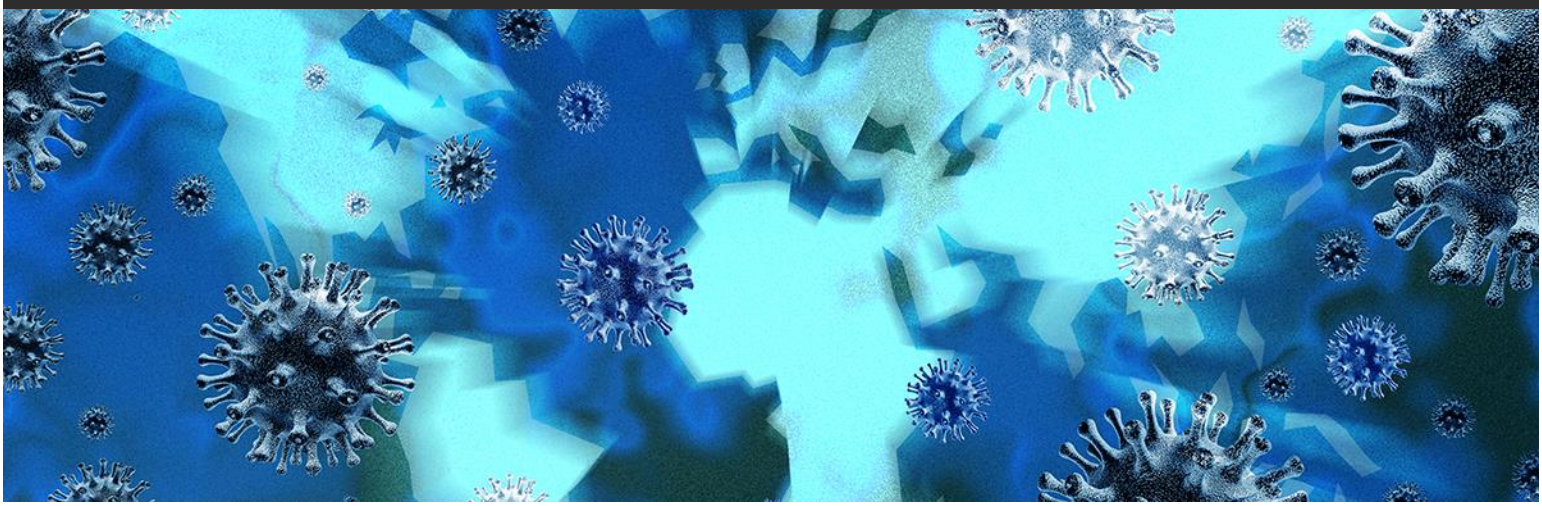
GT GreenbergTraurig

Alert | Health Emergency Preparedness Task Force: Coronavirus Disease 2019



April 2, 2020

Cybercriminals Adapt Old Scams to Capitalize on COVID-19

While many companies across the United States transition to remote working, scammers are taking this opportunity to target vulnerable and unsuspecting employees. Some emails and websites promising information about keeping safe from, and offering resources for, the Coronavirus Disease 2019 (COVID-19) pandemic have turned out to be scams that push malware, ransomware, and disinformation, or attempt to steal passwords and personal information. One wrong click may become a time-consuming and costly interruption to business operations across a company. With the upsurge in attempted cybercrime, it's important for employees to be aware of cyber hygiene.

Think Before Clicking

- Clicking on links that appear in emails from individuals outside of the organization, on unknown websites, and in instant messages may be risky. Hover over and review unusual links before clicking on them.
- Some suspicious links will direct you to pages where entries for financial or personal information are required. Be cautious about sharing business, personal, or financially sensitive information over the Internet, especially on websites lacking Secure Sockets Layer (HTTPS) encryption. Instead, you may visit the main website of the company in question, find their phone number, and give them a call.

Think Before Downloading

- Consider where an email is from and whether the email address is correct. Does the attachment look genuine? Consider, for instance, misspellings and the context of whether the purported sender would normally send you such an attachment. If you're not sure, consider contacting the person you think has sent it or your IT department and double-check.

Companies have seen an uptick in three types of COVID-19 cyber scams in particular: phishing attacks, ransomware attacks, and fake websites and applications. Companies should be aware of these common attack types and trends, consider educating their employees about them, and take steps to be prepared to quickly address any instance where one of their employees have fallen victim to a cyber-attack. With more employees working remotely, Privacy, Security, or IT teams may wish to remind employees about the below cyber scams and the steps employees should take to keep data secure when working remotely.

1. **Phishing is on the Rise**

Phishing is a cybercrime in which an individual is contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personal information, banking and credit card details, and passwords. Phishing schemes may be sophisticated and may even include elements like official imagery or email addresses that look similar to email addresses used by official businesses. Likewise, phone calls and texts from scammers pretending to be official businesses or government representatives may include information like your name or phone number to try to convince you that they're real.

Since the end of Feb. 2020, phishing emails have spiked by over 600% as cyber-criminals look to capitalize on the fear and uncertainty generated by the COVID-19 pandemic, according to a security vendor.

Last week, the U.S. Federal Bureau of Investigation (FBI) warned individuals to "look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government." The FBI warned that "[w]hile talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money."

2. **Ransomware Attacks Are More Prevalent**

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system, files, or data and demands ransom payment to regain access. There are several different ways that ransomware can infect a device. One of the most common methods is through malicious spam, which is unsolicited email that is used to deliver malware. The email might include booby-trapped attachments, such as PDFs or Word documents. Once an individual opens or downloads the attachments, the malware is automatically downloaded and installed. Many health systems, public health agencies, and even the federal government have become the target of ransomware attacks over the last few weeks.

3. **Fake Websites and Apps "Relating" to COVID-19 Are Popping Up**

Attackers are developing many kinds of websites and applications with fake or fraudulent information, including:

- Websites that may look like they belong to a government or global organization and encourage visitors to download and install applications, which, upon download, may crash or display a message saying it's not available in that specific region while it starts asking for permission to access sensitive data from the user's phone.
- An app that may claim to provide access to a real-time virus-tracking map, including heatmap visuals and statistics, but in fact, is laced with ransomware.
- An app that may claim to notify users as soon as anyone infected with COVID-19 is nearby, but actually locks the victim's phone and demands a ransom to lift the encryption.

It may be helpful for employees to ensure that they are visiting legitimate government websites and decline to download any extraneous applications while using their work-provided computers and mobile devices. Employers may wish to direct their employees to a list of approved COVID-19 resources.

As cybercrimes and scams continue to evolve, it's important to stay up to date on the latest trends, how to best protect your organization, and keep employees informed.

For more information and updates on the developing COVID-19 situation, visit GT's Health Emergency Preparedness Task Force: Coronavirus Disease 2019.

Author

This GT Alert was prepared by:

- Kate Black | +1 305.579.0500 | blackk@gtlaw.com