Love at first sleight: a review of scammer techniques in online romance fraud

Marc Kydd
Lynsay A. Shepherd
Andrea Szymkowiak
Graham I. Johnson

This version of the contribution has been accepted for publication, after peer review, but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record in available online at: http://dx.doi.org/10.1007/978-981-99-6974-6_18

Use of this accepted version is subject to the publisher's Accepted Manuscript terms of use.

Love at First Sleight: A Review of Scammer Techniques in Online Romance Fraud

Marc Kydd, Lynsay A. Shepherd, Andrea Szymkowiak, Graham I. Johnson

School of Design and Informatics, Abertay University, Bell Street, Dundee, DD1 1HG, United Kingdom.

Contributing authors: m.kydd1800@abertay.ac.uk; lynsay.shepherd@abertay.ac.uk; a.szymkowiak@abertay.ac.uk; g.johnson@abertay.ac.uk;

Abstract

Romance fraud, where a scammer exploits a victim for monetary gain under the guise of 'true love', is a relatively new form of cybercrime which has become increasingly prevalent. Attempts to tackle romance fraud have been made by law enforcement and dating platforms. The latter commonly utilise awareness campaigns, informing users about the risks associated with online dating and how to spot warning signs. However, such campaigns tend to be overly generic, repeatedly giving the same advice. Other campaigns provide vague or outdated advice, which leaves readers unable to protect themselves. This paper presents a state-of-the-art review of the varying approaches that scammers can take on the path to exploiting their victims both in selecting a suitable target and keeping them engaged as part of the scam. Findings highlight that methods by which scammers target, select, and exploit victims of romance fraud can vary greatly. Rather than following a strict structure as depicted in awareness campaigns, romance fraud is a continually evolving, and unique form of cybercrime with multiple variations at each stage of the process. These variations also lay the foundations for future studies on the overlap of cybercrime and abuse, and the role of organised crime in romance fraud.

Keywords: Romance fraud, online dating, scams, cybercrime, human-centered cybersecurity

1 Introduction

Romance fraud is a form of social engineering, whereby fraudsters create a fake profile on dating platforms and strike up a relationship with potential victims, with the end goal of conning them out of money. The resulting damage to victims can be devastating. Although the victim is most often targeted for financial exploitation, romance fraud has also been leveraged for blackmail, sexual abuse, and drug smuggling [1–3]. It is a cruel form of cybercrime where victims experience both heavy financial losses and the end of a relationship which felt real to the victim [2, 4, 5].

Dating platform users are also perhaps uniquely vulnerable, given the emphasis often placed on being 'authentic' and 'open' about their life when creating a profile and interacting with others. This typically translates into users being much more transparent about their lives with other users to increase the chance of a match [6]. However, such transparency also makes users prime targets for scammers.

Following the COVID-19 pandemic, many across society have turned online like never before [7, 8] for work, entertainment, and to forge connections. Online dating platforms have seen a considerable increase in users as many have decided they would rather not go through these challenging times alone [9]. While many of these new users are looking for love, some seek monetary gain through romance fraud. Although instances of romance fraud have been steadily climbing over the past decade, the onset of the pandemic has exacerbated the occurrence of this type of crime.

Attempts have previously been made to tackle romance fraud by law enforcement and the dating platforms themselves, using awareness campaigns informing users about the risk of online dating and warning signs to look out for. However, such campaigns tend to continually provide the same advice. In an attempt to remedy this, other campaigns instead attempt to make the advice given so vague that individuals are left confused and unable to protect themselves [5].

This paper explores romance fraud from the scammers' perspective and highlights that it does not follow the set pattern often portrayed in typical awareness campaigns. Previous attempts to clearly define what is and is not a romance scam have often left users confused to the extent that victims of these scams do not recognise that they have been scammed in the manner the awareness campaign is supposed to guard against [5]. Romance scams are a complex and adaptive form of cyber-enabled scams that are specifically crafted for maximum effectiveness against each victim. This state-of-the-art review on scammer techniques highlights the varying approaches scammers can take on the path to exploiting their victim, both in selecting a suitable target and keeping them engaged as part of the scam. Ultimately, this paper seeks to deepen the broader understanding of why romance fraud continues to be so effective by examining and classifying the techniques and tactics used by scammers, with a view to create a framework that allows to identify techniques to address this form of cybercrime. Figure 1 provides an overview of these approaches and the different phases involved in romance fraud, from finding a potential victim to various exploitation phases that are discussed in the following sections.

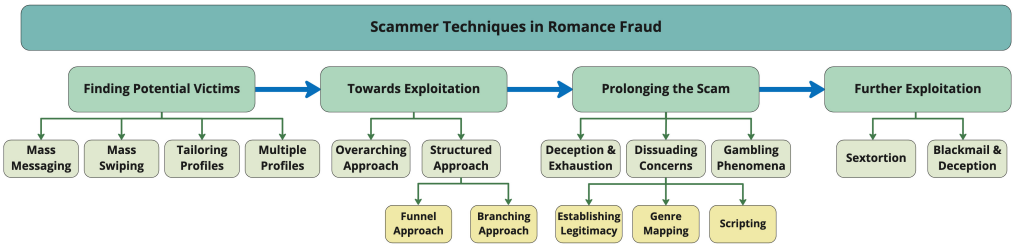

Fig. 1: Overview of scammer techniques in romance fraud.

2 Finding Potential Victims

Romance fraud is perhaps unusual compared to other forms of cybercrime because it typically requires sustained involvement from the scammer and buy in from the victim. Rather than sending out thousands of non-specific phishing emails, romance fraud requires that the scammer be actively involved over an extended time period, interacting with an intended victim. Scammers may spend a considerable amount of time building rapport with a potential victim who may cease communication when they realise a scammer attempts to exploit them. Therefore, to ensure the effectiveness of the attempted fraud, there are several approaches the scammer can draw from to lure the "right" kind of victim.

2.1 Mass Messaging

The most straightforward approach is to message as many accounts on dating platforms as possible. By 'matching' with every available account, scammers can rely on the fact that, statistically, someone will reply. In a study of user behaviour on the Chinese dating platform Jiayuan (世纪佳缘), it was found that scam accounts were much more active than legitimate users [10]. Most users contacted less than five accounts concurrently, with particularly active users reaching around thirty concurrent matches. Scammers, however, frequently contacted over 100 accounts at once, much more than that of the typical user. Such high numbers are likely to be a conservative estimate, as these accounts were flagged as suspicious and blocked before their owners could contact more users.

Flooding a wide range of users with messages from the scammer is one approach to finding a victim. However, this 'brute force' method has the potential to be easily detected, and blocked. Thus, scammers have instead attempted a subtler, but potentially more effective approach, exploiting features of the dating platforms.

2.2 The Match-Making Process

Many platforms have simplified the user matching process down to a single swipe on the individual's mobile device: swipe right for yes, expressing interest for a potential romantic candidate, and swipe left for no interest. A match is made if two users mutually swipe right on each other's profiles. Rather than engaging in online chat over an extended period, the swiping gesture dramatically increases the speed with

which users can indicate their interest or not in another user. However, by reducing the matching process down to indicating mutual interest with a single gesture, such a practice is also ripe for exploitation by scammers. By leveraging the speed at which connections to new users can be made, scammers can reach a wider range of users in a much shorter time span than with traditional chat-oriented dating platforms. In fact, by simply swiping to indicate interest in every available user, scam accounts can significantly increase their pool of victims [11]. Such disingenuous behaviour is challenging to detect on dating platforms, allowing scammers to build up a collection of potential victims within a relatively short timeframe.

2.3 Tailoring Profiles

Simply attempting to 'game' the dating platforms does not mean the scammer will find a suitable victim, however. The scammer requires a means of tailoring how they appear on the platform to maximise the likelihood of a suitable victim getting in contact. The profile plays a critical role in online dating, often being the first thing that users see about a potential match. It is a place for users to express themselves, to share hobbies, interests, and what they are looking for in a potential partner. These factors also make the profile an opportunistic place for scammers to target their victims.

Considerable thought goes into crafting a deceptive profile, and the details thereof can vary significantly depending on the targeted victim. In a study of over 5,000 known scam accounts, scammers were found to adjust almost every facet of their profiles to appeal to the victim's profile [12],for example, matching their interests. Further, the location of the scammer appears to influence the style of misleading profiles they create. Scammer profiles originating from Nigeria, Malaysia, and South Africa typically presented false male profiles featuring individuals around the age of 50. Ukraine, Senegal, and the Philippines, meanwhile, were more likely to present false female profiles of individuals closer to 30. Female profiles were also less likely to declare themselves divorced or widowed, compared with male profiles.

Although the scammer's location shaped some aspects of the profile, the target country also influenced what kind of scam profiles were presented to users [12]. Each country appeared to have a unique archetype of a scam profile. Globally, the most common was that of a white male or female working in the military or an engineering occupation. However, users in the United Kingdom were typically presented with fake accounts claiming to be a divorcee. Indian users tended to see males who were in a 'businessman'-type role. Meanwhile, accounts in Eastern Europe most commonly saw white males or females working in the accounting profession.

2.4 Multiple Profiles

Yet a singular profile will not work for every kind of potential victim. Therefore, it is not uncommon for scammers to have multiple accounts across multiple dating platforms [10, 13]. The practice of creating multiple accounts is not wholly unique to scammers; legitimate users are also known to engage in such practice [14]. In some instances, users create multiple accounts with differing details to appeal to a broader

range of potential partners. The details altered could mean misconstruing factors such as relationship status, age, weight, socio-economic status, and interests.

The profile picture, arguably the first piece of information many potential partners will see, was also a point of intense consideration. In interviews with users, it was noted that they wanted 'something decent' to use for their profile [14]. What 'decent' means in this context appeared to vary between users. Some used an image of themselves where they were clearly visible in a generally tidy environment; others went so far as to get professional photos taken.

This practice of 'slightly' adjusting how users present themselves is widespread enough that 51% of users confirmed that at least one aspect of their profile could be considered misrepresentative [14]. Users did state that they were not doing this for malicious purposes but as means of managing impressions such that someone they believed was genuinely interested in them would be attracted.

Although using multiple accounts shows similarities between legitimate users and scammers, a key difference between users and scammers is that illegitimate accounts were significantly more verbose in their profile descriptions than those of genuine users [15]. While users would keep to around 54 words in their profile descriptions, scammers used approximately 105 words. This variance is likely due to dating platform users being conscious of how online platforms can use their data [16]. While legitimate users were concerned about how the information they present about themselves could pose a privacy issue, scammers producing fake accounts appear not to be affected by this. As such, fake scammer profiles can be much more expansive as the details presented do not pose any privacy or security concerns to the scammer themselves.

3 Towards Exploitation

Scammers can utilise a wide range of approaches to lure victims. Whether it be mass messaging users or hijacking recommendation systems, targeting specific demographics via account profiles or testing dozens of variations of tailored profiles, it is only a matter of time before a scammer finds a potential victim. Once a potential victim has been identified, the focus shifts to building an authentic connection with the victim which can later be exploited. The following sections detail the varying approaches to exploitation once a contact with a potential victim has been established.

3.1 Overarching Approach

Though there are many steps that scammers can take their victims through in an attempt to exploit them, the speed with which this goal is realised will vary. The bluntest approach is to ask for a large amount of money early in the conversation - the 'face-in-the-door' approach [17]. Although risky to the scammer, attempting to defraud the victim in this manner offers several potential benefits. For one, it avoids the need for building a false narrative and general trust with the victim before attempting to make a request, allowing the scammer to exploit the victim much faster. 'Face-in-the-door' also acts as a test of the victim's suggestibility to the scammer. If the victim complies with such a large request so readily, the scammer can be reasonably confident that future requests will also be met. Requesting a large amount of money

also sets the victim up for future exploitation, as subsequent requests for money can be rationalised much more easily, if they are less than the initial large sum the victim transferred and if there is already buy-in from the victim..

Alternatively, a subtler approach can be found within the 'foot-in-the-door' approach. As the converse of the 'face-in-the-door' method, this tactic sees the scammer request small amounts of money that are likely to increase gradually over time. Rather than risk the victim being shocked at a sudden large request and ceasing communication, small transfers are much less likely to raise suspicion. As such, this method allows the scammer to gradually drain the victim of funds over a more extended period - all the while doing so without the victim being fully aware of the accumulative total they have transferred. The gains from deploying a 'foot-in-the-door' approach can also be amplified by using this method in tandem with multiple scam accounts. By making requests for small amounts of money to a large number of victims, scammers may be able to exceed the gains of the 'face-in-the-door' method by drawing resources from multiple, unsuspecting victims at once.

3.2 Structured Approach

Although these two '-in-the-door' approaches illustrate how the scammer can approach the victim at the moment of exploitation, they do not acknowledge the steps the scammer must lead the victim through to arrive there. Moreover, the scammer must conduct a long and often varied process to build sufficient influence over the victim to exploit them. In this regard, there are two key frameworks that romance fraud scams tend to follow.

3.2.1 Funnel Approach

Carter [18] considers romance fraud to follow a funnel approach. As the victim becomes more entwined with the scammer, it becomes more difficult for the victim to realise just how far they have been misled. The approach (Figure 2) follows a fairly linear path, beginning with the victim initially coming into contact with the scammer. From here, the scammer can prime the victim, introducing key concepts (e.g., a sad life story or unfortunate circumstance) as part of the false narrative that will be leveraged at later stages. Expanding upon this, the scammer may also attempt to contextualise and rationalise any requests for money. The requests may be situated within other details of the scam to make the appeals either less obvious or more neatly integrated with the false narrative. Past this point, the scammer can begin to move towards exploitation, usually evoking a 'crisis'-like situation. The scammer will also attempt to isolate the victim by either downplaying the importance of the request for money, or by increasing the sense of urgency such that the victim feels there is no time to seek external input or conversations with external others such as friends or family. Finally, the victim is extorted of their money before the scammer ceases communication or works towards further exploiting the victim.

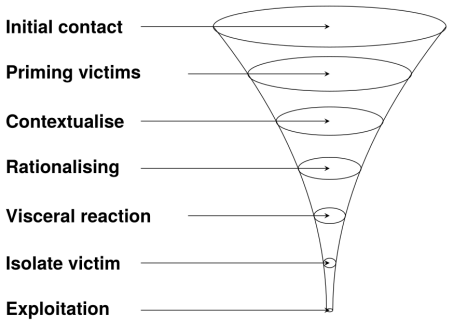

Fig. 2: The funnel approach, based on work by Carter[18]

3.2.2 Branching Approach

An alternative view on how romance fraud operates has been identified and iterated upon in the form of the branching approach [1, 19, 20]. It is a framework that allows for more variety in what constitutes romance fraud, and the steps scammers may take their victims through to exploit them. The framework has been iteratively refined and expanded over the years, as new tactics are discovered. It has expanded to include alternative approaches to romance fraud along with broadly related topics [20]. Most notably, the framework incorporates forms of exploitation which do not initially fall under the traditional view of economic exploitation as the defining outcome of romance fraud. The critical difference between the funnel and branching approaches is the acknowledgement of user autonomy and personal complexity throughout the scam i.e., the impact victim individuality which plays a vital role in how the scammer approaches them. Thus, the scammer personalises their responses to the behaviour of the victim. While the funnel approach views romance fraud as a downward spiral once the user begins conversing with the scammer, the branching approach notes how the user responds to requests from the scammer to influence the direction of the scam.

The branching framework begins by viewing the victims' desire to find an 'ideal partner' as the catalyst for romance fraud. With this mindset, the victim inadvertently discovers what is perceived as the 'perfect' profile (created by the scammer). Here, the user can critically assess the profile and determine whether they think it is a legitimate account. Should the victim initiate conversation, the scammer can begin a grooming process akin to the funnel approach (priming, contextualising, rationalising, etc.). At this point the branching aspect emerges, posing either a crisis scenario akin to the 'face-in-the-door' or a less obvious scenario similar to 'foot-in-the-door'. Should either method be successful, and the victim is exploited, the scammer can then iterate this process by introducing new scenarios, or by escalating existing ones until the victim is exhausted of funds or realises they are being scammed.

4 Prolonging the Scam

While the scammer can attempt to extort the victim early in the conversation, greater gains can be made by gradually extorting funds over a more extended time period. Ensuring the victim stays engaged throughout the scam is paramount for the scammer.

4.1 Deception and Exhaustion

To ensure the victim feels engaged and desired, scammers may attempt to personalise the narrative of the scam to their victim [21]. Typically, this is done by the scammer building a general persona in their profile description and gradually refining and adjusting factors to appeal to the victim, as they get to know them better. By adopting this approach, victims are given a personalised 'love story' where events, interests, perspectives and other factors conveniently match between the scammer and the victim.

A less sophisticated approach is to wear down the victim over time. One means of doing this is to solicit money when the victim is sleep-deprived, either by contacting the victim with a crisis at unfavourable hours or chatting with the victim for extended periods (i.e., upwards of 12 hours) [3]. By operating in a manner that may reduce the victims' decision-making abilities, scammers can further suppress any concerns or doubts the victim may have.

4.2 Dissuading Concerns

Scammers can take various steps to dissuade the victims' concerns and establish an air of legitimacy, particularly in cases where the scammer is pretending to be in a professional occupation. In this regard, scammers can pull from one or more frameworks to control the victim's perspective, namely by establishing legitimacy, using genre-mapping, and engaging the victim in scripting [22].

4.2.1 Establishing Legitimacy

By dissuading any immediate concerns, the victim may have about requests for money, the scammer can build a level of trust that can be exploited later. Indeed, the main objective of the scammer is establishing and maintaining the initial interaction with the victim. If the victim is unsure about the legitimacy of the account, they may cease further communication. As such, the scammer must communicate a sense of urgency and importance and believability in the early stages of exploitation.

One technique is to attempt to match the victim's perspective at the incredulity of the scammers request, forestalling suspicion on the victim's part (e.g., 'You won't believe'), or emphasize the freedom of choice the victim has (i.e., 'Do whatever you want'). By presenting requests in this manner, the scammer attempts to create a connection with the victim as if the scammer themselves cannot believe the request being made. By making the victim feel in control of the situation, this can make them more pliable to requests as any decisions feel as if they are entirely self-generated by the victim.

4.2.2 Genre-Mapping

Genre-mapping, whereupon the scammer acts in a manner consistent with their persona, can serve as a way of suppressing any doubts the victim may have. If the scammer behaves in their role as the victim would expect, the victim may be more likely to go along with requests from the scammer. For example, if the scammer is impersonating a businessperson, using the expected language and jargon associated with business activities can help persuade the victim that what the scammer says is legitimate. Additionally, when it comes to requests for money, referring to previous fictitious business partners who have become rich from the scammer's 'deals' can help persuade the victim to part with their money also.

4.2.3 Scripting

Alternatively, rather than the scammer performing an act to convince the victim of their legitimacy, scripting seeks to have the victim begin acting as part of the scammer's story. The approach may involve signing some agreement to accept the requests of the scammer. Doing so may convince the victim to accept the offerings are real and that the scammer is acting legitimately. Making the victim engage more deeply in the scam and constantly acknowledging that any offerings are legitimate, makes it harder for the victim to work their way back out of the scam. Similarly, the scammer may present timed tasks that must be completed, or the offering will be retracted. Again, this forces a sense of urgency and engagement in the story, making it harder for the victim to assess the situation critically.

4.3 Gambling Phenomena

In cases where the scam is more developed, and the victim is more engaged, scammers can seek to leverage gambling-like behaviour in the victim [19]. In numerous instances of romance fraud, victims continue giving money to the scammer even when they were getting nothing in return.

In this scenario it could mean buying plane tickets to finally meet the scammer in person, only for a crisis or other delay to be introduced to prevent a meet-up. Alternatively, the victim may pay to help fund a business venture, under the impression they will get a return on the investment. The investment will then inevitably fail, requiring yet more money from the victim, or may never be mentioned again. In these scenarios, the victim will typically disregard their continued 'bad luck' and continue complying with subsequent requests for money because they have been encouraged by being so close to meeting their would-be partner.

5 Further Exploitation

Romance fraud can be portrayed as a purely economic crime. However, while economic abuse is the defining element of many cases, a straightforward bank transfer is not the only way that scammers can attempt to exploit their victims. Contemporary research has broadened the understanding of what constitutes romance fraud, to incorporate sextortion and even criminal activity [3, 23].

5.1 Sextortion

The likes of sextortion marks a significant shift away from the standard idea of romance fraud - most notably, the victim is often aware they are being exploited.

Sextortion focuses on exploiting an individual with the threat of revealing intimate material to the public [24] if a ransom is not paid [25]. The scammer does not need to view sextortion as the overarching goal of the scam. Rather, scammers can gradually build intimacy with the victim, resulting in images and messages sent by the victim, which may later be used for blackmail if more typical romance fraud methods no longer work. As opposed to the scammer having to siphon funds from the victim without raising suspicion, sextortion can potentially allow the victim to be extorted for greater amounts as they are aware of the reputational damage that may result from failing to comply with a scammers requests [23].

5.2 Blackmail and Deception

In more extreme examples, romance fraud can lead to victims unknowingly being blackmailed into drug smuggling [3]. The approach is often framed as a means of meeting the scammer where the victim travels to a foreign country but does not actually meet the scammer due to 'a mix up'. Instead, a 'friend' of the scammer visits the victim and offers a present or similar for their trouble. The victim is persuaded not to open the present until they return home. This package will likely contain drugs or other illegal materials, which, if the victim clears customs, will be collected by an affiliate of the scammer.

Although such an outcome is likely to only occur in extreme circumstances, it does point towards romance fraud expanding to encompass broader forms of crime. In particular, there appears to be the suggestion that romance fraud does not just have to be about exploiting a singular victim. Rather, victims are becoming increasingly involved in such scams to the point of being unwittingly complicit in criminal activity.

5.3 The Complexity of Romance Fraud

Romance fraud can follow different paths, depending on the techniques used by the scammers. An overview of the phases was presented in Figure 1, whilst Table 1 provides a description of defining features for each phase. This broad variation indicates that scammers are not likely to adopt the same pattern when selecting and exploiting users. Rather, users are vulnerable to being targeted by numerous different approaches. This variation, along with the cyber-enabled aspects of romance scams, have made it challenging for law enforcement to determine what constitutes a 'crime scene', with poor definitions leading to evidence either being missed or mis-reported [26]. Consent is also a challenging issue in cases where sexual material has been exchanged with the scammer. In such instances, victims often exchanged materials knowingly and consensually. However, they did so under the impression that the scammers' reasons were legitimate making the retroactive withdrawal of consent difficult [26]. More broadly, the diversity of scammer tactics has created difficulties for law enforcement to meaningfully address instances of romance scams. In many jurisdictions, romance scams are treated as a form of fraud and, as such, only the monetary loss factors into sentencing.

This means that despite the immense emotional damage caused to victims, sentences are rarely influenced by this aspect [27]. Such difficulties in defining and investigating romance scams arguably play a role in why this form of cyber-crime has seen such a rapid increase over the past decade. In the United States alone, reported losses to romance scams were placed at $81 million in 2013[28]. A decade on, losses are now reported to be at $736 million [29]. Such a dramatic increase indicates that romance scams is becoming a key interest for cyber criminals looking to make a considerable return from exploiting users.

Table 1: Description of scammer techniques used in romance fraud.

Technique	**Description**	**Defining Feature(s)**
Mass Messaging	Contacting many accounts via chat features [10].	Leveraging the number of users to find a victim.
Mass Swiping	Swiping to indicate interest on as many accounts as possible [11].	Exploiting platform recommendation algorithms to find a victim.
Tailored Profiles	Individual profiles to interest target demographics [12].	Targeting specific groups.
Multiple Profiles	Producing numerous profiles with variations to target broader range of users [10, 13].	Targeting multiple specific groups.
Overarching Approach	A general approach. The scammer asks for money [17].	Either a large amount of money is requested early in the conversation, or the scammer starts small and asks for increasing values.
Funnel Approach	A structured path from initial contact to exploitation [18]	Instances of romance fraud follow a pre-determined path with no victim autonomy.
Branching Approach	Acknowledges users individuality and illustrates a more flexible and iterative path towards romance fraud [1, 19, 20].	Acknowledges victim autonomy and allows scammers to iterate and adapt over the duration of the scam.

Continued on next page

Table 1: Description of scammer techniques used in romance fraud. (Continued)

Technique	Description	Defining Feature(s)
Sextortion	More aggressive pursuit of money or other assets from victim. Victim is usually aware of being extorted [23–25].	Used as a means of further exploiting the victim should regular romance fraud techniques no longer work or the victim becomes aware of the scam.
Blackmail & Deception	Extorting the victim with usually explicit material or engaging the victim in illegal activity. Ambiguous victim awareness of being extorted [3].	Used as a means of extorting the victim further once suspicions are raised, or integrated as one extortion method used over the course of the scam.

6 Conclusion

Romance fraud is a more recent development in the field of cybercrime, but it has cemented itself as one of the most devastating forms of fraud. It rarely follows the pre-determined structure exemplified in awareness campaigns and other media which focus mostly on simplistic examples of romance fraud. Rather, this paper illustrates the numerous means by which scammers target, select, and exploit victims of romance fraud. Identifying the different stages involved may allow the derivation of means to address these, e.g., blocking accounts with known scammer images before the initial contact stage, or highlighting red flags in a conversation at the exploitation stage.

The analysis presented in this paper furthers the current understanding of how scammers operate in romance fraud; however, additional work is required. A clear area of future research is to examine the overlap between romance fraud and other forms of cybercrime, most notably social engineering and gender-based violence. Such work may shed light on influences scammers draw upon to coerce their victims. The relationship dynamics of romance fraud also merit exploration. The inherently global nature of cybercrime allows scammers to target a wide range of victims and helps develop coordinated criminal outfits. By examining how group dynamics play a role in organised crime, insights into how multiple scammers collaborate may be found.

Romance fraud continues to evolve, introducing new exploits to target victims. The rapid increase in the number of victims and money lost over the past decade demands more responsive and actionable safeguards for users. By better understanding how scammers carry out fraud, constructive interventions and safety measures can be developed to protect users.

Acknowledgements

The authors are grateful for the funding and support received from Abertay University as part of the R-LINCS2 studentship programme.

References

[1] Whitty, M.T.: Anatomy of the online dating romance scam. Security Journal **28**(4), 443–455 (2015) https://doi.org/10.1057/sj.2012.57

[2] Cross, C., Dragiewicz, M., Richards, K.: Understanding romance fraud: Insights from domestic violence research. The British Journal of Criminology **58**(6), 1303–1322 (2018) https://doi.org/10.1093/bjc/azy005

[3] Whitty, M.T.: Drug mule for love. Journal of Financial Crime **ahead-of-print**(ahead-of-print), 1–18 (2021) https://doi.org/10.1108/JFC-11-2019-0149

[4] Whitty, M.T., Buchanan, T.: The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking **15**(3), 181–183 (2012)

[5] Cross, C., Kelly, M.: The problem of "white noise": Examining current prevention approaches to online fraud. Journal of Financial Crime **23**(4), 806–818 (2016) https://doi.org/10.1108/JFC-12-2015-0069

[6] Duguay, S., Dietzel, C., Myles, D.: The year of the "virtual date": Reimagining dating app affordances during the covid-19 pandemic. New Media & Society **00**(0), 1–19 (2022) https://doi.org/10.1177/14614448211072257

[7] Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X.: Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security **105**, 102248 (2021) https://doi.org/10.1016/j.cose.2021.102248

[8] Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., Díaz-Castaño, N.: Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19. Journal of Contemporary Criminal Justice **37**(4), 480–501 (2021) https://doi.org/10.1177/1043986221102279

[9] Ting, A.E., McLachlan, C.S.: Intimate relationships during covid-19 across the genders: an examination of the interactions of digital dating, sexual behavior, and mental health. Social Sciences **11**(7), 297 (2022) https://doi.org/10.3390/socsci11070297

[10] Huang, J., Stringhini, G., Yong, P.: Quit playing games with my heart: Understanding online dating scams. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 216–236. Springer, Springer (2015). https://doi.org/10.1007/978-3-319-20550-2_12

[11] Pizzato, L.A., Akehurst, J., Silvestrini, C., Yacef, K., Koprinska, I., Kay, J.: The effect of suspicious profiles on people recommenders. In: International Conference on User Modeling, Adaptation, and Personalization, pp. 225–236. Springer, Springer (2012). https://doi.org/10.1007/978-3-642-31454-4_19

[12] Edwards, M., Tangil Rotaeche, G.N.S., Peersman, C., Stringhini, G., Rashid, A., Whitty, M.: The Geography of Online Dating Fraud. IEEE. https://www.ieee-security.org/TC/SPW2018/ConPro/ Accessed 2018-05-24

[13] Cross, C., Layt, R.: "i suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. Social Science Computer Review **40**(4), 955–973 (2022) https://doi.org/10.1177/089443932199931

[14] Whitty, M.T.: Revealing the 'real'me, searching for the 'actual'you: Presentations of self on an internet dating site. Computers in human behavior **24**(4), 1707–1723 (2008) https://doi.org/10.1016/j.chb.2007.07.002

[15] Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., Whitty, M.: Automatically dismantling online dating fraud. IEEE Transactions on Information Forensics and Security **15**, 1128–1137 (2019) https://doi.org/10.1109/TIFS.2019.2930479

[16] Lutz, C., Ranzini, G.: Where dating meets data: Investigating social and institutional privacy concerns on tinder. Social Media+ Society **3**(1), 1–12 (2017) https://doi.org/10.1177/20563051176977

[17] Whitty, M.T.: Mass-marketing fraud: a growing concern. IEEE Security & Privacy **13**(4), 84–87 (2015) https://doi.org/10.1109/MSP.2015.85

[18] Carter, E.: Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. The British Journal of Criminology **61**(2), 283–302 (2021) https://doi.org/10.1093/bjc/azaa072

[19] Whitty, M.T.: The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology **53**(4), 665–684 (2013) https://doi.org/10.1093/bjc/azt009

[20] Whitty, M.T.: Who can spot an online romance scam? Journal of Financial Crime **26**(2), 623–633 (2019) https://doi.org/10.1108/JFC-06-2018-0053

[21] Kopp, C., Layton, R., Sillitoe, J., Gondal, I.: The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. International Journal of Cyber Criminology **9**(2), 205–217 (2015) https://doi.org/10.5281/zenodo.56227

[22] Carter, E.: The anatomy of written scam communications: An empirical analysis. Crime, Media, Culture **11**(2), 89–103 (2015) https://doi.org/10.1177/17416590155723

[23] Rege, A.: 10v3. c0ns. In: 2013 APWG eCrime Researchers Summit, pp. 1–9. IEEE, IEEE (2013)

[24] O'Malley, R.L., Holt, K.M.: Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. Journal of interpersonal violence **37**(1-2), 258–283 (2022) https://doi.org/10.1177/08862605209091

[25] Cross, C., Lee, M.: Exploring fear of crime for those targeted by romance fraud. Victims & Offenders **17**(5), 735–755 (2022) https://doi.org/10.1080/15564886.2021.2018080

[26] Khader, M., Yun, P.S.: A Multidisciplinary Approach to Understanding Internet Love Scams:Implications for Law Enforcement. Elsevier Inc., ??? (2017). https://doi.org/10.1016/B978-0-12-809287-3.00018-3

[27] Gillespie, A.A.: Just the money? does the criminal law appropriately tackle romance frauds? Journal of International and Comparative Law **8**(1), 143–174 (2021). Publisher: Sweet and Maxwell-Thomson Reuters

[28] (IC3), I.C.C.C.: 2013 IC3 Annual Report. https://www.ic3.gov/Media/PDF/AnnualReport/2013_IC3Report.pdf

[29] (IC3), I.C.C.C.: 2022 IC3 Annual Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf