Social Media Scams

Social media is a common way to keep in touch, especially during the COVID-19 pandemic. Social media has played a key role in keeping families and friends connected through these stressful times. Unfortunately, much like our family and friends, fraudsters also use social media. Social media scams have been around for a long time and fraudsters have now adapted their schemes to exploit the pandemic. Although there are many schemes on social media, some examples exploiting the pandemic are promotions touting COVID-19 prevention and cures, discounted products and services as well as charity donation schemes.

Common Social Media Scams:

You can protect yourself from fraudsters by recognizing the warning signs of their schemes, rejecting their attempts and reporting these suspicious activities to your local police and the Canadian Anti-Fraud Centre. Here are a few social media fraud examples that you might see during the pandemic:

Prevention and Cures: Essential Oil Scam – You may see a scam with misleading claims that essential oils will prevent or cure COVID-19. Remember that there is no proven treatment for COVID-19 according to health authorities. Be cautious of any investment schemes into these so-called cures. As always, consult with a trusted financial professional for investment guidance before you invest any money and do not try to buy a product advertised as a COVID-19 cure.

Data Trawling on Social Media – You may receive a catchy quiz in your social media feed that has a COVID-19 theme. An example might be “test your COVID-19 knowledge now”. The quiz will be strategically worded to trick you into providing your personal information like your mother’s maiden name, your pet’s name, your children’s name or your city of birth, for example. Fraudsters can then use the personal information you provided to try to access your online accounts. Never give out personal information on quizzes or to other unknown sources.

Payment for Non-existent Pandemic Products or Services – You may get an advertisement on social media offering COVID-19 themed products or services. Fraudsters will pressure you by creating urgency with a limited time offer deal. In some cases, COVID-19 testing kits have been advertised but the kits do not exist or the kits are not safe. Once the fraudster gets your money, the product may never be delivered or it may not be what you thought you were purchasing such as a COVID-19 test kit that does not work. Unsafe or fake COVID-19 test kits could put you, your family and others in your community at risk.

Catfishing and Impersonation of Officials – Fraudsters may impersonate trustworthy individuals in the community, like health care workers, government officials or even police. In catfishing scams, fraudsters will try to persuade you to donate your money to a worthwhile cause like COVID-19 vaccine or to pay a “fine” to avoid “charges”. These fraudsters may also try to obtain your personal information such as your Social Insurance Number. Do not send any money or provide any personal information.

Protect Yourself from Social Media Scams:

- **DO NOT** put your personal information on social media. Consider using a nickname instead of using your real name. Do not put your real birthday on your account.
- **DO NOT** partake in social media quizzes or online questionnaires that require personal information.
- **DO NOT** click on suspicious advertisements or promotional links, especially for COVID-19 cures. Do your research prior to buying any products and services. Read the reviews and see what others have to say.
- **DO NOT** purchase medication or drugs online from an untrusted source. Consult with your family physician.
- Only accept people you know as "friends" on social media platform.
- Review your social media account's privacy settings to ensure your personal information is protected.
- Donate to accredited or known charitable organizations through their official channels.

When to Contact the Police

If you are a victim of fraud in which you have incurred a financial loss and/or given out your personal information, call your local police to report the incident. Record details of your interaction with the fraudster including phone numbers, email addresses and communication with the fraudster. Photographs or screenshots of the messages are helpful. If you have **not** been a victim of a fraud but have information related to scams, please report this to the Canadian Anti-Fraud Centre through the website or email at info@antifraudcentre.ca.

Helpful Links

Canadian Anti-Fraud Centre - https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Consumer Protection BC - https://www.consumerprotectionbc.ca/2020/04/covid-19-protecting-yourself-from-scams-and-fraud/

Better Business Bureau - https://www.bbb.org/article/news-releases/16992-scam-alert-that-facebook-quiz-might-be-a-big-data-company-mining-your-personal-information

Better Business Bureau - https://www.bbb.org/article/tips/8767-bbb-tips-10-steps-to-avoid-scams

Government of Canada - https://www.canada.ca/en/public-safety-canada/campaigns/covid19.html

Government of Canada - https://www.canada.ca/en/health-canada/services/drugs-health-products/disinfectants/covid-19/list.html#tbl1