COVID-19 & Cybersecurity – Maintaining Vigilance During the Pandemic

Apr 16 2020

Posted By: Joseph M. Russell & Patrick M. Bergin

Practice Area: Information Technology, Data Privacy and Security

For many businesses throughout Wisconsin, employees have been working remotely for weeks and IT Departments have been working long hours to ensure that employees can continue to work remotely, with minimal disruption and with secure connections. Many people are dealing with issues while working at home by constantly toggling back and forth between work and the real-time updates about the spread of the coronavirus and its impact on what they can and cannot do for the foreseeable future. In short, people may *not* be thinking of best cybersecurity practices and hygiene. They should be. If not, this difficult work environment may become even more challenging and the ability to work remotely could be severely compromised, as well as the security of the sensitive information networks maintain.

It is within these unique working circumstances that hackers and cybercriminals continue to see great opportunity. They will exploit whatever toehold they can gain in a business computer network. Coronavirus-themed phishing and email-spoofing attacks continue to rise dramatically. Hackers are hoping distracted workers will more readily open otherwise suspicious email, click on malicious links or attachments related to COVID-19 updates on new infections, deaths, curves and cures – or new sources of funding available to employers and employees affected by the pandemic, such as benefits under the recently passed Coronavirus Aid, Relief and Economic Security ("CARES") Act. Distracted employees may not think twice before acting in response to such emails and, in doing so, unwittingly allow unauthorized persons into their networks.

The FBI urges vigilance during the COVID-19 pandemic and has set up fbi.gov/coronavirus to help Americans track the various scams that have emerged that seek to exploit opportunities the pandemic and our unique working environments have created. Following are a few specific examples of current threats.

Government Agency Scams
In recent weeks the FBI reports that cyber actors have engaged in phishing campaigns against first responders, launched distributed denial-of-service ("DDoS") attacks against government agencies, and created fake COVID-19 websites that quietly download malware to victim devices. Based on recent trends, the FBI assesses these same groups will target businesses and individuals working from home via telework software vulnerabilities, education technology platforms, and new Business Email Compromise schemes.

Business and Consumer Scams
The FCC is tracking COVID-19 consumer scams, fcc.gov/covid-scams, including text scams impersonating government agencies. The FCC recently learned of a text scam claiming to be from the "FCC Financial Care Center" and offering $30,000 in COVID-19 relief. There is no FCC program to provide relief funds. The text is likely a phishing attempt to get banking or other personal information from victims. The Better Business Bureau is also warning of a text message scam impersonating the U.S. Department of Health and Human Services informing recipients that they must take a "mandatory online COVID-19 test" using the included link.

With this backdrop in mind, it is important to remember a few fundamentals to minimize cybersecurity risk now and in the weeks ahead as stay-at-home guidelines remain in effect:

- Alert your users that coronavirus-themed phishing campaigns and email-spoofing attacks have spiked dramatically. Users may be encouraged, for example, to click on a Centers for Disease Control ("CDC") or World Health Organization ("WHO") URL but, if they do, they may be redirected to a phishing site from which cybercriminals may obtain Outlook usernames and passwords from unsuspecting users. Simply don't click it if it looks suspicious.
- Mandate, if possible, that workers use company-owned computers and sign into virtual private networks ("VPNs"). Remind employees that policies regarding the proper use of company technology are still in effect and enforceable while they are working remotely.
- To ensure that your internet-based meetings are private, utilize available features to set a password for the meeting, only distributing the password to intended participants, and not posting the password in a public forum.
- Monitor and review access logs for detection of unusual activity.
- Remind your employees not to use public wifi and to routinely change their password on their home wifi.
- Enable Multi-Factor Authentication whenever possible.
- Limit your users' rights and permissions with the principle of "need-to-know."
- Scrutinize and question third-party software or telework vendors to ensure that critical security controls are not compromised by new software. In particular, the FBI reports that malicious cyber actors may use legitimate-looking telework software—which may be offered for free or at a reduced price—to gain access to sensitive data or eavesdrop on conversations; in addition, cyber actors may also use phishing links or malicious mobile applications that appear to come from legitimate telework software vendors.
- Be careful about COVID-19 stimulus check scams. Checks will be sent via U.S. Mail and you should not give anyone your bank account information or accept a fee for expedited payment, etc. Also, email and SMS text scams are heating up that claim you must pay a fine for leaving your house and directs people to pay the fine via a "government" website with a '.US' extension. Official U.S. Government websites all end with ".GOV".

Most importantly, have an incident-response plan in place in the unfortunate event your network's cybersecurity is breached. This plan should include contact information of insurers (ideally, your policy already covers breaches but it will also require that notice of a breach must be timely given) and outside counsel who can coordinate a rapid investigation and response (such as coordinating with forensic investigators) to mitigate the damage of any data breach.

Together, we can all flatten the curve of these COVID-19 scams.
