LAW ALERT

March 30, 2020

By: Leora F. Ardizzone, Esq.

RMF
RUSKIN MOSCOU FALTISCHEK P.C.
Smart Counsel. Straight Talk.

Practicing Good Cyber-Hygiene

Cyber scammers are ever alert to crises and COVID-19 is no exception. People who perceive a crisis are more vulnerable to being duped and taken advantage of and companies must be aware of the risks and remind all employees to practice good cyber-hygiene:

Home computers: With people working from home, it is vital that people secure their home computers to avoid scammers seeking to infiltrate their home systems with things like key logging software and other malware. It is important that home users maintain up to date anti-virus software, update their operating systems so that the most current patches are in place. In addition, home users, should be careful about all the things listed below so that they do not unwittingly download malware into their home computers that can be transmitted or exploited for nefarious purposes.

Fake emails: Fraudsters are out in full force, masking their identity with fake credentials pretending to be CDC, WHO or other organizations claiming to have vital health information about the virus and avoiding infection. Criminals will use the vulnerabilities in your network to upload malicious software that can steal data or crypto lock vital data. Make sure to remind all employees not to open emails from unknown sources. People seeking information about the virus, testing and treatment should go to legitimate sources including the CDC, WHO, FDA, and their local health department.

Phishing Emails: With the stimulus package poised to be signed by the President, there is an increased risk of phishing emails that scammers will use to obtain personal and/or corporate information under the guise of providing economic stimulus checks from the government. In addition to the government loans and grants that may become available with the stimulus package, phishing emails can also seek money for fake charities, fake cures, fake testing kits, etc.

Fake Testing, Treatments, Supplies, etc: In addition to the risks of phishing scams, the FBI warns of fraudsters claiming to offer coronavirus testing and treatments which are only available from health care providers. Additionally, scammers are claiming to sell equipment and supplies, such as personal protection equipment, that are counterfeit or will never actually be delivered despite payments being made. www.cdc.gov and www.fda.gov provides information about legitimate supplies and equipment.

The FBI’s list of cyber-hygiene practices include the following:

• "Do not open attachments or click links within emails from senders you don't recognize."

• "Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall."

• "Always verify the web address of legitimate websites and manually type them into your browser."

• "Check for misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in .com" instead)."

• "If you believe you are the victim of an Internet scam or cyber crime, or if you want to report suspicious activity, please visit the FBI’s Internet Crime Complaint Center at www.ic3.gov."

If you believe you have been the victim of a cyber-attack or other data breach, Ruskin Moscou Faltischek is here for you and ready to help. Please contact

Steven J. Kuperschmid
skuperschmid@rmfpc.com
(516) 663-6686

Leora F. Ardizzone
lardizzone@rmfpc.com
(516) 663-6538