



CANADIAN ANTI-FRAUD CENTRE BULLETIN

Crypto Investments

2022-03-03

FRAUD: RECOGNIZE, REJECT, REPORT

Fraud Prevention Month is a campaign held each March to inform and educate the public on the importance of protecting yourself from being a victim of fraud. This year's theme is impersonation, and focuses on scams where fraudsters will claim to be government officials, critical infrastructure companies, and even law enforcement officials. The Canadian Anti-Fraud Centre will be sharing advice through our website, Facebook and Twitter pages. We encourage you to follow and visit our social media profiles often for fraud prevention information. Don't forget to use #FPM2022 on all fraud prevention posts all month!

Investment scams were the highest reported scams based on dollar loss in 2021. Victims of investment scams reported a total loss of \$163.9 Million to CAFC. In most of these cases, the investment opportunities offer higher than normal, or true monetary, returns which often result in investors losing most, or all, of their money. The majority of the investment scam reports involve Canadians investing in crypto currency after seeing a deceptive advertisement. It typically involves victims downloading a trading platform and transferring crypto currency into their trading account. In most cases, victims are not able to withdraw their funds. It is very likely that many of the trading platforms are fraudulent or controlled by fraudsters. In addition to crypto trading scams, the CAFC also receives reports on suspected fraudulent Initial Coin Offerings.

Variations of Crypto Investment Scams

- The victim is approached on a dating or social media website. In some cases, the scam starts as a romance scam and quickly turns into an "investment opportunity". Because suspects have gained the victim's trust, it can lead to a high dollar loss for the victim.
- In some reports, suspects have compromised victim's friend's social media accounts. Because the victim believes they are communicating with a friend or a trusted person, they are easily convinced to take advantage of the "investment opportunity".
- The suspect calls a victim directly and convinces them to invest into crypto currency. In many cases, the suspect asks for remote access to the victim's computer. The suspect shows the victim a fraudulent crypto investing website and convinces the victim to invest based on the potential exponential growth of the investment. In many cases, the victim will invest over a long period of time and, in the end, will realize that the funds can not be withdrawn.
- An email is received by the victim offering a crypto investment opportunity.



Royal Canadian Mounted Police
Gendarmerie royale du Canada



Competition Bureau
Canada

Bureau de la concurrence
Canada



Ontario Provincial Police

Canada

- The victim comes across an advertisement on social media. After the victim clicks on the ad and provides their contact information, suspects contact the victim by telephone and convince them to invest.

Warning Signs

- Investment opportunities with higher than normal returns.
- Unsolicited telephone, email or social media investment offers.
- Displays of urgency so you don't miss out.
- An individual met on a dating or social media website who quickly attempts to convince you to invest into crypto currency.
- A friend tells you about a crypto currency investment opportunity via social media or email.
- Telephone calls from crypto investment companies.
- Fraudulent ads posted on the internet or social media.
- Request to transfer your crypto investment to an alternate crypto address.

How to protect yourself

- Be careful when sending cryptocurrency. Once the transaction is completed, it is unlikely to be reversed.
- As proceeds of crime and anti-money laundering regimes around the world create regulatory frameworks that treat businesses dealing in crypto currencies as money service businesses, Canadians need do their research to ensure they are using reputable and compliant services.
- If you receive a suspicious message from a trusted friend, reach out to them through a different means of communication to confirm that it is them.
- Verify if the investment companies are registered with your Provincial Securities Agency or the National Registration Search Tool (www.aretheyregistered.ca).
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project.
- Be wary of individuals met on dating or social media who attempt to educate and convince you to invest into crypto currency.
- 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!

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