Connecticut Bar Association

Guidance on Cyber Threats Associated with COVID-19

What is the Threat?

Many companies are experiencing malicious cyber attacks leveraging the Coronavirus outbreak. Most commonly, cyber criminals are distributing COVID-19 themed phishing emails, (a) requesting login or other personal information either directly in the email or when the recipient clicks on a hyperlink and is redirected to a website, (b) attaching unsolicited documents that when opened download malware onto the user's systems, or (c) soliciting donations on false pretenses. In many instances, these emails appear to be from trusted sources, such as government agencies, news outlets, or non-profits like the World Health Organization (WHO), the United Nations (UN), and the Center for Disease Control (CDC).

What can I do to protect myself and my company?

Five big takeaways:

--Treat as suspect ANY LINK that purports to be about how far COVID-19 has spread or how best to avoid or contain it. Only click on that link if you have first confirmed that it is sited at the domain of a bona fide university, research institution, non-profit, government agency, or media outlet. If you cannot confirm the domain's authenticity, do not click on the link. Similarly, check to confirm that any email or notification is from a recognized address for the organization. For example, emails from the World health Organization (WHO) will have an email address such as 'person@who.int' If there is anything other than 'who.int' after the '@' symbol, this sender is not from WHO. WHO does not send email from addresses ending in '@who.com' , '@who.org' or '@who-safety.org'.

--Be even more suspicious of emails that claim to include an attachment containing the same kind of "helpful" information. If the email is a forward by anyone or uses language different than you know the sender typically uses, or is not from someone you know well, do not download the attachment.

--If you are unexpectedly presented with a screen purporting that you have been logged off and now have to log back in, do not follow this prompt. Even if the login screen looks like one from your email or other software provider. Especially if you have recently clicked on or downloaded something related to the pandemic. Instead, save any open work, log off the network as you normally would, and then log back in the usual way.

--If you have not established multi-factor authentication for your email, there is no time like the present!

--If you have been putting off updating your operating systems, again, do so now!

A good source of additional information is the Federal Trade Commission's page on Charity Scams. https://www.consumer.ftc.gov/taxonomy/term/850

What can I do if I am victimized?

If you are victimized, please contact the FBI at www.IC3.gov. Of particular note, if money is stolen from you in one of these scams and you report it to your bank and IC3 within 48 hours of the event, there is a significant chance that your money will be returned.

Prepared by the Connecticut Bar Association's Cyber Security and Technology Committee