Beware of COVID-19 Scams!

As the COVID-19 pandemic continues to evolve, watch out for associated scams. Cybercriminals have been using COVID-19 uncertainty to launch phishing and other attacks, exploiting public fears with targeted attacks. **Review some of the types of scams below.**

False Information Emails

- Fraudsters are sending emails claiming to be from legitimate organizations such as government or public health agencies to provide information about COVID-19.
- The message will advise the receiver to click a link or download an attachment, but the user will download malware onto their computer network or device that could allow cybercriminals to take control, log keystrokes, or access personal information and financial data.

Medical Advice Emails

- Phishers are sending emails that offer bogus medical advice to help protect against or cure COVID-19.
- 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 are targeting business email accounts. With many workers currently working from home, some corporate cybersecurity measures may not be available and criminals are trying to take advantage.
- Employees receive emails purporting to be from Human Resources, advising users to click on a link to read the company's updated Infectious Disease Policy, but clicking downloads malicious software.

Business Email Compromise

- Scammers are imitating a company's Chief Financial Officer and contacting someone in the accounts receivable department to request a list of delinquent clients and up-to-date contact information for each.
- Once the information is received, the criminals quickly contact the clients, inform them they have changed their banking information due to COVID-19 and request payment.

Malicious Websites

- Many fraudulent COVID-19 themed websites have launched since the pandemic emerged.
- Many of these sites leverage John Hopkins University's interactive map that shows you how COVID-19 is spreading throughout the world, with the fraudulent websites using real-time data but also prompting users to download a malicious application.

Other 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.

For more information, visit the Canadian Anti-Fraud Centre website at:
https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Source: CUMIS Risk Solutions Group

alberta central