FBI Warns of Cyber-Based Romance Scams

February 6, 2020

The Federal Bureau of Investigation (FBI) is warning Americans to be on the lookout for cyber-based romance scams.

"Well-rehearsed criminals search dating sites, apps, chat rooms, and other social media networking sites attempting to build “relationships” for the sole purpose of getting your money or your personally identifiable information," says the FBI.

FBI Richmond suggests taking these points into consideration to avoid becoming a victim.

- Only use reputable, nationally-recognized dating websites; however, be aware that scammers may be using them too.
- Research photos and profiles in other online search tools and ask questions.
- Never provide your financial information, loan money, nor allow your bank accounts to be used for transfers of funds.
- Do not allow attempts to isolate you from family and friends.
- Do not blindly believe the stories of severe life circumstances, tragedies, family deaths, injuries, or other hardships geared at keeping your interest and concern.
- If you are planning to meet someone in person you have met online, meet in a public place and let someone know where you will be and what time you should return home.
- If you are traveling to a foreign country to meet someone check the State Department’s Travel Advisories beforehand (http://travel.state.gov/), provide your itinerary to family and friends, and do not travel alone if possible.

"Victims may be hesitant to report being taken advantage of due to embarrassment, shame or humiliation. It’s important to remember, romance scams can happen to anyone at any time," says the FBI.

If you suspect your online relationship is a scam, cease all contact immediately. If you are a victim who has already sent money, immediately report the incident to your financial institution, file a complaint with the FBI’s Internet Crimes Complaint Center (www.ic3.gov), and contact law enforcement.

“Cybercrime is associated with technological tricks and an attacker’s ability to bypass and evade security controls. However, what is just as commonly used are social engineering tricks that manipulate the human psyche through emotions," says Chris Morales, head of security analytics at Vectra. "Defending against technology-based attacks, such as malware, requires the use of technology controls, but defending against social engineering becomes a mental game. Social engineering isn’t new to the cyber world. It has been in use for as long as people have existed. For example, a simple form could be a child manipulating a parent to purchase a toy. The intent of social engineering is to influence people into taking action that might not be in their best interest."

"Which is why cybercriminals have caught on," he continues. "Holidays like Valentine's Day are a particular focal point for social engineering tricks as people tend to have elevated emotions. As many people feel particularly lonely on this day, any kind of attention would be comforting. It is unfortunate that many online predators would be manipulate strong emotions to influence people into performing acts such as sending a financial transaction to someone who they have never met. No matter how desirable a person may sound online, everyone must tread with caution. Only trust those you know in person and even then be cautious. In our connected society, everyone needs to remember to remember a basic rule we were taught as a child, especially with people you can't even look in the eye. Don't talk to strangers."

"For cybercriminals, Valentine's Day is just another holiday and the opportunity for just another scam. If you don't know who the mark is, it's most likely you," Terrence Jackson, CISO at Thycotic says. "Phishing is still the attackers weapon of choice and there will be no shortage of well-crafted emails and messages designed to emotionally engage you and prevent you from making rational decisions. Here are some practical steps that can help you protect your heart and your wallet:

1. If it sounds too good to be true, it usually is.
2. Stay clear of stories that pull at your heart strings from unsolicited sources or strangers that are requesting money.
3. Never share usernames, passwords, bank account numbers or credit card numbers with strangers.
4. Use common sense. That Romeo or Juliet is more likely a scammer than your soul mate.
5. If the request is from someone familiar, call them to verify the request, don't just take a social media message at face value.
6. If your new "love" is on a dating app and one of the first request is for money…Run like the wind!

https://www.securitymagazine.com/articles/91673-fbi-warns-of-cyber-based-romance-scams

https://www.ic3.gov/default.aspx