The Valued Voice

Vol. 68, Issue 48

Wednesday, November 27, 2024

Guest Column: Don't Take the Bait: Outsmarting Today's Phishers

By Matthew Thomson, M3 Insurance (WHA's Premier Partner)

Imagine this:
You're working through your emails on a busy Monday morning when you see a message from your company's CEO, marked "Urgent." It requests you to review a confidential document before an important meeting later in the day. Without a second thought, you click the link, eager to help. But instead of opening the file, you unknowingly hand over your login credentials to cybercriminals.


Matthew Thomson

*That "urgent" request wasn't from your CEO—it was a cleverly disguised **phishing attack**, designed to exploit your trust and your time-pressured routine. Phishing schemes like this are increasingly sophisticated, and even the most cautious employee can fall victim if they're not vigilant. So, how do you stay ahead of these threats? Let's dive into how phishing works and how you can protect yourself and your business.*

Cyber criminals will stop at nothing to bait an unsuspecting victim into falling for a phishing scheme. Phishing is a social engineering attack that utilizes online messaging platforms, primarily email, to convince the victim to do something like open a malicious file, click a link where they share their login details, change the routing of a payment, or share sensitive information with the attackers. With the average person receiving over **100 emails a day,** and our heavy reliance on email communication, it's easy to act impulsively on email content without pausing to question its legitimacy.

Business Email Compromise (BEC), a rapidly growing form of email scam enabled primarily by phishing attacks, targets businesses of all sizes and industries globally, exposing them to potential losses in the billions. According to **Beazley's 2024 cyber risk prediction**, BEC incidents increased by 35% quarter over quarter in the first quarter of 2024. As seen in the graph below, the top industries impacted by BEC attacks are Professional Services, Healthcare, and Financial Institutions.

Security Awareness Training

Cyber criminals, otherwise referred to as threat actors, are constantly changing their tactics, particularly when it comes to phishing. They will use any and every trick in the book to convince the recipient that the email is legitimate. In addition, the phishing email will play on your emotions such that it gets you to act fast without thinking.

To protect your organization against phishing, one key component to the security program is security awareness training. The purpose of this training should be to create awareness of the threats and grow your organization's culture of security. An effective security awareness program must stay up to date with the latest threats and scenarios.

For example, relying on outdated scenarios like the "advance-fee fraud" or "lottery win" is no longer effective. ***Instead focusing on topics like:***

- AI enabling more believable social engineering
- Voice phishing (Vishing) or SMS Phishing (Smishing)
- Fake/fraudulent QR codes

Phishing Testing
Many organizations perform simulated phishing emails to test their employee awareness of social engineering scams. What has often been the determining factor of "success" is mostly focused on reducing the "click rate". However, if the "click rate" is anything greater than 1, that test should be considered a failure for the organization. Is this really the best way to evaluate the effectiveness of your security awareness program?

Using the Carrot instead of the Stick
When considering the intent of phishing training, should the goal be to catch employees and reprimand them for clicking on phishing emails? Or should we focus on raising their awareness and enabling them to act as a digital neighborhood watch? When re-evaluating how to measure success for a phish testing, the primary focus should be on how well employees can identify and report phishing emails and other scams. By having your employees be a "human firewall", it can allow the company's security team to proactively prevent any future teammates from falling victim to the same scam.

Effective phishing training should incorporate:

- Be able to identify the difference between a phish and spam
- Incentivize appropriate reporting of attempted phishing
- Develop a culture of awareness

What to do if you think you are a victim

- **Don't provide any information**: Exit the malicious site immediately without entering any details.
- **Disconnect from the internet**: Go offline to stop any potential malware or data theft.
- **Check for malware**: Run a malware scan on your device to detect and remove any infections.
- **Back up your data**: Use an external device to back up files after ensuring your device is malware-free.
- **Change your passwords**: On a separate device, update passwords for any accounts at risk.
- **Report the phishing link**: Report the scam to protect others after confirming your device is secure.

Key Takeaways
For a security awareness training and phishing testing program to be truly successful, it requires support from every level of the organization. By clearly defining the program's goals and regularly updating it to address evolving threats, you can ensure that your security awareness efforts effectively contribute to keeping your organization cyber-safe.

Reach out to your **M3 Client Executive** to discuss your current protection for your organization and to learn more about cybersecurity risk management.

Other Articles in this Issue