The Cybersecurity Threat of COVID-19

Insights
3.17.20

As people across the world react to the rapid spread of COVID-19, a new threat is emerging; individuals and employers face a risk from hackers trying to take advantage of the demand for information. Hackers have begun using fake government reports, health fact sheets, and tracking maps to deliver malware and harvest personal or sensitive data from people seeking out information on the coronavirus.

Multiple cybersecurity firms have identified different schemes, including cyber criminals imitating government agencies and pushing phishing emails to employees, to lure individuals into revealing sensitive information or infecting their personal and work devices with malware. Concerningly, common schemes involve imitating the World Health Organization (WHO), an HR Department, or company executives, asking employees to sign into applications that require their credentials. Proofpoint, a cybersecurity firm, identified one such phishing scheme disguised as an email supposedly sent by the WHO luring individuals to click on an attached document containing safety measures regarding the spread of the coronavirus.

As COVID-19 spreads across the globe, phishing schemes will become more widespread, and it is critical that companies adhere to appropriate data security practices to avoid falling victim to phishing attacks. Here are a few strategies employers can implement to reduce the risks posed by these attacks:

Remind Employees About the Risks of Phishing Schemes
As more employers encourage or mandate that employees work remotely, it is essential that companies warn employees about the risks associated with phishing schemes. This includes identifying employees who interact with clients, contractors, vendors, or have access to consumer and/or employee information and instructing them to be vigilant for phishing schemes aimed at obtaining sensitive information.

Employers should discourage the use of company email accounts for personal use and redistribute existing cybersecurity and data security policies that address the use of technology within the organization. It may also be prudent to educate employees on the renewed and serious threat posed by coronavirus-themed phishing attacks.

Important Steps to Take to Avoid Phishing and Hacking Schemes

1. **Pay attention to hyperlinks in emails**—Do not always trust that any link is going where it says it is; in applications such as Outlook, hover over the hyperlink to reveal the actual destination to which the link will connect. If the web address shown appears to be suspicious or unknown, do not follow the link.
2. **Do not open attachments from unknown sources**—Even with filters to flag potentially malicious attachments from arriving in inboxes, there is always the possibility of something slipping through. Avoid opening anything that is unsolicited from an unfamiliar source. Forward any suspicious emails to available resources, such as the company's IT Department or Help Desk, for evaluation.
3. **Check grammar/language**—No matter how official an email appears, if the grammar or spelling is incorrect, that should be a red flag. This is not to say that no mistakes means that it is a safe email, but if multiple words are misspelled in an email from a health organization, government, or the company's own HR department, it likely is not from a trusted source.
4. **Use common sense**—Think carefully about what the email is requesting. Would a global organization like the World Health Organization really be reaching out to you directly? Would your health provider request personal information just to provide information on COVID-19? Be cognizant of the supposed purpose behind the email.
5. **Verify with legitimate sources**—If there appears to be a legitimate issue concerning personal information that is addressed in an email, independently verify with the alleged source, whether that be the company's HR Department, a healthcare provider, or a government agency. Do not follow a link or email address contained in the email itself to verify the validity of the sender.
6. **Change password access**—Employers should require, or at least advise employees, to change their passwords every few months and at unpredictable times.
7. **When in doubt, throw it out**—If an employee has any doubts about the validity of an email, the employee simply delete it and move on.

Conclusion

While the spread of COVID-19 has reasonably caused many to seek out information from multiple sources, employers and employees must be exceedingly careful about where they receive their information. Employers should advise employees of the potential risk of these developing cyber-attacks seeking to capitalize on fears regarding COVID-19, reinforce any existing information security training and data security policies, and encourage employees to exercise discretion and remain vigilant when opening emails from unfamiliar sources. Staying ahead of cybersecurity risks is crucial to avoiding personal information or data theft.

Service Focus

Privacy and Cyber