

Avoiding SCAMS and SPAMMING due to COVID-19

According to a TIME article written on March 19, 2020, “people are scrambling to find trustworthy information about the spread of the disease, how they can protect themselves, how they can get tested, and more” (*Austin, Patrick Lewis., TIME MAGAZINE., March 18, 2020.*)

Unfortunately, this has created an opportunity for spammers and scammers of the world to use the situation to take advantage of people, so we want you to be cautious of promotions, products and misinformation. **Some major scams going on are:**

“You can’t buy a COVID-19 cure” – while vaccine trials are underway, there are NO products that prevent or cure the novel coronavirus.

Beware products or promotions that are sent to you by text or email.

For example:

“Because of the COVID-19 outbreak, we are giving out free iPhone11 smartphones to help you spend time at home. Go to (LINK INSERTED HERE). This is likely a scam to get you to click on the link, and not a genuine message. In the case that you get this, ignore and delete the message, block it if you can, and verify with your current provider whether this is a true promotion or not. 99% of the time, it will NOT be.

Scam emails and texts may try to include elements like official imagery or email addresses that look like email addresses used by official businesses. It may even include information like your name or phone number to try to convince you they’re real.

To spot COVID-19 email, phone and/or text scams, look for:

- Generic greetings (Hello Sir/Madame)
- Requests of personal information
- Asking you to update your billing information
- A link to a website that doesn’t look quite right
- The message may seem urgent, trying to pressure you into giving information to avoid cutting off service

One of the other scams we’ve heard of and has been mentioned in news bulletins is that you are notified you have been tested “positive” for the COVID-19 virus. Someone calls you to say you’ve tested positive, and now must provide billing/credit card information. This is a scam. Hang up the phone right away.

Other helpful tips:

- If you don’t recognize the number, let your voicemail get it.
- Contact your service provider directly and ask them about it
- Do not respond to messages or emails. Report it as spam. Delete the message.

The Canadian Anti-Fraud Centre has updated its list of known COVID-19 scams, including:

- Representatives of cleaning or heating companies offering cleaning services for “special air ducts or filters” to protect from COVID-19
- Representatives of local and provincial hydroelectric companies threatening to disconnect power for non-payment
- Representatives of the U.S. Centers for Disease Control & Prevention or the WHO offering to sell fake lists of people with COVID-19 in different neighborhoods
- Representatives of the Public Health Agency of Canada giving false results saying people have tested positive for COVID-19, or tricking them into confirming their health card and credit card numbers for a prescription
- Representatives of the Red Cross and other well-known charities offering free medical supplies, such as masks, in exchange for a donation
- Representatives of government departments sending coronavirus phishing emails and tricking people into opening malicious attachments or revealing sensitive personal and financial details
- Financial advisers pressuring people to invest in hot new stocks related to the disease or offering financial aid or loans to help them get through the shutdowns
- Salespeople going door to door to offer in-house decontamination services
- Private company reps selling fast COVID-19 tests or fraudulent products that claim to treat or prevent the disease.
- Offering fake services or products that relate to COVID-19 or being at home (upgraded phone with a link, etc.)

For this and more helpful tips to avoid scams around COVID-19, visit the Canadian Anti-Fraud Centre’s site and latest bulletin, published March 18, 2020:

<https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm>