CANADIAN ANTI-FRAUD CENTRE BULLETIN

Employment Frauds – New Variation 2025-12-16

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre (CAFC) continues to receive reports about employment frauds. Victims are being solicited with fraudulent job offers through text message, WhatsApp, email, Messenger, and social media ads. These job offers may use the names of real companies but are fake. Victims are tricked into making deposits or sending cryptocurrency and are unable to recover their money.

Overall reported losses to employment fraud have skyrocketed in recent years. In 2022, Canadians reported $7.3 million in losses. This increased to $49 million in 2024. Unfortunately, the trend is continuing in 2025. In the first nine months of 2025 alone, victims have already reported $46.5 million in losses. These numbers show that job fraud is growing quickly, and fraudsters are targeting more Canadians than ever before.

*****New Variation*** Web Surveys and Online or "E-Commerce" Store Jobs**

Fraudsters offering fake work-from-home jobs that involve running online stores or completing web surveys. These offers often appear in social media ads, text messages or through messages on WhatsApp, Telegram, Instagram, Messenger or TikTok.

Victims are promised easy income, small commissions, and flexible work. At first, the tasks look simple, and the platform shows fake earnings to build trust. Victims may even receive a small initial payout. But soon, they are asked to make deposits to continue.

Online Store Jobs: Victims are told to register for a fake online store or e-commerce platform. They are asked to "process orders", "approve transactions" or "manage inventory". They are promised commissions for every completed order. As victims continue, the system begins requesting larger deposits to "upgrade the account", "fix order errors", or "unlock higher commissions".

Web Survey Jobs: Victims are asked to complete paid online surveys. After completing a few simple surveys, the platform claims there are issues and asks for deposits to continue. Victims see a rising fake balance on the screen, but they are unable to withdraw any funds. They are pressured to finish more surveys and to pay to unlock the next level.

Victims often realize it's fraud only when the deposit amounts become too large or when the platform blocks withdrawals.

Boosting Products or "Online Tasks" Variation

Using the names of real companies in Canada, the fraudsters are offering victims freelance job opportunities to "boost" products, apps or videos using software created by the fraudsters. After the victim installs the software and creates an account, they receive "orders" or "tasks" they have to complete. Victims might receive a small payment or commission in order to convince them that the job is legitimate. Victims can earn higher commissions or "move up a level" by boosting more products or videos but need to pay fees to gain access to the additional work.

Victims deposit their funds into crypto accounts or wallets. Victims may also be asked to recruit other victims to increase their earnings. Like crypto investment frauds, victims will see funds in their crypto account but will not have the ability to withdraw the funds they have deposited and earned.

Warning Signs

- A company uses a web-based email instead of an official business domain.
- You receive a job offer you did not apply for.
- You are asked to join a platform, download software, or complete simple tasks for fast money.
- The job requires upfront deposits, "upgrade fees," or "unlock payments."
- You see a balance on the website or app but cannot withdraw it.
- You are asked to recruit others.
- You are asked to receive or forward money through your bank account.
- The offer promises high pay for minimal work.

How to Protect Yourself

- Take time before responding to unknown job messages.
- Verify the company's official website and call their official phone number.
- Never send deposits or pay fees for a job.
- Avoid downloading unknown software or apps.
- Do not share personal information or ID documents with unverified contacts.
- Be careful when sending cryptocurrency; in most cases, it cannot be reversed.

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.