Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Cybercriminals Are Exploiting The Coronavirus Outbreak

By **Ben Kochman**

Law360 (March 20, 2020, 5:08 PM EDT) -- Hackers are exploiting vulnerabilities stemming from the global coronavirus pandemic, including distracted workers and stretched-thin IT staff, as cybersecurity attorneys say the spread of COVID-19 has also brought with it a spike in data security incidents.

The spread of the virus that causes COVID-19 presents countless understandable reasons for employees not to have information security at the top of their minds. But companies need to double down on cyberdefense during the crisis, industry lawyers say, as the shift to remote work gives hackers more ways to infiltrate networks and to take advantage of potentially panicked staff.

"Companies were expecting a computer virus, not a human virus, as the most likely threat, but it's a human virus that has made businesses more reliant than ever on their systems," said Brenda Sharton, global chair of Goodwin Procter LLP's privacy and cybersecurity practice.

"And with everyone working remotely, the risks are even higher if someone takes the systems down."

Sharton said she had been responding to more than five times more data security incidents than usual in the last few weeks as companies adapt to the virus outbreak. “Cybercriminals love a crisis," she said.

Even the most sophisticated attackers often use a simple method to gain access to a victim's systems: phishing emails, designed to dupe employees into clicking on links and divulging login credentials on websites controlled by the hackers. In their attempts to bait people into clicking, cybercriminals exploit confusion and fear, seizing on whatever issue is in the news, from political scandals to even, in May 2018, the General Data Protection Regulation, or GDPR.

It's hardly surprising that cybercriminals have sent coronavirus-themed phishing emails as well. In February, the data security company Trustwave released a report with screenshots of emails sent by hackers posing as the Centers for Disease Control and Prevention and the World Health Organization, asking people to click on phony links for more information about the virus.

Ransomware attacks, in which hackers lock organizations out of their own systems and demand digital currency in exchange for regaining access, do not appear to have slowed down either. A local health agency in Illinois, the Champaign-Urbana Public Health District, told the magazine Mother Jones earlier this month that a ransomware attack knocked offline its website, which serves more than 200,000 people.

Cybersecurity attorneys also report an uptick in "business email compromise" attacks, in which hackers use a variety of methods to dupe workers into sending wire transfers to cybercriminals posing as their associates, often by using "spoofed" forgeries of company email addresses.

“Any time when there is a distraction that would divert a business from its normal business practices, that’s the time when cybercriminals strike," said Jena Valdetero, co-head of the the data privacy and security team at Bryan Cave Leighton Paisner LLP.

Valdetero said the surge in data security incidents could be attributed in part to a surge in people working remotely, including with unsecure internet connections and using IP addresses outside a company's network, making it difficult for IT staffers to keep track of who is accessing company systems.

Then there's the panic problem. Employees experiencing understandable stress about the spread of the virus may be less prone to be vigilant about detecting phishing emails or attempts by hackers to pose as someone's boss, for example, by making a forged email account and requesting sensitive data.

"If you're trying to socially engineer your way into someone's network, and you know someone is upset because they are working from home or stressed about the virus, all of those things are factors that hackers are counting on," Valdetero said.

"They exploit human weakness and human stress, and right now the whole world is under stress."

The crush of employees unexpectedly moving to remote work in recent weeks — as well as the expectation of constant updates about how companies are responding to the virus — has also led to a new high in the speed and intensity of online communications going back and forth, potentially giving hackers more room to sneak in their fraudulent messages.

“Businesses have been trying to position themselves as engaged with their clients and consumers in order to remain relevant and be a resource, but the effect of that is that it has created so much content and communications,” said David Katz, partner in the privacy, cybersecurity and data management practice at Adams and Reese LLP.

“Hackers are taking advantage of this by hiding among those communications and creating very sophisticated forms of messaging that appear legitimate.”

Attempted cyberattacks in the wake of the coronavirus outbreak span all industries, but the normal top targets, including health care and financial industries, should be on particularly high alert, industry attorneys say.

“There’s definitely an awareness in the financial space that everyone wants to close their deals now given the uncertainty in the market, and that means wire transfer requests flying across email,” said Alessandra Swanson, a partner in the transactions practice at Winston & Strawn LLP and former privacy investigator at the U.S. Department of Health and Human Services.

Beyond educating employees on the risks of phishing attacks and spoofed emails, anyone handling a wire transfer order should take extra steps right now to make sure cybercriminals are not trying to divert payments to themselves. That could mean calling someone to double check that a payment is correct, or taking a closer look at the sender's email address.

"It's a matter of communicating some really common sense instructions to your employees," Swanson said.

"This really is an unprecedented time for everyone, and employees are faced with working remotely while being home with their families and in some cases educating their children going throughout their day," Swanson added. "So there’s a strong likelihood that they will be distracted when reading their emails."

Cybersecurity also should be a priority for the legal industry itself, as it shifts to communicating with clients about sensitive issues through emails, phone calls and video chats, experts gathered by the American Bar Association said in a webinar on Thursday.

Steps organizations can take to mitigate their risks include mandating that workers use company-owned computers and sign into virtual private networks, or VPNs, that remote workers can use to connect to a shared network. Employers should then be frequently patching their VPNs with the latest security fixes and using multifactor authentication as another layer of protection, the U.S. Cybersecurity and Infrastructure Security Agency warned in an alert sent to businesses last week.

The agency suggested that companies adopt what they called a "heightened state of cybersecurity" as they shift to telework — a sentiment shared by attorneys advising clients who are being targeted with cyberattacks amid the pandemic.

--Editing by Peter Rozovsky.