INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

Phishing Prevention in Healthcare

Institute for Homeland Security

Sam Houston State University

Janis Warner

Kamphol Wipawayangkool

Abstract

Phishing is currently one of the most common cybercrimes. To trick people into sharing personal information or installing malicious software, hackers pretend to have legitimate identities. The healthcare sector is particularly vulnerable because there is so much sensitive data involved, such as financial and medical records. Patients may be at risk if their information is exposed, or healthcare systems are interrupted. Thus, to protect everyone in healthcare from potential disasters, phishing prevention strategies are key. This research provides an overview of phishing focusing on Texas hospitals' vulnerabilities and current practices. Recommendations from three IT security experts are outlined as well as best practices for phishing prevention. Finally, an introduction to and an example of a benchmarking project is provided aimed at improving IT security for phishing.

Keywords: Phishing, Healthcare, Texas hospitals, Benchmarking

Background

Phishing is an attempt to hook possible victims with "bait", i.e. something that the targeted receiver will view as authentic and will act on what was received in a way that the hacker gains access to a system. Phishing can be done using email, text messages, phone calls, and social media, but emails are the most prevalent. An infamous case in 1996 was attackers pretending to be America Online (AOL) employees duped users into providing their login information (Phishing.org, n.d.). Since this incident, phishing tactics have evolved in complexity.

There are a variety of phishing attacks. Deceptive phishing, the most common, refers to hackers posing as legitimate companies to steal personal information. Spear phishing aims at specific people or organizations to gain access using detailed personal information to make the message even more convincing. Whaling, a form of spear phishing, targets high-profile individuals such as CEOs. Clone phishing sends an email that looks identical to a genuine one with malicious links or attachments. Pharming redirects users from a legitimate website to a fake one, typically through DNS poisoning or host file manipulation.

Phishing is a serious threat as it is effective and inexpensive to act. In 2023 alone, the Anti-Phishing Working Group found more than five million scams (APWG, 2023). Furthermore, it was the most used attack method in 2022, according to Verizon Data Breach Investigations (Verizon, 2022).

Phishing attacks can cause severe damage. For instance, between 2013 and 2015, Google and Facebook paid a man pretending to be a hardware company for fake invoices over $100 million (Ikeda, 2019). In 2015, executives at Ubiquiti Networks were the victims of a spear phishing attack. This led to hackers using the executives' emails to ask the employees for international money transfers, resulting in a loss of $46.7 million (Goldman, 2015). In 2014, the North Korean cybercrime group Lazarus tricked Sony Pictures Entertainment with phishing emails, resulting in leaks of unreleased films, confidential emails, and employees' personal information (Savov, 2015). In 2017, as a DocuSign system was hacked, its customers received phishing emails with forged documents loaded with malware (Cluley, 2017).

Over time, phishing tactics have evolved to incorporate more social engineering techniques and exploit human emotions in current events or crises. For example, there was a rise in phishing scams pretending to be health officials during the COVID-19 pandemic.

Phishing in Healthcare

The healthcare industry in the United States has become a top target of phishing attacks, because of the following reasons. First, healthcare-related information has high value in the black market. Second, the entire sector is very dependent on digital technology.

There is a large amount of sensitive information stored in healthcare organizations. Hackers can not only sell information such as patient records, insurance details, and financial data online but also steal identities. For example, hackers can pretend to be well-known healthcare providers or insurance companies and send emails asking victims to share their private information. If victims fall for it, hackers can sell the information on the dark web or use it for medical fraud.

Because healthcare operations heavily rely on information technology, phishing attacks can compromise patient care. Phishing emails may also include ransomware which attacks mission critical systems, encrypts them, and demands payment for the decryption key. For example, the National Health Service (NHS) in the UK was struck by the WannaCry ransomware in 2017 (Ghafur et al., 2019). As a result, appointments, emergency cases, and treatments were delayed or canceled altogether.

Digital transformation, including remote work and telehealth, accelerated by the COVID-19 pandemic has made the healthcare sector even more susceptible to phishing. Taking advantage of this trend, hackers attempt to send phishing emails with COVID-19 updates or telehealth appointments. These scams attempt to obtain personal information or to install malware.

U.S. healthcare organizations have also been impacted by phishing attacks. For example, Anthem Inc., one of the largest health insurance companies in the U.S., was hijacked by a phishing attack in 2015. This data breach exposed personal information of over 79 million people, including names, birthdays, medical IDs, social security numbers, and email addresses. To resolve the lawsuits, a $115 million settlement was reached (Bloomberg, 2017). Similarly, a phishing attack on American Medical Collection Agency (AMCA) resulted in a loss of personal and financial information of over 21 million patients (Davis, 2021). Moreover, this attack affected its clients such as Quest Diagnostics and LabCorp. In 2015, a phishing attack stole over 4.5 million patients' information from UCLA Health (Pagliery, 2015). This case also led to lawsuits and large investments in cybersecurity improvement. Finally, in 2020, UCSF Medical School had to pay $1.14 million to phishing hackers to decrypt critical research data which also included COVID-19 treatment development (Tidy, 2020).

Phishing Practices in Texas Hospitals

In Texas, hospitals have been active in looking for ways to tackle phishing. For example, UT Southwestern Medical Center in Dallas has initiated an information security management strategy which includes security awareness training and phishing simulations. Employees can also report suspicious emails with the PhishAlarm button in Outlook (UT Southwestern Medical Center, 2023). The program aims to educate employees on what consequences phishing and ransomware attacks can cause, such as loss of data, interrupted services, compromised patient safety, and brand damage.

A collaboration among organizations has also been established. The Texas Hospital Association (THA) is working with hospitals in Texas to improve their cybersecurity practices (Texas Hospital Association, n.d.). In this partnership, the organizations that come from both healthcare and cybersecurity will share data, best practices, and solutions for handling cyber threats.

A recent massive security breach that highlights how critical but weak data protection in healthcare is the HCA Healthcare system incident. At least 11 million patients' information such as names, contact information, and visit details were stolen to sell on a dark web forum (Ivanova, 2023).

Insights from Information Security Experts

Phishing attacks present a persistent and evolving threat to the healthcare sector, necessitating a multifaceted defense strategy. Insights gathered from interviews with three information security experts: 1) Mary E. Dickerson, Associate Vice President and Chief Information Security Officer at UTHealth Houston, 2) Ray Jay Yepes, Chief Information Risk Officer at the North Carolina Department of Health and Human Services, and 3) Monty St John, Senior Director of Security Research at Apollo Information Systems reveal comprehensive approaches that combine technical defenses, human factors, and organizational collaboration to mitigate these risks effectively.

Building a Dedicated and Intelligent Team: A specialized team focusing on phishing is essential. This team should be capable of not only addressing immediate threats but also conducting proactive intelligence gathering, including monitoring activities on the dark web. Understanding what information attackers already have or can easily obtain can significantly enhance defense strategies.

Interactive and Rewarding Training Programs: Employee training should be engaging and interactive. Simulated phishing campaigns, where employees participate in team competitions, can make learning about phishing fun and competitive. Incentives such as paid time off (PTO) for successful identification of phishing attempts can drive participation and attention. This approach has proven to be very effective in increasing awareness and vigilance among staff.

Focus on Social Engineering: Understanding the social engineering tactics used by attackers is crucial. Communication should extend beyond technological defenses to include executives and staff, educating them about how social engineering exploits human vulnerabilities. Using game theory to incentivize training and analyzing why certain sectors are targeted more frequently can provide deeper insights into phishing dynamics.

Analyzing Attraction Metrics and Decision Models: Examining why criminals choose specific targets can help in developing more targeted defenses. For example, some organizations are more vulnerable due to the availability of public data. By understanding these dynamics, healthcare organizations can better anticipate and mitigate phishing risks.

Engaging in Hacking Training: Participating in hacking training sessions to understand the tactics and techniques used by cybercriminals can provide invaluable insights. This knowledge helps in developing robust countermeasures and staying ahead of evolving threats.

Tailored Approaches and Partnerships: Phishing attacks manifest differently across sectors. For example, in healthcare, attackers may use more focused tactics, leveraging organizational charts and public information. Therefore, a tailored approach that recognizes these differences is essential. Viewing security as a partnership between the Information Security team and users rather than imposing punitive measures fosters a more supportive and collaborative security culture.

Continuous Education and Training: Continuous and adaptive training programs are vital. Rather than relying solely on challenging phishing simulations, which can demoralize staff,

incorporating regular, practical training sessions can keep employees informed and prepared. Education should be a continuous process, reinforcing good practices and updating staff on the latest phishing tactics.

Incentives and Cultural Change: Creating a culture of security awareness requires both education and motivation. Incentives for good security practices and recognition of employees' efforts can help in building a proactive security culture. Engaging employees in a positive manner, where their role in cybersecurity is acknowledged and rewarded, significantly enhances their participation and vigilance.

The insights from these information security experts highlight the importance of a comprehensive and human-centric approach to phishing prevention in healthcare.

Best Practices for Phishing Prevention

Clearly, healthcare organizations must implement comprehensive security strategies to handle phishing. These strategies involve employee training, technological defenses, incident response planning, and adherence to regulatory requirements.

Employee Training and Awareness

- Regular training programs are essential to help staff recognize phishing attempts and understand the importance of following security protocols. Training should include real-world examples and best practices for identifying and responding to phishing emails.

- Simulated phishing exercises can reinforce training and improve awareness by providing employees with hands-on experience in spotting and reporting phishing attempts.

- Creating a culture of security awareness within the organization helps ensure that employees remain vigilant and proactive in their defense against phishing attacks.

Technological Defenses

- Email Filtering and Security Software: Implementing advanced email filtering solutions can detect and block phishing emails before they reach employees' inboxes. Endpoint security software can identify and neutralize malware, reducing the risk of infection.

- Multi-Factor Authentication (MFA): Using MFA adds an extra layer of security, making it more difficult for attackers to gain access even if they obtain login credentials. This is especially critical for accessing sensitive systems and data.

- Secure Communication Channels: Ensuring that all communications within the organization are secure can help prevent phishing attacks that target internal messaging systems.

Incident Response Planning

- Developing and regularly updating incident response plans ensures that healthcare organizations can quickly and effectively respond to phishing attacks, minimizing damage and downtime. This includes having clear protocols for reporting and managing phishing incidents.

- Conducting regular security audits and penetration testing helps identify vulnerabilities and ensure that security measures are up-to-date and effective.

Regulatory Compliance and Policies

- Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) is crucial for protecting patient data. Healthcare organizations must ensure that their security practices meet or exceed regulatory requirements.

- Establishing clear policies and procedures for handling sensitive information can help prevent unauthorized access and reduce the risk of data breaches.

In addition, to further strengthen their defenses, healthcare organizations can benefit from adopting benchmarking practices. Benchmarking allows organizations to compare their cybersecurity strategies and outcomes with those of their peers, fostering an environment of continuous improvement and innovation.

Benchmarking – A Preventative Weapon Against Phishing

"The goal of benchmarking is continuous improvement, something all businesses should aim for. Comparing your business to others can help you generate ideas that you can adopt to get ahead." (Fallon, 2023)

Benchmarking has been around since the early 1900's when business owners started comparing themselves to competitors (Benchmarking Group, 2024). However, the development of the modern benchmarking approach has been credited to Dr. Robert Camp when he was at Xerox in the 1970's (Camp, 2006).

While benchmarking has been around for a while, it has typically been used to improve production and operations. As the risk of phishing continues to escalate, benchmarking can be an important approach to reduce that risk and continuously improve information technology security in an organization.

Approaches to Benchmarking

There are several sources for information and methodologic guidance to conduct a benchmarking study. One well documented guide with a framework and tools available to members has been developed by the American Society for Quality (ASQ) (ASQ, 2023). ASQ (2023) has identified two types of benchmarking. Technical benchmarking which compares the design of products and services of one organization against competitors. The second ASQ (2023) category is competitive benchmarking which looks at how an organization is doing compared to leading competition regarding critical attributes of the organization such as processes, functions or values relative to the focal organization's products or services. The example ASQ (2023) gives is to survey your customers as to how they rank the focal organization's product or services in comparison to their leading competitor. Marketing can then use the data from the survey to appropriately guide their efforts.

ASQ (2023) recommends a five-phase procedure to successfully benchmark (see Appendix A for the full list of steps). The first phase, and perhaps the most important, is titled "Considerations" and outlines four main items to be considered before planning the benchmarking exercise. Considerations should be addressed to provide the best chance of a successful benchmarking project. These considerations include clearly understanding your own processes so you will know exactly what you are comparing and making sure to have management support to ensure the significant investment is not wasted. The other phases are planning, collecting, analyzing and adapting your processes based on findings.

Although the ASQ benchmarking procedures could apply to any benchmarking study, their categories are focused more on production emphasizing comparison of products and services. The American Productivity & Quality Center (Harper, 2019) has identified four types of benchmarking- performance, where quantitative data is gathered and compared; practice, where qualitative information is gathered and compared; internal benchmarking where metrics and/or practices from different units in an organization are compared; and external where metrics and/or practices from a focal organization is compared to one or more other organizations.

Example of Benchmarking for Phishing

The ABC Company hired June Lockerbee, a new Chief Information Security Officer (CISO), who quickly realized they had a major phishing problem with a phishing prone percentage (PPP) of 55%. Their industry average was 32.4%. Upon review, June discovered the company was developing and running phishing attacks (creating a counterfeit phishing email, sending to employees and seeing how many attacks were successful) and gave optional virtual awareness training. The optional training consisted of a one-hour online video that employees were encouraged to watch at least once a year. The video had not been updated since it was produced 3 years prior.

June requested and received funding and management support to improve the PPP. She knew a half dozen other CISOs in her industry through professional associations that had discussed how they bettered their phishing exposure. Thus, June selected benchmarking to begin improving the process by looking at other successful companies. The project goals were:

1. Reduce the PPP to 32.4% or less.
2. Make the phishing prevention process as efficient as possible.

A cross-functional project team was formed. They documented the current phishing prevention process. The project team conducted focus groups in each of the four company departments to see what employees thought of phishing and what might motivate them to watch the training video(s) provided and be more diligent in protecting the company from phishing.

The team conducted a telephone survey of the CISOs from 6 of the companies in their industry that June knew. The team then visited 3 of the companies to see the training materials they used and discuss the HR policies regarding phishing training requirements.

The team put together a benchmarking report for management describing the best practices they had seen at other companies and recommendations for improving their own processes.

The team revisited the phishing process at two points, 6 months then a year, after the adoption of several of their recommendations and found:

1. Their PPP was down to 41.7% then 23.6% (6 months then a year, respectively)
2. The training was originally 1 hour of training, at 6 months it was 45 minutes and at 1 year it was 20 minutes.

Conclusion

Phishing is a serious threat to the healthcare sector. To protect sensitive information and patients' trust and safety, healthcare organizations need to embrace multi-faceted comprehensive strategies, including training, technological defenses, robust incident response plans, and strict adherence to regulatory requirements. The collaborations among the Texas Hospital Association and other organizations in healthcare and cybersecurity highlight the importance of sharing expertise, best practices, and innovations. Indeed, as phishing continues to evolve, benchmarking, either internally between units or externally between organizations, is no longer an option but a necessity as a best practice. By comparing their cybersecurity practices to those of their peers, healthcare organizations can identify gaps and adopt best practices, ensuring they remain at the forefront of cybersecurity defense. While advanced technologies such as artificial intelligence will help with future developments in phishing detection and prevention, the human element—ensuring that employees are well-educated, prepared and motivated—will remain key to any successful cybersecurity strategy.

References

1. American Society for Quality (ASQ). (2023, December 18). *What is benchmarking?* https://asq.org/quality-resources/benchmarking
2. Anti-Phishing Working Group. (2024). *Phishing attack trends report – 4Q 2023*. https://docs.apwg.org/reports/apwg_trends_report_q4_2023.pdf
3. Benchmarking Group. (2024, May 10). *The history of benchmarking, aka the "bench-mark"*. https://benchmarking.com.au
4. Bloomberg. (2017, June 26). *Anthem agrees to $115 million settlement over data breach*. Data Center Knowledge. https://www.datacenterknowledge.com/data-breaches/anthem-agrees-to-115-million-settlement-over-data-breach
5. Camp, R. C. (2006). *Benchmarking: The search for industry best practices that lead to superior performance.* ASQC Press.
6. Cluley, G. (2017, May 16). *DocuSign admits hackers accessed its customer email database, sent out malware*. Bitdefender. https://www.bitdefender.com/blog/hotforsecurity/docusign-admits-hackers-accessed-its-customer-email-database-sent-out-malware/
7. Davis, J. (2021, March 12). *41 states settle with AMCA over 2019 data breach affecting 21M patients*. Health IT Security. https://www.healthitsecurity.com/news/41-states-settle-with-amca-over-2019-data-breach-affecting-21m-patients
8. Fallon, N. (2023, October 30). *What is benchmarking in business?* Business News Daily. https://www.businessnewsdaily.com/15960-benchmarking-benefits-small-business.html
9. Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digital Medicine*, 2(1), 98. https://doi.org/10.1038/s41746-019-0161-6
10. Goldman, D. (2015, August 10). *Hackers siphon $47 million out of tech company's accounts*. CNN Business. https://money.cnn.com/2015/08/10/technology/ubiquiti-hacked/index.html
11. Harper, M. (2019, November 13). *What are the four types of benchmarking?* AQPC.org. https://www.apqc.org/blog/what-are-four-types-benchmarking
12. Ikeda, S. (2019, April 9). *The phishing scam that took Google and Facebook for $100 million*. CPO Magazine. https://www.cpomagazine.com/cyber-security/the-phishing-scam-that-took-google-and-facebook-for-100-million/
13. Ivanova, I. (2023, July 11). *HCA Healthcare says hackers stole data on 11 million patients*. CBS News. https://www.cbsnews.com/news/hca-healthcare-data-breach-hack-11-million-patients-affected/
14. Pagliery, J. (2015, July 17). *UCLA Health hacked, 4.5 million victims*. CNN Business. https://money.cnn.com/2015/07/17/technology/ucla-health-hack/index.html
15. Phishing.org. (n.d.). *History of phishing*. https://www.phishing.org/history-of-phishing
16. Savov, V. (2015, September 2). *Sony Pictures hacked: The full story.* The Verge. https://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream
17. Texas Hospital Association. (n.d.). *Quality and patient safety programs*. https://www.tha.org/services-for-hospitals/clinical-services/
18. Tidy, J. (2020, June 29). *How hackers extorted $1.14m from University of California, San Francisco*. BBC. https://www.bbc.com/news/technology-53214783

19. UT Southwestern Medical Center. (2023, June 6). *Use caution to protect personal data, UTSW network.* https://www.utsouthwestern.edu/employees/information-security/awareness/updates/use-caution.html
20. Verizon. (2023, June 6). *2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket*. https://www.verizon.com/about/news/2023-data-breach-investigations-report

Appendix A*

Competitive Benchmarking

Competitive benchmarking compares how well (or poorly) an organization is doing with respect to the leading competition, especially with respect to critically important attributes, functions, or values associated with the organization's products or services. For example, on a scale of one to four, four being best, how do customers rank your organization's products or services compared to those of the leading competition? If you cannot obtain hard data, marketing efforts may be misdirected and design efforts misguided.

Benchmarking Procedure

Considerations

- Before an organization can achieve the full benefits of benchmarking, its own processes must be clearly understood and under control.
- Benchmarking studies require significant investments of manpower and time, so management must champion the process all the way through, including being ready and willing to make changes based on what is learned.
- Too broad a scope dooms the project to failure. A subject that is not critical to the organization's success won't return enough benefits to make the study worthwhile.
- Inadequate resources can also doom a benchmarking study by underestimating the effort involved or inadequate planning. The better you prepare, the more efficient your study will be.

Plan

1. Define a tightly focused subject of the benchmarking study. Choose an issue critical to the organization's success.
2. Form a cross-functional team. During Step 1 and 2, management's goals and support for the study must be firmly established.
3. Study your own process. Know how the work is done and measurements of the output.
4. Identify partner organizations that may have best practices.

Collect

5. Collect information directly from partner organizations. Collect both process descriptions and numeric data, using questionnaires, telephone interviews, and/or site visits.

Analyze

6. Compare the collected data, both numeric and descriptive.
7. Determine gaps between your performance measurements and those of your partners.
8. Determine the differences in practices that cause the gaps.

Adapt

9. Develop goals for your organization's process.
10. Develop action plans to achieve those goals.
11. Implement and monitor plans.

*From ASQ website – https://asq.org/quality-resources/benchmarking accessed on 5/7/2024

Janis A. Warner, PMP is an Associate Professor of Management Information Systems at Sam Houston State University. Before receiving her PhD in Business Administration with an MIS concentration, she worked for 23 years in the private sector for organizations including Accenture and Pulte Homes in roles including IT Support Manager, Internal Auditor, Division Controller and Systems Design Manager. This experience led her to develop a passion for the user-oriented socio-technical approach to IT security. Research interests include human behavior and information technology security, project management, and case study pedagogy.

Kamphol Wipawayangkool is a Professor of Management Information Systems in the College of Business Administration at Sam Houston State University. He received his PhD in Information Systems from the University of Texas at Arlington. His research interests include information security management, knowledge management, and teaching and learning. He was the recipient of the College of Business Administration Teaching Award in 2023 and a Center for Community Engagement Fellow in 2023-2024.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Warner, J., & Wipawayangkool, K. (2024). Phishing Prevention in Healthcare (Report No. IHS/CR-2024-1021). Sam Houston State University, Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/W4CNJ