CANADIAN ANTI-FRAUD CENTRE BULLETIN

Romance Scams 2024-02-12

FRAUD: RECOGNIZE, REJECT, REPORT

Every year around Valentine's Day, fraudsters are on the look-out for unsuspecting victims who are looking for love and companionship. Victims are typically contacted on dating websites or social media and then asked to switch to a different method of communication. It is common for suspects to use real pictures found on social media of real people (ie. business people, members of the military, family photos), pet photos and hobbies. Fraudsters quickly profess their love to gain their victims' trust, affection, and money. This type of fraud relies heavily on victim emotions and may last for months, years, or until the victim has nothing left to give. The fraudsters will never end up repaying the victim and continue to make empty promises while asking for more money.

Some recent variations include the use conversational attacks where fraudsters send random text messages to victims. The messages often read "where are you?", "where have you been?" or something similar. Once the victim responds, a conversation is started and the fraudster attempts to build a relationship with the victim.

Another prevalent variation is the ''CryptoRom''. In these cases, fraudsters convince the victim to invest into a fraudulent cryptocurrency platform with the promise of large monetary returns. In fact, fraudsters may even let the victim cash out some of their investment returns only to get them to invest a larger amount.

In addition to Crypto Investing, the CAFC is still receiving reports of fraudsters requesting money for various reasons, including:

- a personal/family emergency,
- claims they have no access to their existing funds,
- unexpected business expenses, legal expenses or professional fees,
- investing in a new business and they need the victims' help, and
- travel fees to return home.

Warning signs

Beware of:

- profiles that seem too perfect,
- someone you haven't met in person professes their love to you,

- a suspect that tries to move communication to a more private or different method of communication (email, text, social media platform, etc.),
- any attempts to meet in person get cancelled or there's always an excuse to not meet-up,
- a person who discourages you from talking about them to friends and family,
- a suspect acting distressed or angry to force you into sending more money,
- poorly written messages or messages addressed to the wrong name,
- an individual who "introduces" you to their family on social media to legitimize the relationship, or
- unsolicited text messages from phone numbers you don't recognize.
- Get rich quick investment opportunities.
- Be wary of individuals met on dating sites or social media who attempt to educate and convince you to invest into crypto currency.

How to protect yourself

- Don't give out your personal information (name, address, DOB, SIN, banking credentials).
- Don't accept friend requests from people you do not know.
- Don't invest your money in platforms provided by people you don't know.
- Be careful who you share images with. Suspects will often use explicit pictures to extort victims into sending more money.
- Protect your online accounts.
- Never send money to someone you haven't met.
- Don't respond to text messages from phone numbers you do not recognize.
- Beware of fraudsters asking you to open and fund new crypto accounts, they will direct you to send it to wallets they control - **Don't!**
- Learn more tips and tricks for protecting yourself.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the CAFC's online reporting system or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.