CANADIAN ANTI-FRAUD CENTRE BULLETIN

The Sophistication of Fraud 2026-03-16

FRAUD: RECOGNIZE, REJECT, REPORT

Fraud is affecting Canadians every day, and it continues to grow in both scale and complexity. Perpetrators are constantly changing their tactics and using new technologies to make fraud look real and convincing. Fraud Prevention Month is an opportunity to raise awareness, share practical tips, and encourage Canadians to slow down, verify information, and report fraud to help protect themselves and others.

Fraudsters are using advanced technology, including artificial intelligence (AI), automation, and professional-looking tools, to make fraud harder to detect. These tactics allow criminals to impersonate trusted people, companies, and platforms, increasing the chances that victims will believe the interaction is real.

Some of the methods Canadians may encounter include:

- **Deepfakes** - AI generated videos that appear to come from trusted individuals or public figures
- F**ake crypto investment websites and apps** designed to look like legitimate trading platforms
- **Employment frauds** that include realistic job postings, interviews, and official-looking documents
- **Automated messaging and encrypted communication tools** used to contact large numbers of people quickly

Employment Fraud and Malicious Apps

Employment fraud continues to evolve and often appears very professional. Perpetrators often pose as employers and guide victims through a hiring process that includes interviews, contracts, and training materials.

In many cases, victims are asked to download malicious applications or apps as part of the job. These apps may claim to be used for work tasks, communication, or payment. Once installed, they can be used to steal personal information or move money without the victim's knowledge.

Behind these frauds, perpetrators rely on professional-looking infrastructure, such as fake websites or platforms that are linked to crypto investments or fraudulent payment systems. This setup helps make the fraud appear legitimate while allowing criminals to move funds quickly and anonymously.

Crypto Investment Fraud

Crypto investment fraud often appears similar to legitimate online trading platforms. Perpetrators use professional-looking websites or apps that claim to offer investment opportunities, real-time returns, or expert advice.

To attract victims, perpetrators use deepfake videos, social media posts, and sponsored online ads that feature trusted individuals or well-known names. These tactics are designed to build trust and create a sense of urgency.

Similar to employment fraud, victims may be directed to download malicious apps or use fake investment platforms that show false profits. Once money is deposited, victims may be pressured to invest more or pay additional fees, only to find they cannot withdraw their funds.

Warning Signs – How to Protect Yourself

- Be cautious of unsolicited job offers, especially those received through social media messaging apps or unsolicited text messages
- Verify the employer by checking their official website and contact information
- Never download apps or software as part of a job offer unless you can confirm they are legitimate
- Be alert! If you are asked to move money, accept payments in your personal bank account, or use crypto as part of the job, there is a good chance it's fraudulent
- Be skeptical of investment opportunities that promise guaranteed or unusually high returns
- Verify if the investment companies are registered with your Provincial Securities Agency or the National Registration Search Tool.
- Avoid pressure to act quickly or keep the opportunity secret
- Be wary of promotions using celebrity images, deepfake videos, or sponsored ads
- Never download unknown investment apps or send money to platforms you cannot independently verify
- Remember that legitimate investments allow you to withdraw funds without paying extra fees

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police. Also visit the Report Cybercrime and Fraud website to report online or by phone at 1-888-495-8501.