BLANKROME

Cybersecurity & Data Privacy

JUNE 10, 2020 • NO. 12

FBI Alert: Enhanced Threat of Cyber Fraud Tied to COVID-19

As the coronavirus global health emergency continues apace, cyber criminals have continued their concerted effort to exploit this crisis for financial gain via cyberattacks and scams tied to COVID-19. In recent weeks, threat actors have ramped up COVID-19 attacks at such an alarming pace it prompted the Federal Bureau of Investigation ("FBI") to issue a series of alerts warning the business community and the public of the significantly increased cyber threats. In its most recent alert, the FBI warns against the enhanced threat of fraud-based cyber scams, which it notes will likely increase. Companies must be on alert for Internet-based fraud and take appropriate measures to ensure the security of their networks and systems, especially as their employees continue to work remotely for the foreseeable future.

The Current Threat Environment: Like Nothing We Have Seen Before

As the country grapples with the immediate public health and economic fallout of COVID-19, a related crisis has simultaneously emerged: criminals seeking to pray upon an anxious public. The speed at which criminals are devising and executing schemes tied to COVID-19 is—in the words of the FBI—"truly breathtaking." According to the FBI, the sheer variety of frauds uncovered is shocking, including offers of sham treatments and vaccines, bogus investment opportunities in non-existent medical companies, and calls from fraudsters impersonating doctors demanding payment for treatments.

FBI Issues Alert Warning Against Increased Threat of COVID-19-Related Fraud

Recently, the FBI issued its newest in a string of alerts warning of cyber fraud as the COVID-19 pandemic has grown deeper. This most recent alert follows prior FBI warnings regarding a rise in COVID-19 business email compromise ("BEC") schemes and, more specifically, cloud-based BEC attacks.

In its newest alert, the FBI notes a precipitous increase in cyber-attacks fueled by fraudulent motives, including the following:

scammers targeting websites and mobile apps designed to track the spread of COVID-19 and using them to implant malware and steal financial and personal data;

thieves posing as national and global health authorities, including the Centers for Disease Control and Prevention ("CDC") and the World Health Organization ("WHO"), to conduct phishing campaigns by sending emails designed to trick recipients eager for reliable health information into downloading malicious code; and

perhaps most dangerously, criminals using COVID-19 as a lure to deploy ransomware, malicious software that will lock a computer system until a ransom is paid, with an emphasis on targeting hospital and local government operations in particular.

In addition, the FBI also cautions that the implementation of the $2 trillion Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") will propel fraudsters' schemes even further, as cyber criminals are already developing methods to steal the critical financial support that is being provided as a lifeline for communities, companies, and individuals.

Compliance Tips

The FBI notes that with the significant rise in fraudulent cyber-attacks, businesses and individuals alike must be vigilant and avoid opening email attachments or clicking on links from unrecognized senders; be cautious of requests for account information; and always confirm any transmission of information or funds is being sent to a legitimate recipient.

Beyond these tips, to further mitigate the significantly increased risk of fraudulent cyber-attacks and scams tied to COVID-19, businesses should consider the following practices:

- **Educate Employees to Be on Heightened Alert:** Companies need to educate their employees about the significant risk of COVID-19 cyber-attacks and instruct them to adopt a heightened state of cybersecurity. This is especially so as employees continue to work remotely.

- **Defend Against Phishing Attacks:** One of the largest COVID-19 cyber risks is "phishing"—whereby third parties share links, such as COVID-19 health-related information, that result in the downloading of malware or lead to malicious websites that harvest credentials or other personal information. Employees should be educated on how to spot attempted phishing attacks and proper cyber habits to avoid being victimized by phishing. This includes never transmitting personal or business information through email; only downloading files from trusted sources; and being suspicious of emails with generic greetings, spelling errors, and improper grammar style.

- **Defend Against Ransomware Attacks:** Another major COVID-19 security threat is ransomware. Because ransomware is frequently being deployed through links claiming to provide COVID-19 health-related information, employees should be cautioned to only use trusted sources from government and research institution websites when seeking out COVID-19 health information, and never click on health-related links provided in emails.

- **Increased Security for Remote Network Devices:** With remote work arrangements employees are now outside traditional organizational/corporate firewalls and may be using unsecured Wi-Fi networks, which makes their devices particularly vulnerable to cyber-attacks. As such, companies should add extra layers of security for remote devices that connect to their organizational networks, which can be accomplished through measures such as: (a) implementing "multi-factor authentication" ("MFA"), which uses two or more identity components—such as a password and a fingerprint—to authenticate a user's identity; (b) managing privileged access; and (c) utilizing the principle of least privilege, which provides employees with only the minimum amount of network privileges for them to be able to complete their job duties and responsibilities.

- **Software Updates:** Because cyber criminals are targeting and exploiting vulnerabilities as a primary method of hacking remote devices, employees must be instructed to regularly check that all patches/other updates that address security vulnerabilities on their remote devices are downloaded in a timely manner. Employees should enable all automatic software updates on their devices and only visit vendor sites directly when attempting to download updates (rather than clicking on advertisements or email links).

- **Incident Response Plans:** Finally, companies should anticipate a percentage of COVID-19 cyber-attacks will prove successful, as planning for these incidents in advance will help minimize any damage caused. Companies should maintain incident response plans that define a clear procedure to follow in case of a security incident and can be implemented immediately with adequate resources to minimize the impact of the event.

Conclusion

As demonstrated by the wave of recent alerts from the FBI (as well as other governmental agencies), the current health crisis has spiked the threat of cyber-attacks and scams to an unprecedented level. This will not only continue—but grow even larger—in the coming weeks and months. As such, companies must both increase the level of their technical cyber defenses and ensure their remote workers remain educated and on alert for potential cyber-attacks to mitigate the risk of being on the receiving end of a potentially lethal security incident.

As part of its COVID-19 Task Force, Blank Rome LLP's Cybersecurity & Data Privacy team can assist in providing key counseling and guidance with respect to any issues or concerns relating to the increased risk of COVID-19 cyber-attacks, as well the necessary policies, procedures, and protocols to fully mitigate the risks associated with remote working arrangements and other cyber threats that will persist during the current public health crisis. And if your organization suffers a any type of security incident during the ongoing public health crisis, Blank Rome's data breach incident response team is available 24/7 and can provide immediate assistance with rapid response and crisis management following any type of breach or security event.

For additional information, please contact:

David J. Oberly, Cincinnati Office
Associate, Cybersecurity & Data Privacy, Privacy Class Action Defense
513.362.8711 | doberly@blankrome.com

©2020 Blank Rome LLP. All rights reserved. Please contact Blank Rome for permission to reprint. Notice: The purpose of this update is to identify select developments that may be of interest to readers. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.