COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE



Don't let coronavirus fears leave you vulnerable to hacking schemes



By Jaclyn Jaeger | Tue, Mar 17, 2020 2:16 PM

As more companies around the world require, or highly recommend, that their employees work remotely to prevent the further spread of the novel coronavirus, hackers who thrive off fear see this as an opportune time to carry out a cyber-attack. In this time of fear and uncertainty, it's more critical than ever to practice good security hygiene (just think of it as the technical version of proper handwashing).

"This is a moment that a lot of hackers across the world have been preparing for," says Brian Finch, a partner at law firm Pillsbury who co-leads the firm's coronavirus response team. "This is an opportunity to conduct pretty robust cyber-espionage, if not cyber-hostage taking. We are already seeing a spike in cyber-attacks, including on remote connection services."

Coronavirus-related schemes have been occurring with such frequency, in fact, that in the United States the Department of Justice has made them an enforcement priority. "The pandemic is dangerous enough without wrongdoers seeking to profit from public panic, and this sort of conduct cannot be tolerated," Attorney General William Barr wrote in a March 16 **internal memo** to all U.S. attorneys' general. "Every U.S. Attorney's office is, thus, hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic."

"This is a moment that a lot of hackers across the world have been preparing for. This is an opportunity to conduct pretty robust cyber-espionage, if not cyber-hostage taking. We are already seeing a spike in cyber-attacks, including on remote connection services."

Brian Finch, Partner, Pillsbury

Hackers prey on fear, so a common hacking scheme works like this: "Using simple phishing techniques, bad actors are targeting individuals with e-mails that appear to come from an official source. The emails purport to share helpful information about the virus and encourage readers to open an attachment, which then downloads malware to infect their computer and gather personal information," explains Jake Olcott, vice president of government affairs at BitSight.

In his memo, Barr cited reports of "individuals and businesses selling fake cures for COVID-19 online" as one example of a fraudulent scheme going around (the Federal Trade Commission is **similarly cracking down** in this area). He also cited reports of phishing emails from attackers impersonating government healthcare authorities, like the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC). In February, WHO itself **warned of criminals** disguising themselves as WHO officials to steal money or sensitive information.

On March 16, the U.K. National Cyber Security Center (NCSC) announced that it's **urging companies** to follow its online guidance, including **how to spot phishing emails** and **how to mitigate malware attacks**. "We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the coronavirus outbreak," said NCSC Director of Operations Paul Chichester. "In the event that someone does fall victim to a phishing attempt, they should look to report this to **Action Fraud** as soon as possible."

Cyber-security tips

Across all industries, it is critical that companies and employees review security practices, controls, and protocols to reduce the risk of opportunistic cyber-threats amid the coronavirus. Here are some tips:

1. Verify the authenticity of communication by healthcare authorities. Phishing attacks can come from a myriad of communication platforms—emails, text messages, phone calls. "Be wary of any form of communication that requires you to click on a link, download an attachment, or ask for any kind of personal information," says Heinan Landa, CEO and founder of Optimal Networks, an IT services firm. Upon receiving communication from a person or organization purporting to be from a government health authority, verify its authenticity *before* responding.

2. Watch for red flags. "Look for spelling errors and bad grammar and beware of anything asking you to download content or provide sensitive information to receive information/tips on how to protect yourself from coronavirus," Landa says. "Even if you are led to what looks like an official webpage after clicking on a hyperlink in an e-mail, if a pop-up message comes up asking you for any kind of information, do not provide it."

3. Educate employees and keep them informed about cyber-threats. "Organizations must implement effective security awareness training, such as teaching employees how to recognize and report phishing attempts," Olcott says. "While people are sometimes painted as a company's weakest security link, they can also be an organization's best defense against cyber-attacks."

4. Be aware of security vulnerabilities posed by third parties. Third parties pose significant risk to all industries, but amid coronavirus hysteria healthcare organizations are especially **vulnerable to cyber-attacks** for the protected health information and other sensitive data they handle. Often, third parties are targeted by threat actors "with the intent of penetrating the upstream networks of hospitals and health systems," Olcott says. "To combat this threat, healthcare organizations need a way to gain visibility into the security postures of these third parties and continuously monitor them over time for potential security gaps or malware infections."

5. Adhere to industry regulations when working remotely. "Some industry sectors are subject to regulatory cyber-security requirements for remote access," states a **client alert** from law firm Crowell & Moring. "Government contractors, for example, may be subject to specific technical controls established by NIST SP 800-171, including for access control,

awareness and training, configuration management, incident response, media protection, physical protection, and system and communications protection. This is a good time for government contractors to review their system security plans for compliance with these controls for teleworking."

Recent research reveals how coronavirus-related schemes are evolving. According to **research conducted by Proofpoint**, new coronavirus-themed e-mail attacks, for example, are attempting to disrupt global shipping by targeting susceptible industries, "including manufacturing, industrial, finance, transportation, pharmaceutical, and cosmetic companies (in that order)," Proofpoint said.

Practicing robust and regular cyber-security hygiene should *always* be top-of-mind, but the coronavirus pandemic really puts security practices to the test. Companies, financial institutions, healthcare organizations, and others that have truly healthy security practices should find themselves immune to the coronavirus.

RATE THIS RESOURCE

Select your rating

