BLANKROME

Cybersecurity & Data Privacy

MARCH 2020 • NO.1

How to Prepare for Coronavirus-Themed Phishing Attacks

In recent weeks, the coronavirus (COVID-19) has taken the United States by storm, causing panic and fear across the country. The recent outbreak, which originated in China and is now spreading across the world, has been declared a Public Health Emergency of International Concern ("PHEIC") by the World Health Organization ("WHO"). As the virus continues to proliferate at a rapid pace, cyber criminals are taking advantage of this period of heightened fear and anxiety to target companies and their workers with sophisticated phishing attacks designed to steal sensitive personal data, install malware to launch a ransomware attack, or simply gain access to a company's networks or systems—where they can wreak havoc in a number of ways. Businesses of all sizes and across all industries must effectively guard against this noteworthy cybersecurity and privacy threat. And be prepared to take immediate action in the event they become a victim of a successful phishing campaign.

THE SIGNIFICANT THREAT POSED BY CORONAVIRUS-THEMED PHISHING SCHEMES

Announcements and alerts pertaining to the coronavirus continue to go out at a rapid pace, with health organizations offering guidance and advice and news organizations providing minute-by-minute updates. Employers are also rapidly responding to the crisis, communicating regularly with their employees to protect the health of their workers and their organizations. And as the virus continues to dominate headlines, cyber criminals are taking advantage of the fear and panic to carry out sophisticated phishing scams targeted at unsuspecting victims, via both e-mail and Internet sites.

According to cybersecurity firm Proofpoint, Inc., the number of phishing attempts mentioning coronavirus has increased significantly since the end of January. The problem has become so significant the WHO recently issued a statement on its website, *Beware of Criminals Pretending to Be WHO*.

As the crisis continues to expand further, hackers are deploying cyberattacks in a range of different ways. One common technique is to disguise e-mails directed to employees as originating from their employers or high-level management, such as updates on company contingency plans and travel restrictions. Here, cyber criminals utilize social engineering to target employees with malicious messages, hoping they are even more susceptible than normal and will quickly click on a link or otherwise act without thinking in response to urgent alerts from management. As just some examples, these e-mails have been crafted to mirror a company's purchase order for facemasks, provide purported information about remote-working plans, and dupe employees into wiring funds to fraudulent accounts.

Cyber criminals are also leveraging the emergency as cover to both send phishing e-mails and deploy malicious links on websites, disguised as providing health-related information or products to protect against the risk of contracting the coronavirus. While cyber criminals often tailor phishing scams to seasonal events, such as tax season W-2 scams, the success rate of these traditional phishing scams is dwarfed by those tied to critical world events, such as the current coronavirus emergency. As just one example, hackers are targeting unsuspecting recipients with e-mails—purportedly originating from a virologist—that contain malicious links and attachments that they claim provide information on how to guard against the spread of the disease.

COMPLIANCE STEPS

To protect against the heightened risk of coronavirus-themed phishing scams, companies should consider the following best practices:

- **Cybersecurity and Data Security Policies:** First, companies should ensure they have cybersecurity and data security policies addressing the use of technology within the organization. To protect against phishing attacks, it is especially important companies maintain a corporate communications policy, which sets forth detailed guidelines as to how the company will communicate securely with other members of the organization. This is vital to preventing employees from being tricked into complying with requests that appear to come from co-workers, but originate from malicious third parties. In addition, it is best to assume employees will, at some juncture, fall victim to phishing attacks. As such, is imperative companies maintain a phishing incident-response policy which can be implemented immediately with adequate resources to respond to a successful phishing scam. A timely and effective response to a successful phishing attack can significantly limit the impact of the attack on the organization's operations and financial health.

- **Employee Awareness and Education:** Companies should ensure their employees are educated on the significant threat posed by coronavirus-themed phishing attacks. While traditional cybersecurity defenses—such as firewalls and malware monitoring software—can effectively guard against phishing scams to some degree, the strongest defense is employee awareness. As a starting point, companies must warn employees not to provide any personal data through e-mail, and to be on high alert for coronavirus-themed cyber fraud. Companies must also educate employees on how to spot attempted phishing attacks and provide employees with best practices to follow. Key tips include being suspicious of e-mails with generic greetings and improper grammar style; never clicking on a link without first verifying the destination of the link by hovering the user's cursor over the URL to determine the link destination; and never transmitting sensitive personal or company information via e-mail.

- **Maintaining a Security-First Workforce and Work Culture:** Lastly, companies and their management should focus on regularly communicating information, tips, and best practices regarding phishing issues to all members of their workforce. Similarly, as vigilance is the key to thwarting phishing attacks, companies must consistently instill in employees the importance of remaining cognizant of the ongoing threat of phishing scams—especially during this period when the coronavirus will continue to dominate the news for the foreseeable future. With the proper amount of time and effort, companies can quickly develop a culture and mindset that maximizes employees' commitment to making cybersecurity a priority in their day-to-day activities, which in turn can play a significant role in stopping coronavirus-related phishing attacks before they wreak havoc on a company's systems and finances.

THE FINAL WORD

Vigilance and strict adherence to proper data security practices/habits are key to avoiding being on the receiving end of a coronavirus-themed phishing attack. In the event your company does experience a successful phishing attack, it must take immediate action to minimize the fallout.

If you find yourself the victim of a phishing campaign, Blank Rome's data breach incident response team is available 24/7 and can provide immediate assistance with rapid incident response and crisis management following a phishing-related data breach. And if a phishing attack ultimately results in litigation, Blank Rome's experienced, nationwide privacy class action defense team can step in and provide a robust defense to any type of breach-related litigation.

Finally, if you suspect your company may have been targeted by a phishing campaign, Blank Rome's cybersecurity and privacy professionals can assist with providing key counseling and guidance with respect to any concerns relating to potential or suspected data breaches.

For additional information, please contact:

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

Jeffrey N. Rosenthal, Philadelphia Office
Partner, Privacy Class Action Defense, Business Litigation
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