Cullen | Dykman

COVID-19 Brings Increased Cybersecurity Risks As Many Employees Shift To Working At Home

April 2, 2020

The coronavirus (COVID-19) outbreak has disrupted businesses of all sizes throughout the United States. Social distancing measures issued by the federal government as well as many local governments are designed to curb the spread of the virus and have forced a vast number of employees to work from home. With employees having to quickly adjust to working remotely and with IT departments overwhelmed in trying to assist employees with these adjustments, hackers have used this as an opportunity to prey on businesses and employees while they are at their most vulnerable. Below are a number of issues that businesses, their employees and IT departments should be aware of to help avoid falling victim to a cybersecurity attack during the COVID-19 pandemic.

Increased Hacking and Scam Attempts Following the COVID-19 Outbreak

The FBI, FCC, and other law enforcement agencies have issued warnings in recent days regarding an increase in the number of fraud attempts related to the COVID-19 outbreak. Experts believe that part of this rise in fraud is due to hackers and scammers seeking to take advantage of businesses and employees whose daily routines have been disrupted by the outbreak. One major issue that has come up in recent weeks is individuals' use of private devices that may not have the same security measures installed as the devices that are provided by an employer. Hackers and scammers have used this as an opportunity to avoid employers' typically strong security protocols to attack unsuspecting individuals.

The COVID-19 outbreak has also overwhelmed IT departments as they scramble to assist businesses and employees in shifting to a work from home system on short notice. This has caused many IT departments to fall behind on their normal network and system maintenance, which could provide additional opportunities for fraud. Some non-essential businesses have suspended operations entirely, which could make them more vulnerable to cyberattacks.

Additionally, videoconferencing site Zoom—which has seen an explosive rise in the number of users in the past month as more and more individuals schedule virtual meetings—has come under scrutiny due to privacy and encryption concerns. Hackers have been able to intercept videoconferences and access users' video-cameras. These potential security issues have caused the New York Attorney General to look into Zoom's practices and possible flaws.

COVID-19 Related Scams

Some scammers are going a step beyond their normal schemes by creating COVID-19 related scams. Many of these scam attempts have come in the form of calls or emails alerting an individual that they may have come into contact with someone with COVID-19 or an offer to provide an individual with COVID-19 testing or information. Scammers will then seek to get an individual to provide them with personal information or to click a link that will download malware onto an individual's devices.

Officials have also seen a rise in scams related to COVID-19 related websites. In recent weeks, cybercriminals have sought to get individuals to visit websites that are seemingly related to the COVID-19 outbreak but are really designed to steal an individual's personal information. Experts believe that COVID-19 related domains are 50% more likely to be a scam than any other type of domain.

Tips to Maintain Cybersecurity

During these uncertain times, it is more important than ever for businesses, their employees, and IT departments to be on the lookout for possible cyber scams. Employees should be consistently reminded to be skeptical of any email that comes from an unknown source, particularly emails that attempt to get the recipient to use a download link. Employees should also be made aware of the increase in COVID-19 related scams, and told to check with their IT department before visiting COVID-19 related websites.

IT departments should split their time between assisting those who need help getting set up to work from home and ensuring that the business' cybersecurity protocols are up to date. IT departments should also seek to have employees use devices that contain similar cybersecurity measures to those they would typically use when working from an office.

We will continue to keep you updated on any further developments related to cybersecurity and the COVID-19 outbreak.

If you have questions regarding cybersecurity risks and how it may impact you and your business, feel free to contact Ariel E. Ronneburger at (516) 296-9182 or via email at **aronneburger@cullenllp.com** or Ryan Soebke at (516) 357-3784 or via email at **rsoebke@cullenllp.com.**

Practices

- Commercial Litigation

Attorneys

- Ryan M. Soebke
- Ariel E. Ronneburger