

From dating to defrauding: Online romance scams surge as criminals cash in on lonely South Africans

Issued by [ESET](#)

9 Feb 2023

Catfishing, sextortion, phishing and other romance scams are big business for fraudsters. Carey van Vlaanderen, chief executive officer at [ESET Southern Africa](#) says knowing how to spot red flags can mean the difference between being deeply in love and knee-deep in debt.



Carey van Vlaanderen, chief executive officer at [ESET Southern Africa](#)

Dating sites can be a wonderful place to meet new people, make connections and find a romantic partner, but as the popular *Tinder Swindler* documentary showed, it's easy to fall in love and fall victim to dating scams involving romantic con artists. With February being the month of love, it's important that online daters know how to protect themselves in the digital dating space.

Data from the Federal Trade Commission in the United States showed that in 2021 reported losses to romance scammers were up nearly 80% compared to the previous year. This was followed by an alert issued by the FBI which noted victims of romance fraud lost \$1bn in 2021 alone. While current reliable figures are difficult to establish, romance scams, both in South Africa and across the globe, are likely to be underreported because of the personal nature of the crime and victims' feelings of embarrassment.

According to the South African Banking Risk Information Centre (SABRIC) some terror groups have been targeting South Africans to finance their criminal acts through romance scams. It also reports that online dating scams are used by

fraudsters to launder the illicit proceeds of crime. In 2021, eight suspects were arrested in Cape Town in connection with an online dating scam and stealing more than R100 million from victims in various countries.

Don't fall for the rom-con

Online dating or romance scams are financially and emotionally costly as fraudsters exploit people's vulnerabilities, trust, and feelings of loneliness. When visiting online dating platforms, be aware of photos that look too good to be true. An image search on Google can help you determine if the photo is authentic or a stolen or stock photo. Other red flags include requests for private information such as your ID number, declarations of love alarmingly early in the relationship, or a request for money to help them out of a situation.

Another new trend in 2022 was an increase in reports of romance scammers luring consumers into fake cryptocurrency investment schemes.

Falling for deception

While dating scams have multiple layers of deception, they all rely on gaining a victim's information which should give everyone pause to think about how the management of personal information can allow criminals to build a detailed profile of their target.

A common modus operandi is scammers using emotional manipulation to get a victim to send money, gifts, or personal information. Another common, and extremely traumatising, form of deception is sextortion. This begins as a seemingly normal relationship before the scammer pressures the victim into sending intimate photos or videos which are used as material to blackmail the victim.

Catfishing is another common trick scammers use which lures the victim into a relationship based on the attacker's fictitious online persona. Once the victim is on the hook, the scammer will send messages about being in financial trouble with promises to pay the money back later.

How to protect your feelings and your finances

- Scammers seldom ask for money at the beginning of an interaction. Instead, they may express money worries in casual conversation or use financial trouble as a reason not to meet.
- Carefully consider the decision to leave verified dating apps to message privately. Not only does this give the fraudster access to your mobile number, but dating apps also provide mechanisms to report scammers and unsafe behaviour.
- Don't send a person money. No matter how convincing their story may be. Talk to someone you know and trust for their perspective on the situation.
- Never share any information that may compromise you, including photos or videos.
- If you decide to meet someone in person that you've met online be sure to set up the meeting in a safe, public place, and ensure a trusted friend or family member is aware of your arrangements.

▮ **Eset launches solution to address SOHO security concerns** 15 Apr 2024

▮ **Don't gamble with your cybersecurity** 29 Feb 2024

▮ **Avoiding job scams, and finding a job you love** 9 Feb 2024

▮ **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024

▮ **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET



ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.

[Profile](#) | [News](#) | [Contact](#) | [Twitter](#) | [Facebook](#) | [RSS Feed](#)

For more, visit: <https://www.bizcommunity.com>