COVID-19: The Rise in Cyber Fraud

APRIL 2020

FULLER LANDAU LLP

The Canadian Anti-Fraud Centre (CAFC) issued a bulletin on March 18, 2020, alerting the public to fraudsters exploiting COVID-19 to facilitate fraud and cyber crime.[1] This comes in the form of fraudulent emails sent to unsuspecting Canadians who are being inundated with information about COVID-19. It is important for your company's employees to be cautious when clicking on links that appear to provide information on the virus and/or request donations to an online charity.

Here are some cyber threats your company may face from fraudsters:

Identity Theft

There are several types of identity theft. When personal information is compromised, it can be a catalyst for engaging in credit card fraud. For example, once credit card information is accessed, the fraudster may call the credit card company to change the billing address. The fraudster can then put through charges that may not even be noticed for some time.

On a more complex level, the fraudster may use the personal information obtained in a sequence of events that results in identity theft and harm to the victim's good name. For example, the fraudster can use the personal information to apply for loans, credit lines or mortgages or commit other types of fraud such as applying for a driver's license. These activities can have a lasting impact on the victim's credit score and reputation and be time consuming to reverse.

Phishing Emails

Phishing emails, where a hacker poses as a valid source, fool employees into believing they are legitimate emails. For instance, your employee receives an email supposedly from PayPal indicating that their account has expired, and their personal information is required to reactivate the account. Once the employee enters their information, the hacker will then obtain the employee's credit card and password details.

[1] *Source: https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm*

BE AWARE THAT CRA WILL NEVER SEND AN EMAIL REQUESTING PERSONAL INFORMATION.

Warn your employees of the following types of phishing emails during the pandemic:

- Emails purportedly from the Red Cross or other charitable organizations offering free medical products (e.g. masks) in return for a charitable donation;
- Emails asking to verify your personal information in order to receive Canadian government subsidies;
- Emails urging readers to open a link for information containing an update of new cases of infection around their city;
- Emails seemingly from the Public Health Agency of Canada saying you have tested positive for the COVID-19 virus;
- Offers of fake cures and vaccines; and
- Loan and financial service companies offering loans and debt consolidation services.

A link in a phishing email can open to a website purporting to be the sign-in page for Microsoft Outlook. The page looks very similar to the legitimate Microsoft Outlook interface that asks for your password. The fraudsters use the entered password to access all your employees' emails to search for personal information. Other variations of this scheme may suggest the user download a file or program to access information. Fraudsters could also infect your employees' computer with malware and lock it until they receive a ransom payment.

Phishing Schemes and Canada Revenue Agency (CRA)

It is important to be aware of CRA phishing tax schemes, where the fraudster sends an email purporting to request information from CRA, which of course, is phishing for personal information.

Be aware that CRA will never send an email requesting personal information. The CRA only sends information requests by mail.

According to the CRA website[2]:

The CRA may:

- notify you by email when a new message or a document, such as a notice of assessment or reassessment, is available for you to view in secure CRA portals such as My Account, My Business Account, or Represent a Client
- email you a link to a CRA webpage, form, or publication that you ask for during a telephone call or a meeting with an agent (this is the only case when the CRA will send email containing links)

The CRA will never:

- give or ask for personal or financial information by email and ask you to click on a link
- email you a link asking you to fill in an online form with personal or financial details
- send you an email with a link to your refund
- demand immediate payment by Interac e-transfer, bitcoin, prepaid credit cards or gift cards from retailers such as iTunes, Amazon or others
- threaten you with arrest or prison sentence

[2] *Source: https://www.canada.ca/en/revenue-agency/news/newsroom/tax-tips/tax-tips-2018/what-to-expect-cra-contacts-you.html*

WARN YOUR EMPLOYEES OF THE TYPES OF PHISHING EMAILS DURING THE PANDEMIC.

What Your Employees Can Do

Here are some simple tips to reduce the risk of becoming victimized by a fraudster:

- Do not open attachments or click links within emails from senders you do not recognize.
- Ensure that the sender is a legitimate domain name and has no spelling errors.
- Hover over links within emails to ensure that the link address matches the one in the email.
- Check for spelling errors or incorrect domain names within a link.
- Do not provide your username, password, and other personal data in response to an email.

Should you require assistance or want to learn more, please reach out to your advisor or the forensic accounting team at Fuller Landau.

COVID-19 RESOURCES HUB

Visit our COVID-19 Resources hub for the latest information on Canadian and US government programs as well as helpful resources for business owners, including free webinars.

fullerllp.com/covid-19-resources/

ABOUT THE AUTHOR

Bruce Roher, CPA, CA, CBV, CFE, CFF is a Partner and leader of our Forensic Accounting and Valuations team.
He can be reached at 416-645-6526 or broher@fullerllp.com.