



---

## Mitigating Phishing Attacks in Healthcare Institutions: A Need For Comprehensive Incidence Response Plan

Albert Nkrumah<sup>1</sup>, George Asante<sup>2</sup>, William Asiedu<sup>3</sup>

bert7jr@gmail.com<sup>1</sup>, gasante@aamusted.edu.gh<sup>2</sup>, wasiedu@aamusted.edu.gh<sup>3</sup>

<sup>1,2,3</sup> Department of Information Technology Education, Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, Kumasi, Ashanti Region, Ghana

---

### Article Information

Received : 26 Feb 2025

Revised : 8 Jun 2025

Accepted : 20 Dec 2025

---

### Keywords

Hospital, Phishing, cybersecurity, Response plan, Incidence

---

### Abstract

In recent years, the healthcare industry has witnessed a sharp increase in the number of security breaches, particularly phishing incidents, leading to the compromise of millions of sensitive patient records. The study aimed to explore Phishing Attacks in Healthcare. Specifically, the study seeks to investigate the prevalence of phishing attacks within community hospitals and develop comprehensive incident response plans that outline the steps to be taken in the event of phishing attacks. The study developed comprehensive and effective strategies for mitigating the risk of phishing attacks within Community Hospitals in Kumasi Metropolis. A quantitative research approach was adopted. The target population comprised IT professionals and healthcare administrators of community hospitals in Kumasi Metropolis. From the target population, a total of 9 hospitals were selected, where 97 respondents were used. Simple random and purposive sampling techniques were used in choosing the community hospitals and participants respectively. A structured self-administered questionnaire was utilized to gather the required data. The study revealed a high frequency of community hospital phishing attacks, with 57.7% encountering phishing attacks 1-2 times within 1-2 years, 6.4% experiencing a number of phishing incidents over 3-4 years, and 42.3% experiencing more than 5 phishing attacks within 1-2 years. The findings revealed that community hospitals frequently encounter several types of phishing attacks, including smishing, spear phishing, email phishing, clone phishing, vishing, and whaling attacks. The study concludes that implementing the ACSC Incident Matrix 2022 framework would be instrumental in helping hospitals effectively assess and manage cyber threats. It was recommended that CSA in collaboration with the MoC and Ghana Health Service, should launch national awareness campaigns focusing on the dangers of phishing attacks, particularly within the healthcare sector.

## A. Introduction

Over the past two decades, the internet has undergone a remarkable transformation, significantly expanding its influence and importance in society [1]. The internet has become a cornerstone of modern life, playing a pivotal role in shaping national competitiveness, driving innovation, facilitating globalization, and simplifying daily tasks for individuals around the world [2] [1]. However, alongside the countless benefits brought about by this digital revolution, there has been a simultaneous rise in the threat of cyber-attacks and cyber-threats in today's interconnected world. These malicious activities have evolved into a pervasive global problem, capable of causing widespread havoc on a massive scale within mere minutes [2]. The repercussions of cyber-attacks are severe among healthcare institutions, encompassing substantial financial losses, breaches of sensitive data, damage to equipment, disruptive denial-of-service attacks, and widespread network outages [1].

Healthcare data holds immense value in today's digital age, making it an enticing target for cybercriminals seeking to exploit vulnerabilities in the system. According to research by Priestman et al., healthcare data has emerged as a prime target for hackers due to its sensitive nature and potential for lucrative gains [3]. One of the most prevalent methods employed by cybercriminals to infiltrate healthcare systems is phishing [3]. Phishing is a deceptive tactic used by cybercriminals to extract valuable information, such as usernames, passwords, or medical data, for nefarious purposes. This method typically involves sending targeted communications, such as emails or messages, to unsuspecting recipients, urging them to click on malicious links or download malware [4].

Ghana has been grappling with a concerning surge in phishing incidents, as highlighted by several studies [5] [6]. This growing trend has raised significant alarm bells within the country's law enforcement and cybersecurity sectors. The prevalence of cybercrime has become a pressing issue, with reported cases witnessing a stark 33% rise between 2018 and 2019 alone in Ghana [7]. The escalation of phishing attack in Ghana has not gone unnoticed, prompting authorities to take proactive measures to address this mounting challenge [8]. As the digital landscape continues to evolve and technology becomes more integrated into daily life, the risks associated with cyber threats have become increasingly apparent in Ghana. From phishing scams to identity theft and financial fraud, individuals and organizations across Ghana are vulnerable to a wide array of cyber threats.

Despite the alarming prevalence of cybercrime in the healthcare sector, there remains a dearth of information regarding response plans outlining the necessary steps to be taken in the event of a security breach at healthcare centers in Ghana, especially amidst the rapid digitalization taking place. This highlights the critical need for comprehensive and effective incident response plans tailored to address the unique challenges and vulnerabilities faced by healthcare organizations in Ghana, ensuring the protection of patient data and the integrity of healthcare services in the face of escalating cyber threats. This study aimed at mitigating Phishing Attacks in Healthcare institution. The study specifically seeks to Investigate the prevalence of phishing attacks within community hospitals in

Kumasi Metropolis and develop comprehensive incident response plans that outline the steps to be taken in the event of phishing attacks.

## **B. Literature Review**

### **B.1. Prevalence of Phishing Attacks in Hospitals**

Phishing is one of the most organized crimes of the 21st century, representing a significant threat in the digital age [9]. It involves the use of malicious tactics to deceive individuals into divulging personal and sensitive information [9] [10]. Specifically, phishing is a type of cybercrime that employs social engineering techniques to fraudulently acquire information such as passwords, credit card numbers, and other confidential data [11]. This is typically done by sending spoofed emails that appear to come from legitimate and popular websites. These emails often contain links to fake versions of the websites, prompting unsuspecting victims to enter their credentials [12]. Once the information is entered, it is captured by the perpetrators, who then use it for illegal activities.

Phishing is a leading cause of healthcare data breaches and the attacks appear to be increasing [13]. Hospitals, pharmacies, care centers and other healthcare organizations are prime targets for malicious cyber-criminals. There are a few reasons for this: healthcare organizations deal with huge amounts of personal and private data, which can be hugely valuable for criminal groups [13]. According to the 2022 IBM X-Force Threat Intelligence Index, phishing is the leading infection vector in cyberattacks. Phishing attacks often lead to significant data breaches, compromising vast amounts of sensitive information. These breaches can involve hundreds of thousands, or even millions, of records stolen after employees inadvertently disclose their credentials or download malware by responding to phishing emails. One of the most notable incidents occurred in February 2015, when Anthem Inc. announced a cyberattack and data breach, marking the largest healthcare data breach ever reported [14]. This breach involved 78.8 million records of its plan members. According to the cybersecurity firm Mandiant, the breach began on February 18, 2014, when an employee at one of Anthem's subsidiaries opened a phishing email. This action triggered the download of malware, enabling hackers to remotely access computers and move laterally across systems. At least 50 accounts and 90 systems, including Anthem's data warehouse, were compromised in the attack [14].

In May 2019, the Oregon Department of Human Services became the target of a spear phishing attack that successfully deceived nine employees, granting attackers access to their email accounts for a period of 19 days [15]. These compromised accounts contained sensitive personal information related to clients in welfare and children's services programs, including names, addresses, and Social Security numbers [15]. As a result, 625,000 individuals were affected by this breach. Later, in December 2020, MEDNAX revealed that a hacker had infiltrated multiple email accounts within its Microsoft 365 environment in June of that year. The breach exposed the protected health information of 1,290,670 individuals. MEDNAX was providing support and services to the American Anesthesiology business, owned by North American Partners in Anesthesia, leading to the compromise of records belonging to 1,269,074 American Anesthesiology patients.

In April 2020, the Fortune 500 insurance company Magellan Health suffered a sophisticated social engineering phishing attack [16]. The attackers impersonated one of Magellan's clients, which enabled them to infiltrate the company's network and deploy ransomware. This incident compromised the information of 1,013,956 Magellan Health members [16]. The breach extended to other Magellan units, with an estimated total of around 1.7 million records compromised. This attack followed a previous phishing incident in the previous year, which had affected 55,637 plan members [16]. In 2023, the healthcare industry faced an unprecedented surge in data breaches, reaching an all-time high and highlighting persistent cybersecurity concerns [16]. According to a report by HIPAA, there were 114 data breaches involving 100,000 or more records. Among these incidents, 26 involved breaches of over 1 million records, and five involved breaches exceeding 5 million records. The most significant of these breaches affected a staggering 11.27 million records, underscoring the critical need for enhanced data security measures within the healthcare sector [16]. This alarming trend illustrates the growing vulnerability of healthcare organizations to cyber threats and the urgent necessity for comprehensive strategies to protect sensitive patient information.

## **B.2. Implementation of phishing attack measures**

Phishing attacks are becoming increasingly sophisticated and frequent [16]. Implementing measures against cybercrime is crucial and includes tools like public key infrastructure, intrusion detectors, and prevention strategies through firewalls, anti-virus programs, anti-spam filters, and anti-spyware [17]. Alder highlights the Four Pillars of Phishing Defense, which consist of an email security gateway, a web security solution, regular security awareness training for the workforce, and multi-factor authentication. When these measures are effectively put in place, healthcare organizations can establish a robust defense against phishing attacks. This comprehensive approach significantly reduces the risk of costly data breaches, ensuring the protection of sensitive information and maintaining the integrity of their systems [16].

### **1. Email Security:**

The primary technical defense against phishing attacks is the implementation of a secure email gateway or spam filter. Secure email gateways work by scrutinizing email headers to block known malicious IPs and verifying that email senders are authorized to use the specified email address or domain [18]. They analyze email content for keywords indicative of phishing attempts and follow hyperlinks within emails to identify malicious websites [18]. Additionally, outbound filtering is employed for data loss prevention, ensuring that sensitive information, such as protected health information (PHI), is not sent externally. This feature also helps identify compromised mailboxes that may be used to distribute phishing emails both internally and externally. These solutions are highly effective, blocking over 99% of spam emails, known malware, and most phishing emails [18].

### **2. Web Security:**

Email security solutions alone are not sufficient to fully protect against phishing attacks; they should be complemented by a web security solution [19].

While email security solutions focus on filtering malicious content within emails, web security solutions provide an additional layer of protection by addressing threats from a different angle. They block access to websites designed to harvest credentials or host malware, thus adding a crucial safeguard against phishing attacks. Web security solutions, also known as web filters, DNS filters, or web protection solutions, are essential for real-time defense. They offer time-of-click protection by blocking access to malicious hyperlinks as users attempt to visit potentially dangerous sites [18] [20]. This is particularly important because even the best email security solutions can occasionally miss malicious links, allowing some phishing emails to reach inboxes.

#### 3. Security Awareness Training:

Phishing attacks continue to pose a significant threat, necessitating comprehensive strategies to protect healthcare institutions [19]. While technical defenses, such as secure email gateways and web security solutions, play a crucial role in blocking the majority of phishing attempts, it is equally important to address the human element in cybersecurity [19].

#### 4. Multi-factor Authentication:

In the event that credentials are compromised through a phishing attack, the potential damage extends far beyond the immediate breach [16]. Once attackers gain access to user accounts, they can exploit these credentials to launch further attacks. To mitigate such risks, multi-factor authentication (MFA) serves as a crucial last line of defense. MFA requires users to provide an additional form of authentication beyond just their password before gaining access to an account. This could involve a token, a one-time code sent to a mobile device, or biometric factors such as a fingerprint or facial scan. According to Microsoft, implementing MFA can block up to 99.9% of automated attacks on accounts, thereby significantly enhancing security and protecting against the misuse of compromised credentials [16].

### **B.3. Theoretical Framework**

This study used Diffusion of Innovation (DoI) Theory as a basis of analysis. DoI developed by E.M. Rogers in 1962, stands as one of the foundational theories in social science. Rogers' DoI theory emerged from pioneering efforts in the implementation of innovations [21]. The theory categorizes adopters into several groups based on their readiness and ability to embrace new ideas. These categories are innovators, early adopters, early majority, late majority, and laggards. Each group has distinct characteristics that influence their adoption behaviors [22]. Innovators are the first to adopt an innovation. They are adventurous, risk-taking, and willing to experiment. Early adopters follow, and they are often respected opinion leaders who embrace change and influence others. The early majority is more deliberate and takes longer to adopt new ideas, but they provide a critical mass that helps propel the innovation forward. The late majority is skeptical and adopts an innovation only after the majority has tried it. Finally, laggards are the last to adopt, resistant to change and influenced mainly by tradition and past experiences. Understanding these categories is crucial for effectively introducing and promoting new ideas, behaviors, or products. By

recognizing the different characteristics and motivations of each group, strategies can be tailored to encourage adoption across the entire social system.

Adoption of a new idea, behavior, or product, often referred to as "innovation," does not occur simultaneously within a social system. Instead, it unfolds as a process wherein certain individuals are more inclined to embrace the innovation earlier than others. References [23] [24] [25] have highlighted that early adopters possess distinct characteristics compared to those who adopt innovations at a later stage. When aiming to introduce an innovation to a specific population, it becomes crucial to comprehend the traits of the target audience that may facilitate or impede the adoption process. In an increasingly digitized healthcare landscape, the battle against phishing attacks has become a critical focus for IT professionals, cybersecurity experts, and healthcare administrators. These stakeholders play pivotal roles in overseeing healthcare data protection and privacy compliance. To enhance the adoption of anti-phishing innovations within healthcare institutions, it is essential to understand how these professionals perceive the key features that determine the acceptance and use of new technologies. The DOI Theory provides a valuable lens through which these perceptions can be analyzed.

1. Applying DOI Theory to Mitigating Phishing Attacks:

Innovators in healthcare institutions are typically technology enthusiasts who are willing to take risks to implement cutting-edge solutions. Early Adopters are often respected opinion leaders who recognize the need for improved cybersecurity measures. The Early Majority adopts new technologies once they see their practical benefits and when they become convinced of their effectiveness. The Late Majority and Laggards are typically more skeptical and resistant to change. They may require more convincing and support to adopt new technologies. By applying the principles of the DOI, healthcare institutions can strategically promote the adoption of anti-phishing measures. Understanding the factors that influence adoption and tailoring approaches to different adopter categories can lead to more effective and widespread implementation of cybersecurity practices. This, in turn, enhances the overall security posture of healthcare organizations, protecting sensitive patient information and ensuring the continuity of critical healthcare services.

#### **B.4. Australian Cyber Security Centres (ACSC) Incident Matrix Framework**

ACSC Incident Matrix Framework is a structured approach to managing and mitigating cyber incidents in Australia. Between 1 July 2020 and 30 June 2021, the ACSC responded to over 1,500 cyber security incidents, showcasing the significant volume of cyber threats faced by Australian organizations and highlighting the critical role of the ACSC in safeguarding digital environments [26]. The primary purpose of the ACSC Incident Matrix Framework is to facilitate a swift and effective response to cyber incidents while ensuring alignment with an organization's security objectives and overall business goals. By doing so, it aims to minimize the operational and financial impacts of cyber threats and enhance the resilience of Australian organizations to emerging cyber risks [26]. The framework is designed

with the following core objectives to ensure a holistic and systematic approach to incident management:

- **Guidance on Responding to Cyber Incidents:** The framework provides a clear and detailed roadmap for organizations to follow when responding to cyber incidents. This ensures that all steps taken are efficient, effective, and in alignment with best practices.
- **Defining Roles and Responsibilities:** By outlining the roles, responsibilities, accountabilities, and authorities of individuals and teams involved, the framework promotes coordination and accountability during incident response efforts. This clarity helps avoid confusion, ensuring that critical actions are assigned and executed promptly.
- **Compliance with Legal and Regulatory Requirements:** The framework emphasizes adherence to legal and regulatory compliance obligations, ensuring that organizations address cyber incidents within the bounds of applicable laws and regulations. This reduces the risk of penalties and enhances stakeholder confidence in organizational governance.
- **Internal and External Communication Processes:** Effective communication is a cornerstone of incident management. The framework establishes protocols for internal coordination and external communication, ensuring that relevant stakeholders, including regulators, clients, and the public, are informed appropriately and promptly.
- **Post-Incident Activities for Continuous Improvement:** The framework promotes a culture of continuous learning by incorporating post-incident analysis and reporting. Organizations are encouraged to evaluate their response efforts, identify areas for improvement, and implement measures to strengthen their defenses against future threats [26].

The ACSC Incident Matrix Framework provides organizations with a comprehensive and structured approach to managing cyber threats. By focusing on prevention, timely response, and continuous improvement, it ensures that organizations are better equipped to address the evolving cyber threat landscape. Furthermore, it reinforces the importance of organizational preparedness, effective teamwork, legal compliance, and strategic communication in managing incidents effectively. This framework serves as a critical tool for organisations like healthcare institutions to not only mitigate the impact of cyber incidents but also to build resilience and foster trust in the face of increasing cyber threats.

### **C. Research Methodology**

With respect to the research issue under consideration, the researchers are of the opinion that a quantitative view of the study presents the researchers with a better understanding of mitigating phishing attacks in healthcare institutions. The quantitative research method adopts a deductive and objective view, which is characterized by tangible data such as counts, weight, mass, and other physical measures [27]. The population of the study includes all the community hospitals in Kumasi Metropolis that have websites and confirmed to be active. The study included 17 community hospitals with active websites. The population is made up of relevant stakeholders involved in information security management within these hospitals such as IT professionals, and healthcare.

To arrive at the sample size, a total of 9 hospitals were selected from the 17 community hospitals in Kumasi Metropolis, Ghana. In the selection of participants, 97 participants were sampled from the community hospitals. Simple random and purposive sampling technique were used in selecting the community hospitals and participants respectively. Simple random sampling technique was used in selecting the community hospitals in Kumasi Metropolis in order to represent effectively the whole study area. In the selection of the IT professionals, and healthcare administrators, purposive sampling was employed. The purposive sampling technique was used because it was the best means of getting the IT professional and the administrators who oversee healthcare data protection and privacy compliance.

A well-structured google form of closed ended questionnaire was designed to gather information from the respondents. The researchers send the google questionnaires to the respondents through the e-mail address and WhatsApp number. The google form of questionnaire was used because they can reach a large number of respondents within a short time. In addition, Australian Cyber Security Centre (ACSC) incident matrix was adopted to assess the phishing incident Response plan. SPSS version 23 was also used for the processing of all the closed-ended items that were entered for analysis. Descriptive statistics such as frequencies, percentages, mean and standard deviation were used to analyse the data obtained from the respondents and the results were presented in Tables.

## D. Results of The Research

### D.1. Demographic Characteristics

Demographic characteristics of the respondents was sought; the researchers deemed it necessary to look into demographic characteristics of the respondents because they make a person who he or she is.

**Table 1.** Demographic characteristics of respondents

Characteristics	Responses	Frequency (N)	Percentage (%)
Gender	Male	90	92.8
	Female	7	7.2
Age (years)	Below 25years	6	6.2
	25-34years	50	51.5
	35-44years	26	26.8
	45-54years	15	15.5
Academic qualification	Diploma/certificate	2	2.1
	Bachelor degree	82	84.5
	Masters degree	13	13.4
Years working in the current role	1-3year	41	42.3
	4-6years	45	46.4
	7-10years	11	11.3

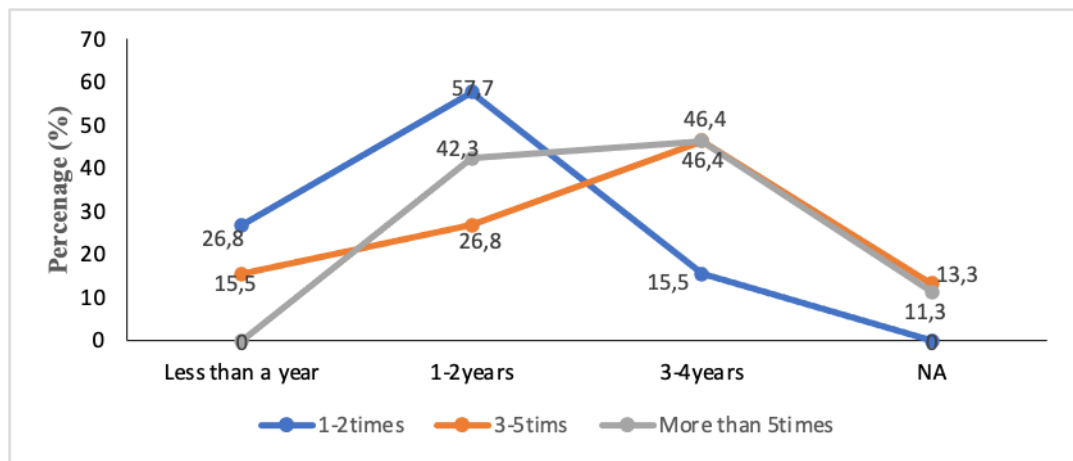
The data presented in Table 1 indicates that 92.8% of the IT and administrative staff at various community hospitals were males, while only 7.2% were females. This suggests that the majority of the respondents who participated in the study were men, highlighting a gender imbalance within the IT and administrative roles in these hospitals. The data on the age distribution of respondents reveals that a small proportion, 6.2%, were under the age of 25, indicating relatively few younger participants. The largest age group was between 25-34 years, accounting for 51.5% of the respondents, suggesting that most of the individuals in this study were in their early working years. 26.8% of the respondents were aged 35-44 years, while 15.5% were aged 45-54 years, representing mid-career professionals. This breakdown indicates that the majority of participants were in their prime working age, particularly in the 25-44 age range.

The data in Table 1 indicates that only a small portion of respondents, 2.1%, held a diploma or certificate qualification. However, the vast majority, 84.5%, had attained at least a first-degree education, highlighting that most respondents were well-educated at the undergraduate level. Additionally, 13.4% of the respondents held a master's degree, showing that a significant number had pursued further advanced education. The data on the number of years respondents have worked at their current hospital shows that 42.3% have been employed for 1-3 years, indicating a significant portion of relatively newer staff. Meanwhile, a slightly higher percentage, 46.4%, have been working for 4-6 years, suggesting that a

substantial number of respondents have a moderate level of experience in their institutions. Lastly, 11.3% of the respondents have been with the hospital for 7-10 years, representing a smaller group with more long-term experience at the current institution.

## D.2. Prevalence of Phishing attacks within Community Hospitals

This section examines how frequently phishing attacks occur within community hospitals. To gather this information, participants were asked to report how many times they have encountered phishing attempts. The responses are visually represented in Figure 1 to Figure 3, offering insights into the frequency of such incidents.



**Figure 1.** Times phishing attempts

Fig 1 illustrates the frequency of phishing attacks experienced by respondents within community hospitals over different time frames. According to the data, 26.8% reported encountering phishing attacks 1-2 times in less than a year. In contrast, a larger group of 57.7% indicated that they experienced phishing attacks 1-2 times within 1-2 years. Finally, 15.5% reported having encountered phishing attacks 1-2 times over the span of 3-4 years. This portion reflects a longer timeline, indicating that while phishing incidents may not be as frequent over the years, they are still a concern for some community hospitals. The data further revealed that 15.5% of the respondents indicated that their hospitals experienced phishing attacks 3-5 times in less than a year. In a slightly longer context, **b** reported encountering 3-5 phishing attacks within 1-2 years. Furthermore, a significant proportion of respondents, 46.4%, noted that within 3-4 years, their hospitals had encountered phishing attacks 3-5 times. Additionally, 11.3% indicated that the question was not applicable to their experience.

As shown in the Fig, the data reveals that 42.3% reported experiencing more than 5 phishing attacks within 1-2 years. Furthermore, 46.4% indicated that over a period of 3-4 years, their hospitals encountered phishing attacks more than 5 times. Additionally, 11.3% selected the option indicating that the question was not applicable to their situation. The insights from the Fig emphasize the ongoing and

frequent nature of phishing attacks within community hospitals, underlining the urgency for enhanced training, resources, and strategies to bolster defenses against these cybersecurity threats.

Table 1 provides a detailed overview of the types of phishing attacks experienced by community hospitals. The responses from the respondents were measured with mean and standard deviations and the significant mean level was fixed at 3.0.

**Table 2.** Responses on phishing attack experience by community hospitals

S/N	Phishing attack experience by hospitals	Mean	Std. Dev.
Ph1	There have been smishing (SMS phishing) attempts targeting our hospital's staff	4.76	.956
Ph2	There have been instances of spear phishing targeting specific individuals in our hospital.	4.66	.956
Ph3	We have experienced email phishing attacks in our hospital.	4.46	.693
Ph4	We have encountered clone phishing emails (duplicates of legitimate emails with malicious links).	3.39	1.271
Ph5	Our hospital has experienced vishing (voice phishing) attacks.	3.28	1.256
Ph6	There have been incidents of whaling attacks in our hospital.	3.24	1.248
Ph7	Our hospital has faced phishing attempts through social media platforms.	2.77	.637

*Mean  $\geq 3.0$  = Agreed*

From Table 2, the respondents indicated that their hospital has experienced various forms of phishing attacks, with a strong consensus on the prevalence of specific types. Smishing, or SMS phishing, which targets staff through fraudulent text messages, was particularly notable, with a high mean score of 4.76 and a standard deviation of 0.956. This suggests that smishing attempts have been frequently encountered and are widely recognized as a threat within the hospital. Similarly, spear phishing, which involves targeted phishing attempts aimed at specific individuals within the hospital, was also commonly reported. The mean score for this type of attack was 4.66, with the same standard deviation of 0.956, indicating that such attacks are also a significant concern and have affected specific staff members. Email phishing attacks, another prevalent form of phishing, were also acknowledged by the respondents, with a mean score of 4.46 and a lower standard deviation of 0.693. This suggests that while email phishing attacks are common, there is slightly less variation in respondents' experiences with this type of attack compared to smishing and spear phishing.

The respondents reported encountering various types of phishing attacks in their hospitals, with clone phishing emails being a notable threat. The mean score for this type of attack was 3.39, with a standard deviation of 1.271, indicating that it is a concern, but with more varied experiences among the respondents. Vishing, or voice phishing, where attackers attempt to deceive individuals via phone calls, also received attention, with a mean score of 3.28 and a standard deviation of 1.256. This suggests that vishing attacks have occurred, though the experiences with it varied among staff. Whaling, a more targeted phishing attack aimed at high-profile individuals such as executives or decision-makers within the hospital, was

also recognized as a threat. The mean score for whaling was 3.24, with a standard deviation of 1.248, indicating that it has been encountered, though not as consistently across the board. Overall, the study's findings reveal that community hospitals frequently encounter several types of phishing attacks, including smishing (SMS phishing), spear phishing, email phishing, clone phishing, vishing (voice phishing), and whaling attacks.

**D.3. Incident response plans outlining the steps in the event of phishing attacks**

The ACSC Incident Categorisation Matrix 2022 framework developed by the Australian Cyber Security Centre (ACSC) was adopted. This matrix helps organizations manage cyber threats effectively by assessing the impact (or effect) and the significance of the incident. The effect (Impact, Success, Sustained, and/or Intent) refers to how successful and severe the phishing attack was. However, the significance (Sensitivity of the Organisation) aspect assesses the importance or sensitivity of the organization targeted by the phishing attack. An attack on a critical national infrastructure organization would be classified as more significant than one targeting a less critical entity.

Community Hospitals adoption of ACSC Incident Categorisation Matrix as part of their incident response plans can categorize the incident using the matrix, they can determine the appropriate response based on the attack's severity. A high-severity attack will demand immediate, large-scale actions, while lower-severity attacks may involve less drastic measures. The ACSC Incident Categorisation Matrix adoption by the hospitals can prioritize and manage phishing attacks. Fig 2 shows how incidents are categorized and guiding the appropriate response.



disruption of essential system and associated service	C6	C5	C4	C3	C2	C1
Extensive comprise	C6	C5	C5	C3	C3	C2
Isolated comprise	C6	C6	C5	C4	C3	C3
Coordinated low-level malicious attack	C6	C6	C5	C4	C4	C3
Low-level malicious attack	C6	C6	C6	C6	C6	C6
Unsuccessful malicious attack	C6	C6	C6	C6	C6	C6
	Member(s) of the public	Small organization(s)	Medium-sized organisations	State government academia/R&D Large organisation	Federal government Government shared services	National security system of national significance

Significance (i.e. sensitivity of the organisation)

Figure 2: Adopted incidents matrix

In hospital's cybersecurity framework, the severity of a phishing incident plays a crucial role in determining the type and scale of the incident response and crisis management actions that will be taken. Higher severity incidents, like those leading to data breaches of sensitive patient information or disruptions in critical healthcare services, will trigger more intensive response measures. Based on the severity, the hospital activates different levels of response protocols. For minor incidents, internal IT teams might handle the issue with minimal disruption, while severe incidents may require full crisis management, including immediate mitigation, communication plans, and even external support.

The hospitals cannot solely rely on the support system from the government for managing phishing incidents. Each hospital must have its own incident response plan to ensure that it can handle threats quickly and effectively without depending entirely on external help. This means hospitals in Ghana must invest in their own cybersecurity infrastructure, training, and response teams to ensure that they can respond to phishing attacks in a timely and appropriate manner, tailored to the hospital's specific needs and operations.

Table 3 shows details about how different levels of phishing incidents are classified, from minor to critical. This classification would guide the hospital in choosing the appropriate level of response and determine when to escalate an incident for external assistance.

Table 3: Incident classification

#	Incident classification	Descriptions
1	Critical	<ul style="list-style-type: none"> <li>• Over 80% of staff (or several critical staff/teams) unable to work</li> <li>• Critical systems offline</li> <li>• High risk to/definite breach of sensitive client or personal data</li> <li>• Financial impact greater than Ghs100,000</li> <li>• Severe reputational damage – likely to impact business long term</li> </ul>
2	High	<ul style="list-style-type: none"> <li>• 50% of staff unable to work</li> <li>• Non critical systems affected</li> <li>• Risk of breach of personal or sensitive data</li> <li>• Financial impact greater than Ghs50,000</li> <li>• Potential serious reputational damage</li> </ul>
3	Medium	<ul style="list-style-type: none"> <li>• 20% of staff unable to work</li> <li>• Small number of non-critical systems affected</li> <li>• Possible breach of small amounts of non-sensitive data</li> <li>• Financial impact greater than Ghs25,000</li> <li>• Low risk to reputation</li> </ul>
4	Low	<ul style="list-style-type: none"> <li>• &lt;10% of non-critical staff affected temporarily (short term)</li> <li>• Minimal, if any, impact</li> <li>• One or two non-sensitive/non-critical machines affected</li> <li>• No breach of data</li> <li>• Negligible risk to reputation</li> </ul>

Source: ACSC (2024)

Community hospitals in Ghana, particularly those facing phishing attacks with varying frequencies – ranging from 1-2 times per year to more than five times annually over a period of 1-3 years or even longer – need to adopt a systematic approach to managing these incidents. A classification system, similar to the ACSC Incident Categorisation Matrix, would be beneficial in categorizing phishing attacks based on their severity. This approach allows hospitals to respond to phishing incidents in a structured and efficient manner, ensuring the appropriate level of action is taken according to the severity of the attack.

#### 1. Low Severity Incidents:

For hospitals that experience minor phishing attempts, perhaps only once or twice in a year, where the attack is limited to a few unsuccessful emails, the response would be relatively simple. These phishing attempts may not have any immediate impact, but they still require attention. On the Response Strategy:

- *Internal IT response:* The hospital's IT department can handle such cases by identifying the phishing emails and blocking the sender. Email filters should be updated regularly to detect common phishing tactics.
- *Awareness training:* Employees should be notified of the phishing attempt and reminded of ongoing cybersecurity training, including recognizing phishing emails and reporting suspicious communications.
- *Review and log incident:* The incident should be documented for future reference and used to refine the hospital's anti-phishing policies.

#### 2. Moderate Severity Incidents

Hospitals experiencing phishing attacks 3-5 times a year, particularly over a period of 1-3 years, are likely to face incidents where some credentials may have

been compromised, or sensitive systems could have been exposed to minor risks. In such cases, hospitals must employ more robust responses. On the response strategy:

- *Immediate account lockdown:* Compromised accounts should be locked, and the affected users must be logged out of the system.
- *Password reset and MFA enforcement:* All compromised accounts must undergo password resets, and multi-factor authentication (MFA) should be enforced to add an extra layer of protection.
- *Incident investigation:* IT staff should investigate how the phishing email bypassed existing filters, assess whether sensitive data was accessed, and track any malicious activity. Logs and network traffic should be reviewed.
- *Notification and remediation:* Affected users and relevant departments should be informed. Awareness training should be refreshed for all employees, with specific lessons from the phishing attack highlighted.

### 3. High Severity Incidents

When phishing attacks occur more than five times in a year, or when hospitals experience more severe breaches where sensitive patient data or key systems are compromised, a more aggressive response is required. On the response strategy:

- *Incident response team activation:* The hospital's cybersecurity team or incident response team should immediately be mobilized to assess and mitigate the damage.
- *System isolation:* Affected systems or networks should be isolated to prevent the spread of the attack. Backup systems should be prepared for critical functions.
- *Data breach protocols:* If sensitive patient data or other critical information has been compromised, the hospital must follow data breach protocols, which may involve notifying the affected patients, healthcare regulators, and law enforcement.
- *Forensic investigation:* A detailed forensic analysis should be conducted to identify the extent of the breach, how the phishing attack was successful, and what data was accessed.
- *Recovery and restoration:* Compromised systems must be restored from backups, with all vulnerabilities addressed before they are brought back online.

### 4. Critical Severity Incidents

For hospitals that have experienced more than three years of regular phishing attacks, or where a major breach has caused widespread disruption to healthcare services, the response must be swift and coordinated. On the response strategy:

- *Full crisis management:* A full crisis response plan must be activated, involving hospital leadership, IT, legal, and communications teams. External cybersecurity experts may need to be brought in to assist with containment and mitigation.
- *Systemwide shutdown (if necessary):* If the attack is severe enough, the hospital may need to shut down its IT systems and switch to manual operations for critical functions, such as patient care.

- *Engagement with national cybersecurity authorities:* In cases where the phishing attack severely impacts hospital operations, national cybersecurity agencies like the Cyber Security Authority (CSA) in Ghana may need to be contacted for support.
- *Public and patient communication:* The hospital must communicate with patients, employees, and the public regarding the attack, explaining the steps being taken to resolve it, the extent of the impact, and timelines for restoration of services.
- *Comprehensive recovery:* After the attack is mitigated, systems must be thoroughly checked and restored. Any compromised systems should be rebuilt, and security protocols should be upgraded. This may involve patching vulnerabilities, resetting credentials, and implementing stronger access controls.

Through the adoption of a classification system, community hospitals in Ghana can better handle phishing attacks, ensuring that each incident receives the appropriate response based on its severity. This structured approach will strengthen the hospital's overall security posture and enhance its ability to safeguard patient data and hospital operations.

**D. Post Incident Review**

The community hospital must conduct a comprehensive evaluation of Post Incident Review (PIR) after experiencing a cybersecurity incident. The purpose of a PIR is to identify the root causes of the incident, assess the effectiveness of the response, and determine areas for improvement. The review can take two forms: *Hot Debrief*-This is an immediate discussion held after the hospital has recovered its networks and systems. It focuses on capturing fresh insights while the incident is still recent. *Formal Debrief*-Held after a more detailed incident report is completed, typically within two weeks, this formal review delves deeper into the causes and responses to the incident. Key questions to address during the PIR include:

- Root causes: What were the underlying issues that led to the incident?
- Preventability: Could the incident have been avoided? If so, how?
- Response Effectiveness: What aspects of the response worked well?
- Future Improvements: How can the hospital's response be enhanced for future incidents?

Any recommendations or improvements identified during the PIR should be documented in an Action Register, which can then be used to track and implement necessary changes. During the PIR, PPOSTTE model can be used to reflect on critical elements of the incident response. This model helps ensure a thorough examination of the incident by breaking it down into key components:

**Table 4.** PPOSTTE model

#	Categories	Issue
1	Personnel:	Who was involved, and how did they respond?

---

2	<b>Policies:</b>	Were the hospital's cybersecurity policies effective?
3	<b>Operations:</b>	How well did operational processes work during the incident?
4	<b>Systems:</b>	Were hospital's IT systems robust enough to withstand the attack?
5	<b>Training:</b>	Were staff adequately trained to handle the incident?
6	<b>Technology</b>	Was the technology in place sufficient to detect and mitigate the incident?
7	<b>Evaluation</b>	How should the overall response be evaluated and improved?

---

By using the PPOSTTE model, the community hospitals can systematically review their incident response and identify actionable steps to strengthen their cybersecurity posture.

### **E. Discussion**

The study highlighted that a notable portion of hospital staff reported encountering phishing attacks within 1-2 year. It appeared from the study that community hospitals frequently encounter several types of phishing attacks, including smishing (SMS phishing), spear phishing, email phishing, clone phishing, vishing (voice phishing), and whaling attacks. These findings align with previous reports in the healthcare sector. For instance, Alder highlighted a similar incident at UnityPoint Health, where a phishing campaign between March and April 2018 involved SMS phishing, phishing emails, and whaling attacks [16]. In that case, the attackers impersonated UnityPoint executives, leading to the compromise of employee email accounts. Similarly, Hovhannisyan reported that in 2022, over 50 million patient records were compromised through a variety of phishing attacks, including email phishing, vishing, and whaling [28]. This represented a 44% increase in hacking incidents in healthcare, underscoring the widespread and rising threat that phishing attacks pose to hospitals. These findings reinforce the need for robust cybersecurity measures within healthcare institutions, as these attacks can lead to significant breaches and loss of sensitive patient information.

The findings also align with the HIPAA report, which noted a significant increase in phishing attacks within the healthcare industry in 2023. The industry saw an unprecedented rise in email phishing, clone phishing, vishing, and whaling attacks, contributing to numerous data breaches [15]. According to HIPAA, there were 114 breaches that involved 100,000 or more records, with the most severe breach affecting 11.27 million records. These statistics underscore the persistent cybersecurity challenges healthcare institutions face. The study found that the ACSC Incident Matrix 2022 framework would help the community hospitals to manage cyber threats effectively by assessing the impact and the significance of the incident. The classification system is beneficial in categorizing phishing attacks based on their severity. This approach allows hospitals to respond to phishing incidents in a structured and efficient manner, ensuring the appropriate level of action is taken according to the severity of the attack.

### **E. Conclusion**

Ghana is facing a significant rise in phishing incidents, particularly impacting critical institutions like hospitals. This surge has drawn attention from both law enforcement and cybersecurity sectors, highlighting the urgent need for stronger defenses. The study revealed that phishing attacks pose an ongoing challenge for community hospitals, occurring at varying frequencies over different time frames. The persistence of these incidents emphasizes the importance of long-term strategies, including improved cybersecurity measures, staff training, and awareness programs, to protect sensitive patient data. Critical vulnerabilities such as unsecured networks, untrained staff, weak authentication protocols, and insufficient security audits exacerbate the risk of phishing attacks, leading to financial strain and reputational damage. Despite the emotional and financial toll on hospital staff, the overall productivity remains unaffected. The study concludes that implementing the ACSC Incident Matrix 2022 framework would be instrumental in helping hospitals effectively assess and manage cyber threats. The CSA in collaboration with the Ministry of Communication (MoC) and Ghana Health Service, should launch national awareness campaigns focusing on the dangers of phishing attacks, particularly within the healthcare sector. These campaigns should educate healthcare professionals and the general public about phishing techniques, prevention measures, and the importance of reporting suspicious activities.

#### **F. Acknowledgement**

I would like to express my deepest and sincerest appreciation to George Asante for his valuable guidance, advice, support as well as motivation. I also acknowledge the help of the various lecturers at the Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development, for the knowledge imparted in me and also helped in the completion of my Masters degree studies.

#### **G. References**

- [1] S. Dawodu, A. Omotosho, O. Akindote and S. Ewuga, "Cybersecurity Risk Assessment in Banking: Methodologies and Best Practices," *Computer Science & IT Research Journal*, vol. 4, pp. 220 - 243, 2023.
- [2] K. AL-Dosari, N. Fetais and M. Kucukvar, "Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenge," *Cybernetics and Systems*, vol. 55, no. 2, pp. 302-330, 2024.
- [3] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan and J. N. Sebire, "Phishing in healthcare organisations: threats, mitigation and approaches," *BMJ Health Care Inform*, vol. 26, pp. 1-13, 2019.
- [4] B. T. Akinbowale, O. Ademuyiwa, A. A. Akinyele and O. D. Akinwale, "Postnatal home visit: An effective strategy to a successful postnatal care," *Research Journal of Health Sciences*, vol. 11, no. 4, pp. 377-383, 2023.
- [5] E. M. Kwofie, "Cybercrime in Ghana: Trends, challenges and prospects," *International Journal of Cyber Criminology*, vol. 13, no. 2, p. 127-139, 2019.
- [6] R. K. Nartey, "Ghana: A victim of cybercrime.," *Modern Ghana.*, pp. 13-23, 2021.
- [7] D. Ennin and R. O. Mensah, "Cybercrime in Ghana and the Reaction of the

- Law.," *Journal of Law, Policy and Globalization*, vol. 84, p. 36, 2019.
- [8] O. Agyemang, R. O. Mensah and E. Asare, "User perceptions of information security: Evidence from Takoradi Technical University," *Journal of International Cooperation and Development*, vol. 5, no. 3, p. 14, 2022.
- [9] A. Di Nicola, "Towards digital organized crime and digital sociology of organized crime," *Trends in organized crime*, pp. 1-20, 2022.
- [10] J. Świątkowska, "Tackling cybercrime to unleash developing countries' digital potential," *Pathways for Prosperity Commission Background Paper Series*, vol. 33, pp. 1-13, 2020.
- [11] M. M. Ali and N. F. Mohd Zaharon, "Phishing-A cyber fraud: The types, implications and governance," *International Journal of Educational Reform*, vol. 33, no. 1, pp. 101-121, 2024.
- [12] A. K. Ghazi-Tehrani and H. N. Pontell, "Phishing evolves: Analyzing the enduring cybercrime," In *The New Technology of Financial Crime*, pp. 35-61, 2022.
- [13] J. Witts, "Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know," Retrieved from <https://expertinsights.com/insights/healthcare-cyber-attack-statistics/>, Vols. Accessed: June, 20, 2024., 2024.
- [14] D. Dolezel and B. Hewitt, "Social determinants of health literacy: a cross-sectional exploratory study," *Health Promotion International*, vol. 38, no. 5, pp. 1-27, 2023.
- [15] S. Alder, "2020-2021 HIPAA violation cases and penalties," *The HIPAA Journal*, pp. 1-20, 2022.
- [16] S. Alder, "Healthcare Data Breaches Due to Phishing," *HIPPA Journal*, pp. Retrieved from <https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/>. Accessed: June, 20, 2024., 2024.
- [17] F. A. Khiralla, "Statistics of cybercrime from 2016 to the first half of 2020," *International Journal of Computer Science and Network Security*, vol. 9, no. 5, pp. 252-261, 2020.
- [18] M. M. Singh, R. Frank and W. M. Zainon, "Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1658-1668, 2021.
- [19] A. Petrosyan, "Outcomes of successful phishing attacks in companies worldwide 2021-2023.," Retrieved from <https://www.statista.com/statistics/1350723/consequences-phishing-attacks/>. Accessed: August, 6, 2024., 2024.
- [20] K. Abouelmehdi, A. Beni-Hessane and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of big data*, vol. 5, no. 1, pp. 1-18, 2018.
- [21] E. M. Rogers, "Diffusion of Innovations," Retrieved from <https://www.goodreads.com/book/show/134781>. Accessed: July, 5, 2024, 2005.
- [22] C. Pinho, M. Franco and L. Mendes, "Application of innovation diffusion theory to the E-learning process: higher education context," *Education and*

- Information Technologies, vol. 26, no. 1, pp. 421-440, 2021.
- [23] R. Frei-Landau, Y. Muchnik-Rozanov and O. Avidov-Ungar, "Using Rogers' diffusion of innovation theory to conceptualize the mobile-learning adoption process in teacher education in the COVID-19 era," *Education and information technologies*, vol. 27, no. 9, pp. 12811-12838, 2022.
- [24] S. M. Faisal and S. Idris, "Innovation factors influencing the supply chain technology (sct) adoption: Diffusion of innovation theory," *International Journal of Social Science Research*, vol. 2, no. 2, pp. 128-145.
- [25] M. K. Okour, C. W. Chong and F. A. Abdel Fattah , "Knowledge management systems usage: application of diffusion of innovation theory," *Global Knowledge, Memory and Communication*, vol. 70, no. 8, pp. 756-776., 2021.
- [26] Australian Cyber Security Centre (ACSC), "Cyber Incident Response Plan," in Retrieved from <https://www.cyber.gov.au/>. Accessed: July, 5, 2024., 2024.
- [27] M. Casula, N. Rangarajan and P. Shields, "The potential of working hypotheses for deductive exploratory research," *Quality & Quantity*, vol. 55, no. 5, pp. 1703-1725, 2021.
- [28] G. Hovhannisyan, "The healthcare sector needs better defence against phishing. ." in Retrieved from <https://www.openaccessgovernment.org/healthcare-sector-phishing-cyber-attacks/162396/>. Accessed: June, 20, 2024, 2023.