Straight to the heart of the matter: towards effective means of combating romance fraud

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

This poster was presented at the Third International Conference on Behavioural and Social Sciences in Security, BASS23, Bath, UK, 11-13 July 2023

Kydd, M., Shepherd, L. A., Szymkowiak, A., & Johnson, G. I. (2023). *Straight to the heart of the matter: towards effective means of combating romance fraud*. Poster session presented at Third International Conference on Behavioural and Social Sciences in Security, 11-13 July 2023, Bath, United Kingdom.

Straight to the Heart of the Matter: Towards Effective Means of Combatting Romance Fraud

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

School of Design and Informatics, Abertay University, Bell Street, Dundee, UK

{m.kydd1800, lynsay.shepherd, a.szymkowiak, g.johnson}@abertay.ac.uk

1. Abstract

Romance fraud, whereby a scammer feigns romantic interest in a user of a dating platform to financially exploit them, has increased rapidly over the past decade with known losses increasing from $80 million to $750 million in the US alone.

Implementing effective countermeasures against such crimes has proven difficult; awareness campaigns are often vague and confusing while support groups are either unavailable or unattended due to victims being too distraught or ashamed to seek help. This work aims to highlight current issues and proposes alternative approaches in tackling romance scams.

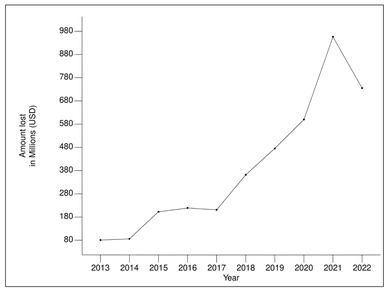


Figure 1: Losses to romance fraud increased dramatically between 2013-2023.

2. Introduction and Aim

Romance fraud has rapidly increased over the past decade to become a near billion-dollar crime industry (IC3, 2013; IC3, 2023; Figure 1). Through feigning romantic interest, scammers aim to exploit a victim's trust. Such exploitation can leave victims confused, isolated, and financially devastated.

To prevent the risk of, and mitigate the damage from, romance fraud, a range of approaches have been taken, from the easily distributable awareness campaign, to the tailored peer support group. Such measures have shown promising results. However, they aim to educate users before or after a crime has occurred. In contrast, the aim of this work is to argue for safeguards which can operate *during* online romantic interactions – lessening the need for users to remember complicated warning signs and for law enforcement to carry out the difficult process of collecting digital evidence.

3. Current Approaches

Preventative Measures

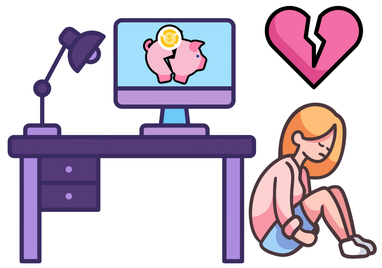
Awareness Campaigns

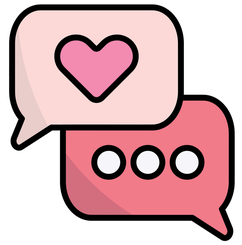
Awareness campaigns offer a simple and easily distributable means of warning the public about the risks of romance fraud. Through highlighting common scammer tactics, users can, in theory, apply the message to their own situation.
However current awareness campaigns suffer from an issue of 'white noise' whereby users were left confused on what constituted romance fraud due to awareness campaigns overly complicating the underlying message (Cross, 2016).

Self-Education

By taking proactive steps to bolster their own understanding, users can be better equipped to handle suspected romance fraud, however current approaches appear limited almost exclusively to simple online searches (Cross, 2022).

Given the often-explicit nature of romance fraud, users often found that relevant materials were blocked by their Internet Service Provider (Maeng, 2022). Other issues accessing relevant materials involved being served proprietary file formats not all users could access, or links to materials no longer available.





Are current preventative measures against online romance scams effective?

Supportive Measures

Peer Support Groups

Peer support groups offer tailored face-to-face advice and support to victims of romance fraud, potentially reducing the financial and emotional damage victims may feel (Cross, 2019).

While peer support groups provide help to victims, they are not without their issues, however. Although in-person peer support groups are positively received by participants, attendance did not reflect this. As much as 90% of attendees report not attending a session one year on from their first visit (Van Uden-Kraan et al., 2011). This may suggest victims may no longer see the need to engage with or desire further support.

Law Enforcement

By reporting cases of romance fraud to authorities, victims can be assisted, however, the reality shows that this is not always the case.

In a study of how Action Fraud, the UK's national fraud reporting centre, recorded reported data, it was noted that a considerable amount of information was either missing or misreported (Correia, 2019). This included cases not being assigned a specific investigator, and the amount lost being recorded. Broader demographic information, such as age, ethnicity, and background, were also not recorded, thereby continuing issues in the underreporting of romance fraud in minority groups.

4. Proposed Solutions and Conclusions

The approaches most widely used and discussed in this work illustrate that current approaches are not meeting the needs of victims – both in terms of preventing romance scams and supporting victims thereof.

A critical rethink of how romance scams are tackled is merited. Users taking pro-active steps in the form of self-education illustrate that users want to be informed on protecting themselves against such scams and safety measures should work closer to acknowledge this autonomy in decision-making. The generic nature of awareness campaigns meanwhile suggests that an approach more context-dependent should be considered – such as integrating warning systems with the dating platforms directly.

By building safety measures into dating platforms, this allows for greater opportunity to protect users from harm and offers areas to introduce real-time safeguards. Through deploying safety measures which operate as the user converses back and forth with the potential scammer, this removes the need for the user to remember potential warning signs and instead be alerted to suspicious activity as it occurs.

Romance fraud is a complex and evolving form of cybercrime; safeguards deployed against it should be equally adaptive to users' needs. By exploring countermeasures which integrate with dating platforms directly, a more flexible approach can be taken to inform, educate, and protect users.

References

- I.C.C.C. (2013), "2013 IC3 Annual Report". Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2013/IC3Report.pdf
- I.C.C.C. (2023), "2022 IC3 Annual Report". Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2022/IC3Report.pdf
- Cross, C. and Kelly, M. (2016), "The problem of 'white noise': examining current prevention approaches to online fraud", Journal of Financial Crime, Vol. 23 No. 4, pp. 806-818. https://doi.org/10.1108/JFC-12-2015-0069
- Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019), "Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content". ACM transactions on computer-human interaction : a publication of the Association for Computing Machinery, 26(5), 32. https://doi.org/10.1145/3336141
- Cross, C., & Layt, R. (2022), "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. https://doi.org/10.1177/0894439321999311
- Maeng, W., & Lee, J. (2022), "Designing and Evaluating a Chatbot for Survivors of Image-Based Sexual Abuse". Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems.
- Cassandra Cross (2019), "You're not alone: the use of peer support groups for fraud victims", Journal of Human Behavior in the Social Environment, 29:5, 672-691, DOI: 10.1080/10911359.2019.1590279
- Van Uden-Kraan, C. F., Drossaert, C. H., Taal, E., Smit, W. M., Bernelot Moens, H. J., & Van de Laar, M. A. (2011), "Determinants of engagement in face-to-face and online patient support groups". Journal of medical Internet research, 13(4), e106. https://doi.org/10.2196/jmir.1718
- Correia, S.G. (2019), "Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales". Crime Sci 8, 4. https://doi.org/10.1186/s40163-019-0099-7
- Norris, G., Brookes, A. & Dowell, D. (2019), "The Psychology of Internet Fraud Victimisation: a Systematic Review". J Police Crim Psych 34, 231–245. https://doi.org/10.1007/s11896-019-09334-5