DATING, DMS, AND DEEPFAKES OH MY!

Unpacking the new age of relationship scams

THIS MONTH'S TOPICS:

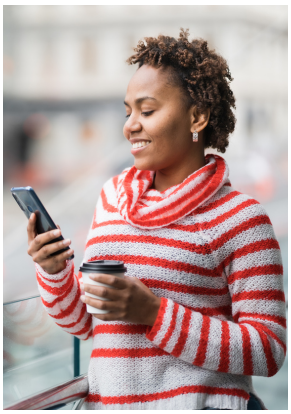
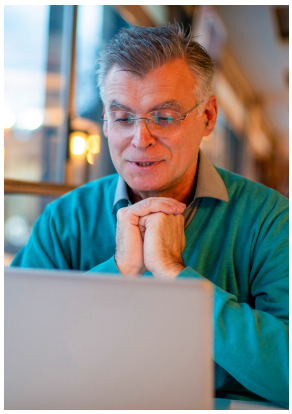
Valentine's Day has come and gone, but romance scams don't stop after February 14th!

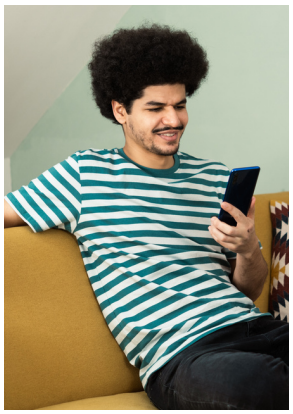
There are many ways that cybercriminals can carry out romance scams. They might catfish with someone else's pictures, or use deepfakes to make fake videos and voices. Most will try to gain the user's trust and then ask for money.

In this month's newsletter, learn more about romance scams. If you aren't in the market for romance, know that these tactics are used in other scams, as well, so you can use these tips to not only help friends and family stay aware, but also for yourself.

ROMANCE SCAMS

THE NUMBERS



WHAT ARE THEY?

Romance scams occur when a scammer creates a profile on a dating or social media site. They typically use fake pictures and move the relationship along quickly, claiming they are in love. After gaining the person's trust, the scammer tries to move the conversation off the platform and ask for money. With the rise of deepfake technology, scammers can now even mimic voices and make convincing videos using another person's identity.

WARNING SIGNS

- They claim they are away for business or military service.
- They avoid meeting in person.
- They say they are about to inherit a large sum of money.
- They say they are in trouble or have a friend in danger.
- They ask for money or personal information early on.

ROMANCE SCAM STATS

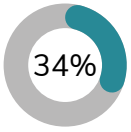
57M
Use Dating Apps in the US

4.4K
Median Individual Loss

1.3B
Dollars lost in the last 5 years

#3
Rated Scam by Consumer Affairs

of romance scams start on social media



of money lost was sent via cryptocurrency

IS SOMEONE YOU KNOW BEING SCAMMED?

It can be difficult to discuss a potential romance scam with a loved one. If you think someone you know is being scammed, do a reverse image search on their match's profile picture. Encourage them not to give the person money. If they are clearly being scammed, consider going to the authorities and report the scammer's account to the dating site or app.

Deepfakes and Artificial Intelligence

WHAT ARE DEEPFAKES?

Deepfakes are videos or pictures that have been digitally altered using artificial intelligence. They are used to change a person's appearance or alter what they say or do in a video. While deepfake technology is exciting, it can also be used to mimic celebrities or carry out scams.

HOW ARE THEY EVOLVING?

Scammers use deepfake videos and voice recordings to make their romance scams more convincing. While some use fully AI-generated images, others make deepfakes mimicking celebrities. There are many ways to spot deepfakes, but this technology is always evolving so deepfake images and videos might be harder to identify as time goes on.

TIPS

- AI-generated images might have unnatural lighting, or issues with the teeth or eyes.
- Request a video call or meeting in person.
- In videos, look for any unnatural blinking, strange mouth movements, or lack of emotion.

SPOT THE 3 AI-GENERATED IMAGES

A.

B.

C.

D.

E.

F.

Answer: C, D, and F are AI-Generated

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

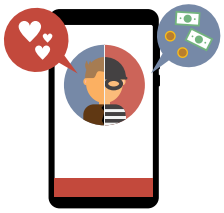
Nadine was scrolling through social media when a message appeared from a man named Mark. He said he was impressed with her art. Nadine thanked him. Mark's account didn't have many followers or pictures, but she was pulled in by his kind message and his model-like looks. They talked for weeks and eventually Nadine asked him to hop on a video call. While the service was spotty, she was convinced it was the same man in the profile picture. They spoke on the phone many times, too. Mark was from England, and he spoke with an English accent which helped confirm Mark was real.

Mark professed his love for her. He wanted to meet her, but claimed he needed money for a flight and his medical bills before he could come since his cards weren't working. He promised to pay her back after. Nadine used most of her savings to pay for his bills. Eventually, Nadine's sister stepped in. She did a reverse image search and found that Mark wasn't who he said he was. He was using someone else's identity to scam Nadine.

Did you spot the red flags?

- Nadine should have been more wary of Mark coming on so strong and contacting her unsolicited.
- While it was good Nadine asked Mark to hop on a video call, she should not have taken the blurry video and English accent as reasons to fully trust him.
- Nadine should have been more skeptical when Mark asked her to send him money.

Reverse image searches are a great way to confirm someone's identity. If the search shows the person has another identity, and the relationship exhibits other red flags of romance scams, it is best to stop talking to them. Many scammers will claim they are the one being impersonated and try to trick the user into staying.



Voices can be faked using artificial intelligence. This means scammers could sound like a celebrity, have an accent, or sound like someone you know. Unnatural pronunciations or pauses are some telltale signs, but as AI voice changers improve, they will be harder to spot. Remember to think twice before trusting someone just because of their voice.

CYBER NEWS

FEBRUARY
2024

704% INCREASE IN DEEPFAKE "FACE SWAP"

Research just came out stating that there was a 704% increase in deepfake "face swap" attacks throughout 2023. Face swapping refers to scammers using tools, many of which the general public has access to, to manipulate pictures and videos of themselves. One of the main dangers of these convincing videos is that many pass a "liveness" test which is used to remotely verify a person's identity. It is important to be aware of the prevalence of these tools as they are continuing to grow in popularity.

UPDATES & EVENTS

-February 7th was Safer Internet Day. Give the children in your life a cyber tip to help them stay safe online.

-March 1st is World Compliment Day!

FAKE PASSWORD MANAGER APP

A fake password manager app was spotted in app stores. The fake app mimicked the real LastPass app with a similar design and description. The cybercriminals even copied over a few reviews from the real app to the fake one. The app was used to steal users' credentials. Luckily there were some signs to spot the scam. The app name was misspelled for starters. There were also very few ratings on the fake app. The app has been taken down, but this story serves as an important reminder to check apps closely before downloading, since cybercriminals will likely continue to spoof apps in the future.