Yukon Information and Privacy Commissioner

211 Hawkins Street, Suite 201
Whitehorse, Yukon Y1A 1X3
T: 867.667.8468
F: 867.667.8469
1-800-661-0408 ext. 8468
www.ombudsman.yk.ca

Advisory on scams and misinformation regarding COVID-19

Issued May 11, 2020

During the COVID-19 pandemic, many people are understandably focused on concerns about health or the economy. However, the pandemic has also led to new and perhaps unexpected vulnerabilities which can put our personal information and our finances at risk.

In particular, texting, email, phone calls and social media are being used to mislead people and trick them into giving out personal or financial information, often by playing on fears and concerns about COVID-19. A number of recent media reports have discussed some of these issues. Please see the *Further Reading* section below for links to some of these media reports.

This advisory from the Yukon Information and Privacy Commissioner is meant to create additional awareness of these problems and provide advice about what to do.

What is happening

Cybercriminals have launched various campaigns to collect personal and financial information from Yukoners and others in order to commit theft (identity theft or theft of your money, or both).

Social media, email, text messages and robo-calls are being used to impersonate various government agencies (such as Revenue Canada), businesses, or non-government organizations (such as the World Health Organization or the Red Cross). The content of the messages varies. For example, they may:

- tell you that you have been in contact with someone infected with COVID-19;
- ask you to collect your Canada Emergency Response Benefit (CERB) cheque;
- ask for donations to non-profit organizations in order to support the fight against the pandemic;
- offer face masks or other personal protective equipment (PPE) for a cheap price;
- offer treatments or false/sensational information regarding COVID19.

There are and will continue be a variety of these and other messages using COVID-19 concerns to coax you into providing your personal information.

The messages often contain links leading to websites, which will usually ask you for personal information such as your name, phone number, banking information, social insurance number, etc. Giving out this kind of personal information may result in identity theft and/or fraudulent purchases made on your behalf. As well, messages may contain attachments or links to websites containing malware, which will infect your computer or other devices.

What individuals can do

It is very important to verify the authenticity and credibility of the source of any messages you receive and, if you are not able to do so, to disregard them, delete them, and not share them with anyone else.

Screenshots, photos, videos, links to unverified resources, or claims of expertise regarding COVID-19 can easily be forged by cybercriminals.

It is always a good idea to verify information via multiple reputable sources before acting on it.

Check with the organization in question to ask what types of communication channels it uses, what kinds of information it will (or will not) request via these channels, and ask for any verification methods it has provided. For more detail, see section below.

Official channels for information regarding the COVID-19 outbreak include:

https://www.who.int/
https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html
https://yukon.ca/en/coronavirus-updates

What organizations should do

Cybercriminals are especially adept at impersonating organizations through texting, email and social media. Once these criminals know how an organization sends out messages to the public, there are many techniques that they can use to profit from forging these communications.

Organizations, such as public bodies or custodians as set out in the *Access to Information and Protection of Privacy Act* (ATIPP Act) and *Health Information Privacy and Management Act* (HIPMA), often have legislated responsibilities to protect personal information and personal health information. They are encouraged to take actions to assist Yukoners in not falling victim to scams by implementing measures such as the ones set out below.

- Be sure to never ask that personal information be transmitted via text, email or social media. These platforms are typically insecure and do not protect privacy by design or default.
- Identify, preferably beforehand, the communication channels they plan to use or are already using.

- Provide details on what types of information they will, or will not, request via these communication channels. For example, some organizations include messages in emails and voicemails, as well as on their websites, stating that certain personal information (such as passwords) will never be requested and should never be provided over certain communication channels.
- Provide resources that give people instructions about how to verify communications that appear to be, or may actually be, from them. This gives citizens the ability to spot requests that appear out of the ordinary and understand how to verify their authenticity.
- These verification methods should be risk-assessed and relatively easy for the public to use. An example is to simultaneously post them on an official website.

Further reading

https://www.cbc.ca/news/politics/covid-scams-fraud-crime-1.5551294?cmp=rss

https://www.occrp.org/en/daily/12238-covid-phishing-scam-i-will-infect-your-family

https://www.cbc.ca/news/technology/phishing-messages-surge-coronavirus-1.5513315

https://www.bnnbloomberg.ca/a-list-of-known-scams-related-to-covid-19-canadian-anti-fraud-centre-1.1408896

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

The purpose of this document is to inform Yukoners about the risks to privacy associated with recent scams and misinformation regarding the COVID-19 pandemic and to support public bodies subject to the ATIPP Act and custodians subject to HIPMA in meeting their privacy and security obligations under these laws.

This document is not intended as, nor is it a substitute for, legal advice. This document is not binding on Yukon's Information and Privacy Commissioner.