Be Vigilant – Against the Virus and Cyber Crime

By: Stacy Cole on April 1, 2020 on graydon.law

In the time of Covid-19, it's more important than ever to be vigilant about your health. But that's not the only thing about which you need to be extra careful.

Scammers and hackers are working overtime to take advantage of the public's intense focus on the pandemic and exponential increase in remote work. Covid-19 phishing emails have already been an issue for weeks. Data incidents are on the rise, even when overall workforce productivity may be down.

The BBC, for example, has reported on a number phishing emails from hackers preying on people at this vulnerable time. They include emails with phishing links, asking people to click for a "secret" coronavirus cure, claiming that "we know the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. …" Or emails are notifying the recipient of a "tax rebate," where all he has to do is click "access your funds now" to go to a fake government site and input all his financial information. And there are many more.

If you can imagine a legitimate topic of great public concern—vaccines, economic relief, donation opportunities—there are hackers using those concepts to take advantage of this collective moment of weakness.

Just last week, the U.S. Attorney's Office in the Central District of California announced the arrest of a southern California man, Keith Lawrence Middlebrook, for "fraudulently solicit(ing) funds [from investors] with promises of massive profits for a company he called Quantum Prevention CV Inc." He made multiple social media videos, with more than two million views, in which he claimed he had developed a "Coronavirus prevention pill" and an "injectable cure." Middlebrook was charged with one count of wire fraud, after getting caught when he delivered the so-called prevention pills to an undercover agent posing as an investor. U.S. Attorney Nick Hanna warned that "[w]hile this may be the first federal criminal case in the nation stemming from the pandemic, it certainly will not be the last."

Even while we are inundated with daily updates on legitimate Covid-19 news from the

government, health professionals, and trusted sources, people still turn to conspiracy theorists and miracle promisers looking for someone to blame or a ray of hope. Scammers know that fear can lead to desperation, which can lead to riskier choices and big mistakes.

And when the workforce is spread out, with people working in relatively isolated circumstances, companies' risks rise. Employees don't have their office neighbor to yell down the hall to, asking them to come and take a look at this "weird email." Or they may feel that since they're removed from the office, they can click on riskier links and go to riskier sites—even while connected remotely to their office network. Of course, when a workforce is connected to an office network remotely, without employees tucked away safely behind a central firewall, hackers know there are potentially more network access points and more opportunities to get in by brute force or an open port.

This doesn't even address the inherent privacy issues with remote work. Is your personal digital assistant in range and listening in on all your work calls? Are you remembering to lock your desktop when you step away? Are you leaving confidential documents in plain sight? While the risks associated with doing so may seem low in your own house, taking a more lax attitude is not going to translate when we do return to the office. Even worse, that lax attitude may result in a breach of privacy laws or client contracts.

It may seem like the sky is falling while the sky is falling. But there are some steps you can take to mitigate some of this increased risk.

- **Communicate**. Make sure your teams know about these amplified perils. Remind them about their continuing privacy obligations, and that the hackers are working overtime. Share examples of scam emails, and push out additional phishing training. Make sure your teams know who to contact—and feel comfortable doing so—if they think there might be a security issue.

- **Lock it down.** Your IT staff is probably stretched pretty thin at the moment. But meeting all the obligations of setting up remote workstations for hundreds, if not thousands, of employees cannot push aside the obligations to patch, maintain firewalls, and monitor for suspicious activity. Your people are going to be looking for workarounds and IT is going to feel the pressure of making them happy. Make sure IT is empowered to say "no," and that leadership backs them up and leads by example. Security has to stay at the forefront.

- **Get help.** There are numerous resources available to help companies stay vigilant. From software solutions to business advisors, make sure you're asking questions. No one has all the answers right now, but more heads together will lead to a better result.

- **Insurance.** Pull out your policies and make sure you've got the right coverage for your current circumstances, including cyber and privacy coverage. Now is the time to review those policies—before you get the dreaded call: "I think I clicked on a link I shouldn't have… ."

- **Plan.** Do you and your team know what to do in the event of security breach with everyone off site? Data breach protocols often involve triage teams working together, face to face. How will the group communicate if no one can access a conference line or work email because the network is locked up by ransomware? Make sure your policies and protocols are updated with alternative methods of contact for your people.

Just because you or your team may be working from home, or working less frequently, don't let your guard down. Now is the time to step up security awareness and your program.

If you have questions regarding these pressing issues, please contact any of our **Graydon Cybersecurity and Data Privacy attorneys**.