Cybercriminals are Taking Advantage of COVID-19: Tips to Reduce Risk

By Melissa K. Ventrone, Jeffrey R. Wells / Mar 13, 2020

With COVID-19 now a global pandemic, numerous scams, phishing campaigns, and malicious websites are proliferating. COVID-19's impact is quickly shifting how businesses operate. Many employees are now working remotely in distributed operations. This increase in remote work arrangements, both temporarily and permanently, is creating significant growth in network access and traffic which provides more opportunities for threat actors to strike. Historically, cybercriminals leverage attacks during holidays, weekends and other busy and stressful times.

Organizations should remain diligent and prepare for an increase in efforts targeting account take over, business e-mail compromise, ransomware, fraud and malware campaigns delivered through malicious decoy documents as well as other opportunistic attacks. Be aware of COVID-19-themed phishing campaigns using Word and PDF documents that include names like ' coronavirus response', 'coronavirus practices,' and 'coronavirus safety.' Attackers are also using images and names of entities like the UN, WHO, CDC, FDA, and commercial companies in targeted fraud and phishing campaigns. We are seeing "trojan" viruses being distributed via websites that are using the ongoing coronavirus epidemic as a lure. These websites show information about the coronavirus with an embedded video that, once clicked, the malicious executable virus is downloaded.

Of important notice, malicious actors have created a COVID-19 tracker map that impersonates the John Hopkins University coronavirus tracker map, complete with the University's identifying logos and COVID-19 data, to infect visitors with a trojan attack designed to steal sensitive data.

How to Reduce Risk:

- Be especially wary of any e-mail or other communications that contain information pertaining to COVID-19, especially from outside your organization or forwarded by someone.
- Do not open any e-mail that appears to come from the UN, WHO, CDC, FDA, etc., unless your organization is in the healthcare field.
- As with all phishing attacks, it is recommended that users disable macros in Microsoft Office unless you absolutely require them.
- When seeking information about COVID-19, visit only trusted websites. Before submitting any information, make sure the site's URL begins with "https" and includes a closed lock icon near the address bar.
- Only click on a link if you are sure it is a trusted website. Do not click on links that appear in untrusted e-mails, tweets, or instant messages.
- Use an anti-phishing toolbar. Safari, Chrome, Firefox and Internet Explorer offer free anti-phishing toolbars.
- Use trusted antivirus software and ensure that it is kept up to date.
- Use a high-quality desktop firewall, and where appropriate a network firewall, to act as a buffer between you, your computer and outside intruders.
- As a rule, you should never share personal or financially sensitive information over the Internet.

This COVID-19 pandemic provides malefactors an opportunity to breach security. Continue to follow your existing network and security protocols but with extra diligence regarding phishing and other malicious attempts using concerns about the coronavirus.