CANADIAN ANTI-FRAUD CENTRE BULLETIN

Relationship and Romance Fraud 2025-02-14

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/or companionship.

Romance variation

Victims are typically contacted on dating websites or social media, 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. Once a connection is made victims will be asked to switch to a different method of communication such as Whatsapp, Signal and others. 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.

Common reasons fraudsters request money:

- 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.

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.

Relationship investment fraud

In these cases, fraudsters develop a relationship with the victim and convince them 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. Suspects will "coach" victims on how to invest in their fraudulent crypto currency platforms. Unfortunately, once the victim requests to withdraw their investment, they are unable to do so.

New variation

A newer variation being reported is often referred to as "approval phishing". While "approval phishing" has existed for some time now, more recently this fraud tactic is being adopted by fraudsters engaged in romance and relationship frauds. Suspects develop a relationship with the victims and convince them to invest into crypto, they are then deceived into granting access to their cryptocurrency accounts by those

posing as trusted services. After being coached on how to acquire cryptocurrency such as Etherium or Tron, a fake request is sent by fraudsters that appears to come from the crypto service, asking the user to "approve" access to their wallet. By clicking "approve," the individual unknowingly gives control of their funds to the third party. The fake requests closely mimic legitimate apps and services, making them look authentic to the user. In some cases, victims may receive a transfer request asking them to click on a link to accept and victims may unknowingly be providing the "approval" to access their wallet.

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
- Someone offering to "coach" you on crypto investing
- Emails appearing to be from your crypto service provider asking you to click on links
- 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
- Never send money to someone you haven't met
- Enable Multi-Factor Authentication (MFA) on your accounts
- 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!**
- If you have granted a suspect access to your crypto account, follow the OPP's checklist to revoke the token approval
- Learn more tips and tricks for protecting yourself

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police and to the CAFC's online or by phone at 1-888-495-8501.