PEOPLE RESOURCES

# How to spot phishing scams arising from COVID-19

Source: Canadian Bankers Association

Scammers are taking advantage of the novel coronavirus disease (COVID-19) pandemic by sending fraudulent emails that attempt to trick you into revealing your personal information or clicking on malicious links or attachments.

The emails may look authentic and may include logos or branding for the World Health Organization or other government or public health agencies. In a variation of the scam, fraudsters are calling Canadians with requests for donations or offering fraudulent laboratory testing.

**How to spot a scam**

Email scams are attempts to have you volunteer your personal information to criminals, including your credit card information, or to install malware on your computer or mobile device. There are simple steps you can take to avoid becoming a victim:

- **Be skeptical.** Fraudulent e-mails can look like they come from a real organization. If you have any doubts about an e-mail purporting to contain health information or requesting donations for Canadians affected by COVID-19, don't use the toll-free number, e-mail address or website address provided because they may link you to the fraudsters. Instead, use a phone number, e-mail address or website address that you know is correct. Up-to-date information about COVID-19 can be found on the Public Health Agency of Canada website or on your provincial health agency website.
- **Be vigilant.** Never send personal and/or financial information by e-mail.
- **Check the "from" address.** If you hover your curser over the name, you will see the actual electronic email address. Some phishing attempts use a sender email address that looks legitimate but isn't – a red flag is when email domain doesn't match the organization that the sender says they are from.
- **Never click on suspicious links or attachments.** Phishing emails often include embedded links that look valid, but if you hover over them, you can usually see the real hyperlink. If the hyperlinked address isn't the same as what appears in the email, it's probably a phishing attempt. Does the email include an attachment that you weren't expecting? Never open suspicious attachments.
- **Protect your devices.** As always, make sure that your home computer is protected. Install anti-spam, anti-spyware and anti-virus software and make sure they are always up to date.

If you receive a phishing email, there are two things you should do: report it and delete it. Reporting a fraudulent email to the organization being spoofed can help prevent other people from being victimized. To report a fraudulent email, be sure to send the email as an attachment.

The Canadian Anti-Fraud Centre has compiled a list of the reported scams exploiting COVID-19.

PEOPLE RESOURCES

The government of Canada has information for Canadians about COVID-19, including a toll-free phone number and email address here: https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection.html

Please speak with your HR Partner about taking Black & McDonald's Information Security eCourse on Litmos. The course is intended to familiarize you with the principles of cybersecurity, and the precautions necessary to protect information, company resources and people against unauthorized access or attacks. Every employee has a role to play in protecting the information of our company, as well as protecting company data. This course will take approximately 20 minutes to complete.