



Lionsview Seniors Planning

COVID-19 Frauds Update

Sgt. Peri Mainwaring, Community Response Sergeant – District **February 16, 2021**





Types of Frauds

Fraudulent Phone Calls

Phishing Emails/Texts

Door to Door





COVID 19 Fraud & Scams

Fraudsters always try to profit from misinformation and during times of increased anxiety by targeting vulnerable people.

- Uncertainty and misinformation have been more prevalent than usual during the COVID-19 pandemic
- Increased isolation





Fraudulent Phone Calls

Scammer impersonating a government organization such as the CRA, Service Canada or a Public Health Agency

Caller demands urgent action: request for personal information and payment via gift cards or bitcoins

Royal Canadian Gendarmerie royale



Do not give your personal information to anyone and do not make payments to resolve threats





Phishing Email/Texts

Fraudster sends email/text with a request for action:

Text message or email that tricks you into opening a website link, that steals the information you provide or into opening a malicious attachment.

Example: The message has content related to COVID-19 vaccines and once you click on them it freezes your computer, makes you call a toll free number and they demand money to unfreeze your account

Do not click on suspicious links that you receive via text or email.





Request for Donations

Residents can receive request from unauthorized or fraudulent charities requesting money for victims, products, or research – this has been occurring in person, online and via phone calls

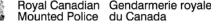
Example: Known charities offering free medical products (e.g. masks) for a donation.

Don't feel pressured into making decision, always verify that a charity is registered prior to making a donation.

***See tips at the end of this presentation.









Fraudsters posing as government agencies

- Offering fake lists for sale of COVID-19 infected people in your neighbourhood
- Giving false results saying you have been tested positive for COVID-19
- Tricking you into confirming your health card and credit card numbers for a prescription
- COVID 19 themed phishing email







—Fraudsters posing as private companies

- Phone call from someone claiming to work for a pharmaceutical company; offering a "6 shot vaccine system" which you receive by mail after paying large sums of money
- Cleaning or Heating companies
 - offering duct cleaning services or air filters to protect from COVID-19
 - selling household decontamination services





Fraudsters posing as private companies

- Offering assistance with filling out CERB applications for a fee
- Loan and financial service companies
 - offering loans, debt consolidation and other financial assistance services









COVID-19 Tests & Vaccine Scams

Private companies may contact you with an offer to sell fraudulent products that claim to treat or prevent COVID 19 or provide rapid COVID 19 tests

- Be aware that only hospitals, medical practioners or official testing centers can perform tests, provide treatment, etc.
- No other tests are genuine and there are currently no products that can prevent COVID19 other than the approved vaccines.





Trusted Resources

- Refer to <u>Government of Canada COVID-19</u> health, financial and security resources
- Refer to <u>Financial Consumer Agency of Canada COVID-19</u> information
- Reference the latest health information from these legitimate sources:
 - Coronavirus disease (COVID-19) (Public Health Agency of Canada)
 - Coronavirus disease (COVID-19) outbreak (World Health Organization)
- Contact your insurance provider to answer any health insurance questions





Trusted Resources

- Make sure you have anti-virus software installed and keep your operating system up to date
- Refer to the Government of Canada webpages on the <u>Canada</u> <u>Emergency Response Benefit</u>
- Report any unauthorized credit applications to the associated financial institution and the credit bureaus: Equifax and TransUnion







Controlled substance scam

- Feb 2021: The CAFC is receiving reports of an ongoing fraud in B.C. where citizens are receiving threatening letters that claim the letter contained a controlled substance and if payment is not made they face death.
- The public can continue to keep themselves safe by doing the following:
- Immediately put the letter, envelope and contents in a sealable bag, either a sandwich bag or freezer bag
- Sanitize the area where you opened the letter
- Wash your hands
- Call the police about the letter

Royal Canadian Gendarmerie royale Mounted Police du Canada



Extortion

- Ongoing extortion scams include:
- Bomb threat
- Denial of Service (DOS)
- Explicit video
- Hitman
- Hostage
- Hydro
- Immigration extortion
- Ransomware
- Sextortion











Other ongoing scams & related crime

- Online shopping
- Romance Scams
- Device security
- Mail and package theft







Reporting Fraud

To report a fraud or scam contact the Canadian Anti-Fraud Centre at 1-888-495-8501, or if you have lost money due to a fraud or scam, call North Vancouver RCMP at 604-985-1311.







Protecting yourself - phone scams

- Phone scams:
- How to protect yourself: If you receive a call from an unknown number, it is best not to answer it. If answered, do not provide, nor confirm personal or banking information over the phone unless you can validate that the caller is legitimate.

(be aware that fraudsters may be 'spoofing' a legitimate number – it may appear to be a government agency but the

INCOMING CALL

number is masked)







Protecting yourself – text scams

Text scams

- How to protect yourself: Should you receive a text message stating they are a charity, keep yourself safe and don't click on any link, and don't reply to the text message. Simply proceed to delete it immediately.
- *** follow up with steps to verify it is a legitimate charity



—Protecting yourself – door to door scams

Door to Door

- Example: Fraudster says they are doing home tests to detect COVID 19
- How to protect yourself: There are currently no such home detector tests available. Only hospitals can perform the tests and no other tests have been approved by public health.
- Do not answer the door to someone who is trying to sell you anything or pretends to be from the public health system.

Protecting yourselffake charities

Fake charities

 How to protect yourself: Verify publicly available information about the charity, including its name, address and telephone number. A legitimate charity will provide information about the charity's mission, how your donation will be used and proof that your contribution is tax deductible. You can also ask the charity for their registered charitable tax number and confirm the charity's registration information by calling

1-800-267-2384.

