BankOnITUSA®

INFORMATION SECURITY BRIEF

FEBRUARY 2022

HERE ARE SOME SIGNS TO WATCH FOR BEFORE OPENING YOUR HEART AND CLICKING ON ANY LINKS OR SENDING MONEY:

Be wary of any love interest that asks for money via gift card, money transfer, or cryptocurrency — they are likely scammers.

Romance scammers are quick to profess their love. Be suspicious of overzealous potential partners.

Scammers will also tell you they cannot meet you because they are overseas for military service, work, etc. These days they might tell you they can't meet due to the pandemic lockdown.

Potential partners might ask you to send them money for a phone to keep chatting, travel expenses to meet you, medical expenses, or other requests for money — all are likely scammers.

From Russia with Love

Valentine's Day is just around the corner, so are the scams and other cyber threats.

Cyber attackers pay attention to the headlines. The con artists often incorporate current events in their scams to play on unwitting victims' emotions and catch them with their guards down. There's a new variant of COVID spiking? Here's an email with malicious links to fake treatments or COVID tracking sites. Bad actors also watch the calendar. At Christmas, they try to lure us with deceptive emails and texts about package deliveries that appear to be from FedEx, UPS, or Amazon. These cybercriminals try to prey upon our deepest feelings, and no event or holiday, or sentiment is off-limits to them.

They'll even toy with your heart on Valentine's Day.

The Federal Trade Commission (FTC) reported that 2020 losses related to romance scams increased by 50% over 2019, and today they are at an all-time high. Romance scams can begin in any number of ways, including the use of emails, text messages, fake dating website profiles, and phone calls where the scammer works to build a relationship with an individual before asking for money, often to pay for travel to meet the would-be romantic partner.

With the overall increase of cyberattacks from foreign adversaries, Valentine's Day provides bad actors with another opportunity not only to take your money but also to infect your devices and systems with ransomware, viruses, and other malware you don't want.

The Federal Trade Commission has published material titled What You Need to Know about Romance Scams. It has sound advice for identifying a potential cyber attacker, tips on how not to become a victim, and how to report such scams.

For more information about how ransomware and diplomacy are increasingly related, read Ukraine Government Websites Hit by Cyberattack from *The Wall Street Journal.*