FS-ISAC | Security Tips Newsletter

7 February 2025 | Issue No. 18

Security is *Everyone's* Responsibility

Love is in the Air, or is it?

Summary

February 14th is right around the corner and love is in the air. Are you confident that the person special person you are talking to via the Internet is *who they say they are?*

A romance scam is a type of confidence ruse where a criminal pretends to be romantically interested in a victim to gain their trust and steal money. Scammers may use dating sites and social media to target victims.

According to Yale Cybersecurity, "The average loss from a romance scam was $4400 in 2022. Nearly 70,000 people reported a romance scam to the Federal Trade Commission (FTC), with total reported losses of an astounding $1.3 billion."

Why Should You Be Worried?

Scam artists play on emotion. They may email photos to create a bond with the victim. Once that emotional bond is cemented, they often say they all they need is to be wire transferred funds and when received, will travel to meet them.

There are other scenarios where a person arrives at the persons home with "family members" who then physically and emotionally abuse the victim.

Whatever the case, it begins with that first wire transfer which makes it easier to avoid meeting in person - and more plausible when they ask for money for a medical emergency, an unexpected legal fee, or some over emergency.

If someone you meet online needs your bank account information to deposit money, they are most likely using your account to carry out other theft and fraud schemes.

Here's What You Can Do

Regardless of whether you are the victim or care for a family member, the Federal Bureau of Investigation wants you to think and talk with a trusted friend or family member:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.

- Research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.
- Go slowly and ask lots of questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.
- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you have only communicated with online or by phone.
- If your financial institution has investigated the matter and tell you it's a scam – believe them, they are looking out for your best interests.

Lots of people have found love online — but many have found crooks and criminals too. So, during this special time of year when love is in the air, remember to be careful with your heart *and* your wallet.

What to Do if You are Scammed

- If you feel an email contains a scam, don't respond. Block the sender.
- If it's a phone call – hang up!
- Set emotion aside, if it's too good to be true, it usually is.
- If you provide your personal information (account, date of birth, online banking user ID, password, etc.) contact your financial institution immediately.
- Verify *then* trust the source.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your financial institution, contact them immediately.

12120 Sunset Hills Rd, Reston
VA 20190