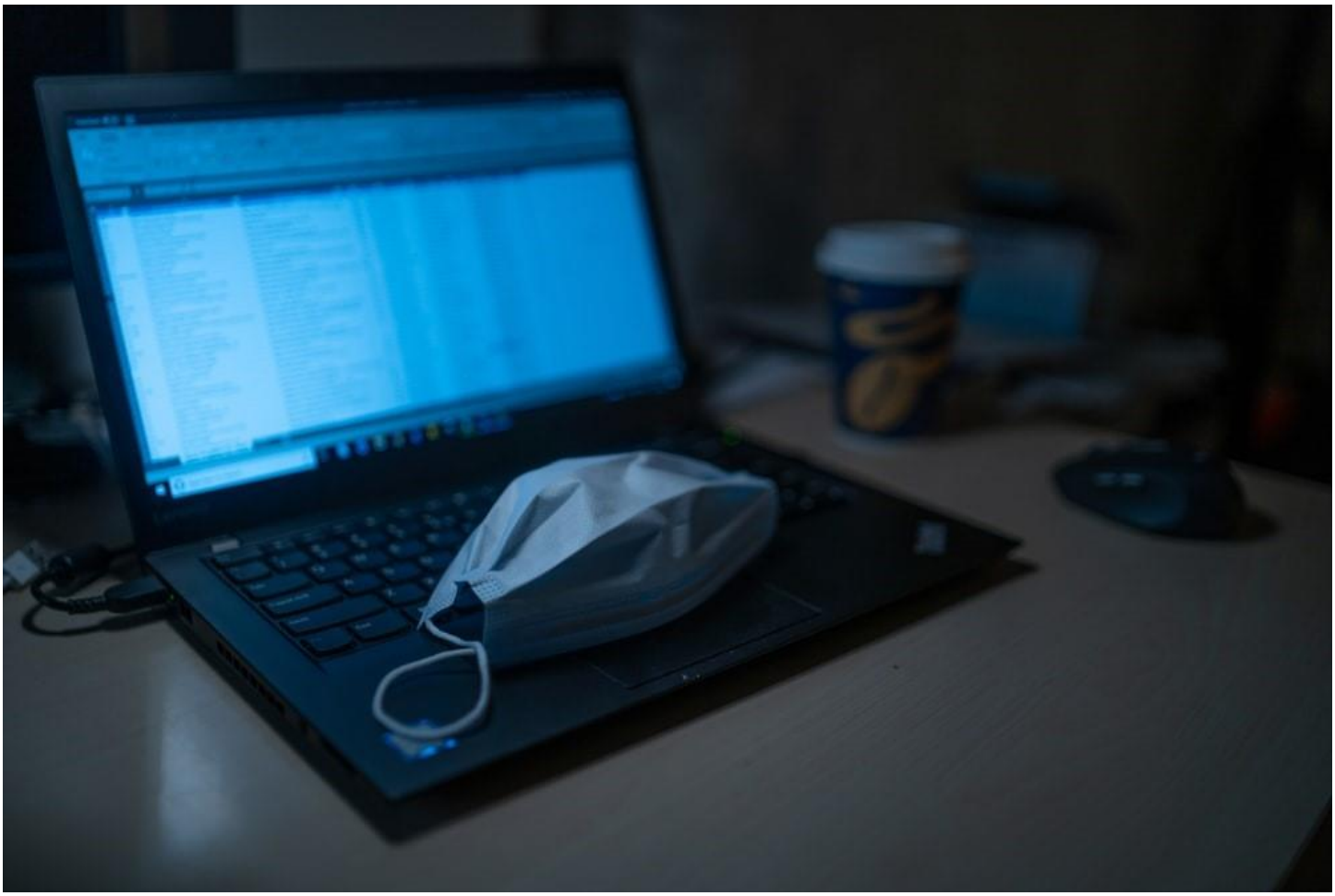
3-25-2020

The Coronavirus's Cyber Implications

Johnny Nguyen
Cardozo Arts & Entertainment Law Journal

The Coronavirus's Cyber Implications

BY JOHNNY NGUYEN/ ON MARCH 25, 2020



On January 30, 2020, the World Health Organization declared the outbreak of a respiratory disease named "SARS-CoV-2" a "public health emergency of international concern."[1] The disease, also known as the "coronavirus," is believed to have originated in Wuhan, China, and has now been labeled an international pandemic, or a global outbreak of disease.[2] As of March 15, 2020, there have been a total of over 3,000 confirmed cases in the United States, with at least 61 of them resulting in deaths.[3] Several countries have declared a state of emergency, and the United States has recently followed suit.[4] New York City announced that it would close public schools, and many other cities around the country have ordered businesses and restaurants to close, even issuing curfews.[5]

The implications of shutting down offices across New York City, one of the world's largest economic powerhouses, are far-reaching. Some of these are economic. However, others, likely less considered, involve security concerns. For instance, many attorneys are now being asked to work from home.[6] In addition, many law schools have switched to online learning platforms to protect students from potentially contracting the coronavirus.[7] While some firms are implementing a mandatory "work from home" (WFH) policy, others are requiring

their employees to alternate days with office appearances with WFH days.[8] Because the coronavirus is such a new and quickly developing event, many people are looking for more information about it in order to best protect themselves while also maintaining their daily lives. Many employees are continuing to stay updated with their employer's work policies through email. This is (and has been) one method hackers can obtain private information about the employer and its employees. For example, the European Central Bank just sent a letter to financial institutes warning of an increase in "cyber-security related fraud" targeting both customers and banks through methods such as phishing emails.[9] Emails that may seem like an employer's updates on its WFH policies may actually be from a hacker.

Another type of phishing email may include website or download links that seem like PDFs offering coronavirus safety measures.[10] For instance, a PDF named "CoronaVirusSafetyMeasures_pdf" actually included malware that infects a victim's computer.[11] Another type of email included a "three-page coronavirus-themed Microsoft Office document purported to be from the Center for Public Heath of the Ministry of Health of Ukraine."[12] Phishing emails have even imitated The Centers for Disease Control (CDC), pushing fake messages stating that "the virus has officially become airborne . . . and there have been confirmed cases of the disease in your location."[13] The email contains links to websites that look like legitimate CDC login pages, which then ask the victim to enter their credentials.[14] After doing so, the victim is sent to the legitimate CDC website, completely unaware that their information has been compromised.

With hackers looking to take advantage of coronavirus fears, how can employers and employees protect themselves? The Computer Fraud and Abuse Act (CFAA) criminalizes the intentional access of "a computer without authorization or exceed[ing] authorized access" of a broad range of information from areas such as financial records, United States departments or agencies, or from any protected computer.[15] The "information from any protected computer" clause of the CFAA has been broadly disputed in several cases. In *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit held that an employee's alleged installation of a program on an employer's computer that caused deletion of the employer's files violated the CFAA.[16] Conversely, the Ninth Circuit held that a former employee that e-mailed documents from his work computer to himself and to his wife while he was employed did not violate the CFAA.[17] Because the CFAA can be interpreted so broadly with its "information from any protected computer clause," employers and employees must stay informed on company policies in order to improve security, especially when coronavirus fears are heightened.

There are several policies that businesses can implement to make the transition to remote working safe and seamless for its employees. One is to determine whether there are established security guidelines for remote work and remote access to company information systems.[18] By ensuring that employees are up to date on accessing company information systems remotely, the risk of information compromise decreases. Additionally, employees

should be made aware of the types of information that they need to safeguard. For instance, intellectual property, work product, customer information, and confidential business information should all be protected with a heightened sense of security when working remotely.[19]

One of the best ways of preventing employees from falling prey to coronavirus related phishing attacks is to educate employees on reliable sources of information for coronavirus related updates. Employers and employees must be aware that the virus "presents an opportunity for hackers and wrongdoers to gain access to resources."[20] Most importantly, employees should be on alert because email scams are more potent when tied to a health scare.[21]

Because no one knows how long the coronavirus will be around for, people will continually look for updates regarding its status and ongoing effect on the world. This will create a prolonged situation where hackers will continuously look to exploit the general public's fear to gain access to private information. Businesses can protect themselves by educating their employees with both up-to-date information regarding the virus and company policies regarding handling sensitive information.

Johnny Nguyen is a Second Year Law Student at the Benjamin N. Cardozo School of Law and a Staff Editor at the Cardozo Arts and Entertainment Law Journal. Johnny is interested in contractual disputes and commercial litigation. Johnny is currently an Outreach Chair of the Asian-Pacific American Law Students Association chapter at Cardozo.

---

[1]Centers For Disease Control and Prevention, Coronavirus Disease 2019 (COVID-19), https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/summary.html (last visited Mar. 21, 2020).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Staci Zaretsky, *Biglaw Coronavirus Policy Tracker: Which Firms Will Let Lawyers Work From Home?* (Mar. 13, 2020), https://abovethelaw.com/2020/03/biglaw-coronavirus-policy-tracker-which-firms-will-let-lawyers-work-from-home/.

[7] *Id.*

[8] *Id.*

[9] *Chris Baynes*, *Coronavirus: Banks urged to prepare for surge in cyberattacks as hackers look to exploit crisis* (Mar. 6, 2020), https://www.independent.co.uk/news/business/news/coronavirus-banks-cyber-attacks-hackers-crime-european-central-bank-a9381286.html.

[10] Elizabeth Montalbano, *Spread of Coronavirus-Themed Cyberattacks Persists with New Attacks* (Mar. 6, 2020), https://threatpost.com/coronavirus-themed-cyberattacks-persists/153493/

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] 18 USCA § 1030.

[16] *See International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (2006).

[17] *See LVRC Holdings LLC, Brekka*, 581 F.3d 1127

[18] Christopher J. Buontempo, Cynthia J. Larose, *Coronavirus (COVID-19): Managing Cyber Security Risks of Remote Work* (Mar. 13, 2020), https://www.natlawreview.com/article/coronavirus-covid-19-managing-cyber-security-risks-remote-work

[19] *Id.*

[20] Victoria Hudgins, *As Coronavirus Spreads, Some Firms May Struggle to Pivot to Remote Work* (Mar. 4, 2020), https://www.law.com/legaltechnews/2020/03/04/as-coronavirus-spreads-some-firms-may-struggle-to-pivot-to-remote-work/

[21] *Id.*