An official website of the United States government

October 2024 OCR Cybersecurity Newsletter

Social Engineering: Searching for Your Weakest Link

Cyber threats targeting individuals often take the form of social engineering, where attackers attempt to convince someone to engage in actions or reveal information that can put themselves and their organizations at risk. Social engineering is an attempt to trick someone into revealing information (*e.g.,* a password) that can be used to attack systems or networks or taking an action (*e.g.,* clicking a link, opening a document).[1] Between 2019 and 2023 large breaches (*i.e.*, breaches of unsecured protected health information (PHI) involving 500 or more individuals) reported to the HHS Office for Civil Rights (OCR) as a result of hacking or IT incidents increased 89%.[2] Cybersecurity is often framed solely as a technology issue where protection can be provided by simply purchasing the newest security tool. But according to a recent report, 68% of breaches involved attacks on humans, not technology.[3]

Social engineering attackers attempt to manipulate their targets by using an ever-evolving arsenal of technology and deceit. Such attacks can take many forms including emails, texts, calls, or even videos that appear to be from trusted individuals, companies, or institutions. Using such manipulative techniques can often bring an attacker quicker and easier success than attempting to breach an organization's cyber defenses. In short, social engineering is so prevalent because it works. The end game for social engineering attackers is varied. Attackers could be seeking money, to disrupt an organization's operations, or to gain access to sensitive information. This newsletter discusses common social engineering threats and how individuals and HIPAA regulated entities can defend against them.

Phishing is one of the most frequent social engineering attacks. A phishing attack attempts to trick individuals into providing sensitive information electronically. This is most often accomplished through the use of email where the attacker sends an email purporting to be from a trustworthy source, for example, an organization's HR department, a large retailer, a delivery service, or a financial institution. The attacker appears to provide a legitimate reason to click a link in the email. For instance, a phishing email that claims that you have been added to a new office communication or collaboration group, such as a Microsoft Teams Channel. When the employee clicks the link, they are taken to a forged website that looks nearly identical to the website they expect to see. At the forged website, they are asked to enter their username and password to validate their identity. Once they have provided their credentials the attacker can now use those credentials against the individual's organization and information systems.

The HIPAA Security Rule requires that HIPAA covered entities[4] and business associates[5] (regulated entities) identify and protect against reasonably anticipated threats or hazards to the security or integrity of electronic (ePHI),[6] but attackers have learned that successful cyber-attacks against an employee may be easier than attacking an organization directly. For this reason, a phishing email targeting an organization may not only be sent to an employee's work email but may also be sent to their personal email. If successful, the phishing attack then compromises the employee's personal device which may be used to access work emails and is often also a method of authentication into their employer's network. In another scenario, if

an employee accessing their personal email from their work device clicks on a malicious link from a phishing email, malicious software could be installed on the work device and potentially spread across the organization.

Smishing is a form of social engineering that uses Short Message Service (SMS) messaging (*i.e.*, text messages) to trick someone into downloading malicious software or clicking on a link to a malicious website to get the text message recipient to share sensitive information such as their username and password. Typically, the individual receives a message stating that they need to take some immediate action or face a negative consequence. For instance, the message may come from a bank asking to confirm a large withdrawal or it could pretend to be from your employer asking you to reset your password to access your work email. The message will include a link to a website or may even include a phone number to call. The attacker's goal is to have the individual click on a link that directs them to a malicious website or to call the number listed where the attackers can attempt to manipulate the individual.

Some tips to avoid a successful smishing or phishing attack include:

- Be suspicious of links sent via SMS messaging or emails that are not expected. While many may be legitimate, there are many more that are not. An individual should mistrust messages offering prizes or deals too good to be true.
- Do not call a number sent through an SMS message or unexpected email, especially when such messages or emails attempt to convey a sense of urgency. Instead, lookup the number to the organization supposedly contacting you and call to confirm the information.
- Never provide sensitive information such as usernames, passwords, or personally identifiable information. Instead, call the organization requesting such information using a known good phone number (such as the organization's customer support number from their website) to verify why they need your sensitive information. Do not rely on a phone number provided in the SMS message or email as those could belong to the attacker.

Baiting is another social engineering attack that is very similar to smishing and phishing in that it uses electronic means to tempt an individual into acting in a way they know they should not. Baiting involves an enticement or bait to lure an

individual in. Most often this takes the form of something valuable. This enticement may not come to an individual's work email but rather through their personal email and often involves winning a prize or being selected for something of value. To claim the prize, the individual is typically provided a link to click on. This link then installs malicious software on their computer or phone, or it takes them to a website that installs the malicious software. This may not seem like a threat to an individual's organization since it infected their personal device or email, but people may use their personal devices as a second form of authentication when using multi-factor authentication or a person, if permitted, may access their personal email from a work device. By compromising an individual's personal device or email, the attackers are now one step closer to bypassing the security controls that the organization uses to protect itself and secure sensitive information such as ePHI.

Another form of baiting involves physically leaving something laying around, such as a storage device in a common area like a lobby or parking lot. This form of baiting seeks to exploit someone's curiosity. For example, leaving a USB drive laying on the ground in an organization's parking lot is relying on someone's curiosity to pick it up and plug it into a computer to access the stored information. However, when the USB is plugged in, malicious software is installed. Plugging a USB into a workstation at work could infect their organization's network and compromise sensitive information such as ePHI. Doing this at home could compromise the individual's personal computer which could be used to attack other computers or for remote workers, it could remotely compromise the organization they work for.

Avoiding baiting requires being skeptical of offers that appear too good to be true and of unattended devices. If the offer seems too good or one doesn't recall entering a contest to begin with, they can always search for it online. A quick Google search can often identify the offer as a known threat. Even if a person only falls for the initial message the attackers will then begin trying to manipulate the individual. If a person fails to recognize the initial lure they should still never provide their credentials or click on links from websites that they have not verified.

Deepfakes[7]: Artificial intelligence (AI) technology has advanced to allow for lower cost and lower effort manipulation of video, photos, and audio. These manipulations can replace faces in a video and even synthesize voices in real time. A deepfake is when an individual believes they are communicating with a trustworthy source either

over the phone or via video. It can be hard to detect a deepfake and even harder not to trust what we believe we are seeing with our own eyes. Deepfakes are not limited to manipulated videos. Deepfake technology can be also used to simulate the voice of a trusted individual such as a supervisor or executive in your organization. This threat is called AI cloning and it can apply to a person's voice as well as videos of people. Combining a simulated voice with a spoofed phone number, an attacker could convincingly imitate a CEO making a help desk request to reset their password or to make changes to the network security settings to provide greater access to sensitive data such as ePHI. As technology improves it will become harder to detect deepfakes, but for now there are a few signs to look for.

Some key signs one can look for to discover a deepfake include:[8]

- Inconsistent eye blinking. If a person's face seems slightly off because they don't blink, or they blink too often it could be a sign of a deepfake.
- Facial features lack a clear definition, seem to be melted, or are too smooth.
- A person's mouth movements are not quite synced up with the words they are saying.
- Unnatural skin colorizations.
- Abnormal boundary between hair and background.

If one suspects they are experiencing a deepfake attack, they should ask questions where the answers are not publicly available and that only the real person should know. If still unsure, disconnect and call the person back or text them using phone numbers known to be correct to confirm that the person was real.

The HIPAA Security Rule includes many provisions that can aid regulated entities in preventing or mitigating threats posed by social engineering. The Security Rule requires regulated entities to "[e]nsure the confidentiality, integrity, and availability of all [ePHI] the [regulated entity] creates, receives, maintains, or transmits"[9] and also requires that they "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of [ePHI]."[10] All of the social engineering threats discussed in this newsletter are reasonably anticipated threats to a regulated entity's ePHI and should be considered when regulated entities implement security measures to protect their ePHI.

Informing workforce members about new and emerging social engineering threats can be incorporated into a regulated entity's HIPAA Security Rule obligation to implement a security awareness and training program.[11] Sending simulated phishing emails to test workforce member knowledge of how to identify phishing emails is an excellent method of providing security reminders, another provision of the Security Rule.[12] A well-educated workface is the first line, and often the best line, of defense to halt a cyber-attack before it starts.

However, should a social engineering or other cyber-attack be successful, HIPAA regulated entities are also required to have appropriate safeguards in place that ensure the confidentiality, integrity, and availability of their ePHI. This includes technical safeguards to protect the integrity of ePHI from improper alteration or destruction[13] and allowing access to ePHI to only those granted access rights to such ePHI.[14] Technical solutions that can help mitigate the threat of social engineering threats can include anti-phishing technologies, verifying that received emails do not come from known malicious sites, scanning web links or attachments, and using machine learning or behavioral analysis to detect and prevent potential threats. Granular role-based access, network segmentation, and strict access limits to privileged accounts and administrative tools are ways regulated entities can control and limit access to ePHI.

Regulated entities are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of their ePHI.[15] The results of this risk analysis should inform regulated entities' decisions on their implementation of appropriate administrative, physical, and technical safeguards to protect ePHI. The risk analysis must consider potential risks and vulnerabilities to all of the ePHI a regulated entity holds.[16] Regulated entities should also consider that risks and vulnerabilities to ePHI may change as ePHI is processed and flows within their environment. A comprehensive technology asset inventory (*e.g.*, hardware and software) and ePHI data flow diagrams are valuable tools that can assist regulated entities as they conduct an accurate and thorough risk analysis.

Conclusion

When it comes to cybersecurity, the concept of “trust no one” applies to both businesses and individuals. Attackers have learned how to convincingly imitate our loved ones and our business partners, meaning that nothing can be assumed or taken at face value. Attackers continue to refine their manipulation through social engineering trade craft. All of these threats have a common theme; they all attempt to convince an individual to do something they would not otherwise do normally, or to provide details such as credentials someplace other than where they should be used.

Educating workforce members on these attacks is essential when it comes to an individual’s ability to identify and potentially halt social engineering attacks before they start. Such knowledge is powerful not only to protect individuals in their personal online activities, but also by extension an individual’s employer. This is especially important in the current environment where work is taken home on laptops, smart phones, and through remote work.

Additional Resources:

HHS Social Engineering Attacks Targeting the HPH Sector

- https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf - PDF <https://www.hhs.gov/sites/default/files/social-engineering-targeting-the-hph-sector-tlpclear.pdf>

HHS 405(d) Knowledge on Demand: Social Engineering:

- https://405d.hhs.gov/kod/five-threats/social-engineering <https://405d.hhs.gov/kod/five-threats/social-engineering>

HHS/FBI Joint Social Engineering Advisory:

- https://www.ic3.gov/Media/News/2024/240624.pdf - PDF <https://www.ic3.gov/media/news/2024/240624.pdf>

GAO Science & Tech Spotlight: Deepfakes:

- https://www.gao.gov/assets/gao-20-379sp.pdf - PDF <https://www.gao.gov/assets/gao-20-379sp.pdf>

CISA Avoiding Social Engineering and Phishing Attacks

- https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks <https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>

HHS OCR Cybersecurity Newsletter: Defending Against Common Cyber-Attacks:

- https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html </hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html>

* This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion.

Endnotes

[1] See https://405d.hhs.gov/Documents/405d-infection-series-social-engineering-poster.pdf - PDF <https://405d.hhs.gov/documents/405d-infection-series-social-engineering-poster.pdf> .

[2] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf> .

[3] Verizon. *2024 Data Breach Investigations Report.* (May 2024, p. 8). Available at https://www.verizon.com/business/en-au/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf - PDF <https://www.verizon.com/business/en-au/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf> .

[4] *See* 45 CFR 160.103 (definition of "Covered entity").

[5] *See* 45 CFR 160.103 (definition of "Business associate").

[6] *See* 45 CFR 164.306(a)(2).

[7] "A deepfake is a video, photo, or audio recording that seems real but has been manipulated with AI. The underlying technology can replace faces, manipulate facial expressions, synthesize faces, and synthesize speech. Deep fakes can depict someone appearing to say or do something that they in fact never said or did." *See* Government Accountability Office. *Science & Tech Spotlight: Deepfakes.* (Feb. 2024). Available at https://www.gao.gov/assets/gao-20-379sp.pdf - PDF <https://www.gao.gov/assets/gao-20-379sp.pdf> .

[8] *See* Government Accountability Office. *Science & Tech Spotlight: Combating Deepfakes.* (Mar. 2024). Available at https://www.gao.gov/products/gao-24-107292 <https://www.gao.gov/products/gao-24-107292> .

[9] 45 CFR 164.306(a)(1).

[10] 45 CFR 164.306(a)(3).

[11] *See* 45 CFR 164.308(a)(5)(i).

[12] *See* 45 CFR 164.308(a)(5)(ii)(A).

[13] *See* 45 CFR 164.312(c)(1).

[14] *See* 45 CFR 164.312(a)(1).

[15] *See* 45 CFR 164.308(a)(1)(ii)(A).

[16] *See* 45 CFR 164.306(a)(1).

Content created by Office for Civil Rights (OCR)
Content last reviewed October 25, 2024