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

IIROC NOTICE

Education Notice

Please distribute internally to:
Corporate Finance
Credit
Institutional
Internal Audit
Legal and Compliance
Operations
Registration
Regulatory Accounting
Research
Retail
Senior Management
Trading Desk
Training

Contact:
Suzanne Lasrado
Senior Manager, Financial & Operations Compliance
416-943-5880
slasrado@iiroc.ca

Ryan Li
Director, Information Security
416-943-5890
rli@iiroc.ca

IIROC Notice 20-0083
April 21, 2020

COVID-19 and Cybersecurity – Tips for Advisors and Employees

On March 30, we issued a notice to IIROC Dealer Members alerting them to 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.

Advisors and employees are the first line of defense against successful attacks and must stay aware and vigilant at all times to protect clients, the firm and themselves.

This Notice outlines some tips for individuals on how to prevent and respond to a cyber-attack even when working from home.

Reminder of Common Attacks

- **Phishing** and malicious links continue to be the most prevalent cybersecurity threat that reference COVID-19 received over email and text message. Many cybersecurity providers are seeing a large increase in such attempts across all of the clients they serve and we would like to reiterate the vigilance required of each person to counter such threats:
    - What to do?
        - Hover (i.e., move your mouse over but do not click) over any links to confirm the link is legitimate before clicking it. Be wary of any links that try to convince you to click on a web link or open an attachment
        - If you click on a suspicious link or download or click on an attachment, notify your IT or Information Security team immediately and unplug your network cable/disable your Wi-Fi connection (do not shut down your computer)
    - In general, if you are unsure about the validity of any messages received, please check with your IT or Information Security team.

Phishing examples during COVID-19 pandemic

1. Suspicious/fake emails or text messages from individuals purporting to act for a government organization requesting banking information to deposit pandemic-related funds and assistance.

2. 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 tip:

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.

- **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

(e.g., help desk agent, health official, financial institution, trusted employee, etc.). It is one of the most predominant attacks leveraging changing current events and can involve email, phone calls, text messages, etc. Please be extra vigilant when communicating with others, even if you believe them to be a trusted source.

- What to do?
  - Ask yourself the following questions and your IT or Information Security team if you feel at all concerned:
    - Was this request initiated by you?
    - Is this request a common business practice?
    - Was the request or communication made through the proper channels?
    - Does the communication feel suspicious in any way (e.g., typos, poor grammar, irregular formatting, wrong look and feel, threatening, cryptic, etc.)?
- If you suspect that you have provided information, funds or access to a malicious actor please immediately inform your IT or Information Security team.

Social engineering examples during COVID-19 pandemic

1. Phone calls from fake "help desk" agents requesting credentials over the phone, inquiring about home network set up, or asking for other personal information.

2. Fake health notifications from hospitals/regional governments/health organisations claiming that you or someone from your office has been exposed to the virus and require testing.

Quick tip:

Make sure that you understand and verify with your firm:

- how and who from your firm will communicate with you during this time
- how the business continuity plan changes normal job functions that impact you (including changes to approval processes, if any)
- the contact information for your IT support team.

Computers and Mobile Devices

- General computer and mobile device guidance
  - 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
- Personal/home computers and mobile devices
    - Remember to check for and apply updates and patches to the your operating system and any applications that require them on a timely basis
    - Install and operate anti-virus (AV) and anti-malware software
    - DO NOT download, save or screenshot any personal or sensitive information onto the computer or mobile device
    - If other individuals in your household are using the same device, ensure that you are logged out securely from your account and all firm-related portals and systems before handing over the device to someone else
- Firm-issued computers and mobile devices
    - Familiarize yourself with your firm's policies on whether, and under what conditions, other individuals in your household are permitted to use firm-issued devices
    - Ensure you are regularly receiving software and operating system updates from your firm's IT support team
    - Update mobile device operating system and applications when needed

Home Office Networks

- Use a secure network connection to access your firm's work environment (e.g., VPN, remote access, cloud service web client, etc.)
- If you are using Wi-Fi at home,
    - ensure that the Wi-Fi is using a stringent security protocol (e.g., WPA2) and a strong Wi-Fi password
    - DO NOT use public Wi-Fi or insecure/open connections to access your firm's work environment, client and personal information or records.
- Check for and apply software updates and patches to your home router on a timely basis
- Change the default user names and passwords on home networking equipment (e.g., routers, switches, hubs, etc.)

Document Handling and Communication

- Continue to follow strict document handling procedures (paper and digital documents) and communication as if you were in the office
- DO NOT save documents to non-firm-provided online services or local hard drives
- Adhere as much as possible to a clean desk policy to ensure important documents are not left out or lost
- Communicate through the proper channels for all work related activities (e.g., Email, firm provided instant messenger, etc.)

- Ensure that video-conferencing, web-conferencing and other communication applications being used are secure and accessed through secure means.

Incident Response

- Understand your role in your firm's incident response plan and whom to contact in the event of a cybersecurity incident (e.g., data breach, loss or exposure of customer information, successful email attack, clicking on malicious links, ransomware, lost or stolen mobile device)

Other Resources

Further information and resources on managing cybersecurity threats, including a webinar on Cybersecurity Tips for Advisors, are available on IIROC's cybersecurity site