MFDA™ Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

Contact: Brett Konyu
Director, Member Education and Membership Services
Phone: 416-943-4609
E-mail: bkonyu@mfda.ca

BULLETIN #0816 –M
March 19, 2020

MFDA Bulletin

Membership Information

For Distribution to Relevant Parties within your Firm

Cybercriminals Currently Exploiting the COVID-19 Pandemic

As Members increasingly rely on technology to facilitate work from home arrangements and remotely service clients, there is an increased risk of cybersecurity events. The confusion and evolving circumstances surrounding COVID-19 has created an environment ripe for exploitation by cybercriminals. Cybercriminals are indeed already attempting to exploit this environment and the number of cybersecurity threats is increasing.

The Threats

Members have reported an increase in phishing attempts, including attempts that use the names of the MFDA and other regulators or government agencies.

NPC Dataguard, a security service firm that is working with the MFDA on Member cybersecurity assessments, has issued security alerts regarding exploitation of the COVID-19 pandemic, including *Cybercriminals Exploiting the Current Coronavirus Outbreak with Malicious Health Advisory Email*. This alert states that the cybersecurity community is seeing an increased number of cyberattacks exploiting the COVID-19 outbreak at a time when people around the world are looking for answers and information to protect themselves. Malicious emails promoting maps on the spread of the virus, fake vaccinations for sale, and prophylactic gear have been identified. Some details include:

- A phishing email campaign disguised as a public service announcement from the World Health Organization (WHO) about COVID-19. When the email button is clicked it brings the target victim to a fake landing page that looks like the real WHO page, with a malicious login designed to collect your email password.

- More than 4,000 website domains related to this outbreak have been registered since January 1, 2020. 3% to 5% of those sites are confirmed or suspected to be malicious.

- The distribution of malicious software trojans have also been reported on COVID-19 related emails. These are designed to deliver various forms of ransomware and other malicious tools to achieve data theft, extortion or operational disruption.

Considerations for Members

It is imperative that Members continue to protect themselves against cybersecurity threats and consider the unique threats that the current environment has created.

- The NPC Bulletin outlines some steps Members and their Approved Persons can undertake to protect from, and respond to, a cyberattack including those attempting to exploit the COVID-19 pandemic:

  - **Be aware of the threat**
    - Do not open any email attachments you are not expecting, do not click on unknown ads or links in emails or on websites that you are unfamiliar with, especially on a topical issue such as this current novel coronavirus related to protective gear such as masks, cures, or spread information.
    - Be immediately wary when you are asked to give passwords or any information for any reason, other than the known and trusted site they are intended for.
    - If you receive an email that appears to be from a known or trusted site, do not login by clicking on the email link, but separately access the site by opening a web browser and using a known site address.

  - **Protect your computer**
    - Ensure you have a fully patched computer, operating system, office suite, web browser, utility apps like Adobe and Java, and a powerful and up-to-date anti-malware suite.
    - If it appears you have been attacked by ransomware disconnect your system from your network and the Internet, and contact an IT professional immediately for guidance in recovering your files.

  - **Know how to spot fake email and landing pages**
    - Note any spelling and grammatical errors.
    - Watch for button links to non-secure sites (HTTP).
    - Observe and separately confirm if a link goes to the real site you are intending to go to.
    - Suspect pop-ups asking to verify your email, password or other information the site should already know.

- **Go only to known and verifiable sources of information**
    - Reliable sources of information for the spread and protection from COVID-19 include:
        - Government of Canada Public Health Services
        - World Health Organization (WHO)
- The Canadian government's Centre for Cyber Security and the RCMP are aware of these attacks and are asking victims to report any successful attacks.
- You can click here to learn more and sign up for ongoing cybersecurity alerts from NPC.

DOCs#731198