Phishing Attacks: A Forefront Threat in the Ongoing History of the United States Healthcare Industry

Mohammed Mohammed Raoof

Submitted to: Journal of Medical Internet Research
on: October 25, 2024

Table of Contents

Phishing Attacks: A Forefront Threat in the Ongoing History of the United States Healthcare Industry

Mohammed Mohammed Raoof[1] PhD

[1]Claremont Graduate University Center for Information Systems & Technology Claremont US

Corresponding Author:
Mohammed Mohammed Raoof PhD
Claremont Graduate University
Center for Information Systems & Technology
150 E 10th St, , CA
Claremont
US

Abstract

Background: Phishing is the most prevalent type of social engineering attack. These attacks are harmful in any domain, including the healthcare domain. They compromise individuals' confidential information.

Objective: However, this study investigates the types of phishing attacks experienced by the United States (US) healthcare industry.

Methods: This qualitative study employs the phenomenological research method to explore and understand the lived experiences of phishing attacks in the US healthcare industry. The data were collected from the archived US healthcare breaches report. Although the report may not include detailed information about phishing attacks, data limitations are employed to ensure the study's validity.

Results: However, findings have shown that phishing attacks caused an astonishingly high percentage of affected individuals, an unbelievable 95.5%, from 2014 to 2024, and there were no incidents for the Whaling, Smishing, Vishing, Clone, and Pharming attacks, except only one incident for the spear phishing attacks throughout that duration. Moreover, controlling phishing attacks could help reduce and mitigate the risk of other attacks. For safeguarded solutions in healthcare settings, this study strongly recommends following the National Institute of Standards and Technology (NIST) standards, such as Special Publication (SP) 800-66r2.

Conclusions: While there were no incidents for the Whaling, Smishing, Vishing, Clone, and Pharming attacks, the findings show only one incident for the spear phishing attacks. Moreover, phishing attacks are more severe and dangerous and can affect many individuals more than other attacks. Even though phishing comes in various forms and strategies, we concluded that controlling phishing attacks could help to reduce and mitigate the risk of other attacks. Further studies will be required to analyze the breach report deeply and confirm this statement.
Our study promotes implementing the National Institute of Standards and Technology (NIST) standards, such as the SP 800-66r2 in healthcare settings to minimize the potential risks of various phishing attacks. Overall, our study contributions include spreading awareness of phishing attacks and helping protect healthcare organizations from phishing attacks and other attacks. Furthermore, supporting the vital need for technology developers and engineers to develop robust security mechanisms against phishing attacks.

(JMIR Preprints 25/10/2024:67988)
DOI: https://doi.org/10.2196/preprints.67988

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.

No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✔ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Phishing Attacks: A Forefront Threat in the Ongoing History of the United States Healthcare Industry

Abstract

Phishing is the most prevalent type of social engineering attack. These attacks are harmful in any domain, including the healthcare domain. They compromise individuals' confidential information. However, this study investigates the types of phishing attacks experienced by the United States (US) healthcare industry. This qualitative study employs the phenomenological research method to explore and understand the lived experiences of phishing attacks in the US healthcare industry. The data were collected from the archived US healthcare breaches report. Although the report may not include detailed information about phishing attacks, data limitations are employed to ensure the study's validity. However, findings have shown that phishing attacks caused an astonishingly high percentage of affected individuals, an unbelievable 95.5%, from 2014 to 2024, and there were no incidents for the Whaling, Smishing, Vishing, Clone, and Pharming attacks, except only one incident for the spear phishing attacks throughout that duration. Moreover, controlling phishing attacks could help reduce and mitigate the risk of other attacks. For safeguarded solutions in healthcare settings, this study strongly recommends following the National Institute of Standards and Technology (NIST) standards, such as Special Publication (SP) 800-66r2.

Keywords: Spear Phishing, Whaling, Smishing, Vishing, Clone, Pharming, Ransomware, Artificial intelligence (AI), SP 800-66r2

Introduction

The United States Department of Justice identifies social engineering attacks as among the most dangerous threats worldwide (Salahdine & Kaabouch, 2019). Mike Chapple (2021) summarized the types of social engineering attacks and documented, "Social engineering attacks include phishing, spear phishing, business email compromise (BEC), whaling, smishing, vishing, spam, shoulder surfing, invoice scams, hoaxes, impersonation, masquerading, tailgating, piggybacking, dumpster diving, identity fraud, typo squatting, and influence campaigns."

Although there are various social engineering attacks, phishing is the most prevalent type of social engineering attacks and typically targets data confidentiality (Deane & Kraus, 2021). In fact, the term phishing refers to "fishing for data" by cybercriminals (James, 2005). Moreover, Muslim et al. (2019) noted that ransomware attackers use phishing attacks to establish ransomware attacks. However, some of the general common forms of phishing attacks or phishing strategies are Spear phishing, Whaling, Smishing, and Vishing.

Spear Phishing targets organizations of specific individuals utilizing malicious messaging communication such as emails (Nahmias et al., 2024). Whaling is another form of spear phishing (Mike Chapple, 2021). Both Spear phishing and Whaling target individuals within the organization, but Whaling mainly targets senior management individuals with high profiles within the organizations, such as C-level executives (e.g., CEO). Whaling attacks can result in severe economic losses. For example, the Federal Bureau of Investigation (FBI) reported "losses of $1.4 billion USD due to business email compromise (BEC) scams, with whaling attacks attributed to $675 million USD of these losses", and that occurred in 2017 alone (Pienta et al., 2020).

The other type of phishing is smishing, which functions based on Short Message Service (SMS). It involves scammers sending numerous bait messages by impersonating legitimate government institutions or organizations (Seo et al., 2024). With the growing usage of mobile smartphones, most organizations reach out to their customers via SMS, and phishing criminals have taken advantage of smishing (Akande et al.) Moreover, smartphone messaging is expanding nowadays. Mobile messaging encompasses Multimedia Message Service (MMS), iMessage with the Apple iPhone, and various third-party applications such as Telegram and WhatsApp (Nahapetyan et al., 2024). Given that, smartphone users are highly likely subject to phishing attacks.

Phishing can occur in verbal communications as well. Phishing scammers use telephone techniques

(e.g., mobile phones, voicemails, and Voice-over-IP (VoIP) services) as phishing types to do social engineering attacks. This type of phishing is called vishing; it is also known as ‘voice phishing’ (Bin Adam et al., 2023). Experiencing vishing has several adverse severe outcomes as well; Armstrong et al. (2023) noted, “vishing and other social engineering attacks impact hundreds of thousands of people globally, and approximately 25% of the financial losses stemming from these attacks are never recovered”.

In addition to the general common forms of phishing attacks (Spear phishing, Whaling, Smishing, and Vishing), there are some other types of phishing, such as Clone phishing and Pharming phishing. However, all types of work are based on social engineering and use different deceptive techniques.

Clone phishing technique is used on trustworthy or legitimate websites or emails (e.g., previously delivered emails) to gain victims' trust. Typically, phishing criminals embed them with malicious codes (e.g., links) and present them to victims, pretending to be the original websites or senders (Chaudhuri, 2023). Pharming phishing is slightly different. In this type of phishing, the attackers manipulate particular website traffic to steal confidential information. The Domain Name System (DNS) poisoning or spoofing technique is known in this type of phishing attack. In sequence, the DNS poisoning leads the victims to visit the fake websites (Alkhalil et al., 2021; Domazet, 2019).

The Mechanics of a Phishing Attack

Although there are several types of phishing attacks, there are no particular types and standards for phishing attacks to occur because they are based on social engineering techniques. As such, attackers may use mixed types of phishing. For example, BBC News (2024) reported on 31 July 2020 a phishing attack on Twitter, which is currently named "X". The BBC article was titled “Twitter hack: Staff tricked by phone spear-phishing scam”, and it seems that the phishing attackers used mixed types of phishing, namely spear phishing and vishing. The damage of that attack was extensive. Consequently, the attackers took control of Twitter accounts for famous people and shared a Bitcoin scam, including accounts for Microsoft founder Bill Gates and reality star Kim Kardashian. Moreover, other studies, such as Chaudhuri (2023) noted that spear phishing attacks are one of the techniques and methods for clone phishing attacks.

However, while the main idea of phishing attacks is to target the victims’ data confidentiality, some intend to do other harmful things, including downloading malicious software; for example, some clone phishing attacks involve downloading malware, not just disclosing personal information (Chaudhuri, 2023).

Some techniques may include the scammers starting by establishing communication with the victims via various electronic transmitting technologies, such as phone calls, voice messages, quick response (QR), short message service (SMS), and electronic mail (e-mails) (Rathee & Mann, 2022). The phishing scammers formulate conversations with the victims based on social engineering strategies to gain the victims’ trust (e.g., manipulating the victims' emotions) (Kamau & Kaburu, 2022). According to Rathee and Mann (2022)The phishing attack's lifecycle starts by sending a malicious code represented as a URL link for a phishing website. A phishing website is a fake version of a legitimate or official website; in other words, it is a phony website. Once victims access or click the malicious URL link, they will enter a fake or fraudulent website, which asks the victims to enter their confidential information, such as online account passwords and login information.

In some other techniques, such as pharming phishing, the scammers may add additional alphabetic characters to the domain name. For example, www.amazon2n.com/password-recovery to fool the victims into accessing amazon.com to recover their passwords. The fake website may contain a form asking victims to fill out. This form asks for the victims’ sensitive information, such as their old passwords, make payments, or the faked website may execute and download some malware once the victims access it (Rathee & Mann, 2022). Smartphone users easily fall victim because they are not always able to recognize the details of fake websites due to the small size of their display screens(Akande et al.).

Related Work in the Literature

The author of this study has found several articles in the literature that target phishing attacks in healthcare. Wright et al. (2016) addressed the breaches in the United States (US) healthcare systems, and identified many hospitals in the US affected by phishing attacks between 2014 and 2016, which affected many patients' sensitive information. Although, Wright et al. (2016) provided an example of email phishing and explained spear phishing, but it did not specify the types of phishing attacks for these hospitals.

Moreover, Gordon et al. (2019) targets the practice of email phishing simulation in US healthcare institutions. Particularly from August 1, 2011, through April 10, 2018. (Gordon et al., 2019) noted, "the specific institutions are anonymized herein for security and privacy concerns," but also pointed out that some institutions include hospitals. However, their study focuses only on email phishing.

In another relevant study, Lee (2023) proposed four-step content analytics to analyze over nine years of the web description of the OCR breaching report. The study did not mention the exact yearly range of collected data; it only mentioned analyzing it over nine years. Lee (2023) relied on analysis tools (VOSviewer and NVivo software) for further analysis. However, the findings show that some breaches occurred due to phishing attacks, including their impacts and mitigation efforts. The study also addressed email phishing attacks but did not specify the other types of phishing attacks as well (Lee, 2023).

As we explained above, there are various types of phishing attacks, not just email phishing attacks. Although email is widely used in healthcare organizations, many healthcare organizations run their business using multiple communication methods along with email method, especially when communicating to the outside world; they communicate with their customers (e.g., patients and third parties such as Technology Managed Service Providers (MSPs)) over the phone and SMS. However, our study attempts to reveal the phishing attack types that target the US healthcare industry. This study aims to increase awareness of the various types of phishing attacks in healthcare organizations. Our contribution can help to mitigate the potential risk in the event of a breach exposure. It can also help developers and engineers of technology communication methods develop robust security mechanisms against various types of phishing attacks.

Methodology

This study investigates various phishing attacks experienced by the US healthcare industry. According to Emiliussen et al. (2021), the phenomenology research method “intends to investigate experiences of lifeworlds.” However, this study used the qualitative research method of the phenomenology approach to investigate the phishing attacks in the United States healthcare industry over the past ten years.

Research Question

Considering the various types of phishing attacks outlined in the introduction, namely (Spear phishing, Whaling, Smishing, Vishing, Clone, and Pharming), what types have the US healthcare industry experienced from 2014 to 2024?

Data Collection

This study focuses on phishing attacks only that have occurred in the US healthcare industry. Hence, we relied on the archived breaching report in the U.S. Department of Health and Human Services - Office for Civil Rights (2024). The data were collected from January 1, 2014, to September 1, 2024, in the archived report. The archived breaching report was downloaded using the Comma-Separated Values (CSV) file type. This study used Microsoft Excel to open the CSV file.

As mentioned earlier, we are using the qualitative phenomenology research method to study the phishing attacks experienced by the US healthcare industry. The downloaded report includes the “Web Description” column, which describes the experiences of each reported breach, such as the attack description. Typically, the attack description contains words such as phishing.

Analysis

The content of the “Web Description” field was analyzed in this study based on categories. Hsieh and Shannon (2005) noted, “Categories are patterns or themes that are directly expressed in the text

or are derived from them through analysis."
In our study, the patterns or themes are represented by keywords searched in the "Web Description" field of the archived breaching report. We analyze the Microsoft Excel file directly without analysis tools, particularly based on keyword searches. These keywords are phishing, Spear, Whaling, Smishing, Vishing, clone, and Pharming. As we have introduced the forms and strategies of phishing attacks in the introduction section, the primary rationale for choosing these keywords was grounded in our introduction.

Findings

There were 4574 breaches, and 395,291,156 individuals were affected from 2014 to 2024. However, in this section, we present the results of the data analysis represented by keyword categories. Table 1 below offers a clear overview of our study findings:

Keyword Category	Number of Breaches	Number of Breaches (Percentage %)	Number of Affected Individuals	Number Of Affected Individuals (Percentage %)
Phishing	804	17.6%	393,324,989	99.5%
Spear Phishing	1	0.02%	78,800,000	19.9%
Whaling	0	0%	0	0%
Smishing	0	0%	0	0%
Vishing	0	0%	0	0%
Clone	0	0%	0	0%
Pharming	0	0%	0	0%

Table 1. Numbers of Breaches and Affected Individuals Represented by Keyword Categories

As shown in Table 1, the phishing category shows the total number of individuals affected by phishing attacks as 393,324,989, while the spear phishing category is 78,800,000 as a subcategory of the phishing category. In other words, the phishing keyword showed a total of 804 breaches, but when we compounded the keyword "phishing" with "Spear" as Spear Phishing, we found only one breach.

As noted earlier, the total number of breaches is 4574, and 804 breaches fall under the phishing category. Excluding those related to phishing attacks, the remaining breaches total 3770 (calculated as 4574 minus 804), which is approximately 82.4% (calculated as 3770 divided by 4574, then multiplied by 100). In addition, we have used the below formula to calculate the total number of infected individuals, excluding those affected by phishing attacks from 2014 to 2024, which is 1,966,167, approximately 0.5%:

The total number of individuals infected, excluding those affected by phishing attacks, from 2010 to 2020 = **Total of affected individuals, from 2014 to 2024** - **Total of affected individuals by phishing attacks, from 2014 to 2024**

1,966,167 = 395,291,156 - 393,324,989

5% ≈ 1,966,167 / 395,291,156 * 100

In summary, Table 2 below outlines an overview of these numbers:

Attack Type	Number of Breaches	Number of Breaches (Percentage %)	Number of Affected Individuals	Number Of Affected Individuals (Percentage %)
Phishing Attacks	804	17.6%	393,324,989	99.5%
Non - Phishing Attacks	3770	82.4%	1,966,167	0.5%
All Types of Attacks (Phishing Attacks + Non - Phishing Attacks)	4574	100%	395,291,156	100%

Table 2. *Itemized* Breaches and Affected Individuals from 2014 to 2014.

Moreover, we deeply analyzed the phishing attacks based on the phishing keyword category. Figure 1 illustrates the number of annual breaches, and Figure 2 presents the number of annual affected individuals caused by phishing attacks between 2014 and 2024:

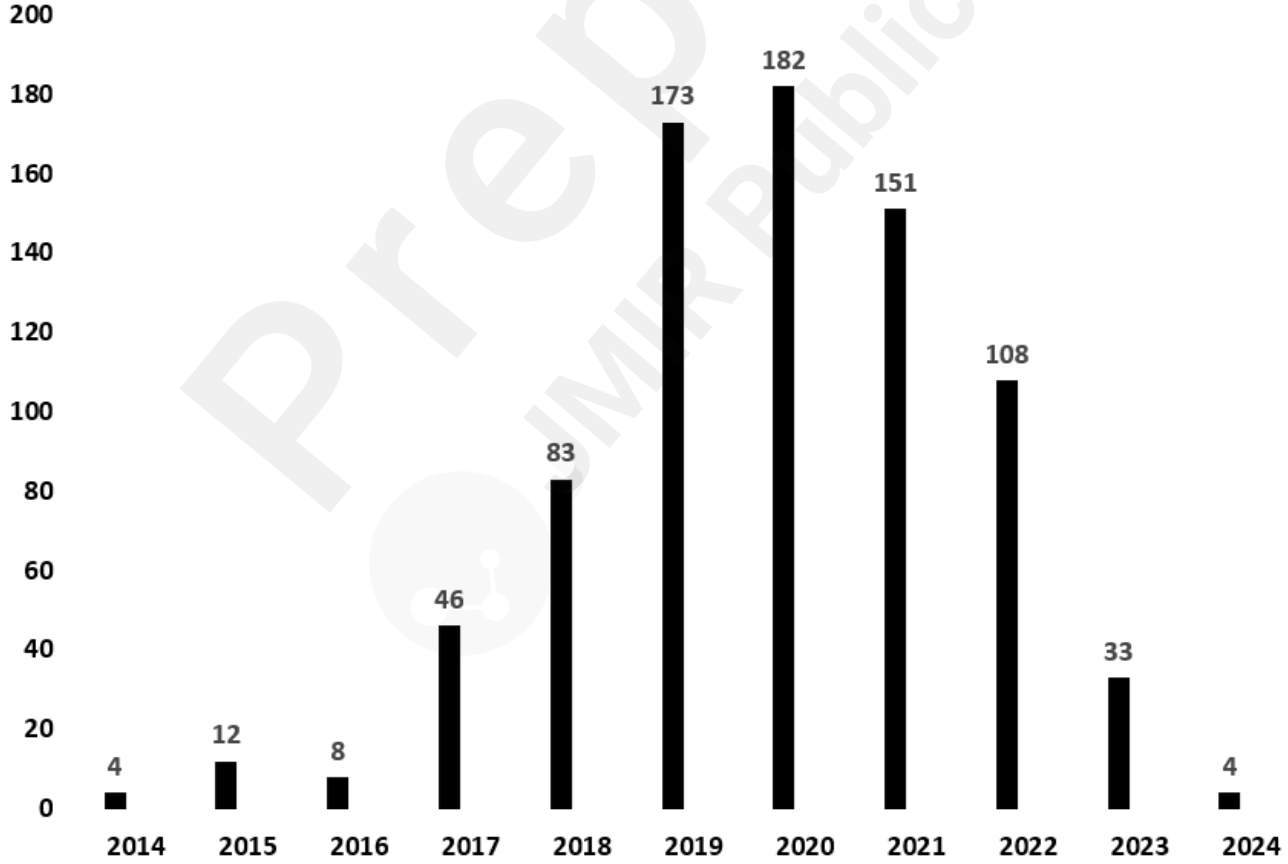

Figure 1. Annual Breaches Caused by Phishing Attacks from 2014 - 2024

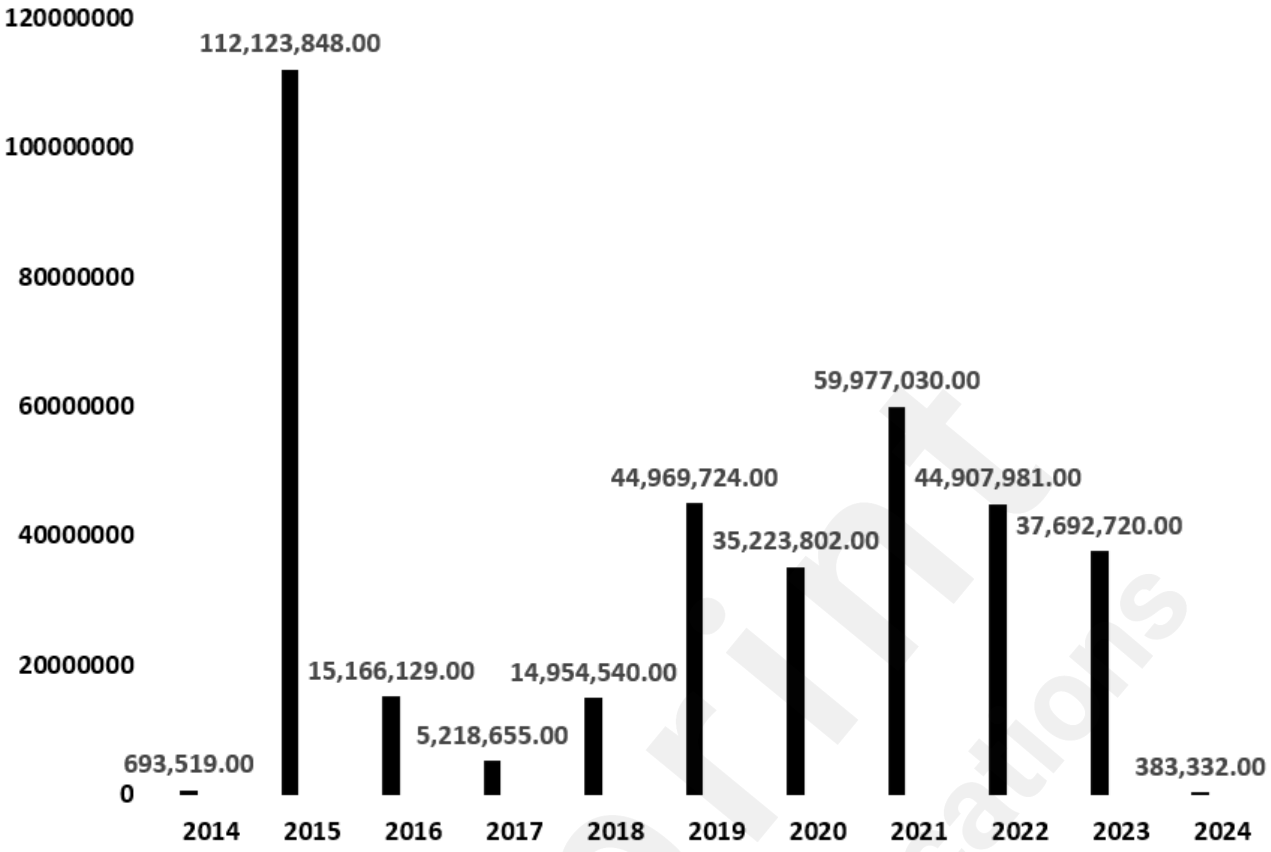

Figure 2. Number of Affected Individuals Caused by Phishing Attacks Per Year

Discussion

As indicated in Table 1, only one breach incident was caused by Spear phishing, and there were no breach incidents for the Whaling, Smishing, Vishing, Clone, and Pharming attacks, except one incident for spear phishing attacks. These findings would answer our research question, but they are based on keyword searches or categories in the archived data breach report from 2014 to 2024. It is important to note that the archived breaching report may not include sufficient information, particularly to identify the incident for Spear, Whale, Smish, Vishing, Clone, and Pharming attacks.

The current data in Table 1 shows that phishing attacks have the highest percentage of affected individuals, 95%. This is a considerable percentage, indicating that phishing attacks are the most dangerous of the other attacks. Alkhalil et al. (2021) outlined several attacks that rely on phishing techniques, such as spyware and ransomware. In other words, phishing attacks are part of the process involved in other attacks. Perhaps this could explain why this percentage is too high. As a result, controlling phishing attacks will help to reduce and mitigate the risk of other types of attacks. Further studies will be required to analyze the breach report deeply and confirm this statement.

Following Table 2, the rate of affected individuals caused by the other attacks is only 5%, caused by 82.4% of breaches. Hence, we noticed that although phishing attacks have fewer breaches, representing 17.6%, their harmful consequences are more severe and dangerous to many individuals than the other attacks. Furthermore, Figure 1 illustrates only 12 breaches in 2015, while Figure 2 displays 112,123848.00 infected individuals as a peak in 2015. Substantially, both Figures confirm an ongoing history of phishing attacks in the United States healthcare industry, mainly from 2014 to 2024.

Regarding the solution, the literature has shown rich information on strategies to mitigate the risk of phishing attacks. For example, Asiri et al. (2024) uses deep learning, a subfield of artificial intelligence (AI), as a real-time detection system for phishing attacks. Moreover, Wright et al. (2016) suggested enforcing user training in healthcare organizations against phishing attacks, employing two-factor authentication and other extra layers of security to mitigate the risk in the event of a

breach exposure.

However, our study strongly recommends the guidelines listed in the National Institute of Standards and Technology (NIST) as a solution, such as NIST SP 800-66r2 (Marron, 2024), the NIST SP 800-66r2 includes risk management that implements appropriate security measures. This helps to minimize and mitigate the potential risk of a breach exposed to phishing attacks or other phishing attacks in healthcare settings.

Limitations

Breach reports that affect less than 500 individuals could show different findings. According to the U.S. Department of Health and Human Services - Office for Civil Rights (2024), It is noted in "As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals."

As noted, the archived US healthcare breaches report only shows breaches that affect 500 or more individuals. This study's findings were demonstrated by data in the archived US healthcare breaches report that affected 500 or more individuals, specifically from 2014 to 2024, and by relying on keyword categories of the chosen research method. The findings could be different if other research methods were employed and other data were used.

Conclusion

While there were no incidents for the Whaling, Smishing, Vishing, Clone, and Pharming attacks, the findings show only one incident for the spear phishing attacks. Moreover, phishing attacks are more severe and dangerous and can affect many individuals more than other attacks. Even though phishing comes in various forms and strategies, we concluded that controlling phishing attacks could help to reduce and mitigate the risk of other attacks. Further studies will be required to analyze the breach report deeply and confirm this statement.

Our study promotes implementing the National Institute of Standards and Technology (NIST) standards, such as the SP 800-66r2 in healthcare settings to minimize the potential risks of various phishing attacks. Overall, our study contributions include spreading awareness of phishing attacks and helping protect healthcare organizations from phishing attacks and other attacks. Furthermore, supporting the vital need for technology developers and engineers to develop robust security mechanisms against phishing attacks.

Acknowledgments

The researcher expresses gratitude to all peer reviewers for their comments and feedback.

Conflict of Interest Statement

The author declares that there are no conflicts of interest.

References

Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O., & Fatokun, A. SMSPROTECT: An automatic smishing detection mobile application. *ICT Express*, *9*(2), 168-176. https://doi.org/10.1016/j.icte.2022.05.009

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Armstrong, M. E., Jones, K. S., & Namin, A. S. (2023). How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. *Human Factors*, *65*(2), 275-287. https://doi.org/10.1177/00187208211012818

Asiri, S., Xiao, Y., Alzahrani, S., & Li, T. (2024). PhishingRTDS: A real-time detection system for phishing attacks using a Deep Learning model. *Computers & Security*, *141*, 103843.

BBC News. (2024). Twitter hack: Staff tricked by phone spear-phishing scam. *BBC News*, *BBC News*,. *Retrieved July 28, 2024, from https://www.bbc.com/news/technology-53607374*. https://www.bbc.com/news/technology-53607374

Bin Adam, W. A., Xuan Tan, I. Y., Lai, C. S., Rahim, N. T., Bin Tham, B. Y., Guo, H., Operations, I. I. C. o.

S., Logistics, & Informatics, D. D. (2023). VishingDefender: An Advanced Vishing Defence System Against Vishing Attacks. In *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)* (pp. 1-8). https://doi.org/10.1109/SOLI60636.2023.10425272

Chaudhuri, A. (2023). Clone Phishing: Attacks and Defenses. *International Journal of Scientific and Research Publications*, *13*, 180-184.

Deane, A. J., & Kraus, A. (2021). *The Official (ISC) 2 CISSP CBK Reference*. John Wiley & Sons.

Domazet, S. (2019). Phishing and pharming attacks aimed at identity theft of internet users. Proceedings/5th International Scientific Conference" Security and Crisis management-theory and practice-SECMAN,

Emiliussen, J., Engelsen, S., Christiansen, R., & Klausen, S. H. (2021). We are all in it!: Phenomenological qualitative research and embeddedness. *International journal of qualitative methods*, *20*, 1609406921995304.

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA network open*, *2*(3), e190393-e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

Hsieh, H.-F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277-1288. https://doi.org/10.1177/1049732305276687

James, L. (2005). *Phishing exposed*. Syngress. http://www.books24x7.com/marc.asp?bookid=10709

Kamau, J., & Kaburu, D. (2022). A Review of Smishing Attaks Mitigation Strategies. *International Journal of Computer and Information Technology (2279-0764)*, *11*(1).

Lee, I. (2023). Analyzing web descriptions of cybersecurity breaches in the healthcare provider sector: A content analytics research method. *Computers & Security*, *129*, 103185.

Marron, J. (2024). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*.

Mike Chapple, J. M. S., Darril Gibson,. (2021). *(ISC)2 CISSP certified information systems security professional. Official study guide, ninth edition*. Sybex.

Muslim, A. K., Dzulkifli, D. Z. M., Nadhim, M. H., & Abdellah, R. H. (2019). A study of ransomware attacks: Evolution and prevention. *Journal of Social Transformation and Regional Development*, *1*(1), 18-25.

Nahapetyan, A., Prasad, S., Childs, K., Oest, A., Ladwig, Y., Kapravelos, A., & Reaves, B. (2024). On sms phishing tactics and infrastructure. 2024 IEEE Symposium on Security and Privacy (SP),

Nahmias, D., Engelberg, G., Klein, D., & Shabtai, A. (2024). Prompted contextual vectors for spear-phishing detection. *arXiv preprint arXiv:2402.08309*.

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, *35*(3), 214-231.

Rathee, D., & Mann, S. (2022). Detection of E-mail phishing attacks–using machine learning and deep learning. *International Journal of Computer Applications*, *183*(1), 7.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89.

Seo, J. W., Lee, J. S., Kim, H., Lee, J., Han, S., Cho, J., & Lee, C.-H. (2024). On-Device Smishing Classifier Resistant to Text Evasion Attack. *IEEE Access*.

U.S. Department of Health and Human Services - Office for Civil Rights. (2024). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. *Retrieved September 1, 2024, from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf*. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Wright, A., Aaron, S., & Bates, D. W. (2016). The big phish: cyberattacks against US healthcare systems. *Journal of General Internal Medicine*, *31*, 1115-1118.