Common scams to watch out for

Scammers go to great lengths to manipulate people. Right now Canadians are falling victim to scams that prey on their vulnerability.

1. Cryptocurrency investment scams

Everyone wants in on the newest, seemingly most lucrative investment offer – and right now, fraudsters are using **market interest in cryptocurrency to lure investors into scams.** They use high-pressure sales tactics and promises of high returns to trick victims out of their savings.

Example: Victims are directed to a specific trading platform to convert their funds into crypto assets, and then encouraged to transfer these assets to a fake investment website to fund an “account.” In some cases, the victim may be instructed to download software to supposedly facilitate asset conversion and transfer, but actually provides fraudsters with remote access to their computer.

Using false statements and the illusion of rapid gains, even allowing partial withdrawal of funds to build trust, fraudsters will strongly encourage investors to make additional deposits. Ultimately, requests to withdraw their assets will fail, fraudsters will stop replying to communications and the victim will lose their funds.

Red flags to look out for:

- If you are unable to validate the investment firm’s reputation or the representative’s professional background with your own independent research.
- If the representative encourages you to download specific software to supposedly assist with transferring funds or purchasing crypto assets.
- If a company offers to recover funds lost to cryptocurrency fraud; this is often a secondary scam.

2. Employment scams

Employment scams involve jobs offering easy money, high wages, flexible working hours or exciting future opportunities. Some of the most common scams include car wrapping, mystery shopping and depositing counterfeit cheques.

Example: A fraudster may employ you to help out with banking transactions. They may send you a cheque and ask you to deposit it into your bank account. Then, they will ask you to transfer the money to another account in exchange for a percentage of the original deposit value. When the original cheque is discovered to be fraudulent, you may find yourself on the hook for its entire value, plus the amount you unknowingly transferred to the fraudster.

Red flags to look out for:

- If the job involves depositing cheques or transferring funds.
- If the job is being offered over email or text, with little or no recruiting process.
- If the posting involves words like "guaranteed" or phrases like "easy money."

3. Overpayment scams

If you’re considering selling anything online, watch out for "accidental" overpayments that exceed the agreed upon price. These scams involve tricking you into refunding money to a fraudster who has

overpaid you with a bad cheque, stolen card and/or email money transfer such as Interac e-Transfer, or wire payment.

Example: A fraudster agrees to buy something from you and “accidentally” sends you a cheque for more than the agreed-on price. The fraudster then contacts you to request a reimbursement for the excess amount. However, what you don’t know is that the fraudster is using a fraudulent cheque to buy the phone. You deposit the cheque using your mobile banking app and see the money appear in your account. Then, you send the excess money back to the buyer by e-Transfer. When the cheque bounces a few days later, the money from the sale of the phone and the reimbursement will be gone.

Red flags to look out for:

- If someone pays you more than the price that you agreed on.
- If they immediately request reimbursement for part of the payment.
- If the transaction involves unusual shipping, processing or customs fees.

4. Business email compromise scams

Business email compromise scams involve a fraudster getting a hold of your funds or merchandise by sending an email that appears to come from a familiar source, making it seem like a legitimate request.

Example: A fraudster may send you an email that appears to come from your boss. The fraudster may have hacked into your boss’ email, or they may be spoofing the account by using an address that differs by one or two characters. The request may involve information the fraudster has obtained through in-depth research, social engineering or by installing malware. Either way, they will request you send money or merchandise to an account or location you’re not familiar with, usually with a sense of urgency. By the time you realize the mistake, the funds or merchandise may be long gone.

Red flags to look out for:

- If the request involves excessive urgency, persuasion, pressure or manipulation.
- If the request involves an address or a bank account you’ve never used before.
- If the address or bank account details don’t match your existing records.

How to avoid scams and protect yourself

- **Avoid giving out personal information.** Don’t give out any information you don’t need to, especially non-publicly available information such as social insurance numbers and account numbers.
- **Limit what you post on social media.** Scammers can target social media to discover personal information; this information can be used to manipulate a vulnerability.
- **Slow down.** Avoid any ‘urgent’ requests and be mindful of responding too quickly with personal or financial information.
- **Reviews emails and URLs carefully.** Emails and websites can look like they are from trusted companies, but if you review the email and URL carefully, you’ll notice a small difference like one extra letter, a period, or a .net instead of .com.
- **Say no to unsolicited calls or emails.** If you’re unfamiliar with the caller or sender, delete the message.
- **Be wary of anyone requesting gift cards, money orders, cheques or wires.** If anyone is requesting these types of payments, the likelihood of fraud may be higher.
- **Independently verify if the request seems out of ordinary.**
- **Sign up for alerts with your bank.** Text Alerts make it easy to keep track of your account activity and monitor for suspicious transactions.

- **Keep your contact information up to date.** Ensure your contact info is always current. That way, we can contact you immediately if they detect unusual activity on your account.
- **Choose passwords that are unique and complex.** Avoid common passwords like “1234561 2 3 4 5 6” or passwords that include obvious personal info. Your password should be at least 12 characters long and combine upper and lowercase letters and special characters (numbers and symbols). Use a favorite song or catch-phrase to help you remember it.

The bottom line

Scams are more common than you think, and anyone can be a target. However, taking proactive steps can help you avoid scams, protect yourself and your finances. Be mindful of sending personal or financial information and think twice if something feels off. Most importantly, though, if you think you’re being scammed or notice strange activity on your account, report it immediately.

Sources:

- *Ontario Securities Commission*
- *Canadian Bankers Association*
- *Alberta Securities Commission*
- *Government of Canada Anti-Fraud Centre*
- *Government of Canada Finance Department: Protection from frauds and scams*