Reported Scams

Here is a snapshot of some of the *current reported* scams courtesy of the Canadian government's anti fraud centre and a variety of reliable news outlets.

Fraudsters are posing as:

Local and provincial electrical power companies

- threatening to disconnect your power for non-payment

Centers for Disease Control and Prevention or the World Health Organization

- offering fake lists for sale of COVID-19 infected people in your neighbourhood

Public Health Agency of Canada

- giving false results saying you have tested positive for COVID-19
- tricking you into confirming your health card and credit card numbers for a prescription
- Red Cross and other known charities
- offering free medical products (e.g. masks) for a donation

Government departments

- sending out coronavirus-themed phishing emails
- tricking you into opening malicious attachments
- tricking you to reveal sensitive personal and financial details

Financial advisors

- pressuring people to invest in hot new stocks related to the disease
- offering financial aid and/or loans to help you get through the shutdowns

Door-to-door salespeople

- selling household decontamination services

Private companies offering fast COVID-19 tests for sale

- only health care providers can perform the tests
- no other tests are genuine or guaranteed to provide accurate results at this time

Selling fraudulent products that claim to treat or prevent the disease

- Unapproved drugs threaten public health and violate federal laws

Cleaning or heating companies

- offering duct cleaning services or air filters to protect from COVID-19

What can you do to protect yourself?

Be Wary

- Trust your instincts. If it sounds too good to be true, it probably is.
- Do not give out login credentials for work or personal accounts over text, email or phone.
- Do not give out your health care information, financial information or other personal information over text, email or phone unless ***you*** initiated the interaction and only if absolutely necessary.

Online Safety Tips

- Be aware of your online presence. Do you post too much personal information on Social Media?
- Inspect links to websites to ensure that connections are secure. Look for the padlock symbol on the top left-hand corner of the URL.
- Better yet, don't click on any links. Try to find the website yourself and make sure the padlock symbol is there.
- Be smart with your passwords. Try not to use words, names, dates of birth, etc. that you post on social media. Ensure you change your passwords regularly and try not to use the same password for more than one site. Better yet, get a password management app so that you never need to think about passwords again.
- Keep your software updated. Often updates contain critical patches to ensure the ongoing security of your software. Always keep your antivirus software up to date.

Protect Yourself

- Be cautious about any communications *that invoke a sense of urgency* while asking you to change data or supply sensitive information.
- If you receive unsolicited emails, phone calls and text messages asking for personal or work information DO NOT give it up. You do not know who you are communicating with.
- Trust only legitimate sources such as official provincial or federal government websites to get information during the pandemic.