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 20-0061
March 30, 2020

COVID-19 and Cybersecurity

This Notice provides information to IIROC Dealer Members on cybersecurity threats arising from the COVID-19 pandemic, and includes some tips to help firms and its employees protect clients' information and itself.

With the COVID-19 pandemic, there is new and changing information available every day. It is natural to want to search for news on websites, open external emails that provide updates on the topic and share these with colleagues and friends.

Unfortunately, with any crisis comes bad actors who will try to exploit the crisis. COVID-19 is no exception. For example, the World Health Organization (WHO) recently published an alert warning of scams and malicious emails claiming to contain information on how to protect yourself from the disease.

Vigilance for Phishing/Malware Attacks

All text messages, emails, attachments, links and websites with coronavirus-themes should be treated with caution as they could contain malware or be part of a phishing attack designed to gain access to your network, personal information and assets.

Please continue to demonstrate care when accessing links or attachments in emails – even if the email is from a known sender. The following are general tips to take when receiving emails:

1) Hover (i.e., move your mouse over but do not click) over any links to confirm the link is legitimate before clicking it.

2) If you click on a suspicious link or access (i.e. download or click on) an attachment, notify your IT service provider and disconnect your internet connection immediately (do not shut down your computer).

3) In general, if you are unsure about the validity of any emails received, please check with your IT service provider.

Again, we urge you to be cautious when viewing such emails, especially those that you are not expecting that are

- requesting you to click on a link or download/open/click an attachment
- asking you to provide personal, login or banking information.

Computers/Mobile Phones

If you are working from home, please keep your laptops, phones and other mobile devices (and access to them) safe and secure. Avoid using unsanctioned or unauthorized devices or accessing unsecure websites or wireless connections.

Your IT service provider should also ensure that your computer will continue to receive critical software security patches while you are working at home.

Please contact your cybersecurity teams or IT service provider with questions.

Account Intrusions

We have noted an increase in potential client account intrusions and encourage Dealer Members to remain vigilant. Dealer Members should ensure that controls or processes put in place to prevent or detect possible account intrusions are operational and working as expected. Such tools may include:

- real-time alerts and post-trade compliance reviews to detect abnormal deviations from a client's normal trading patterns;
- two-factor authentication;
- free downloads of software for clients to install on their computers to provide extra protection;
- procedures for remedial steps to be taken once an account has been identified as compromised, including controls such as suspending accounts and requiring clients to set new passwords or create new accounts;
- blocking access or requiring further authentication if an unrecognized IP address is used; and
- monitoring lists of known fraudulent IP addresses and blocking access by such addresses to the Dealer Member's systems.

As a reminder, IIROC expects any Dealer Member that has experienced problems with account intrusions to advise IIROC of the activity. This is important for IIROC to assess any potential harm to clients and/or market integrity.

Other Resources

Further information and resources on managing cybersecurity threats, including guides and webinars, are available on IIROC's cybersecurity site.