MARC KYDD, LYNSAY SHEPHERD, GRAHAM JOHNSON & ANDREA SZYMKOWIAK

# LOVE BYTES:
## IMPROVING ROMANCE FRAUD PREVENTION

**Romance fraud has substantially increased over the past decade. Traditional preventative and support measures have struggled to keep up with this form of cybercrime, suggesting a more personalised prevention approach is needed.**

### A UNIQUE FORM OF FRAUD

Online romance fraud, whereby a scammer feigns romantic interest in a user of a dating platform to financially exploit them, has surged in recent years. In the US, reported losses have reached $750 million annually, while in the UK, losses have totalled almost £100 million in the past year. These figures may be conservative, as romance fraud is often under-reported due to the embarrassment victims suffer.

Romance fraud goes beyond being a financially devastating cybercrime; it also carries a significant emotional toll. Victims not only experience financial loss but also grapple with the emotional impact of realising that what seemed like a genuine relationship was a scam, with many struggling to accept the fact they have been exploited. The emotional impact often prevents many victims from seeking support due to the feeling that being scammed is a personal failure; others suffer a breakdown in the trust of others.

### A CHALLENGING FORM OF FRAUD

While prior work has focused on analysing meta-aspects such as profile pictures and user bios for scammer-traits, research into how technology solutions can be integrated into the design and application of warnings against romance fraud is limited.

As scammers often tailor their approach, each victim receives a 'personalised love story'. Thus, the awareness campaigns seen most frequently around Valentine's Day, such as TakeFive, often fail to offer targeted, actionable messaging. For example, the TakeFive advice doesn't consider scammers who deploy 'foot-in-the-door' or those who may request photos/videos for later use in sexploitation. Meanwhile, international attempts to raise awareness and standardise messaging, such as the inaugural World Romance Scam Prevention Day, are still in their infancy.

Below, we explore current preventative and supportive measures for victims of romance fraud and argue that a personalised approach is merited to tackle the issue.

### Preventative Measures

Awareness campaigns can help users defend themselves against scammers before they become a threat in the form of a simple, easily distributable means of warning about the risks of romance fraud. By highlighting common scammer tactics, users can, in theory, apply the message to their situation. However, awareness campaigns must be generalisable to different scenarios. This creates the issue of 'white noise' whereby users can be confused about what constitutes romance fraud, with victims failing to see their experience reflected in the messaging.

If users cannot find relevant information through awareness campaigns, they may turn to self-education in the form of online searches. This rudimentary approach poses new challenges.

> **…in the UK, losses [to romance fraud] are placed at almost £100 million in just the past year.**

Given the often-explicit nature of romance fraud in the form of sextortion and blackmail, some users have found that some relevant materials were blocked by their Internet Service Provider – being mistaken for indecent material, due to the keyword searches of 'sextortion' or 'revenge porn' used. In other cases, materials in proprietary file formats cannot be accessed by all users, or links to materials are no-longer available.



### Supportive Measures

For victims of romance fraud, peer support groups offer tailored face-to-face advice. While peer support groups are an important first step for victims on the road to recovery, they are not without issue. Although attendees receive in-person peer support groups positively, continued attendance did not reflect this. As many as 90% of attendees were no longer attending sessions one year on from their first visit. Victims noted the discomfort that comes from being open about extremely private conversations and many opted to listen to others instead. The lack of engagement with the group led some to stop attending, creating a feedback loop where a small group of victims becomes even smaller as more and more no longer attend.

An approach to mitigate the financial damage is reporting cases of romance fraud to the authorities. Correia studied how Action Fraud, the UK's national fraud reporting centre, recorded reported data, suggesting that various pieces of information were either missing or misreported, such as which investigator was assigned to a case, or the amount of money lost in a scam. In cases where victims were exploited of smaller amounts of money over a longer period, it may not be initially clear just how much has been lost and as such the total amount lost was recorded as 'o'; making it harder to determine the severity of the crime. Broader demographic information, such as age, ethnicity, and background, were also not recorded. Failing to record which communities are affected by romance fraud makes it more challenging to create effective outreach programs tailored to minorities who also experience romance fraud.

### A PREVENTABLE FORM OF FRAUD

The above overview illustrates that current approaches are not meeting the needs of users – both in terms of preventing romance scams and supporting victims. Existing methods simply do not have the speed and flexibility to adapt to the scammers ever-evolving playbook – perhaps a critical rethink of tackling romance fraud using a technology or data driven approach may be needed.

While it is encouraging to see users taking proactive steps in the form of self-education (Ibid.), there should be a more curated approach, for example, in the form of a central repository of information. The issues raised around the generic nature of awareness campaigns also suggest that the user's own context should play a more significant role in the advice provided through conversational analysis – using the likes of AI; consideration should be given to directly integrating warning systems with dating platforms such as those on banking apps.

> **Despite the devastating impact of romance fraud… implementing effective countermeasures against such crimes continues to prove difficult.**

Building safety measures into dating platforms can protect users from harm, using real-time safeguards. Our work in deploying AI-backed safety measures that operate as the user converses with the potential scammer removes the need to remember potential warning signs. Instead, they are alerted to suspicious activity as it occurs. While still in the developmental stage, our work shows promising signs of moving romance scam prevention in a more dynamic, responsive, and, hopefully, effective direction; helping keep users safe regardless of the scammer's tactics.

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

*Marc Kydd is a PhD student working on Machine Learning and Usable Security. Dr Lynsay Shepherd is a Senior Lecturer in Cybersecurity and Human-Computer Interaction. Prof Graham Johnson is Professor of Human-Centred Technology. Dr Andrea Szymkowiak is a Senior Lecturer in Human Computer Interaction. The research team are based in the School of Design and Informatics at Abertay University, Dundee.*

Image credit: © *Pawel Czerwinski* | unsplash.com