BLANKROME

Cybersecurity & Data Privacy

JUNE 4, 2020 • NO. 9

FBI Warns Companies to Be Vigilant as COVID-19-Themed BEC Scams Continue to Grow

As the COVID-19 pandemic continues to cause chaos across the globe, cyberattacks seeking to exploit the crisis on the rise as well. In particular, the frequency of COVID-19 business e-mail compromise ("BEC") schemes—a particularly low-tech, but highly damaging type of cyber scam—has risen significantly since the onset of the global health emergency, so much so it prompted the Federal Bureau of Investigation ("FBI") to issue two alerts warning businesses of the growing threat. As such, businesses must take appropriate measures to effectively mitigate the enhanced risk posed by BEC fraud, which is expected to increase even further in the coming weeks and months.

BEC Scams: Low-Tech Fraud with Devastating Consequences.

BEC scams, also known as "CEO fraud" and "man-in-the-e-mail scams," involve tricking victims—often those who perform legitimate funds transfers—to make unauthorized wire transfers or send funds directly to the coffers of cyber criminals. The typical BEC scheme originates with the theft of a corporate executive's credentials by phishing or other means. With those credentials in hand, cyber criminals will then impersonate the executive, sending urgent messages to lower level employees with requests to transfer or wire funds to bank accounts.

According to the FBI's Internet Crime Report, the bureau received approximately 24,000 complaints concerning BEC fraud last year, with losses totaling $1.7 billion—accounting for nearly half of all cybercrime-related losses in 2019. While ransomware frequently garners headlines due to the operational disruption caused by these attacks, cyber criminals have had much more financial success with BEC scams, netting at least 17 times more per incident ($75,000) than ransomware ($4,400).

It should not come as a surprise, then, that BEC was far and away the top source of cyber-related financial loss in 2019. Moreover, BEC fraud is a relatively low-tech and low-cost scam that provides criminals with the ability to focus on high-value targets and high returns, all with minimal risk. This conflux of factors makes BEC scams particularly popular with cyber criminals.

Recent Proliferation of BEC Scams Tied to COVID-19.
Over the years, cyber criminals have become more advanced and sophisticated in their attack techniques and methods, leading them to consider the psychological aspect of their scams.

In particular, fraudsters have become extremely adept at exploiting current events—such as terrorist attacks and natural disasters—and the impact on the targets of their scams. As the COVID-19 crisis has continued to deepen, cyber criminals have adjusted their BEC scams to place a greater emphasis on COVID-19 and enhance the social engineering aspect of their attacks. For example, BEC fraudsters are impersonating vendors and requesting payment outside the normal course of business, citing reasons relating to COVID-19 for the request. Similarly, cyber criminals claiming to be company executives are e-mailing lower-level employees requesting urgent, confidential wire transfers to cover costs due to unexpected issues arising from COVID-19.

FBI Sounds the Alarm on Anticipated Rise in COVID-19 BEC Schemes.
Recently, the FBI issued an alert warning that cyber criminals are actively exploiting the uncertainty surrounding the COVID-19 pandemic to further the effectiveness of their BEC scams. In particular, the FBI reports it recently observed a significant spike in BEC fraud targeting organizations purchasing personal protective equipment or other supplies needed in the fight against COVID-19. The FBI further cautions businesses to anticipate an even greater rise in BEC schemes tied to the COVID-19 pandemic moving forward.

To guard against this heightened risk of BEC scams, the FBI advises businesses and their personnel to be on the lookout for the following red flags: (1) unexplained urgency; (2) last-minute changes in wire instructions or recipient account information; (3) last-minute changes in established communication platforms or e-mail account addresses; (4) communications done only through e-mail and a refusal to communicate over the telephone or through online voice/video platforms; (5) requests for advanced payment of services when not previously required; and (6) requests from employees to change direct deposit information.

In addition, the FBI recommends the following tips to help companies further mitigate the risk of falling victim to BEC scams: (1) be skeptical of any last-minute changes in wiring instructions or recipient account information; (2) verify any changes and information via the contact the company has on file, and do not contact the vendor through the number provided via e-mail; (3) ensure the URL in e-mails is associated with the business it claims to be from; (4) be alert to hyperlinks that may contain misspellings of the actual domain name; and (5) verify the e-mail address used to send e-mails, especially when using a mobile or handheld device, by ensuring the sender's e-mail address appears to match who it is coming from.

FBI Issues Additional Warning on Cloud-Based BEC Attacks.
The FBI also issued a second alert to advise that cyber criminals are targeting organizations that use popular cloud-based e-mail services—***i.e.***, hosted subscription services that enable users to conduct business via tools such as e-mail, shared calendars, online file storage, and instant messaging—with an increasing number of BEC scams. The FBI notes that in doing so, cyber criminals are using tailored phishing kits designed to mimic and impersonate cloud-based e-mail services, making these scams extremely hard to detect as fraudulent. Moreover, the FBI also reports a troubling trend of cyber criminals accessing the address books of compromised accounts to identify new targets and send phishing e-mails, allowing a single successful e-mail account compromise at one business to be pivoted to multiple victims within an industry.

To mitigate the risk of cloud-based BEC scams, the FBI recommends businesses implement the following practices for employees and other end users: (1) enable multi-factor authentication for all e-mail accounts; (2) verify all payment changes and transactions in person or via a known telephone number; and (3) educate employees about BEC scams, including preventative strategies such as how to identify phishing e-mails and how to respond to suspected compromises.

The FBI also recommends that businesses work with their IT administrators to implement the following practices to further mitigate the threat of cloud-based BEC fraud: (1) prohibit automatic forwarding of e-mail to external addresses; (2) add an e-mail banner to messages coming from outside your organization; (3) prohibit legacy e-mail protocols, such as POP, IMAP, and SMTP, that can be used to circumvent multi-factor authentication; (4) ensure changes to mailbox login and settings are logged and retained for at least 90 days; (5) enable alerts for suspicious activity, such as foreign logins; and (6) enable security features that block malicious e-mail, such as anti-phishing and anti-spoofing policies.

Conclusion.
BEC fraud has continued to grow, evolve, and become significantly more sophisticated and deceptive in recent years. As such, BEC scams now represent one of the most destructive types of security threats faced by companies across all industries. And like many other types of security threats, the prevalence of BEC scams has risen precipitously as the COVID-19 pandemic has progressed, with fraudsters aiming to exploit the expanding scope of the crisis. Moving forward, these same groups will continue to target businesses and individuals with new BEC schemes for the foreseeable future.

Companies must therefore remain vigilant and take active steps to mitigate the burgeoning security threat posed by BEC scams. At the same time, as cyber threats continue to develop and evolve at a rapid pace, companies must also stay current on the latest trends and developments to stay ahead of the curve and effectively defend against these risks, which will remain active and substantial for the duration of the current public health crisis.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy team can assist in providing key counseling and guidance with respect to any issues or concerns relating to the enhanced risk of BEC attacks, as well the necessary policies, procedures, and protocols that are needed to fully mitigate this significant security threat. And if your organization suffers any type of security incident during the COVID-19 pandemic, 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:

Jeffrey N. Rosenthal, Philadelphia Office
Partner, Business Litigation, Privacy Class Action Defense
215.569.5553 | rosenthal_j@blankrome.com

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