https://doi.org/10.1136/bmj.n71.

Pan, J. A., Winchester, D., Land, L. and Watters, P. (2010) Descriptive data mining on fraudulent online dating profiles. *18th European Conference on Information Systems (ECIS)*, 1–11. https://aisel.aisnet.org/ecis2010/145.

Pizzato, L. A., Akehurst, J., Silvestrini, C., Yacef, K., Koprinska, I. and Kay, J. (2012) The Effect of Suspicious Profiles on People Recommenders. In *User Modeling, Adaptation, and Personalization: 20th International Conference*, UMAP 2012, Montreal, Canada, July 16-20, 2012. Proceedings 20 (pp. 225-236). Springer, Berlin Heidelberg.

Rege, A. (2009) What’s love got to do with it? Exploring online dating scams and identity fraud. *International Journal of Cyber Criminology (IJCC)*, **3**, 494–512.

Rege, A. (2013) 10v3.c0ns: a criminological investigation of online dating crimes. In *2013 APWG eCrime Researchers Summit*, pp. 1–9. IEEE. https://doi.org/10.1109/eCRS.2013.6805773.

Rogers, R. W. (1983) Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. In Cacioppo, J., Petty, R. (eds), *Social Psychophysiology*. Guilford Press, New York.

Saad, M. E., Norul, S. and Zamri, M. (2018) Cyber romance scam victimization analysis using routine activity theory versus Apriori algorithm. *International Journal of Advanced Computer Science and Applications (IJACSA)*, **9**, 479–485.

ScamDigger. (2021). *ScamDigger*. https://scamdigger.com/

Scamwatch (2023) Scamwatch. *Australian Competition and Consumer Commission (ACCC)*. Available at:. https://www.scamwatch.gov.au/ (accessed June 14, 2023).

Shaari, A. H., Kamaluddin, M. R., Paizi@Fauzi, W. F. and Mohd, M. (2019) Online-dating romance scam in Malaysia: an analysis of online conversations between scammers and victims. *GEMA Online® Journal of Language Studies*, **19**, 97–115.

Smeitink, H. (2021). *A Postmodern Love Story*. MS Thesis. Utrecht University, Netherlands. *https://www.fraudehelpdesk.nl/wp-content/uploads/2021/02/Thesis-Hester-Smeitink.pdf*

Sorell, T. and Whitty, M. (2019) Online romance scams and victimhood. *Secur. J.*, **32**, 342–361.

Steyerl, H. (2011) Epistolary affect and romance scams: letter from an unknown woman∗. *October*, **138**, 57–69.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A. and Whitty, M. (2020) Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, **15**, 1128–1137.

Tao, H. (2022) Loving strangers, avoiding risks: online dating practices and scams among Chinese lesbian (*lala*) women. *Media Cult. Soc.*, **44**, 1199–1214.

Thompson, S. (2016) In defence of the ‘gold-digger’. *Oñati Socio-Legal Series*, **6**, 24.

TinEye. (2023). *Reverse Image Search. TinEye*. https://tineye.com/ (accessed January 21, 2023).

Wang, F. and Topalli, V. (2022) Understanding romance scammers through the lens of their victims: qualitative modeling of risk and protective factors in the online context. *Am. J. Crim. Justice*, **1-37**. https://doi.org/10.1007/s12103-022-09706-4.

Wang, F. and Zhou, X. (2022) Persuasive schemes for financial exploitation in online romance scam: an anatomy on *Sha Zhu Pan* (杀猪盘) *in* China. *Vict. Offenders*, **18**, 915–942.

Webster, J. and Drew, J. M. (2017) Policing advance fee fraud (AFF): experiences of fraud detectives using a victim-focused approach. *Int. J. Police Sci. Manag.*, **19**, 39–53.

Whitty, M. (2013) The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam. *Br. J. Criminol.*, **53**, 665–684.

Whitty, M. (2015) Anatomy of the online dating romance scam. *Secur. J.*, **28**, 443–455.

Whitty, M. (2018) Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychol. Behav. Soc. Netw.*, **21**, 105–109.

Whitty, M. (2019) Who can spot an online romance scam? *Journal of Financial Crime*, **26**, 623–633.

Whitty, M. (2020) Is there a scam for everyone? Psychologically profiling cyberscam victims. *Eur. J. Crim. Policy Res.*, **26**, 399–409.

Whitty, M. and Buchanan, T. (2012) The online romance scam: a serious cybercrime. *Cyberpsychol. Behav. Soc. Netw.*, **15**, 181–183.

Whitty, M. and Buchanan, T. (2016) The online dating romance scam: the psychological impact on victims – both financial and non-financial. *Criminol. Crim. Just.*, **16**, 176–194.

Whitty, M., Edwards, M., Levi, M., Peersman, C., Rashid, A., Sasse, A., Sorell, T. and Stringhini, G. (2017) Ethical and social challenges with developing automated methods to detect and warn potential victims of mass-marketing fraud (MMF). *WWW’17 Companion*, 1311–1314. https://doi.org/10.1145/3041021.3053891.

Yandex Search. (2023) . *Yandex*. Available at: https://yandex.com/ (accessed January 21, 2023).

Yu, H.-F., Ho, C.-H., Juan, Y.-C. and Lin, C.-J. (2013) *LibShortText: A Library for Short-Text Classification and Analysis*. Available at: https://www.csie.ntu.edu.tw/&#x007E;cjlin/libshorttext/ (accessed January 21, 2023).