Love is in the "Err"



Don't Make the Costly Error of Falling for a Romance Scam!

Division of Information Security FEBRUARY 2024

With Valentine's Day upon us, love is in the air. And when thoughts turn to love, many people now turn to dating apps and social media to find new relationships.

Take Sam, for example. Sam is having a pretty good start to the year. He just got a raise and just got back from a big trip to see his favorite band. He joined a dating app and Sarah instantly messaged him. Turns out Sarah likes the same band he does and they

quickly bond over it. After many weeks of messaging back and forth, they start planning to get together; however, Sarah lives far away and can't afford a ticket. Sam feels he can cover the ticket since he just got that raise. He sends Sarah the money, but never hears from her again. Turns out "Sarah" was a cyber criminal and Sam fell prey to a romance scam. "Sarah" had been following Sam's social media accounts. "Sarah" knew from Sam's posts what bands he liked, knew he'd gotten that raise, and knew which dating app he was joining in order to target him.

Romance scams are on the rise. The Federal Trade Commission (FTC) reports that "people reported a record \$547 million in losses to romance scams in 2021."





The scammers will target someone on dating apps or social media and then start a



virtual whirlwind romance, telling them very early on that they are soulmates and meant to be. The Better Business Bureau (BBB) explains that once the scammer establishes an online relationship, they will begin to test the waters and ask for money. Small amounts at first. The BBB even has an example where a scammer sent gifts first. They sent "gifts such as flowers or chocolates, and then asked for small sums of money for supposed minor emergencies." The requests then increased over time and one woman who was scammed was left with debts of nearly a hundred thousand dollars.

<u>In another article, the FTC breaks down</u> the lies that romance scammers use to keep the scam going. Twenty-four percent of victims

reported that the scammer told them that someone close to the scammer was "sick, hurt, or in jail." Eighteen percent of victims reported that the scammer actually pretended to

help the victim by taking the money in order to teach the victim "how to invest." Another eighteen percent reported that the scammer claimed to be "in the military far away" to keep the scam going and explain why they could never meet in person.

That same article shows how scammers prefer to get paid in ways that are unrecoverable, with 19 percent wanting cryptocurrency, 14 percent preferring wire transfers, and the most, 24 percent, looking for gift cards. And although gift cards were the preferred type of scam, the most money was lost to crypto and wire transfers which accounted for 34 and 27 percent of lost funds, respectively.

The FTC has some tips to avoid getting scammed:

Nobody legit will ever ask you to help—or insist that you invest— by sending cryptocurrency, giving the numbers on a gift card, or by wiring money. Anyone who does is a scammer.

If someone tells you to send money to receive a package, you can bet it's a scam.

Talk to friends or family about a new love interest and pay attention if they're concerned.

Try a reverse image search of profile pictures. If the details don't match up, it's a scam.

And the Secret Service bolsters that list with these additional tips you can follow to avoid being a victim of a romance scam:

Be careful of what you post online.

Use reputable websites, although keep in mind that scammers are on these as well.

If you develop a relationship online:

Research the person's photo and pro-

Ask guestions. If a person seems too good to be true, they probably are.

Beware if you are asked for inappropriate photos or financial information. Do not send money to people you meet online and have never met in person.

Be suspicious if the person fails to show up for multiple attempts to meet and always has an excuse.

Romance scammers are counting on their victims' being too embarrassed to report the crime after it occurs. So be careful out there with your data, but also be careful with your heart. Make sure neither ends up in the wrong

hands! If you, or a loved one, has fallen victim to a scam, report it to the FTC at Report-Fraud.ftc.gov.

NOTE: The links in this document are for informational purposes only and do not signify an endorsement of any products contained within the linked sites/files.

Please contact <u>cybersecurity@ihs.gov</u> with any questions or comments about this newsletter.



Darling, help me. Send me some

and

from

7

g

8

money

2

a

3

S

to

a