Protect yourself against fraud during COVID-19

Fraud has increased since the start of the COVID-19 pandemic and has caused many Canadians to lose money or have their identity stolen. Learn how to recognize fraud and scams, what precautions you can take, and what to do if you suspect you've fallen victim to fraud.

The information below is only a highlight of some of the common types of scams and fraudulent techniques used by fraudsters. Your best defense is to take precautions, stay alert and report any suspicious activity.

Common fraud techniques and how to protect yourself

Scammers and fraudsters try to trick you into sending money, revealing your personal information or accessing harmful websites or files. They often use scare tactics, such as telling you that you'll be in trouble or that you'll face fines or punishment if you do not do what they say. Others may try to sell you a product or service but require you to pay a fee up front.

Telephone fraud

Common warning signs

- The caller uses an automatic dialer to deliver a pre-recorded message.
- The caller speaks in a way that pressures or scares you into giving them information or money.
- The caller claims to be from the government, collection agency or police, telling you that you owe money or are under investigation for a crime.
- The caller claims to be from your financial institution or a government department needing to verify your personal or financial information.
- The caller claims to be from a loan or financial service company, health agency, or other reputable company or business, and tries to get you to make a payment up front for a product or service.
- The caller claims to be from a charitable organization and asks you to make a donation.
- The caller tells you that a family member or loved one is in trouble and in order to help, you need to provide money or banking information.

Protect yourself

- **Hang up immediately if you think the call may be a scam** or if you suspect the person is not who they say they are.
- **Hang up on suspicious callers and telemarketers who seem to be fishing for personal information.** They may ask for information such as:
  - Your name
  - Your address
  - Your birthdate
  - Your social insurance number (SIN)
  - Your credit card or banking information
- **Do not give personal information or account details over the phone** unless you have checked that who you are speaking with is legitimate:
  - Look online for the contact information of the company the caller claims to be from and call the company to confirm.
  - Verify any calls with your credit card company by calling the phone number on the back of your credit card.
  - Verify Canadian charities with the Canada Revenue Agency (CRA)
  - Verify collection agencies with the appropriate provincial agency.

Protect yourself against fraud during COVID-19

Fraud through email, text, instant messaging or mail

Common warning signs

- The email, text, message or letter claims to be sent from the government, your financial institution or a company, but looks different from other correspondence you've received in the past.
- The email address, website address, telephone number or mailing address is not exactly the same as your financial institution or the company that it claims to be.
- The email, text, message or letter is not addressed directly to you. For example, it may say "Dear Customer".
- You're asked to click on a link or respond and provide payment, personal information or financial information.
- The formatting or the graphics in the email, webpage or letter look slightly different or appear to be of lower quality. Some links may not work and there may be grammar and spelling errors.

Protect yourself

- **Verify the email address, website address, telephone number and mailing address to make sure that it is legitimate.** You can do this by checking the official website of the company or organization.
- **Check the sender's real email address** by hovering over the sender name or looking at the "from" address and see if their email domain matches the organization that they say they are from.
- **Don't use the telephone number, email, website or mailing address provided to you.** If you need to contact the company or agency, use the contact information you know to be correct.
- **Do not send sensitive personal information (such as your SIN) over the internet.**
- **Log directly into websites you choose to visit** instead of clicking on links through email or messages.
- **Install anti-spam, anti-spyware and anti-virus software** on your computer and/or mobile device(s) and make sure they are up to date.
- **Keep your systems** (such as Windows on your computer, or the operating system on your cell phone) **up to date.**
- **Create hard-to-guess passwords** and change them frequently. Do not reuse the same password for important accounts.
- **Do not choose security questions that can be answered using public information.**
- **If you are paying for something online, make sure the website you are using is secure.** Look for a padlock icon in the website address bar or check that the website address starts with "https" instead of "http" (the "s" means that it is secure).

Protect yourself against fraud during COVID-19

General tips

Be skeptical. Banks and government agencies do not send text or instant messages to ask for personal information or account details. Do not provide your personal information, click suspicious links, or reply to suspicious emails, messages or letters. Learn how to recognize a scam and what to expect when the CRA contacts you.

Verify who you are speaking to. Contact organizations and companies directly using their publicly listed information.

Check your statements regularly. Check your financial and credit card statements often and report any suspicious transactions to your bank or credit card company as soon as you notice them. You can also keep track of your tax and benefits information by registering for My Account on the CRA website.

Report fraud. If you are a victim of fraud, report the incident to your local police and keep any related evidence. The information may be used in an investigation.

If you wish to report any general fraudulent or suspicious activity, you can contact the Canadian Anti-Fraud Centre, through its website at www.antifraudcentre.ca, or by telephone at 1-888-495-8501.

Resources on COVID-19 fraud

For more information on various types of fraud and how to protect yourself, including information on government benefit scams and other scams during COVID-19, view the following resources below.

CERB and common scams during COVID-19 – Prosper Canada
Frauds and Scams Database – Financial and Consumer Services Commission (New Brunswick)
Fraud Prevention - Canadian Bankers Association
Identity 101 (information on identify theft) - Government of Canada
Protection from frauds and scams – Financial Consumer Agency of Canada (FCAC)
Protect yourself from scams and fraud – Canadian Anti-Fraud Centre
Slam the scam – Protect yourself against fraud – Canada Revenue Agency (CRA)