Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 230 (2023) 874–878

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN 2023)

Healthcare 4.0: A Review of Phishing Attacks in Cyber Security

K S N Sushma[a*], Viji C[b], Rajkumar N[c],Jayavadivel Ravi[d] ,Stalin M[e], Najmusher H[f]

b,c,d,e Department of Computer Science & Engineering, Alliance College of Engineering and Design, Alliance University, Bangalore, Karnataka, India.
f Department of Computer Science & Engineering, HKBK College of Engineering, Bangalore, Karnataka, India.
a Research Scholar, School of Computer Science and Engineering, REVA University, Bangalore, Karnataka, India.
1 sushmakyerra@gmail.com

Abstract

The rapidly developing scene of Healthcare 4.0, has turned into a fundamental concern. This paper dives into the multi-layered domain of medical care network safety, with specific emphasis on the persistent phishing assaults. We examine the motivation for cyberattacks and the challenges involved. In this paper we review the phishing attacks in medical care, talking about preventive measures to handle this danger. By embracing this through methodology, Healthcare organizations can sustain their protections, shield patient information, and maintain the trustworthiness of medical care frameworks, all while encouraging a culture of network safety status in the computerized age.

Keywords: Cybersecurity, healthcare systems 4.0, threat, vulnerability, social and Phishing attacks.

1. Introduction:

Cybersecurity is termed as the protection of data, devices, hardware, and software against being exposed to hacking by hackers. One of the major sources of information about individual data is healthcare organizations which maintain huge data with ill-maintained security systems. Thus, making it more open to attackable [1].

The face of healthcare systems has been revolutionized in terms of communications, patient health monitoring, and healthcare devices such as telemedicine/telehealth into medical IoT devices. Thus, increasing the number of digital data via computerizing the system leads to a huge amount of data daily. While promising healthcare services from the hospitals the data is stored in cyberspace. This information includes the personal data of patient including their health records, credit card details personal information, etc.., Given the current vulnerabilities to cyberattacks, it is imperative to prioritize and promptly address cybersecurity concerns within healthcare systems [2].

The term Healthcare 4.0, also known as Health 4.0 or Healthcare Industry 4.0, is to narrate the fourth

10.1016/j.procs.2023.12.045

industrial spin shock on the healthcare division. It discusses the incorporation of advanced digital technologies and connectivity into healthcare services. However, it also includes the threats, data security, and regulatory compliances as a part of new emerging technologies in this field [3].

2. Motivation for the cyberattack in healthcare organizations [4][5][6]:

- High worth for patient data in the black market. The full set of medical credentials can cost up to $1000.
- Medical devices are not intended to be designed against security attacks rather than for specific medical assistance. This can lead to easy access of the device not only for the data and sometimes even they can take control over the system and endanger human lives.
- Medical treatment for a patient is a long-term and sensitive procedure and often requires shift-based monitoring. so medical staff have remote access to the devices including smartphone access or personal devices. if this happens even after attacks there will be a time lag to know the information that the device is under attack.
- Smaller budget allocation and smaller organizations where there is no maintenance of systems that support the data against the attackers.
- Out-dated technology usage including the software and hardware which is a good benefit to the hacker to easily access the data.
- Unwillingness of staff members to learn the new technology and paying little or no attention to protecting the data.

3. Challenges in cyber security in healthcare organizations:

Healthcare 4.0 largely relies on a backbone of connected devices for specific purposes which can be a collection of medical information, patient monitoring systems that can alarm the systems if the patient is in a dangerous condition, or even medical devices that can be implanted within the patient body itself [5].so what makes it is challenging to maintain the cyber security in healthcare organizations. Let's explore a few points.

1. *The email phishing attack*: Though it was a commonly known attack in the form of email it can lead a potential data loss if it occurs. It appears to be a common mail received from the IT team to the billing in charge asking about the change in the password for the payment system. if this attempt is successful it can lead to misuse of financial data and patient data as well.
2. *The ransom ware attack*: Ransom ware is a type of cyber-attack that blocks the access of hospital systems including scheduled operations systems, billing systems, and all other records that have potential data. After blocking the systems from access, the attackers demand money from the organization. Exposure to small organizations especially leads to serious damage to the data and affects the organization financially.
3. *The misplacement or unauthorized acquisition of equipment or data:* Robbery of devices such as handheld or laptops is no longer a wonder to individuals. If the hacker could open the laptop there is possibility of a financial loss and data loss as well.
4. *Data loss caused by insiders, whether accidental or intentional:* Whether it is intentional or accidental it causes prominent consequences for patients, healthcare services, and organizations. This can be practiced for financial gains or personal gains. Most cyber-attacks are caused by insiders since there is not enough knowledge of the seriousness of the threat.
5. *Attacks on devices that are connected in the organization may affect patient safety:*
   A medical device that is connected via the internal network is ill-maintained or not maintained against the authentication. This may result in the manipulation of patient treatment procedures, such as modifying glucose levels or radiation settings during patient testing.

Once we have grasped the challenges and recognized the necessity of cyber security in healthcare organizations, the next question arises: how can we effectively integrate the best practices or solutions to address this issue? Now, let's address one of the most formidable challenges in the realm of cyber-attacks within the context of healthcare 4.0. In this section, we will delve into technological solutions for combating phishing attacks in this highly advanced healthcare environment.

4. Introduction to phishing attacks:

The significant advancement of Healthcare 4.0 and its healthcare services guides the digital communications between patients and hospital services leading to phishing attacks. Phishing is a sort of cyber-attack that draws in unique devices and moves toward getting delicate data from clients. Phishing is a social engineering assault that hackers apply to get delicate data from clients [7]. In phishing, attackers can act like trusting entities to the user via email, instant messages, and social media. It is noticed that 17% of phishing attacks happened from 2016 to 2019. where the majority is occupied by malware by 28% [11]. These phishing attacks occur in the real world, in real-time are Anthem Data Breach (2015), NHS WannaCry Ransomware Attack (2017),

Scripps Health Ransom ware Attack (2021), and COVID-19 Vaccine Distribution Phishing Attacks (2020-2021) For instance, a user might receive a deceptive message from an attacker who impersonates a bank, falsely claiming that their account has been credited. An example of such screenshots is displayed below in Figure 1 and, how does this phishing work? Let's have a diagrammatical view of the scenario below in figure 2.

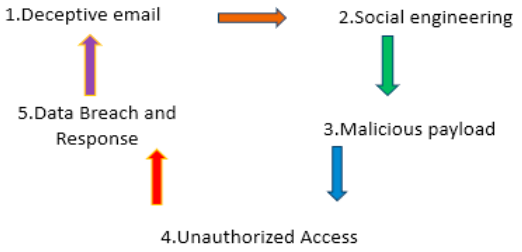

Figure 1. Attacker Deceptive message

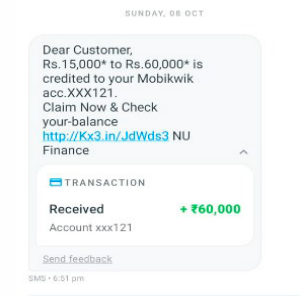

Figure 2. Workflow of Phishing attack

4.1 Background of phishing: Phishing is a deceptive cyberattack method where malicious actors impersonate trustworthy entities to trick individuals into revealing sensitive information. Common types of phishing include [6][8][9].

Deceptive email*:* Attacker email: The attacker sends a misleading email, showing up as a confided-in source, to a medical services worker.

Social engineering Deception**:** The email pretends to the recipient with immediate action needed advising them to open the attachment link.

Malicious payload: Malware activation: Interaction with the payload activities malware on the recipient's device.

Unauthorized Access**:** Attackers Access**:** The attacker gains authorization to the organization network.

Data Breach and Response: Data Theft: Sensitive patient data is hacked or stolen.

4.2 Prevention measures: A multi-layered way to deal with email security includes carrying out numerous safety efforts and components at various levels to make efficient protection against different sorts of email dangers, including phishing, malware, and other malicious exercises. This approach means to give a better email security methodology. This step-by-step procedure offers a well-structured and organized framework for implementing a multi-layered email security strategy, ensuring that your organization is fully equipped to effectively counter email threats [9].

1. Assessment and planning: Understanding the type of users their skills, data types, and adaptable security requirements can help to maintain measurable security goals.

2. Risk Assessment: Analysing vulnerabilities and their behaviours can help to a better understanding of the consequences of email attacks.

3. Security layer selection: Based on the assessed data choose security layers such as gateways filtering, and behavioural; analyse, and prioritize according to the needs.

4. Technology and tool selection: Choosing the right mix of these innovations and instruments, contingent upon your association's necessities and financial plan, is urgent for a safeguard against phishing attacks. The choice of tools may likewise rely upon your association's size, industry, and explicit email security requirements. Here are some key technologies and tools with examples shown in Table 1.

Table 1: Technological tools

S.no	Technologies	Tools
1	Email Security Gateways [10]	Cisco Email Security, Proofpoint Email Protection
2	Anti-Phishing Solutions[11]	Microsoft Defender for Office 365, Barracuda Phish Line
3	Behavioral Analysis and Anomaly Detection[12]	Darktrace, Cofense Triage
4	User Awareness and Training[9]	KnowBe4, PhishMe (now Cofense)
5	DNS Filtering[13]	Cisco Umbrella, OpenDNS
6	AI and Machine Learning [14]	Palo Alto Networks Cortex XDR, Cybereason
7	Email Authentication Protocols[15]	Implementing SPF, DKIM, and DMARC for email authentication
8	Email Encryption[16]	Virtru, Mimecast Email Encryption
9	User Behavior Analytics (UBA)[9]	Splunk UBA, Exabeam
10	Secure Email Gateways [17]	Fortinet FortiMail, Sophos Email Security
11	Phishing Simulators[18]	PhishMe (now Cofense) Simulator, GoPhish

5. Implementation and Configuration: Deploy the chosen tools and techniques within the email infrastructure as per the organization's requirements. After deployment test and validation thoroughly to configured layers.
6. User Training and Awareness: User training is crucial in any security strategy. Even the best security systems are ineffective without informed and vigilant users. Investing in technology alone is insufficient; users must be educated to recognize and counter security threats. Prioritizing user training empowers your employees, making them the first line of defence against cyber threats.
7. Monitoring and Incident Response: Set up on-going observing of email traffic and security occasions involving SIEM frameworks and layout alarming instruments for uncommon exercises.
8. Feedback and Improvement: clients report dubious messages and accumulate input on the adequacy of safety efforts. Consistently update and tweak your email security technique in view of feedback, threat intelligence, and emerging threats.
9. User Engagement and Awareness: Keep clients drawn in and informed about the most recent email dangers and the significance of following security arrangements. Cultivate a culture of safety mindfulness inside the association to improve general security.

5. Conclusion:

In conclusion, safeguarding Healthcare 4.0 against the persistent threat of phishing attacks requires a multi-pronged approach. The incorporation of advanced threat detection tools and predictive models is essential for real-time identification and mitigation of phishing attempts. Equally important is the commitment to continuous user education and awareness campaigns, extending not only to healthcare professionals but also to patients who play a crucial role in maintaining the security of their own health data. By weaving together these key components, we can create a robust cyber security environment that adapts to the dynamic nature of the digital healthcare landscape.

References:

[1] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10).
[2] Alami, Hassane, Marie-Pierre Gagnon, Mohamed Ali Ag Ahmed, and Jean-Paul Fortin. "Digital health: Cybersecurity is a value creation lever, not only a source of expenditure." Health Policy and Technology 8, no. 4 (2019): 319-321.
[3] Al-Jaroodi, Jameela, Nader Mohamed, Nader Kesserwan, and Imad Jawhar. "Healthcare 4.0–Managing a Holistic Transformation." In 2022 IEEE International Systems Conference (SysCon), pp. 1-8. IEEE, 2022.
[4] O'Brien, N., Ghafur, S., & Durkin, M. (2021). Cybersecurity in health is an urgent patient safety concern: we can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management, 26(1), 5-10
[5] Sendelj, R. and Ognjanovic, I., 2022. Cybersecurity Challenges in Healthcare. In Achievements, Milestones and Challenges in Biomedical and Health Informatics (pp. 190-202). IOS Press.
[6] Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. Maturitas, 113, pp.48-52.
[7] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms. International Journal of Advanced Research in Computer and Communication Engineering ISO, 3297, 2007.
[8] Damodaram, Radha. "Study on phishing attacks and antiphishing tools." International Research Journal of Engineering and Technology 3.01 (2016): 700-705.
[9] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), 3410.
[10] Fan, L., Ma, Y., Kou, W., Kang, D., & Wang, T. (2015, January). Mail security gateway mechanism for email security. In 2015 International Symposium on Computers & Informatics (pp. 1709-1716). Atlantis Press.
[11] Nisha, T. N., Digant Bakari, and Charmi Shukla. "Business E-mail Compromise—Techniques and Countermeasures." In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 217-222. IEEE, 2021.
[12] Boddy, A. J., Hurst, W., Mackay, M., & El Rhalibi, A. (2019). Density-based outlier detection for safeguarding electronic patient record systems. IEEE Access, 7, 40285-40294.

[13] Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. Access denied: The practice and policy of global internet filtering, 1(1), 58.
[14] Kanwal, M., & Thakur, S. (2017, May). An app based on static analysis for android ransomware. In 2017 International Conference on Computing, Communication and Automation (ICCCA) (pp. 813-818). IEEE.
[15] Nightingale, Stephen. Email authentication mechanisms: DMARC, SPF and DKIM. US Department of Commerce, National Institute of Standards and Technology, 2017.
[16] Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., ... & Seamons, K. (2016, May). " We're on the Same Page" A Usability Study of Secure Email Using Pairs of Novice Users. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 4298-4308).
[17] Assumption, S. P. (2013). Magic Quadrant for Secure Email Gateways. Inquiry
[18] Abroshan, Hossein, Jan Devos, Geert Poels, and Eric Laermans. "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process." IEEE Access 9 (2021): 44928-44949