Trending COVID-19 Scams to Be Aware of

A pandemic makes a perfect breeding ground for frauds and scams that rely on fear and confusion to be successful. The risks multiply as people are physically isolated from friends, family and neighbours.

Vulnerable targets, such as elderly or naïve people, more often fall victim to campaigns that have the appearance of friendship or for a good cause. However, with education and awareness, the scammers success can be significantly reduced

Current Fraud Schemes

The following is a partial list of COVID-19 scams being run in Canada and the U.S.

- Duct cleaning companies offering "special filters" to clean the air of the Covid-19 virus and other household decontamination services.
- Callers pretending to be utility companies threatening to cut your power because you are behind in your bill payments. This is particularly confusing because some utilities are deferring payments in the crisis.
- Fake World Health Organisation (WHO) posts and emails or other apparently credible organisations, Centre for Disease Control (CDC), Alberta Health, that contain phishing links or other computer malware infections.
- Fake sites or emails requesting you to click to check on COVID-19 infection maps of your city or to see an updated list regarding your school.
- "Breaking news" and other fake information sites.
- Offers to sell you a list of names of your neighbours that are infected, or infected retail stores etc.
- Selling fake COVID-19 tests.
- Selling fake COVID-19 prevention drugs.
- Fake charity appeals, such as fake red cross masks for donation scam.
- Robocalls, with fake virus updates.
- Texts from fake "governments" requesting you to respond.
- Fake websites, soliciting money for a good cause, often using images of respected persons to lend credibility.
- Gift card scams, including emails with a gift card as a reward for working at home all you have to do is click on the link to activate it.
- Fake airline refunds.

Be Aware

Most of the scams ask for personal information such as health care number, social insurance number or credit card information. They may also ask for wire transfers or e-transfers of funds for charities. No reputable charity or government agency would ask for these.

To increase your security and reduce opportunities for criminals to defraud you, or your loved ones, follow this checklist of don'ts:

- DON'T click on links you don't know. (To check legitimacy, go directly to the website of the reputable organisation).
- DON'T give personal information over the phone
- DON'T press any numbers on you phone for more information when you get a robocall and make sure your phone is disconnected when you hang up (hear a dial tone on your land line).
- DON'T respond to texts from unfamiliar names, or ones saying they are from the government, an aid agency or department. Legitimate organizations and governments do not send texts asking for personal information, account numbers or funds.

MNP is here to help you navigate these uncertain times. For more information, contact Lisa Majeau Gordon, National Leader, Forensics and Litigation Support, at 780.453.5375 or lisa.majeaugordon@mnp.ca