Online Dating & Discovery Association

World Romance Scam Prevention Day: Understanding scammer behaviour and how platforms can prevent and protect

To mark World Romance Scam Prevention Day, the Online Dating and Discovery Association (ODDA) is using the month of October to raise awareness of the issue and highlight what our members are doing to remove scammers from their sites. We're also looking at how the industry is using technology to support them.

In this article, the ODDAs Simon Newman (SN) talks to Nick Tsinonis from fraud and scammer detection specialists, Scamalytics.

SCAMALYTICS

SN: Your company helps businesses detect scammers among other things. What prompted you to set up Scamalytics?

NT: In 2011, I was working on a machine-learning matching technology to match daters to each other on a product called IntroAnalytics. We showed Dan from Free Dating our technology and he was impressed with the results and signed up as one of our first customers. He then asked if we would consider using machine learning to help him solve one of the biggest problems the dating industry was suffering from – scammers. They were hitting dating sites like his very hard and were obvious to detect, using the same text and images and coming from the usual countries. We were tasked to try and automate a very tedious task that took away precious time from the customer support team.

We also had the idea of supporting dating sites sharing blacklisted users via a trusted API. We chose to collaborate and create a system from the ground up, featuring real-time detection of scammers and the sharing of blacklisted user data. A year later, Scamalytics emerged, and it continues to evolve and enhance its capabilities to this day.

SN: You work with a range of online dating services as well as other providers in different industries, what trends have you seen over the last few years? Are scammers becoming more sophisticated?

NT: Yes definitely. They are increasingly creating fake profiles and interacting across multiple platforms to expand their reach and remain undetected. Scammers will start on a dating app and often move conversations to less secure channels like WhatsApp, making it harder for dating platforms to detect the scammers.

The evolution in AI technologies in recent years, now means that romance scammers have become more sophisticated, using advanced technology to enhance their deception. They now employ deepfakes and AI-generated profiles to create more convincing personas, making it harder for victims to detect fraud. Additionally, some scammers use automated chatbots to engage multiple targets simultaneously, streamlining the early stages of conversation before switching to a human for more complex manipulation.

Scammers are also playing the long game, investing months or even years in building trust and emotional bonds with their victims before asking for money. This extended manipulation makes it harder for individuals to recognise the scam.

SN: Can you tell us anything about the types of people committing these scams? Are they organised crime gangs or opportunist criminals? Where are they mostly based?

NT: I must say the research is changing year on year but from our current analysis online romance scams are often carried out by a mix of organised crime gangs and opportunistic individuals.

Criminal networks, especially from countries like Nigeria, Ghana, Russia, and Ukraine, use sophisticated operations where multiple scammers collaborate to target victims, often treating it as a business model. Cybercrime groups in Southeast Asia and Eastern Europe also exploit romance scams as part of broader fraud schemes.

In contrast, some scams are committed by individuals acting alone, often motivated by economic hardship. These solo scammers, while less organised, can be highly effective by targeting emotionally vulnerable or wealthy individuals. Scammers from developed nations sometimes act as intermediaries, facilitating international fraud operations.

Scammers commonly use tactics like catfishing, emotional manipulation, and money laundering, preying on their victims' trust. Countries like Nigeria, Ghana, and Malaysia are known hubs for such activities, but the operations are increasingly global. The methods are growing more sophisticated, making romance scams a pervasive and difficult-to-detect crime worldwide.

SN: You also offer a service to check IP addresses for fraud. Can you tell us more about this?

NT: We introduced our IP Address Fraud Risk API a few years ago to give dating sites and other retail and consumer facing websites a way to identify potential problematic and abusive IP addresses for risk.

An IP address can tell us whether it's part of a blacklisted range of IPs we've seen in our analysis online, whether it's a VPN, Bot, or Spam. Other factors we look at are the country, ISP and organisation the IP belongs to. All these factors come together in an algorithm we use to formulate a risk score, and we offer a free service for anyone to check this online at: https://scamalytics.com/ip/

We offer a free basic API service for up to 5,000 API calls per month and then for companies or website owners with larger requirements we offer a staggered pricing depending on volumes and extra data needs. You can find out more here: https://scamalytics.com/ip/api/pricing

SN: What advice would you give to our members about how they can prevent scammers?

NT: Firstly, dating sites should focus on educating users by providing regular tips and warnings on how to identify and avoid scammers. A dedicated safety centre with clear information about common red flags and scam tactics can help users stay alert and protect themselves from falling victim to romance fraud.

Platforms should make it easy for users to report suspicious activity, and regularly monitor these reports to detect and respond to potential fraud. Promptly reviewing flagged accounts and removing scammers from the platform is key to maintaining a safe user experience.

To further enhance security, machine learning analysis and software tools can be used to detect suspicious behaviours, such as repetitive IP addresses, messaging patterns or the use of stolen or AI-generated images. Facial recognition and photo verification technologies also help ensure that profiles are authentic.

Dating sites can also collaborate with law enforcement and anti-fraud organisations to address scam-related incidents quickly and disrupt broader scam networks. These partnerships are valuable for adding an extra layer of deterrence and safeguarding users from fraud.

SN: Looking to the future, how do you think romance scams will evolve over the next 5 years?

NT: In the next five years, romance scams are likely to become more sophisticated, with scammers leveraging the power of cheap and sophisticated AI technology.

We've already seen deepfake technology being used to create convincing fake personas. These advancements could include not just realistic photos, but also videos and voice interactions, making it much harder for users to detect fraudulent profiles. With AI voice cloning, scammers could replicate the voices of real people or invent convincing voices to strengthen emotional ties with victims during phone or voice calls.

Scammers are expected to target niche groups more effectively with AI, focusing on specific demographics. By exploiting shared identities and vulnerabilities, they will refine their tactics to manipulate specific communities.

The integration of financial crimes such as money laundering or identity theft is expected to grow, with scammers possibly shifting to cryptocurrency to make transactions harder to trace. This shift will complicate efforts to track and recover funds for victims.

Scam networks will likely become more automated and organised, with the use of AI-driven chatbots and other automated systems to handle multiple victims at once. This scalability could significantly increase both the volume and complexity of romance scams.

SN: Finally, can tell us a bit more about Scamalytics?

NT: We now have clients in over 45+ countries around the world with some of them in the Fortune 100. Over 7 million users a month access our website https://scamalytics.com/ip from over 200 countries worldwide checking for IP address fraud scores and other IP address-related data.

Scamalytics' future product developments are increasingly focused on harnessing the power of data and AI techniques to tackle the pressing issue of unwanted and potentially fraudulent web traffic that can compromise the integrity of websites.

We are also committed to fostering collaborative partnerships with various industry leaders, and associations such as ODDA recognising that a multifaceted approach is essential in addressing this complex fraud prevention challenge.

This positions Scamalytics as a key player in the fight against digital fraud but also ensures that our clients can maintain trust with their users, safeguarding their reputation and business operations.

SN: Thank you for your time, Nick!

You can find more about Scamalytics on their website: www.scamalytics.com