Contextualised Cyber Security Awareness Approach for Online Romance Fraud

Sara Dickerson
Faculty of Science and Technology
Bournemouth University
Poole, United Kingdom
s4903180@bournemouth.ac.uk

Edward Apeh
Faculty of Science and Technology
Bournemouth University
Poole, United Kingdom
eapeh@bournemouth.ac.uk

Gail Ollis
Faculty of Science and Technology
Bournemouth University
Poole, United Kingdom
gollis@bournemouth.ac.uk

2020 7th International Conference on Behavioural and Social Computing (BESC) | 978-1-7281-8605-4/20/$31.00 ©2020 IEEE | DOI: 10.1109/BESC51023.2020.9348307

***Abstract*—Action Fraud reported 50 million pounds was lost to romance fraud in 2018, a 27% increase on the previous year, despite an increase in publicity and guidance surrounding the issue. Romance fraud is an ever-increasing issue, and the statistics highlight the need for a proactive, adaptable, and bespoke approach to assist online dating platforms in combatting the problem, providing targeted awareness to customers while improving the user experience of dating platforms. Currently, there is no effective approach for increasing user awareness and providing real-time intervention on romance fraud. Existing methods on the platform focus on identifying, preventing, and stopping threat actors with technological measures rather than educating potential victims. This paper discusses the existing state of romance fraud and proposes a solution to mitigate the problems by developing a targeted awareness approach. The solution can be adopted by online dating platforms for early identification and timely intervention. It includes bespoke advisory messages to be provided to the user and risk categorisation criteria as well as workflows and prototypes to assist platforms with implementation. The results from the primary research clearly support the objectives showing that timely intervention helps to mitigate against fraud, decreasing the likelihood of it occurring. This approach offers demonstrable improvements to dating platforms.**

Keywords - romance fraud, awareness approach, dating platforms.

I. Introduction

The focus of this paper is the issue of romance fraud and other cyber-enabled crime on online dating platforms. With cases continuing to increase there is a significant need for a more effective approach to address this issue.

Action Fraud received 4,555 complaints of Romance Fraud in 2018 with approximately £50 million in monetary loss. This is an increase of 27% compared to 2017 [1]. Despite awareness efforts from third parties, such as a local campaign by Cambridgeshire police around Valentine's day and a current national campaign by police forces across the country [2, 3], romance fraud cases are often under-reported due to the victim's embarrassment.

This paper proposes an early detection and timely intervention approach (hereafter called the approach) for dating platforms to combat this issue, providing education and awareness to users at the time it is needed in the online dating process. The results from the controlled experiment conducted as part of this research show that providing the awareness information at the point where the fraud begins enables potential victims to be aware and vigilant. Falling victim to romance scams can have a detrimental impact on victims both financially and mentally, it is therefore vital that action is taken in order to prevent it. The approach uses a range of steps to select a tailored educational message which is displayed to improve awareness and reduce fraud without spamming customers of the platform. The messages provided are bespoke to the identified risk level and only sent when necessary. The approach can be seamlessly implemented into the existing platform infrastructure without disruption to the platform administrators and customers.

II. Background

A. Romance Fraud

Dating services have existed for many years, proving to be successful for individuals wanting to meet a partner, particularly those who have limited time to socialize. They also enable people to connect with those they are unlikely to meet through their daily routine. However, while dating apps can result in fruitful partnerships for many customers, platforms are commonly exploited by cybercriminals to facilitate criminal activity, including fraud and human trafficking. Due to the breadth and diversity of unregulated applications, keeping customers safe is a huge challenge and not always possible.

The issue of romance fraud has been exacerbated by the increased use in dating apps over the past few years. Romance fraud is a key risk on dating platforms but there are few public strategies in place for combatting this complex issue [4]. The threat actor uses a fake profile while pretending to have a real connection with a victim. They often persuade the victim to send money to help them in a situation [5]. Alternatively, they encourage them to unknowingly commit fraud, for example, by re-distributing counterfeit cheques [5]. Irrespective of the motive, romance fraud typically follows the process depicted in Fig. 1.

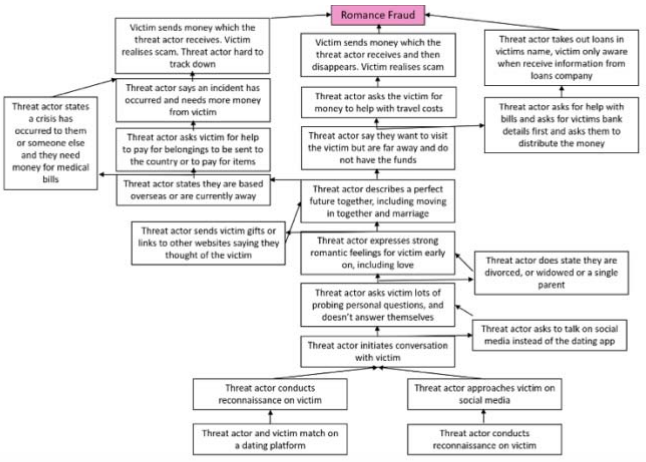

Romance Fraud
Victim sends money which the threat actor receives. Victim realises scam. Threat actor hard to track down
Victim sends money which the threat actor receives and then disappears. Victim realises scam
Threat actor takes out loans in victims name, victim only aware when receive information from loans company
Threat actor states a crisis has occurred to them or someone else and they need money for medical bills
Threat actor says an incident has occurred and needs more money from victim
Threat actor asks the victim for money to help with travel costs
Threat actor asks for help with bills and asks for victims bank details first and asks them to distribute the money
Threat actor asks victim for help to pay for belongings to be sent to the country or to pay for items
Threat actor say they want to visit the victim but are far away and do not have the funds
Threat actor states they are based overseas or are currently away
Threat actor describes a perfect future together, including moving in together and marriage
Threat actor sends victim gifts or links to other websites saying they thought of the victim
Threat actor expresses strong romantic feelings for victim early on, including love
Threat actor does state they are divorced, or widowed or a single parent
Threat actor asks victim lots of probing personal questions, and doesn't answer themselves
Threat actor asks to talk on social media instead of the dating app
Threat actor initiates conversation with victim
Threat actor conducts reconnaissance on victim
Threat actor approaches victim on social media
Threat actor and victim match on a dating platform
Threat actor conducts reconnaissance on victim

Fig. 1. Attack tree of fraud process

The risks associated with online dating have always been apparent, but they have become increasingly significant with society's increased dependency on technology. The precise number of victims of this type of fraud is unknown, partially because of the lack of reporting by victims due to embarrassment but also the lack of common knowledge about the issue. The extent of romance fraud and subsequent loss has rapidly increased following the launch of dating sites, as evidenced by the £23 million increase in reported loss between 2013 and 2018 [1] [6]. A significant challenge is that the effects of falling victim to a romance scam can be long-lasting and include both financial and non-financial impacts [6]. An individual's good nature, vulnerability and willingness to help others are often preyed upon and manipulated by criminals. Dating sites are a hotspot for this due to an individual's desperate search for love. Vulnerable individuals will often be targeted by multiple criminals who have shared knowledge about easy targets obtained by using the cyber kill chain [7]. This information is usually found during the reconnaissance stage of a threat actor's campaign and utilised within the weaponisation stage, assisting the actor in effectively targeting the victim [7].

B. *Personas*

The dating profiles often used by threat actors show an individual with a model-like physique and a charming personality, claiming to live in a populous area such as a city, and other desirable traits. Many fake profiles also state that the threat actor is in the military, providing them with a reasonable excuse as to why they cannot meet up or communicate via phone or video call [6]. The reconnaissance stage of the attack typically involves gathering as much personally identifiable information as possible, mainly through social media platforms, to engage with the victim and groom them to encourage romantic feelings [8].

Typically, victims are individuals in their 50s who have had a failed previous relationship or marriage. It is thought that these people are often targeted as they are looking for a close relationship and are likely to have money saved [14]. Although any gender can be targeted, women appear to be the main victims and constitute 63% of cases of romance fraud [9]–[11]. The threat actor exploits the victim's good-nature and feelings of romance and love in order to manipulate them into helping financially. Fake evidence is sometimes provided to convince the victim that everything is legitimate, reducing any suspicions or concerns. The inclusion of romance provides the victim with a sense of responsibility to help and also a sense of guilt if they cannot assist an individual for whom they have romantic feelings [13].

An overall increase in the number of attempted romance scams has resulted in an increased risk of falling victim, particularly if the threat actor uses sophisticated deception techniques and a particularly vulnerable victim is targeted [13]. The human characteristics of compliance and hopefulness can mean that anyone is a potential victim of romance fraud with research showing that no specific demographic is inherently more at risk of fraud [14]. However, an individual within a particular demographic can be increasingly susceptible to attacks due to threat actors identifying them as vulnerable [13]. Psychological mechanisms could also impact the likelihood of an individual being successfully deceived. Cognitive psychological influences may include how an individual is raised and traits such as risk tolerance, greed or gullibility [15], [16].

C. *Zero-Trust Environments*

Dating platforms are often deemed trustworthy by users because they are known to be monitored and are advertised this way by many sites, particularly if they are a paid service. There is also a perceived underlying level of trust expected as every user ostensibly has the same end goal [17].

In comparison, social media is often viewed as a zero-trust environment [18]. This is mainly due to negative publicity for social media platforms and their protection of customers [19]. However a new issue is arising in which users of dating platforms, a trusted environment, move onto social media or texting, normally a zero-trust environment, after making a connection. This transition is a cause for concern as conversations are not monitored and fake profiles are less likely to be reported, which is why threat actors like to move the conversation to there [20]. The primary reason for users feeling safe despite moving to a zero-trust environment is that they have built a perceived connection with the match within a trusted environment. In this case the trustworthiness has extended from the environment to the match, enabling the victim to feel connection and trust despite only having basic information about the person. Individuals develop an intimate relationship and ignore potential warning signs due to cognitive dissonance [9]. Additionally, research indicates that victims of romance fraud typically have an increased disposition to trust, making it easier for the intimate connection with the scammer to be built [16]. The online disinhibition effect also plays a part in this: individuals' behaviour online does not reflect how they would behave if the same situation occurred offline [21].

D. *Existing Mitigations*

In 2013, many of the largest online dating providers collaborated to form the Online Dating Association (ODA) [22]. The ODA's work includes new technical solutions which are being introduced to deter and prevent fraudulent activity and profiles on the platforms. The organisation also promotes safety and best practices online and in 2017 created a framework for user safety, encouraging platform providers to creatively deliver information to maximise users' security awareness [23]. However, whilst information is available within platforms' security-specific pages, no other forms of awareness campaign appear currently to be present on dating platforms. Most advice focuses on physical safety concerns rather than cybersecurity issues [23]. Additionally, many dating platforms are not part of the ODA and so do not adhere to these minimum requirements.

An example of a platform implementing new technological solutions is Tinder. In January 2020 they announced new safety features including photo verification, a "Safety Center" with tools and resources, and emergency services links for customers out on dates [24]. Technological, awareness and response measures are all beneficial to help combat the safety issue, but cyber threat actors continually seek ways to bypass any technology. They are, for example, already using deep fake technology to fool the platform into verifying a fake profile [25].

In May 2019 seven banks also joined forces, to assist and refund victims of scams where neither the bank nor the victim is at fault [26]. The scheme is beneficial for victims of romance fraud provided that it is the first time they have been defrauded and they have shown due diligence in protecting themselves from falling victim to fraud. However, this was only a temporary measure and does not provide compensation for the emotional hurt and lasting damage experienced by victims. In November 2019 the banks sought to create a permanent solution where each bank provides 3% of revenue into a fund to assist in refunding victims, but unfortunately, a coherent solution could not be agreed [27]. Currently, the only solution would be for the government to pass a law making it a legal requirement for banks to refund victims. However, this may take a long time [28], [29].

Other third party organisations have helped raise the profile of romance fraud using awareness campaigns to reach potential victims, particularly regarding catfishing through social media platforms [1]. These campaigns are predominately directed outside the dating platforms; dating providers are yet to integrate user awareness measures into their platforms to meet the advice of the ODA and Action Fraud [1], [30], [31]. Organisations such as ScamAlytics provide dating platforms with technological mitigations including real-time detection, shared block lists and machine learning to detect fraudsters [32]. In contrast, there are no common approaches that have been applied to increase user awareness on these platforms. The current (technological) solutions focus on preventing threat actors. What is missing is educating victims with contextualised information on the site, where the crime is likely to originate. By intercepting and engaging with the victim at an early stage of the grooming process, the likelihood of being able to stop the fraud progressing before a money transfer occurs is increased. It also assists the dating platform by helping to provide increased safety for customers.

III. Methodology

A. Background study

A literature review was undertaken with the search terms romance fraud, online dating fraud, dating apps, romance fraud case studies, issues with dating platforms and safety issues with dating apps. The findings suggest that there lacks an effective contextualised cyber security awareness approach for mitigating online romance fraud.

B. Materials

In order to test and evaluate the approach, a mock dating platform prototype was developed using Adobe XD, a free tool suitable for user experience design. The design took into consideration the identified gaps within dating platforms and emulated an intervention at the proposed timely stage of the online dating process.

A short questionnaire was used to query participant's perception of their romance fraud knowledge before and after the activity with the prototype and their prior perceptions of security advice (5 single-choice questions). It was also used to collect their answers to the tasks in the activity (6 single-choice questions) and their reactions to the activity (4 single-choice questions and 2 open text questions).

C. Primary research participants

With ethical approval from the institution, primary research was conducted to evaluate the impact of making users more aware of romance fraud during interactions on dating platforms. Twelve participants aged from 19 to 65 were recruited via word-of-mouth. The age range, with a slightly higher number of younger participants (19 to 35), was chosen to be representative of dating platform users. All the participants had themselves used dating platforms. 60% of the participants were female, again mirroring the user demographic for online dating.

Participants were divided into an experimental group and control group with age and gender balanced as equally as possible [33], the mean age of both groups being 35. The experimental group received romance fraud awareness messages. The control group did not receive these targeted messages, but as users of dating platforms they have had the same access to other sources of fraud awareness.

D. Primary research procedure

All participants were asked to answer the initial questionnaire questions and then complete the activity. Within the activity, each participant could make up to four matches. With every match, they were asked to choose a reply to at least one question from the match, such as asking where they live. Before they responded, participants in the experimental group saw an awareness message about romance fraud. All participants had to choose from three predetermined responses, one high risk, one medium and one low. This categorisation was not shown to participants. Data was collected by participants recording their activity responses on the questionnaire and providing additional feedback.

E. Requirements

The core requirements for a solution were identified using existing literature and identifying gaps in current awareness campaigns from the primary research participants' answers regarding existing knowledge of the term romance fraud and the warning signs. The key requirements are for a solution which offers early detection and intervention, can be easily adapted and implemented by online dating platforms, and helps to improve the safety and awareness of users without alarming them or disrupting their user experience.

IV. Design

The design of the solution incorporates findings from the background study to create awareness messages and content for users, building the information into an approach that can be implemented by dating platforms. A business process model and notation diagram displaying how the artefact fits into existing mitigations and processes can be seen in Fig. 2.

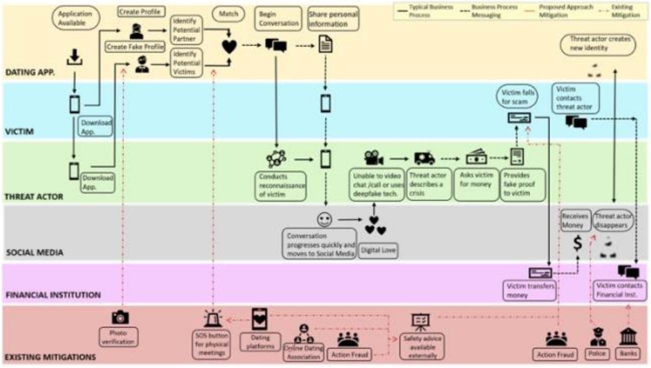

Typical Business Process
Business Process Messaging
Proposed Approach Mitigation
Existing Mitigation
DATING APP.
Application Available
Create Profile
Create Fake Profile
Identify Potential Partner
Identify Potential Victims
Match
Begin Conversation
Share personal information
Threat actor creates new identity
VICTIM
Download App.
Victim falls for scam
Victim contacts threat actor
THREAT ACTOR
Download App.
Conducts reconnaissance of victim
Unable to video chat /call or uses deepfake tech.
Threat actor describes a crisis
Asks victim for money
Provides fake proof to victim
SOCIAL MEDIA
Conversation progresses quickly and moves to Social Media
Digital Love
Receives Money
$
Threat actor disappears
FINANCIAL INSTITUTION
Victim transfers money
Victim contacts Financial Inst.
EXISTING MITIGATIONS
Photo verification
SOS button for physical meetings
Dating platforms
Online Dating Association
Action Fraud
Safety advice available externally
Action Fraud
Police
Banks

Fig. 2. BPMN displaying existing mitigations and the proposed approach

A. Design of workflows

Workflows have been designed as part of the solution to demonstrate how a platform can implement the approach to provide users with advisory and warning messages when required, ensuring they do not cause message fatigue or send messages to users when no advice is needed. As seen in Fig. 3 and 4 below, the workflows contain decisions (e.g. Have a potential threat actor and potential victim been matched? Should the user receive an awareness message? Should the message direct the user to security advice provided by the platform or to a third party such as Action Fraud?) These are represented within a flowchart to clearly demonstrate to a developer the steps needed to integrate the approach into an existing process. The workflow design follows the NIST framework for managing and reducing cybersecurity risk by covering the five key stages to identify, protect, detect, respond and recover, thereby complementing existing cybersecurity practices on these platforms [34].

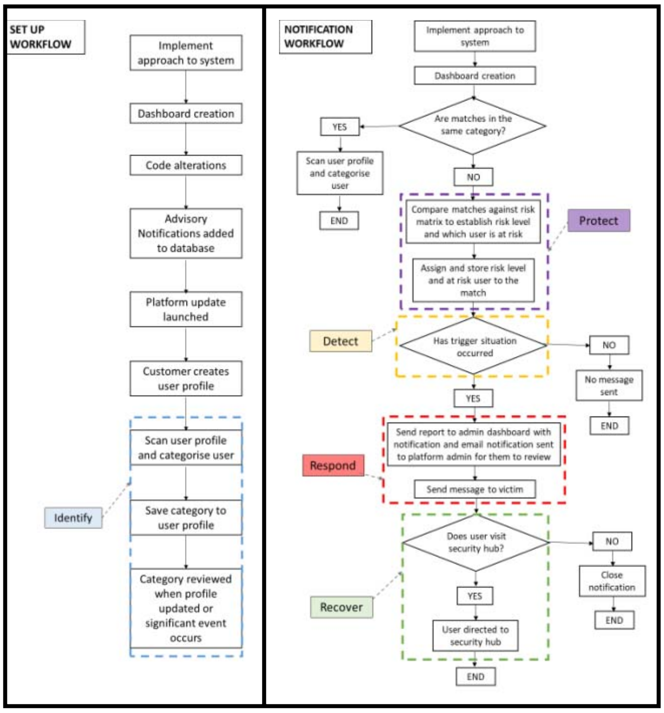

SET UP WORKFLOW
Implement approach to system
Dashboard creation
Code alterations
Advisory Notifications added to database
Platform update launched
Customer creates user profile
Scan user profile and categorise user
Save category to user profile
Category reviewed when profile updated or significant event occurs
Identify
NOTIFICATION WORKFLOW
Implement approach to system
Dashboard creation
Are matches in the same category?
YES
Scan user profile and categorise user
END
NO
Compare matches against risk matrix to establish risk level and which user is at risk
Assign and store risk level and at risk user to the match
Protect
Detect
Has trigger situation occurred
NO
No message sent
END
YES
Send report to admin dashboard with notification and email notification sent to platform admin for them to review
Send message to victim
Respond
Does user visit security hub?
NO
Close notification
END
YES
User directed to security hub
END
Recover

Fig. 3. Workflows

Decisions are informed by the user's likely susceptibility to romance fraud, categorised using pre-defined criteria [16]. When a dating match is made, the categories of both users are checked. If one user has been identified as a potential threat (e.g. a suspected threat actor, potentially suspicious profile characteristics such as a job based overseas, asking for personal information) while the other is a potential victim (e.g. hinting to wealth in their profile or other signs of vulnerability), the information will be stored against the match details. A risk assessment matrix can be used to determine the level of risk posed to the victim and decide what form of advisory messages they will receive. If a trigger situation occurs, the relevant message will be sent to the victim. This method ensures that the message sent is appropriate to the individual and occurs at the point in time where an awareness message is needed.

B. *Design of contextualised messages*

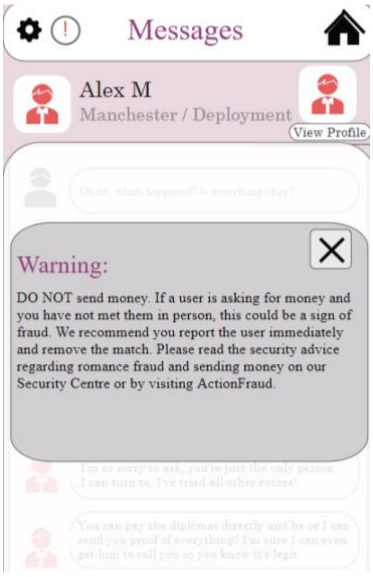
The advisory messages are bespoke to the potential vulnerability of the user and the level of risk posed by the match. For example, if a user has a potentially suspicious profile and responds to questions in a suspicious manner such as withholding many personal details then they would be deemed a potential risk. A user with indications of potential vulnerabilities similar to previous romance victims in their profile, such as being widowed and over fifty, would be deemed a potential victim. If these two users matched and the conversation contained warning signs of romance fraud, then the potential victim would be sent an awareness message appropriate to the severity of risk detected. When two users in the same category, for example, two victims or two threat actors match with each other, it is unlikely they will cause significant harm to one another, so messages will not be sent in this case.

The workflow is designed so that a user will only receive advice if they have been identified as a potential victim, and their match has been identified as a potential threat. Messages will be deployed following an identified trigger situation which is an indicator of compromise. For example, when the topic of marriage has been discussed, low-risk potential victims will not receive a message; however, high-risk victims will see a message as they may benefit from this advice by being more cautious. The overall risk level, established from the level of potential deception and the vulnerability of the individual receiving it, dictates which message if any is sent.

Clearly the assessment cannot include dynamic triggers based on conversation content without scrutiny of the private messages between matched users. This could be achieved by anonymous text analysis which reports only specified characteristics, but it nonetheless represents an intrusion on the privacy of the conversation. Users might equally feel uncomfortable at the idea of the platform profiling them as potential victims or threat actors. This short paper focuses on testing the effectiveness of the approach and showing the feasibility of integrating it into a platform's workflow. The acceptability of the approach demands further work to establish whether users would consider the effect on privacy a worthwhile trade-off to help mitigate the threat. If so, transparency would need to be achieved without undermining the effectiveness of the approach.

C. *Prototype Design for experiment and implementation*

A prototype showing how the approach could look to the user was created in Adobe XD to display an example awareness message a user could receive (Fig. 4.)


Messages

Alex M
Manchester / Deployment

Oh no, whats happened? Is everything okay?

Warning:

DO NOT send money. If a user is asking for money and you have not met them in person, this could be a sign of fraud. We recommend you report the user immediately and remove the match. Please read the security advice regarding romance fraud and sending money on our Security Centre or by visiting ActionFraud.

I'm so sorry to ask, you're just the only person I can turn to, I've tried all other routes!

You can pay the diplomat directly and he or I can send you proof of everything? I'm sure I can even get him to call you so you know it's legit

Fig. 4. Prototype of solution

V. RESULTS

The results from the primary research clearly support the objectives of the research: if advice about potential fraud is provided nearer the beginning of the dating process it would benefit users of the dating platform by making fraud less likely.

A. Quantitative Results

The participants' responses show that the control group responded with more high and medium risk responses than the experimental group. The responses by the control and the experimental groups are compared by risk-level in Table 1.

Group	Percentage (%) of responses		
	High risk response	*Medium risk response*	*Low risk response*
Control Group	15	77	8
Experimental Group	0	31	69

Table 1. The percentage of risk-level decisions made during the controlled experiment activity by the control group and the experimental group

All participants within the experimental group stated that they engaged with the awareness messages they received providing advice about romance fraud. 100% of the experimental group also stated that they read other security information available on the dating platform. In contrast 0% of the control group viewed other security information. This suggests that when participants were prompted to reflect on the security of their interactions through the awareness messages, they were more likely to be security conscious.

The questionnaire also revealed that 100% of the experimental group reported learning new information about romance fraud through the awareness messages, compared with no-one in the control group. This demonstrates that the awareness messages effectively increased user awareness regarding romance fraud.

B. Qualitative Results

Free-text participant feedback within the questionnaire revealed that the awareness messages were well received and helped the participants consider their potential actions rather than act instinctively. All responses to the question "Do you believe the messages were helpful/appropriate? If not, why not?" were positive, with one participant responding "They made me pause and really think about what I was doing. It's easy to get carried away and think you're chatting to a close friend instead of someone you really don't know". Another reported that "…Having the information available before you make a potentially bad decision helped me move away from making a mistake or me losing my information or money". This feedback demonstrates the positive impact the approach had on increasing user awareness and decreasing risk behaviour, both of which reduce the likelihood of the user falling victim to romance fraud. The users suggested potential improvements including a flashing image to emphasise that the message is important and a chat function to access follow-up expert information and advice if needed.

VI. Conclusions and Future Work

Online romance fraud is prevalent and growing in today's technological society. It has devastating financial and emotional impacts, making it vitally important that dating platform providers do more to raise awareness and protect customers. The solution discussed here has shown, in primary research, that users respond more cautiously when given security advice at the time they need to apply it. Future work should trial the approach on a live dating platform as a foundation to exciting developments in both reducing online romance fraud and increasing the awareness of cyber security issues as a whole.

The approach could also be extended to other platforms, for example social media platforms, to reduce the likelihood of fraud occurring in these unregulated environments. The user's personal data on these platforms is likely to be less detailed than is needed to help match them on dating platforms so some of the profiling criteria would need to be adapted to identify potential romance fraud victims and romance scammers, but analysis of message content would be the same. If the criteria are met and a trigger situation such as a request for money occurs, then the steps within the proposed approach can be followed. An applicable awareness message can be sent to the platform user potentially at risk at exactly the time it is needed to prompt them to be cautious, potentially sparing them from devastating emotional and financial loss.

Acknowledgements

We thank all participants for taking part, providing valuable feedback and recognising the value of the project.

References

[1] Action Fraud, 'Don't invest your heart in a fauxmance: victims lose over £50 million to romance fraud | Action Fraud', 2019. [Online]. Available: https://www.actionfraud.police.uk/news/dont-invest-your-heart-in-a-fauxmance-victims-lose-over-50-million-to-romance-fraud. [Accessed: 03-Feb-2020].

[2] Cambridgeshire Constabulary, "Romance fraud," [Online]. Available: https://www.cambs.police.uk/information-and-services/Romance-fraud. [Accessed 23 November 2020].

[3] ActionFraud, "Fall for the person, not the profile," ActionFraud, [Online]. Available: https://www.actionfraud.police.uk/romancefraud. [Accessed 23 Novemember 2020].

[4] M. Whitty, 'The Online Dating Romance Scam: A Serious Crime', 2012. [Online]. Available: http://wrap.warwick.ac.uk/83740. [Accessed: 21-Feb-2020].

[5] The United States Department of Justice, 'Mass Marketing Fraud', 2017. [Online]. Available: https://www.justice.gov/criminal-fraud/mass-marketing-fraud. [Accessed: 03-Feb-2020].

[6] M. T. Whitty and T. Buchanan, 'The online dating romance scam: The psychological impact on victims - both financial and non-financial', 2016. .

[7] Lockheed Martin Corporation, 'Cyber Kill Chain® | Lockheed Martin', 2020. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 03-Mar-2020].

[8] J. Huang, G. Stringhini, and P. Yong, 'Quit Playing Games With My Heart: Understanding Online Dating Scams', 2015.

[9] M. Whitty, 'The scammers persuasive techniques model : development of a stage model to explain the online dating romance scam - WRAP: Warwick Research Archive Portal', 2013. [Online]. Available: http://wrap.warwick.ac.uk/81506/. [Accessed: 21-Feb-2020].

[10] M. Cacciottolo and N. Rees, ‘Online dating fraud victim numbers at record high’, 2017. [Online]. Available: https://www.bbc.co.uk/news/uk-38678089. [Accessed: 20-May-2020]

[11] UK Finance, ‘Over half of those looking for love online vulnerable to romance scams | UK Finance’, 2020. [Online]. Available: https://www.ukfinance.org.uk/press/press-releases/over-half-those-looking-love-online-vulnerable-romance-scams. [Accessed: 11-Apr-2020].

[12] K. Peachey, ‘Women “victims in 63% of romance scams” - BBC News’, 2019. [Online]. Available: https://www.bbc.co.uk/news/business-47176539. [Accessed: 20-May-2020].

[13] T. Buchanan and M. T. Whitty, ‘Online dating romance scam - causes and consequences of victimhood’, 2012. [Online]. Available: http://wrap.warwick.ac.uk/83736. [Accessed: 21-Feb-2020].

[14] G. Norris, A. Brookes, and D. Dowell, ‘The Psychology of Internet Fraud Victimisation: a Systematic Review’, *J. Police Crim. Psychol.*, vol. 34, no. 3, pp. 231–245, Sep. 2019.

[15] R. A. Judges, S. N. Gallant, L. Yang, and K. Lee, ‘The role of cognition, personality, and trust in fraud victimization in older adults’, *Front. Psychol.*, vol. 8, no. APR, Apr. 2017.

[16] M. T. Whitty, ‘Do You Love Me? Psychological Characteristics of Romance Scam Victims’, 2017. [Online]. Available: http://wrap.warwick.ac.uk/89709. [Accessed: 14-Apr-2020].

[17] M. Couch, D., Liamputtong, P. and Pitts, ‘Online Daters and the Use of Technology for Surveillance and Risk Management’, *Int. J. Emerg. Technol. Soc.*, vol. 9, no. 2, pp. 116–134, 2011.

[18] Cisco, ‘Zero Trust Security - Cisco’, 2020. [Online]. Available: https://www.cisco.com/c/en_uk/products/security/zero-trust.html. [Accessed: 03-Apr-2020].

[19] A. Hern, ‘Britons less trusting of social media than other major nations | World news | The Guardian’, 2019. [Online]. Available: https://www.theguardian.com/world/2019/may/03/britons-less-trusting-of-social-media-than-other-major-nations-facebook-twitter. [Accessed: 24-May-2020].

[20] ActionFraud, ‘Romance fraud | Action Fraud’, 2020. [Online]. Available: https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud. [Accessed: 11-Apr-2020].

[21] J. Suler, ‘The online disinhibition effect.’, *Int. J. Appl. Psychoanal. Stud.*, vol. 2, no. 2, pp. p184-188, 2005.

[22] Online Dating Association, ‘ODA | Homepage’, 2017. [Online]. Available: https://www.onlinedatingassociation.org.uk/. [Accessed: 03-Feb-2020].

[23] Online Dating Association, ‘ODA | Framework for User Safety’, 2017. [Online]. Available: https://www.onlinedatingassociation.org.uk/safety-first/framework-for-user-safety.html. [Accessed: 23-May-2020].

[24] Tinder, ‘Tinder Introduces Safety-Focused Updates’, 2020. [Online]. Available: https://blog.gotinder.com/tinder-introduces-safety-updates/. [Accessed: 24-Feb-2020].

[25] British Broadcasting Corporation, ‘Deepfake technology: Can you spot what’s real? - BBC News’, 2020. [Online]. Available: https://www.bbc.co.uk/news/av/technology-51223254/deepfake-technology-can-you-spot-what-s-real. [Accessed: 03-Mar-2020].

[26] K. Peachey, ‘Scam victims to be refunded by banks - BBC News’, 2020. [Online]. Available: https://www.bbc.co.uk/news/business-48385426. [Accessed: 03-Mar-2020].

[27] British Broadcasting Corporation, ‘Banks disagree on how to pay for fraud refunds - BBC News’, 2019. [Online]. Available: https://www.bbc.co.uk/news/business-50431226. [Accessed: 03-Mar-2020].

[28] Citizens Advice, ‘Check if you can get your money back after a scam - Citizens Advice’, 2020. [Online]. Available: https://www.citizensadvice.org.uk/consumer/scams/check-if-you-can-get-your-money-back-after-a-scam/. [Accessed: 03-Mar-2020].

[29] Which, ‘How to get your money back after a scam’, 2020. [Online]. Available: https://www.which.co.uk/consumer-rights/advice/how-to-get-your-money-back-after-a-scam. [Accessed: 03-Mar-2020].

[30] Online Dating Association, ‘ODA | Date Safe’, 2017. [Online]. Available: https://www.onlinedatingassociation.org.uk/date-safe.html. [Accessed: 24-Apr-2020].

[31] Scamalytics, ‘Action Fraud data now available to dating services via Scamalytics | Scamalytics’, 2018. [Online]. Available: https://scamalytics.com/action-fraud-data-now-available-to-dating-services-via-scamalytics/. [Accessed: 21-Feb-2020].

[32] Scamalytics, ‘Scamalytics | Stop Scammers Automatically’, 2019. [Online]. Available: https://scamalytics.com/. [Accessed: 03-Feb-2020].

[33] Lumencandela, ‘Bias in Psychological Research | Boundless Psychology’. [Online]. Available: https://courses.lumenlearning.com/boundless-psychology/chapter/bias-in-psychological-research/. [Accessed: 01-May-2020].

[34] NIST, ‘Uses and Benefits of the Framework | NIST’, 2018. [Online]. Available: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework. [Accessed: 14-Apr-2020].