BLANKROME

Cybersecurity & Data Privacy

APRIL 14, 2020 • NO. 6

Flattening the Scam Curve: Be Prepared for Uptick in COVID-19 Social Engineering Cyber Attacks

In addition to generating an unprecedented public health crisis, the novel coronavirus ("COVID-19") has also created a range of noteworthy cyber risks that pose significant security threats to the networks, systems, and data of businesses across all sectors. Notably, in recent weeks a sharp rise has occurred in social engineering cyber scams targeting employees with malicious content tied to COVID-19. The ongoing uptick in social engineering attacks has been so drastic that it recently prompted both the Federal Bureau of Investigation ("FBI") and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") to issue alerts warning businesses of this markedly increased cyber threat. Accordingly, businesses must be aware of this burgeoning security threat and take proactive steps to mitigate risk, which will only increase as the COVID-19 crisis deepens further.

COVID-19: The Perfect Ingredient for Social Engineering Schemes

Cyber criminals are notorious for quickly adapting their social engineering schemes to take advantage of major events and flashpoints, such as natural disasters and terror attacks. The current public health emergency created by COVID-19—and the resulting fear, anxiety, and uncertainty that continues to grip the public, as well as our desire for information on the pandemic—presents the ideal opportunity for exploitation by fraudsters. As the COVID-19 crisis began to make headlines in January of this year, cyber criminals adapted their attacks to integrate more themes playing on the burgeoning health crisis.

FBI Alert Warns Against the Rise in COVID-19 Social Engineering Schemes

In recent weeks, there has been a sharp increase in the frequency of social engineering attacks seeking to exploit the growing health emergency. The spike has been so drastic that the FBI issued an alert cautioning against the heightened risk of social engineering schemes being carried out under the guise of the pandemic.

In particular, the FBI warns of the threat of e-mails claiming to be from the Centers for Disease Control and Prevention ("CDC") or other organizations allegedly offering information on the virus, as fraudsters are using these links in e-mails

to deliver malware or conduct ransomware attacks. The FBI also advises on the risk posed by websites and apps claiming to track COVID-19 cases, as criminals are also using malicious websites to carry out ransomware attacks as well.

The FBI also highlights the specific threat of phishing e-mails asking to verify personal information in order to receive an economic stimulus check from the government, and notes that government agencies will *never* send unsolicited e-mails seeking private information in order to send money. According to the FBI, it has also observed an influx of phishing e-mails claiming to be related to charitable contributions, general financial relief, airline ticket refunds, fake cures and vaccines, and fake testing kids.

CISA Joint Alert with UK Further Warns Against the Elevated Social Engineering Risk

The recent surge of cyber attacks tied to COVID-19 also prompted CISA to issue a joint alert with the United Kingdom's National Cyber Security Centre ("NCSC") warning against the continued exploitation of the COVID-19 pandemic by cyber criminals and nation-state hackers through the use of social engineering to entice users to carry out specific desired actions like clicking on links, downloading apps, or opening files (such as e-mail attachments) that lead to phishing websites or allow malware and ransomware to be deployed.

To create the impression of authenticity, cyber criminals are spoofing sender information in malicious e-mails to make it appear that these messages are originating from trustworthy sources, such as the World Health Organization ("WHO") or an individual with "Dr." in their title. Another common technique is for malicious actors to send phishing e-mails that contain links to fake e-mail login pages. Similarly, other e-mails will purport to be from an organization's human resources department, advising an employee to open an attachment.

Importantly, CISA notes that both cyber criminals and nation-state actors are likely to continue using social engineering schemes to exploit the pandemic in the coming weeks and months through the use of a range of different types of cyber attacks, such as:

- phishing, using the subject of COVID-19 as a lure;
- malware distribution, using COVID-19-themed lures;
- registration of new domain names containing wording related to COVID-19; and
- attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

CISA notes that it has observed a large volume of phishing campaigns using the social engineering techniques described above, and which include e-mail subject lines such as "2020 Coronavirus Updates" and "2019-nCov: New confirmed cases in your City." In most instances, these e-mails also contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

At the same time, social engineering-related phishing attempts are also being carried out by other means, such as through "smishing"—social engineering through text messages ("SMS"). Similarly, "vishing"—social engineering that leverages voice communication—is also being deployed in current COVID-19 scams. This technique, which takes advantage of the public's misplaced trust in the security of phone services, is often be combined with other forms of social engineering that entice a victim to call a certain number and divulge information.

Compliance Tips

To mitigate the elevated risk of social engineering scams tied to COVID-19, businesses should consider the following best practices:

- **Employee Education and Training:** As a starting point, companies must effectively convey to employees the heightened risk of social engineering attacks tied to COVID-19 that exists at the present time. In addition, employers must also provide their workers with the knowledge and tools they need to effectively handle and diffuse any attempted social engineering attacks they may encounter. In particular, companies should properly educate their workforces on how to spot and address social engineering scams in real time. Beyond training employees on how to identify these attacks, employers should provide their workers with guidance on proper cybersecurity practices to follow to avoid falling victim to a social engineering scam, including the following: (1) do not open attachments provided in e-mails from senders you do not recognize; (2) do not provide sensitive financial or personal information in response to an e-mail or robocall; (3) always verify the legitimacy of a web address before clicking on any links contained in e-mails; and (4) check for misspellings or wrong domains with a link (such as an address that should end in ".gov," but which ends in ".com" instead).

- **Strong Password Practices:** Organizational defenses against social engineering schemes often rely exclusively on users being able to spot attempted social engineering attacks as they occur. However, businesses that widen their defenses to encompass more technical measures can significantly improve their chances of avoiding attempted social engineering attacks. In particular, companies should require multi-factor password authentication for access to all remote devices, which is critical to limiting potential damage when credentials or devices themselves are lost or stolen.

- **User Access Restrictions and Control:** Companies should consider restricting access to sensitive data by remote workers and adhering to the principle of least privilege, in which employees are granted only the minimal level of access or privilege that is necessary for them to carry out their job duties and responsibilities. By ensuring that employees only have access to data that is essential to their jobs, companies can significantly limit the scope of their potential attack surface, which, in turn, can significantly decrease the impact and fallout of a successful social engineering attack.

- **Incident Response:** Companies should anticipate that a percentage of social engineering attacks will prove successful, as planning for these incidents in advance will help minimize any damage caused. In particular, companies should maintain incident response and disaster recovery plans that can be implemented immediately with adequate resources to respond to an executed social engineering scam. Companies should also review their plans with key personnel to ensure that everyone is up-to-speed on their roles and responsibilities in the event the plan needs to be put into action. Realize that law enforcement may not be available to give the assistance they normally would.

Conclusion

Cyber criminals are continually adjusting their tactics to take advantage of new situations, and the current COVID-19 public health crisis is no exception. Malicious actors are working feverishly to take advantage of the public's concern over the health crisis and its high appetite for COVID-19-related information, which presents a prime opportunity to utilize social engineering methods to deliver malware and ransomware, and to steal user credentials.

As such, both businesses and their workers must remain vigilant. In particular, it is critical that companies keep their workforces fully informed of all evolving cyber threats in order to minimize the risk of experiencing a potentially catastrophic security or data compromise event.

As part of its COVID-19 Task Force, Blank Rome's Cybersecurity & Data Privacy team can assist with providing key counseling and guidance with respect to any issues or concerns relating to the increased threat of COVID-19 social engineering schemes, as well as other policies, procedures, and protocols that your organization should have in place to minimize the risk of social engineering scams to the greatest extent possible. And if your organization suffers a successful social engineering attack or other 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:

Jennifer J. Daniels, Pittsburgh Office
Partner, Cybersecurity & Data Privacy
412.932.2754 | daniels@blankrome.com

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