Education is Key to Avoiding Sophisticated Cyber Crime

Urgent message: As digital communication becomes more integral to our daily lives and job functions, cybercriminals are increasingly employing nefarious social engineering tactics like "phishing" to steal valuable information. Urgent care employees must be trained to recognize phishing scams, and how to effectively safeguard themselves and their organizations from attack.

ALAN A. AYERS, MBA, MAcc

As society becomes more 24/7 connected, most of our personal and professional lives reside online. The tools we use to work and play—not to mention our financial accounts—have become increasingly digital, directly accessible from the palm of our hands through our internet-enabled devices.

This of course opens us up to more online scams and fraud than ever before, as opportunistic cybercriminals continue to utilize tried-and-true methods to gain access to our information. And when these cybercrooks fail to steal our data through their brute-force hacking methods, they're now employing a more indirect and sophisticated method: social engineering.

What is Social Engineering?

Social engineering foregoes the use of typical digital hacking tools, and instead relies on the manipulation and exploitation of human psychology to gain access to personal information, financial data, computer networks, and online platforms. So rather than using, say, a computer program to scan for network and software vulnerabilities, scammers will simply assume the guise of a trusted business entity or individual, and deceive their target. Whether it be passwords, bank and credit card numbers, account information, login credentials, or other sensitive data, cybercriminals continue to develop social engineering ruses—some simple, others sophisticated—to prey upon unsuspecting businesses and individuals. Here, we'll briefly look at social engineering tactics and examine how they're carried out, as well as protective measures to avoid falling victim.

Alan A. Ayers, MBA, MAcc is Chief Executive Officer of Velocity Urgent Care and is Practice Management Editor of *The Journal of Urgent Care Medicine*.

Phishing

Phishing is any attempt to manipulate a target into sharing sensitive information such as user names and passwords, bank routing numbers, Social Security numbers, account PINs and credit card details. Phishing attacks work when the attacker assumes the identity of a trusted entity like a bank, well-known company, or other trustworthy source.

Phishing attacks are typically impersonal and sent to millions of random email addresses. They generally employ a "spoofed" or forged email address that appears to have originated from the purported source, when in fact it's from the scammer. Text messages and IM accounts can also be vehicles for phishing scams. The sender will often implore the target to click a link within the message, which is where the trouble begins. Clicking the link can trigger the installation of malware on the device (used to capture account information, monitor network traffic, or remotely control the PC) or send the target to a fraudulent URL to enter sensitive data. The hope is that by sending out mass mailings to millions of potential targets, a small percentage will take the bait and fall into the trap.

So how exactly do phishing targets get fooled? First, the

messages typically contain trusted logos, familiar-looking brand color schemes, and links to familiar websites. Additionally, the phony messages play off the human emotions of greed, fear, loss, gain, and urgency: "Click this link to claim your requested funds now" or "Urgent, your account has been compromised and you must change your password immediately." And even though many mass-mailed phishing messages feature mistakes and grammatical errors, most people don't catch on until it's too late. It's our natural inclination to trust, avoid loss, and receive gains that cybercriminals bank on. And it works, to the tune of billions of dollars in losses each year.

Spear Phishing

Unlike phishing, which is a random and impersonal attack sent to millions of potential targets, spear phishing is aimed at specific individuals or groups. Spear phishing requires scammers to spend time and effort to research their targets in order to gain access to personal details. And as much of our information these days resides online, sites such as Facebook, Twitter, and LinkedIn can provide cybercriminals a treasure trove of information. Once the scammer knows the victim's location, place of employment, friends and colleagues, social networks, and recent online purchases, they set their trap in motion.

Originating from what appears to be a trusted individual or company the target does business with, the spear phishing attack appears legitimate and authentic. These messages contain details that a random scammer couldn't possibly know, making them very convincing. Hence, the target is more likely to click the embedded link or open the attachment. The messages also rely on urgency, offering compelling, personalized explanations as to why passwords, account numbers, and PINs are needed immediately.

Once the information is stolen, the scammers can access and empty bank accounts or open credit accounts in the victim's name. They can apply for loans or use the victim's Social Security number to create a new identity. And since most people use a single password (or some variation of it) for all their accounts, a compromised password essentially gives a cybercriminal the keys to the kingdom.

CEO Fraud

CEO fraud, also known as business email compromise (BEC) or whaling, is similar to spear phishing, but with a critical difference: Rather than posing as a trusted friend or business, the scammer assumes the identity of a high-ranking or influential member of a person's business organization. The aim is to acquire sensitive information or trick the target into completing a wire transfer at the behest of the "CEO."

First, social engineering tactics are employed to compromise a company email address, allowing the scammer to send a phony message from a bigwig, to lower-ranking employees—typically those with access to company finances. In this case, the scammer is still relying on personal details common to spear phishing attacks, but with the added knowledge that the employee will be reluctant to not carry out the boss's orders.

To pull off a fraud of this magnitude, the scammer will research and gather publicly available information about the company: its corporate structure, job titles, and employees in key positions. Then the scammer will craft a convincing email from the "boss"—complete with company logos and a perfectly replicated corporate signature—with just enough detail to sound convincing, but not enough to reveal themselves to be frauds. The "boss" will, for example, need a wire transfer completed outside of normal business hours, and outside of normal channels and procedures. The boss will also be busy, unavailable by phone, and need the request handled urgently. And if the boss's email is convincing enough, the recipient will be hesitant to question their instructions; the FBI reports that over $12 billion was lost between October 2013 and May 2018 due to BEC scams, attesting to how compelling these attacks are.

Awareness and Education

Defending against these attacks begins with awareness and education. Consider the following strategies for protecting yourself and your organization.

Defense Against Phishing and Spear Phishing

- **Be skeptical and suspicious.** Be wary of any unsolicited messages, regardless of the source. Rather than clicking on a link, launch your browser and go to the URL directly to investigate if it's a legitimate message. Also, hover your mouse over a link to check the URL destination. The URL should match the link's anchor text; if it doesn't, it's likely a fraudulent or malicious transmission.
- **Think first, act second.** Scammers bank on you acting impulsively. So when encountering a message that purports to be urgent, time-sensitive, or high-pressure, slow down and assess the entire context of the request before acting.
- **Watch for email hacking.** Even if an email appears to come from a friend, family member, or colleague, that doesn't guarantee that their account wasn't hacked. So, regard odd-looking messages that contain links, downloads, and attachments with suspicion, and double-check with the sender before clicking.
- **Ignore foreign offers.** These are almost always fake. Any legitimate organization who claims you've won a sweepstakes or lottery would contact you directly by phone.

Defense Against CEO Fraud

- **Implement company-wide training and awareness campaigns.** Everyone in your organization, particularly those in sales, IT, HR, and finance should be trained on how to guard against CEO fraud. Training should include examples of real-

Table 1. Examples of Spear Phishing and CEO Fraud Messages

- "I'm in a meeting, but I have something urgent I need you to take care of for me...."
- "This invoice needs to be paid immediately so the contractor can start work today. Please see the attached wiring instructions."
- "I'm on a call with the insurance provider rep now. Can you please reply immediately with a copy of Mary Smith's ID and insurance card?"
- "Your credit card at the hotel for tomorrow night was declined. Can you verify the number or provide a new card to use?"

life CEO fraud cases, how to spot spoofed email addresses, strict protocols pertaining to financial transactions and sensitive data, who to turn to when in doubt, and proper procedures for handling downloads, attachments, and links.

- **Consider two-factor authentication (2FA) for highly sensitive and restricted accounts.** 2FA requires not only the correct login credentials, but a physical device, such as smartphone or security token to complete the login process. This way, even if a password is compromised, the scammer is dead in the water without the accompanying physical device.
- **Robust password management.** All employees should be required to use passwords that include letters, numbers, and symbols; these should also be changed every few months.

Conclusion

Phishing, spear phishing, and CEO fraud are on the rise, with successful attacks costing companies their money and reputations, while leaving ruined careers in its wake. Hence, the onus is on company leaders to educate their workforces about how cybercriminals exploit social engineering to steal sensitive information. Combine this awareness and education with a robust training program on how employees can detect and thwart these scams, and you can operate with the piece of mind and security that your organization is well-protected from a very real threat. ■