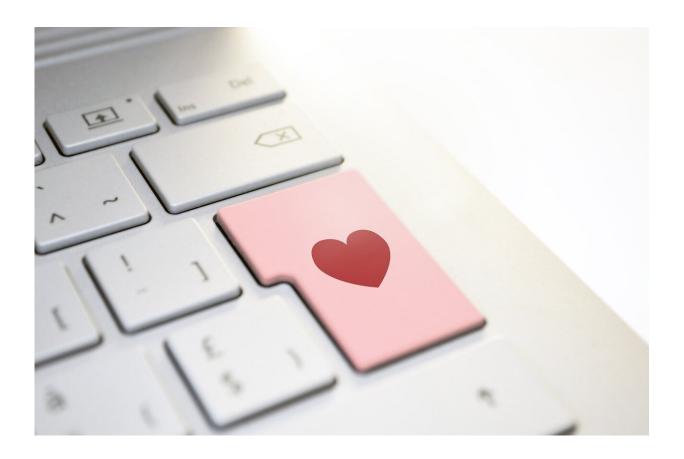# Research reveals online romance scammers' tactics, and how to defend against them

August 7 2023, by Fangzhou Wang

Credit: Pixabay/CC0 Public Domain

In the Netflix documentary "The Tinder Swindler," victims exposed notorious con artist Simon Leviev, who posed as a wealthy diamond mogul on the popular dating app Tinder to deceive and scam numerous

women out of millions of dollars. Leviev is a flashy example of a dating scammer, but criminal operations also prey on emotionally vulnerable people to gain their trust and exploit them financially.

The internet has revolutionized dating, and there has been a surge in U.S. adults using apps to find ideal matches post-pandemic. While these apps offer convenience for connecting with romantic partners, they also open the door to online romance scams. Criminals create both deceptive profiles and urgent scenarios to carry out the scam.

The Federal Trade Commission reports that nearly 70,000 Americans fell victim to online romantic scams in 2022, with reported losses topping US$1.3 billion.

Online romance scams exploit people through calculated online social engineering and deliberately deceptive communication tactics. In a series of research projects, my colleagues from Georgia State University, University of Alabama, University of South Florida and I focused on understanding how scammers operate, the cues that may prompt changes in their tactics and what measures people can take to defend themselves against falling victim to this scam.

How online romantic scams work

Online romance scams are not coincidental. They're carefully planned schemes that follow distinct stages. Research has identified five stages:

- Baiting victims with attractive profiles.
- Grooming victims with intimacy.
- Creating crises to extract money.
- On occasion manipulating victims with blackmail.
- Revealing the scam.

In short, scammers do not swindle victims by chance. They plan their actions in advance, patiently following their playbooks to ensure profitable outcomes. Scammers worm their way into a victim's heart to gain access to their money through false pretenses.

In a previous study, my colleague Volkan Topalli and I analyzed victim testimonials from the website stop-scammers.com. Our research revealed scammers' use of various social engineering techniques and crisis stories to prompt urgent requests. Scammers leveraged social norms, guilt and supposed emergencies to manipulate victims. Scammers also paid close attention to communication patterns and adapted their tactics based on victims' responses. This interplay significantly influenced the overall operation of the scam.

Across the globe, online romance scammers use different techniques that vary across cultures to successfully defraud victims. In my recent research, for example, I looked closely into an online romance scam in China called "Sha Zhu Pan," which loosely translates to "Pig Butchering Scam." In Sha Zhu Pan, scammers bait and groom victims for financial exploitation through well-structured group setups. Multiple scammers across four groups—hosts, resources, IT and money laundering—persuade victims through romantic tactics to invest in fake apps or use fake gambling websites, convincing them to pay more and more without ever receiving their money back. Hosts interact with victims, resources members identify targets and collect information about them, IT creates the fake apps and websites, and the money launderers process the ill-gotten gains.

Deterrence and rewards

Like street robbers, online romance scammers can be influenced both positively and negatively by a range of situational cues that serve as incentives or deterrents.

Our investigation showed that deterrent messages [can significantly affect scammers' behavior](). Here's an example of a deterrent message: "I know you are scamming innocent people. My friend was recently arrested for the same offense and is facing five years in prison. You should stop before you face the same fate." Based on [live conversations]() with active scammers online, our recent analysis suggests that receiving deterrent messages reduced scammers' response rate and their use of certain words, and increased the likelihood that when they sought further communications, they admitted they had done something wrong.

Our observations indicate that scammers not only [diversify their approaches]() to prompt more responses, such as appealing to their romantic relationships, asking for identifying information and requesting victims switch to private chat platforms, but they also use several techniques for getting victims to [overcome their misgivings]() about sending the scammers more money. For example, scammers subtly persuade victims to see themselves as holding more power in the interaction than they do.

Blocking scammers

There are methods that could help users defend against online romance scams.

In experimental findings, my colleagues and I suggest online apps, especially dating apps, implement warning messages. An example would be applying linguistics algorithms to identify keywords like "money," "MoneyGram" and "bank" in conversations to alert potential [victims]() of the scam and deter scammers from engaging further.

In addition, apps can use tools to detect counterfeit profile pictures and other types of image fraud. By concentrating on identifying scammers' use of counterfeit profile pictures, this advanced algorithm holds the

potential to preemptively hinder scammers from establishing fake profiles and initiating conversations from the outset.

How to protect yourself

Online dating app users can take precautions when talking to strangers. There are five rules users should follow to steer clear of scammers:

1. Avoid sharing financial information with or sending money to strangers.
2. Refrain from sending private photos to strangers.
3. Pay attention to spelling and grammar because scammers often claim to reside in English-speaking countries when they actually operate in non-Western countries.
4. Use image and name-reverse searches.
5. Confide in family and friends if you grow suspicious.

One last piece of advice to empower those who have fallen victim to online romance scams: Don't blame yourself.

Take the courageous step of breaking free from the scam and seek support. Reach out to your loved ones, trustworthy third-party organizations and law enforcement agencies for help. This support network is essential in helping you restart your life and move forward.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation