MAY 2020

IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

INVESTOR BULLETIN

COVID-19 and Cybersecurity – Tips for Investors

Protect Yourself

STAY AWARE AND VIGILANT

Investors should be aware of the increased risk of cybersecurity attacks related to the COVID-19 pandemic. Cyber criminals are focusing now on individuals particularly people who are working remotely.
Here are some tips for individuals on how to prevent and respond to a cyber-attack even when working from home:

Common Attacks

PHISHING

Phishing and malicious links continue to be the most prevalent cybersecurity threats that reference COVID-19 received over email and text message.

>>> Watch out for suspicious/fake emails from individuals requesting banking information to deposit pandemic-related funds.

>>> Watch out for suspicious/fake emails or text messages from hospitals/governments/health organizations asking you to click on a link or call a number to obtain more information on the pandemic or treatment options.

Quick Tips:

- Be extra vigilant when communicating with others, even if you believe them to be a trusted source.
- Hover over any links to confirm the link is legitimate before clicking it.
- If you are not sure whether the email or text message you received is authentic, do not click on the link in the message or call the number that sent you a text or voice message. Instead, look up the contact information on the organization's official website using a well-known search engine.

Common Attacks

SOCIAL ENGINEERING

Social engineering is when a malicious actor attempts to deceive a user into sharing sensitive information or transferring funds by presenting themselves as someone else.

>>> Watch out for suspicious/fake emails from individuals requesting banking information to deposit pandemic-related funds or asking you to click on a link or call a number to obtain more information on the pandemic or treatment options.

Protect Your Home Office

COMPUTERS AND MOBILE DEVICES

- Lock your screen or log out if you plan to be away from your computer.
- DO NOT approve any prompt for authentication you have not initiated.
- DO NOT plug in any non-approved USB storage device from an unknown source or that you are not expecting.
- Remember to check for and apply updates and patches to your operating system and any applications that require them on a timely basis.
- Install and operate anti-virus and anti-malware software.
- DO NOT download, save or screenshot any personal or sensitive information onto your computer or mobile device.
- If other individuals in your household are using the same device, ensure that you are logged out securely from all accounts before handing over the device to someone else.

Quick Tip

- Continue to follow strict document handling procedures (paper and digital documents) and communication as if you were at work.