

06 Watch out for — investment frauds and scams



According to Statistics Canada, reports of fraud have increased 64% over the past 10 years.

You've probably heard of friends or family falling victim to scams and frauds. This may even have happened to you. There are phone, text, email and internet scams. There are identity thefts, pyramid schemes, work-from-home scams, and many more. Being aware and cautious about them can help you stay safe.

Cyber fraud is any kind of scam that happens through one of your devices. This worksheet will help you spot cyber fraud about investing. It will guide you on what to do if you fall victim to a fraud or scam.

Cardinals are aware of threats to their nests. They make loud, metallic calls to warn off intruders. Like the cardinal, you need to be aware when it comes to scams and frauds. If you become a victim, report it right away.

These worksheets were inspired by Indigenous financial wellness expert and artist Simon Brascoupé, co-creator of our Managing Your Money booklet.

[Learn more about the inception of these resources and our commitment to reconciliation.](#)

Recognizing cyber fraud

Here are some of the common scams you may come across:

1. Investments that are too good to be true:

These fake investments offer high returns in a short amount of time and with low or no risk.

If you spot this:

Get a second opinion from a registered advisor or trusted member of your support network.

2. Pressure to buy immediately:

Scammers may try and rush you so that you don't think about all the risks before you invest.

If you spot this:

Pause. Do your own research, and check their registration.

3. Investors offering hot tips or insider information:

The tip is likely false, and you could lose your money. Even if it is true, it is illegal to act on insider information.

If you spot this:

Ignore the information.

4. Emails, attachments, and messages from senders you don't know:

These can be attempts to steal your personal information. Or, the messages could contain dangerous files that will access your information.

If you spot this:

Do not open unknown attachments or links. Do not download unknown apps. Never share your personal details with anyone you don't know and trust.

5. Unregistered advisors and businesses:

Your first step is always to check if an advisor or investment business is registered with the Canadian Securities Administrators at www.aretheyregistered.ca.

If you spot this:

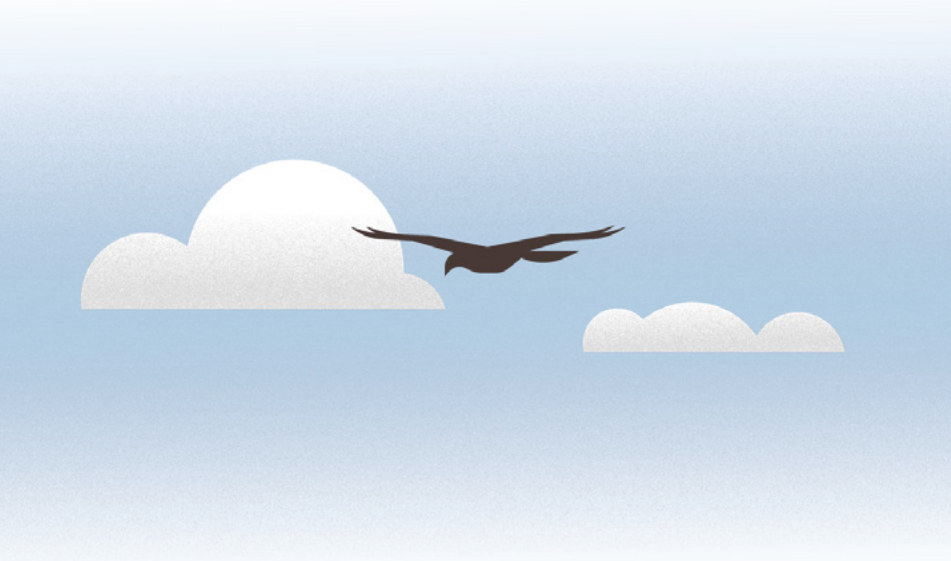
If they are not registered, do not invest with them. Report them to your provincial or territorial securities regulator. You can get the contact information on the Canadian Securities Administrators' website: securities-administrators.ca/. Look for **Contact Us** for contact information.

6. Requests to make immediate payments:

Never pay money to people before checking who they are.

If you spot this:

Take your time to check the information and their identity. Ignore requests for payment for things you did not buy.



What to do if you are a victim of fraud or a scam:

- Report it to the police right away.
- It is also recommended that you report it to the Canadian Anti-Fraud Centre: antifraudcentre-centreantifraude.ca and look for **Report Fraud**.
- Check your financial statements and credit card statements. Check your credit report. You can ask for one free credit report each year from Equifax Canada at consumer.equifax.ca/personal/. Look for **How to get a free credit report**. You can also request one free consumer disclosure from TransUnion Canada at transunion.ca. Look for **Consumer Disclosure**. You can find more information on how to apply and the information you would need by visiting their websites.

If you notice any transactions you did not make in your financial statements, credit card statements, and credit reports, report them right away.

