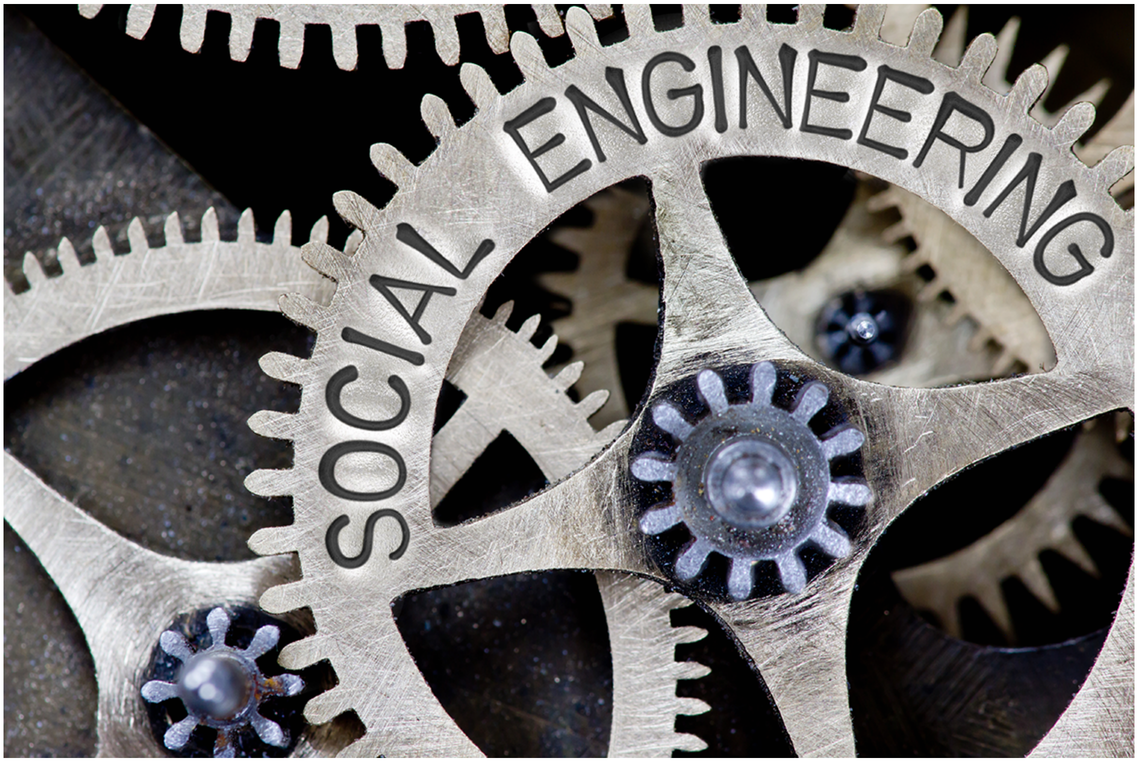
Social Engineering Took Down Giants. Don’t Let It Take You Down, too.



By Rana McSpadden, FACMPE

In September 2023, MGM Resorts International and Caesars Entertainment reported they were victims of a cyberattack. The attack disrupted operations for multiple MGM properties for an extended period of time and ultimately cost the company an estimated $100 million [1]. Caesars Entertainment paid $15 million of the hackers' original $30 million demand to avoid system disruption. In these attacks, hackers stole customers' personal information, such as names, Social Security numbers, and driver's license numbers. These companies take security seriously, so how did hackers access their systems in the first place? They did it through social engineering. There are numerous social engineering tactics but here hackers used information gleaned from LinkedIn to impersonate company employees, call the IT helpdesk, and trick them into providing system access[2].

Would this tactic work in healthcare? It already has. On January 12, 2024, the American

Hospital Association (AHA) reported on a "validated IT help desk social engineering scheme that uses the stolen identity of revenue cycle employees or employees in other sensitive financial roles." [3] Much like the cyberattacks on MGM and Caesars, hackers impersonated hospital employees to trick IT staff into providing user login information. They had enough information on the employee to provide answers to security questions. Once the helpdesk confirmed this information, the hacker would ask to change the password and register a new device, such as a cell phone. By doing so, the new device could be used to bypass multi-factor authentication (MFA). After the hacker gained access to the employee's email and login, they would change payment instructions for their payment processors and have funds redirected to a fraudulent bank account.

Regardless of how basic or sophisticated the cybersecurity program a practice has in place to prevent a cyberattack, social engineering bypasses all of this by exploiting the human factor. There is no way to 100% prevent a cyberattack caused by social engineering, but practices can certainly reduce the risk by educating staff on what to watch for with different types of social engineering.

Types of Social Engineering

The most common form of social engineering is phishing. Hackers send victims fraudulent communication, impersonating legitimate individuals or organizations to collect sensitive information, such as passwords and other personal data[4]. Because the communication looks like it comes from a legitimate source, links embedded in the communication take victims to fake websites used to , download malware or collect login information and other personal data. Email is the most common form of phishing. Some signs to watch for include poor grammar, odd-looking URLs, and requests for personal information[4]. However, hackers are increasingly utilizing generative AI technology, such as ChatGPT, so some warning signs of phishing emails, such as spelling mistakes or poor grammar, are becoming less common.

Phishing by phone, or vishing, is another form of phishing. This is the form of phishing used by the hackers of MGM, Caesars, and the hospital noted by the AHA article referenced earlier.   With vishing, hackers call into an organization and impersonate an employee, IT provider, or other vendor to gain login information or access to the system. Once hackers gain access, they can steal information and/or load malware or ransomware into the system for further exploitation. To prevent vishing, be cautious of unsolicited calls, especially from vendors. Confirm the caller's identity by calling the number the practice has on file for the individual (if claiming to be an employee) or company (if claiming to be a vendor). Caller ID isn’t always trustworthy, as scammers can spoof caller ID to show a legitimate number[5], which is why it is essential to call the number on file rather than rely on caller ID.

Smishing, or phishing by text, is the third form of phishing. Like phishing by email, victims are sent a text, generally with a link to a fraudulent website, to collect personal information, or download malware to the device. Texts may claim to be from a bank, credit card, or delivery service, such as USPS[6]. If this sort of text is received, avoid clicking any links and call financial institutions using the phone number on the back of your credit or bank card rather than using any phone number included in the text.

Phishing and the Office for Civil Rights

Patient data breaches from phishing cyberattacks can result in financial penalties imposed by the government. On December 7, 2023, the Office for Civil Rights (OCR) announced its first settlement of a breach caused by a phishing attack[7]. Lafourche Medical Group of Louisiana notified the OCR on May 28, 2021, of a breach of 34,862 individuals' protected health information when hackers using a phishing attack accessed an employee's email account containing protected health information. The settlement requires Lafourche Medical Group to pay the OCR $480,000 and go under a corrective action plan for two years.

Closing Thoughts

Whether your group is large or small, social engineering and phishing are a threat. Utilizing the services of professional and qualified IT vendors or staff is important. Often, they can customize a cyber program to meet the budget needs of a practice. Educating staff on what to watch for and their responsibilities to prevent cyberattacks is vital as well. SVMIC has a new Compliance Center, which includes new cybersecurity education, along with other useful compliance tools. Additionally, consider testing staff on their ability to spot a phishing email. Companies such as KnowBe4 have testing resources (sometimes free) available.

With the ever-increasing risk of a cyber-attack, it has become a best practice for organizations to thoroughly evaluate their electronic systems for potential security breaches. Staff education is also essential so that personnel understand how their actions might inadvertently provide access to a bad actor. Work with your administration and information systems personnel to assess your system and implement appropriate safeguards as well as develop a comprehensive staff education plan. Resources are available to policyholders in SVMIC's cybersecurity center found HERE on the Vantage® policyholder portal. SVMIC also recommends you talk with your professional business insurance broker to evaluate insurance coverage and determine a level of cyber coverage with which you feel comfortable in the event of a cyber incident.

If you have questions about cybersecurity or access to these resources, call 800-342-2239 or email ContactSVMIC@svmic.com.

If you experience a cybersecurity or other HIPAA-related incident, contact SVMIC as soon as possible by calling 800-342-2239 and asking to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage® account here.

[1]https://www.nbcnews.com/business/business-news/cyberattack-cost-mgm-resorts-100-million-las-vegas-company-says-rcna119138

[2] https://www.forbes.com/sites/noahbarsky/2023/09/20/caesars-and-mgm-boards-lose-cybersecurity-gambles/?sh=279c17e64463

[3] https://www.aha.org/news/headline/2024-01-12-hospital-it-help-desks-targeted-sophisticated-social-engineering-schemes

[4] https://us.norton.com/blog/online-scams/what-is-phishing

[5] https://us.norton.com/blog/online-scams/vishing

[6] https://www.forbes.com/advisor/business/what-is-smishing/

[7] https://www.hhs.gov/about/news/2023/12/07/hhs-office-for-civil-rights-settles-first-ever-phishing-cyber-attack-investigation.html

The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.