ALERT
Beware of COVID-19 Scams

As COVID-19 continues to spread globally, watch out for associated scams. The purpose of this bulletin is to advise credit unions of the COVID-19 related frauds that have emerged and affected Canadians.

Beware of scams related to COVID-19

Cybercriminals have been using the uncertainty of the COVID-19 pandemic to launch phishing attacks and various other scams. As the public continues to seek out information on the disease, cybercriminals will increasingly try to exploit public fears with targeted attacks. The risk solutions group encourages our credit union partners to remind their employees and members to remain vigilant.

Type of Scams

False Information Emails

The fraudsters have been sending emails claiming to be from legitimate organizations, government or public health agencies (e.g. World Health Organization, Public Health Agency of Canada) to provide information about the coronavirus. The email message will advise the receiver to click a link or download an attachment for the information, but the user will likely download malware onto their computer network or device. As with other cyber-attacks, this malware could allow cybercriminals to take control of a device, log keystrokes, or access personal information and financial data.

Medical Advice Emails

Phishers have sent emails that offer bogus medical advice to help protect you against the coronavirus or cure you of it. Users will be provided with a malicious link to download expert information that can heal them or a link to purchase a fraudulent product (e.g. at-home COVID-19 test).

Corporate Policy Emails

Cybercriminals have also targeted employee workplace email accounts. With many workers currently working from home, some corporate cybersecurity measures may not be available, and the criminals are trying to take advantage. Employees may receive emails purporting to be from HR, advising users to click on a link to read the company's updated Infectious Disease Policy. If you click on the fake company policy, you'll download malicious software.

Business Email Compromise

According to a recent report, a cybercrime group well known for BEC schemes in the past, have incorporated COVID-19 into their scams. The group will imitate a company's CFO and then contact someone in the accounts receivable department to request a list of delinquent clients and up-to-date contact information for each client. Once received, they quickly contact these clients and inform them that they have changed their banking information due to COVID-19 and request payment.

Malicious Websites

There have been many fraudulent COVID-19 themed websites launched since the pandemic emerged and recent research has estimated that 50% of the coronavirus themed domain registrations are likely from malicious actors. Many of these sites have leveraged John Hopkins University's interactive map that shows you how COVID-19 is spreading throughout the world. The fraudulent websites are using real-time data from the John Hopkins site, but are also prompting users to download a malicious application.

Other COVID-19 Related Scams

The RCMP recently released a report that listed various other COVID-19 related scams to be aware of, including:

- Unsolicited calls, emails and texts giving medical advice or requesting urgent action or payment.
- Unauthorized or fraudulent charities requesting money for victims, products or research.
- Door-to-door salespeople selling household decontamination services.
- Private companies offering fast COVID-19 tests for sale

See full report here - https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm

Mitigation Measures

- Only use trusted sources for information related to COVID-19. Go directly to their site.
  - World Health Organization – https://www.who.int/emergencies/diseases/novel-coronavirus-2019
  - Public Health Agency - https://www.canada.ca/en/public-health.htm
- Review our previous bulletin on Common Cyber Threats