information

Article

Investigation into Phishing Risk Behaviour among Healthcare Staff

Prosper Kandabongee Yeng [1,*], Muhammad Ali Fauzi [1], Bian Yang [1] and Peter Nimbe [2]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Teknologivegen 22, 2815 Gjøvik, Norway
[2] Department of Information Security and Communication Technology, University of Energy and Natural Sesources, Sunayni P.O. Box 214, Ghana
* Correspondence: prosper.yeng@ntnu.no

Abstract: A phishing attack is one of the less complicated ways to circumvent sophisticated technical security measures. It is often used to exploit psychological (as as well as other) factors of human users to succeed in social engineering attacks including ransomware. Guided by the state-of-the-arts in a phishing simulation study in healthcare and after deeply assessing the ethical dilemmas, an SMS-based phishing simulation was conducted among healthcare workers in Ghana. The study adopted an in-the-wild study approach alongside quantitative and qualitative surveys. From the state-of-the-art studies, the in-the-wild study approach was the most commonly used method as compared to laboratory-based experiments and statistical surveys because its findings are generally reliable and effective. The attack results also showed that 61% of the targeted healthcare staff were susceptible, and some of the healthcare staff were not victims of the attack because they prioritized patient care and were not susceptible to the simulated phishing attack. Through structural equation modelling, the workload was estimated to have a significant effect on self-efficacy risk (r = 0.5, *p*-value = 0.05) and work emergency predicted a perceived barrier in the reverse direction at a substantial level of r = −0.46, *p*-value = 0.00. Additionally, Pearson's correlation showed that the perceived barrier was a predictor of self-reported security behaviour in phishing attacks among healthcare staff. As a result, various suggestions including an extra workload balancing layer of security controls in emergency departments and better security training were suggested to enhance staff's conscious care behaviour.

Keywords: security practice; healthcare; phishing attack; social engineering; smishing

Citation: Yeng, P.K.; Fauzi, M.A.; Yang, B.; Nimbe, P. Investigation into Phishing Risk Behaviour among Healthcare Staff. *Information* **2022**, *13*, 392. https://doi.org/10.3390/info13080392

Academic Editor: Georgios Kambourakis

Received: 12 July 2022
Accepted: 5 August 2022
Published: 18 August 2022

1. Introduction

Digitization refers to a holistic transformation of different sectors by adopting IT systems [1,2]. The systems that are commonly used in the transformation include software applications, networks, and hardware systems. This has been an ongoing course of action in the eHealth space, such as electronic health records (EHRs), medical devices, decision support, and telemedicine, among others. The recent COVID-19 has expedited the adoption rate and expanded the use of information communication technology (ICT) in the healthcare sector. The World Health Organization (WHO) confirmed this by indicating that there has been a tremendous increase in the use of mobile devices such as smartphones, tablets, embedded devices [3,4], and laptops for the self-management of healthcare, diagnosis, treatment, and disease surveillance [5].

Countries in Africa such as Ghana are not left out in the digitization drive in healthcare. Many healthcare facilities have adopted various kinds of ICT systems [6–8], including EHR, to improve their healthcare delivery. The major threat in digitization relates to issues of cyber security, especially the human aspect of information security.

Verizon [9] recently reported that human factors across the globe accounted for a woeful 85% of the cyber security incidents in 2020, suggesting that the human element is now the leading targeted mode of entry into healthcare systems.

According to Healthcare IT News [10], healthcare systems are ideal destinations for cyber criminals to launch ransomware attacks because healthcare provision is associated with time sensitivity and urgency when accessing patient records, especially during an emergency. This creates a sense of urgency for management to pay a ransom in ransomware attack scenarios in order to rescue data. Furthermore, there are many human vulnerabilities in healthcare that can enable attackers to gain illegitimate access to systems. For instance, the healthcare environment consists of people (staff, end users, developers, etc.), working under busy and intensive conditions that can compel them to unintentionally click on malicious links or miss security measures. Most ransomware attacks start with the human as they present the main vulnerability in the hospital. This observation was supported by Chernyshev et al., who identified ransomware to be the most common type of malware in use, of which phishing was the most popular technique often used in data breaches in healthcare [11]. In a ransomware attack, criminals can encrypt data or deny service and demand for ransom to be paid before releasing the service [12]. Phishing methods are often used, which involve sending a malicious message to the targets that aimed to deliver payload into the IT system with the anticipation that at least a one of them would become victims. It is one of the easier ways to circumvent sophisticated technical security measures by exploiting psychological factors of the human elements to gain unauthorized access. The mode of communication that is often used to lure targets includes social engineering-based phishing such as email, SMS (smishing), and voice (vishing) communication. Social engineering-based phishing attacks include deceptive, spear, and whaling approaches. Deceptive phishing involves targeting a larger group of persons, spear phishing targets specific organisations or groups of people, and the whaling approach targets a high-level professionals (including the CEO and the CTO) [13]. The phishers usually craft their messages so that they have a various range of tones such as greed, urgency, curiosity, helpfulness, and fear with the goal of luring the target persons into taking the baits.

This study therefore examined the phishing susceptibility level among healthcare staff in Ghana amidst work and perception factors. It seeks to determine the effect of work factors and perception of healthcare staff and their phishing appraisal threat levels and the ability to resist phishing bait. Such knowledge may help hospital authorities to adopt better strategies to improve upon the security practices of the healthcare staff in a way towards mitigating real attacks. This is a combined study which assesses the targets' actual phishing susceptibility behaviour together with their self-reported security practice relating to phishing. To achieve a better phishing simulation study, a comprehensive literature review on phishing simulation attacks was first conducted to assess and analyse already-used techniques or methods and tools and to determine gaps in the existing studies. Additionally, ICT and cyber security practices were observed in the hospital. This provided better knowledge for the researchers to launch a simulated SMS-based phishing attack termed as smishing [14,15]. This study contributes to the body of knowledge in various ways. The relationship between the actual and self-reported phishing behaviour of the healthcare staff was assessed. Furthermore, our study examined the relationship between work factors and psychological factors on self-reported behaviour relating to phishing. The psychological constructs which met the needs of the study objective were drawn from the health belief model (HBM) [16,17] and protection motivation theory (PMT). The state-of-the-arts pertaining to phishing simulated studies in healthcare was provided. Ethical aspects of in-the-wild studies were also assessed. Furthermore, the reasons why the healthcare staff fell victim to the attack were also collected and examined. To the best of our knowledge, this is the first of its kind within the healthcare space that we conducted such an intensive study, guided by the state-of-the-arts studies. The paper is structured as follows. The background of psychological and work factors in a phishing simulation study is presented. This is followed by the study approaches. Findings on the state-of-the art, click rates, and surveys are then shared. The results are subsequently discussed and a conclusion is presented.

1.1. Perception and Work Factors with a Phishing Simulation Study

Falling victim to a phishing attack is more dominant in security attacks because attackers tend to exploit the psychological factors of their target persons into clicking the links [18]. However, various studies [19–23] in phishing susceptibility in healthcare have not explored these psychological theories, except a study by Jalali et al. which explored the theory of planned behaviour and collected felt trust [24]. This gap in the literature provides a basis for our study in which we explore the relationship between work factors and psychological factors that can be influenced to improve security behaviour relating to a phishing attack. This study therefore explores perception constructs in HBM and PMT. Perception relates to the mindset and psycho-socio-cultural effects of users from an IT infrastructure and how that affects cyber security practice. HBM and PMT theories have been extensively used to explain human behaviour and have been found useful in assessing other information security practices among users [17,25,26]. For instance, Ng et al. investigated the computer behaviour of users having used the HBM. They study identified perceived susceptibility, benefits, and self-efficacy to be determinants of email related to security behavior [17]. Anwar et al. showed that gender has an effect on security self-efficacy. Moreover, Humaidi et al. proposed a comprehensive framework for analysing security practice based on various perception theories [26]. In fact, a mapping review on related theories to assess security practice was conducted by [27] and identified various perception constructs including perceived vulnerability and perceived barriers. As these studies showed that perception constructs are widely used for assessing motivation in information security research, the specific context (i.e., phishing in healthcare) can have major influence on the behavioral intention of users [24]. For instance, the perception of the severity of impact of a non-critical infrastructure may be lower than that of a critical infrastructure such as healthcare in data breach scenarios that violates the availability trait.

In assessing security practices related to phishing among healthcare staff, we therefore opine that it is necessary to explore perception factors in relation to phishing susceptibility. Such factors can then be improved for better security practice in phishing through various intrinsic and extrinsic motivations [28,29]. To this end, psychological constructs that were used in HBM and PMT were deemed suitable to achieving this study objective.

In HBM, the predictor of a person's possible health-related behaviour is dependent on the belief of health threats (illness disease) and the effectiveness of the recommended actions (treatments and medicines) [17,30]. Back in the 1950s, this was derived to prevent sicknesses or help already-sick persons to recover. HBM has been widely used in the healthcare sector as people can perceive the severity of disease and the recommended action to make better health behaviour choices. HBM has found its way into observing information security practice in the human aspect of information security [27,31]. For instance, the human aspects are normally observed for their security susceptibility perception and their belief in the organization's cyber security policy to predict their likelihood behaviour [17]. HBM consists of perceived susceptibility or vulnerability (PV), perceived severity (PS), perceived benefit (PBf), perceived barriers (PBs), cues to action (CA), and self-efficacy (SE). PV is the risk perception of contracting a disease or falling victim to a cyber attack while PS is the perception of the adverse impact of the respective disease (death, disability, family life, or social relation) or security attack (loss of data, punishment, etc.). PBs are viewed as obstacles that are to be overcome in order to follow recommended solutions. In the same trend, the assessment of one's ability or confidence level to follow the recommended solutions is known as perceived SE. Additionally, CA refers to internal or external stimuli that influence one to adapt to the recommended solution. Stimuli include pain, disorders, advice, and knowledge of the situation of victims. PBf includes the perception of the available opportunities of the recommended course of actions. Common drawbacks that have been opined include its limitation to measure attitude, habitual behaviour, or environmental or economic factors with the assumption that the threat knowledge is known by all persons.

PMT on the other hand consists of threat and coping appraisals which are used in decision making by persons under stressful or harmful circumstances [32–34]. The decisions usually involve protecting oneself. The threat appraisal consists of PV and PS, which the person who is involved in the stress or harmful situation uses to appraise the level of the threat. PV measures the level of susceptibility of the person while PS is used to gauge the level of severity of the threatening event. Furthermore, the coping appraisal consists of response efficacy (RE), SE, and the response cost (RC). Within the context of PMT, RE refers to the perception of the effectiveness of the recommended action, while RC is the cost component of the recommended measures.

1.2. Work Factors and Security Practice

In addition to the psychological factors, the work of healthcare staff is characterized by erratic workload [24,34,35] and work emergency [27,36].Work factors in this study refer to work-related events, such as workload and work emergency that are associated with the use of IT systems in healthcare. Workload consists of the quantum of tasks that one has to perform within a given period, while work emergency refers to the urgency used to accomplish a given task [37]. Particularly in healthcare, time is an important factor where therapeutic measures can be required in a timely manner, without which lives can be lost. In some situations, patients can queue for many hours, waiting to be seen by scarce healthcare professionals. All these create work-related stresses which can have an impact on the phishing-related behaviour of the healthcare worker. Even though various research activities [25,26,31,38] dealt with the perception aspect of security practice in healthcare, little is known about how work factors (workload, work emergency) contribute to cyber security practice among healthcare workers. Jalili et al. made efforts to address this by analysing how workload contributes to cyber security behaviours in phishing [24]. However, work factors in healthcare were not completely addressed as work emergency was not included in the study. Moreover, workload that was included only served as a moderating variable and was not related to the perception variables to assess the effects. That is why we ague that since workload and work emergency are mostly associated with healthcare, especially in the COVID-19 pandemic, security practice can be impacted either directly or indirectly. This gap was also realized and proposals for empirical studies [27,34,36]. Relying on the aforementioned thoughts, the following research questions and hypotheses were formed:

- RQ1: What is the state-of-the arts in phishing simulation studies in healthcare?
- RQ2: How can phishing attack simulation study be conducted successfully in healthcare without interfering with the hospital's normal operations and exposing their system to potential attacks?
- RQ3: Are healthcare workers susceptible to phishing attacks?
- RQ4: What circumstances trigger healthcare workers to click on malicious links?
- RQ5: What is the relationship between the actual behaviour and self-reported behaviour among healthcare workers?
- RQ6: What are the ethical requirements for an in-the-wild-field study in phishing simulation?

In a similar study, Jalili et al. estimated the effect of self-reported behaviour on the actual behaviour related to phishing attacks [24]. In that vain, we tried to compare the self-reported security behaviour related to phishing and the actual behaviour of healthcare staff of having clicked the link. As this study focuses on assessing threats of phishing attacks among healthcare staff and their ability to counteract, we expect that staff of hospitals have a good perception of security practices. Therefore, healthcare staff can appraise security threats and overcome risky perceptions to comply with the security policy amidst work factors and perceptions, as shown in Figure 1. Based on this objective, we hypothesized that:

- H1: Work emergency has a negative influence on perceived barrier.
- H2: Work emergency negatively influences perceived vulnerability.
- H3: Work emergency has a negative influence on self-reported security behaviour (IB).

- H4: Work emergency is negatively related to perceived severity risk.
- H5: Work emergency has a negative effect on perceived self-efficacy.
- H6: Workload has adverse influence on perceived barrier.
- H7: Workload is negatively related to perceived vulnerability.
- H8: Workload has a negative effect on self-reported security behaviour.
- H9: Workload has negative influence on perceived severity.
- H10: Workload has a negative influence on perceived self-efficacy.
- H11: Perceived barrier has a negative influence on self-reported security behaviour.
- H12: Perceived vulnerability has a positive influence on self-reported security behaviour.
- H13: Perceived severity has a positive influence on self-reported security behaviour.
- H14: Perceived self-efficacy has a positive influence on self-reported security behaviour.
- H15: Perceived barrier has a negative mediating effect on work emergency and self-reported security behaviour.
- H16: Perceived barrier has a negative mediating effect on workload and self-reported security behaviour.
- H17: Perceived vulnerability has a positive mediating effect on work emergency and self-reported security behaviour.
- H18: Perceived severity has a positive mediating effect on workload and self-reported security behaviour.
- H19: Perceived self-efficacy has a positive mediating effect on work emergency and self-reported security behaviour.
- H20: Perceived self-efficacy has a positive mediating effect on workload and self-reported security behaviour.
- H21: Perceived vulnerability has a positive mediating effect on workload and self-reported security behaviour.
- H22: Perceived severity has a positive mediating effect on work emergency and self-reported security behaviour.
- H23, H24, and H25 are respectively moderating variables of experience, gender, and position that have potential effect on self-reported behaviour.

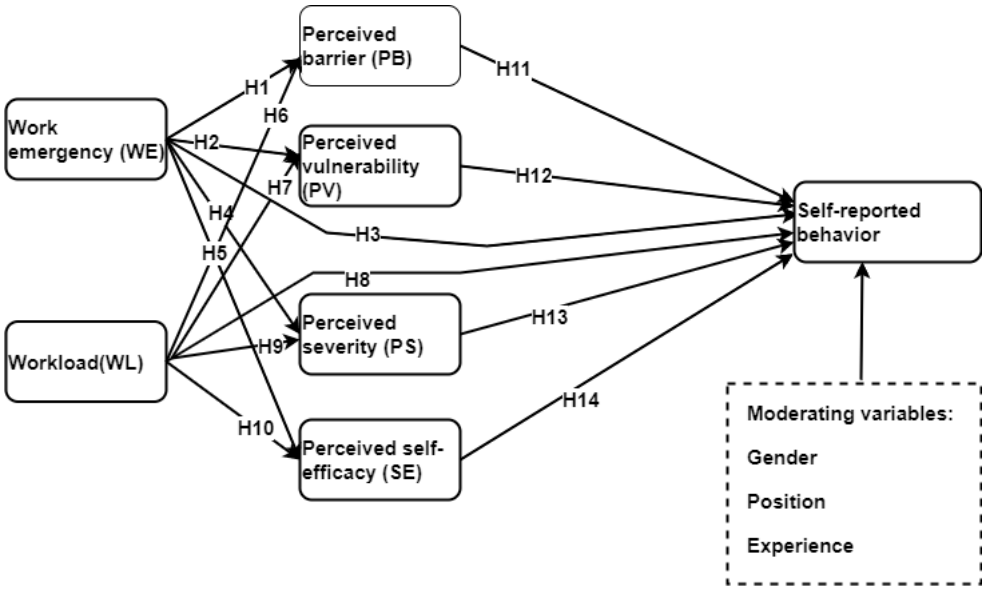

Figure 1. Research model for SMS-based phishing simulation study.

As shown in Figure 1, the latent variables of security perceptions, including PV, PS, PB, SE, work emergency, and workload, are related to the intended security behaviour construct. Additionally, the model also showed the mediating effect of the perception

factors between the work factor constructs and the IB. Position, work experience, and gender were considered as the moderating variables.

2. Research Methodology

Four approaches were used in this study, as shown in Figure 2.

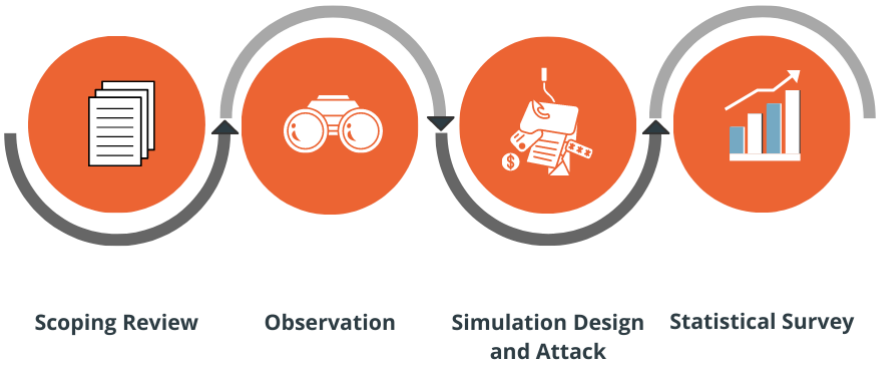

Figure 2. Study processes.

First, a scoping review was conducted that aims to identify phishing simulating study methods/techniques, tools, and study gaps in practically assessed literature. Gray literature was also searched for phishing simulation tools.

This was followed by observing hospitals to understand the ICT and security practices in the hospital. Guided by these, an SMS-based phishing simulation study was set up and deployed. The deployment was carried out alongside a survey of both qualitative and quantitative approaches. The details of each approach are provided in the following subsections.

2.1. Scoping Review

The aim of the review was to address the state-of-the-arts by identifying, assessing, and analyzing the various approaches and techniques for use in critical infrastructure such as healthcare. A scoping review was adopted as the study aimed to assess, analyse, and evaluate topics relating to phishing simulation in healthcare, as categorized in Table 1. We therefore searched for phishing-related practical studies in healthcare in PubMed, Google Scholar, Science Direct/Elsevier, IEEE Explore, and ACM Digital. The scoping review took place between September 2021 and December 2021. The following keywords and phrases were used to combine the keywords: 'phishing attack', 'social engineering', 'healthcare', 'information security practice', and 'information security behavior'. Boolean functions of 'AND', 'OR', and 'NOT' were also used. Peer-reviewed journals and articles were considered. Articles were first selected through a quick read-through of the titles, abstracts, and keywords for records that seem to match the inclusion and exclusion criteria. Duplicates were removed and the rest of the articles were fully read and assessed. Additionally, phishing related tools were further explored in grey literature with the key phrase "phishing tools" in the Google search engine. The findings were reported by adapting to Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram [39].

Table 1. Data categorization and definitions.

No	Categorisation	Definitions
1	Methods/Technique	The scientific approach which was used in the study (e.g., a survey, simulated attack, interview)
2	Tools	Social engineering tools which were used in the study (e.g., gophish,)
3	Psychological, social, and demographic (PSC) factors	Social engineering theories used to coerce targets into clicking on malicious links (PMT, TPB, and TTAT)
4	Storyline strategy	Context within which adversaries craft phishing messages to bait targets
5	Cue	This defines the clue used in the study
6	Security and privacy measure of tools	This describes the behaviour of the tools (e.g., whether the tool collects some sensitive data of the target hospital and targeted persons in the study)
7	Ethical measures	This defines the consideration of the relative effect on participants (e.g., whether participants consented to the study)
8	Risk measures and measures to be adopted to conduct risk-free assessment in the target environment.	
9	Social demographic factors	Factors such as gender, workload, and emergency situations which were considered in the attack
10	Situational context of healthcare staff prior to clicking the link	This defines what the healthcare workers were immediately engaged in prior to clicking the link
11	Susceptibility reasons	This defines the reasons for clicking the link by the staff
12	Survivors bias	Analysis of the characteristics of healthcare workers who only clicked the link without considering those who did not click the link.

2.1.1. Inclusion and Exclusion Criteria

Only articles that were practically implemented in phishing-related studies in healthcare were included in the study. Articles outside the scope including literature in other languages, except English, were excluded.

2.1.2. Data Collection, Categorization, and Analysis

In line with the objectives of this study, data collection and categorization were developed based on authors' discussions. The categories were defined purposely to assess, analyze, and evaluate the studies, as shown in Table 1.

The identified articles were processed based on the categorize that were defined in Table 1. A number of counts (n) and proportions were computed on each category.

2.2. Observation at the Hospitals

We adopted a 'fly-on-the-wall approach' by observing unnoticed healthcare workers' security practice. So, the researchers were introduced to the healthcare workers as temporal staff of the IT department who were to collect feedback on issues relating to the information systems that were being used by the healthcare staff. We presume that healthcare workers would not behave in their usual way if they were aware that their security practices were

being observed [40]. We observed general security practice, but much attention was paid to physical security, internet use, email use, social media use, password management, incident reporting, information handling, and mobile computing, as these areas are prone to security policy violations within the context of the human element [34,41–43]. The purpose of this observation was to complement the review approach to answer RQ2, and thus to understand effective methods of safely and effectively conducting phishing simulation studies in healthcare.

2.3. Phishing Simulation Design and Attack

With regard to social engineering tests, the goal was to determine if healthcare workers using IT systems are able to identify phishing-related malicious messages amidst work factors and their perception. This approach was to find answers to RQ3 and RQ4 together with the hypotheses. Guided by findings from the observations, SMS-based phishing was adopted in this simulation attack because the hospitals had not configured corporate email systems, but rather uses mobile devices such as laptops and mobile phones in their provision of healthcare services. Since this was a simulated study, we did not want to use a critical infrastructure such as healthcare as a test range. Instead, these tests were conducted through the mobile contacts of the healthcare staff. We opined that if healthcare staff can be security-conscious on their cellphones, the healthcare environment can improve. So the plan was that healthcare staff will receive a "malicious message" with a "malicious link". If the target person clicks on the link, the click event would be registered in a database and the person would be redirected to a questionnaire instrument. While other studies have used multiple clicks in similar studies [13,20], the goal of those studies is mainly to access the effectiveness of phishing-related training and education. In this study, a click of the link was used, just as in a recent study conducted by [24]. This is because the goal of Jalali et al. and other current studies is geared towards assessing the effects of theoretical factors.

The questionnaire instrument was used to support in the identification of current circumstances that lead to the clicking of the link together with the behavioural intentions of that user. A secured domain name was registered to look similar to the hospitals' domain, except that the domain name type was different (i.e., information instead). This was the major phishing cue or clue that the researchers wanted to observe from the target. So, a secured online questionnaire tool, created by Nettskjema [44], was used to design a questionnaire for this test. Nettskjema is deemed secured and safe for developing questionnaires as compared to other online forms. Additionally, a website was developed with a database to collect the click events of users. To comply with privacy and security regulations, each click event was encrypted with SHA-256. The click events were collected alongside their date and a time stamp in order to know when each click event occurred. The website was hosted with the registered domain and the link, together with the phishing message, was sent to the targets via SMS. The phishing message was chosen to reflect events that were ongoing at the hospital, including those relating to COVID-19, as shown in Figure 3. The simulation attack began on the 24 November 2021 and ended on the 8th of December 2021. After a week, we closed all responses to the questionnaire and made phone calls to participants to collect qualitative data relating to why they clicked the phishing link. Only participants who remembered having received the SMS and read the content were given audience to provide their responses.

If a respondent clicked on the link of the questionnaire, the click event was first registered in the database and then the questionnaire was opened. To understand the security practice of the respondents, information was collected from the respondents concerning what he or she was engaged in just before clicking the link. The purpose of collecting the information was to understand why the user clicked on the link. For example, the respondent was busy serving patients, etc. This will provide input into providing the needed training with regards to phishing attacks. The personally identifiable records of respondents were not to be stored in the database, and, of course, the link was not actually malicious, as depicted in Figure 4.

Hello,
Your name came up during contact tracing of a victim diagnosed with the delta variant of the coronavirus.
Kindly click the link www.[redacted].info for more detailed information and complete the form to enable the team reach out and assist you with treatment.
Kindly remember to keep this information confidential and private and talk to the team if you have any queries.
Regards, [redacted] Covid-19 Management Team

Figure 3. Deceptive message for SMS-based phishing simulation.

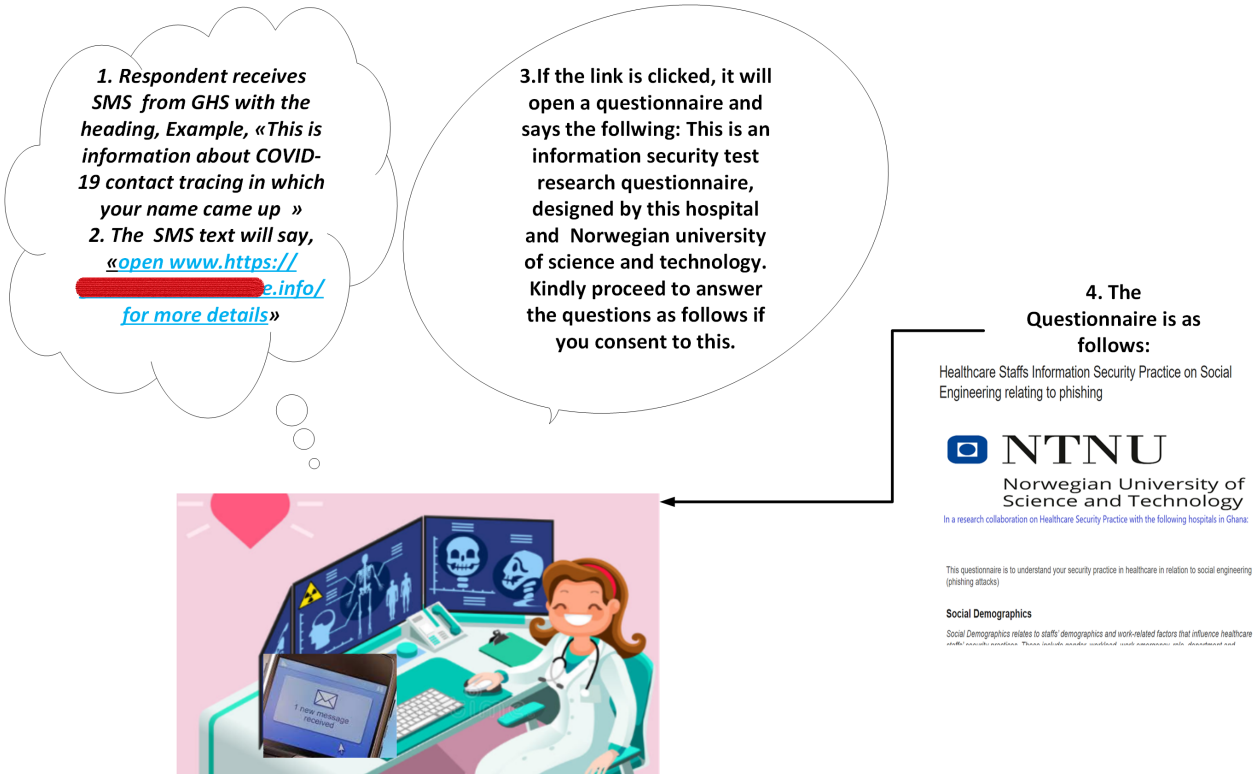

Figure 4. Framework for SMS-based phishing simulation.

2.4. Statistical Survey

A total of 167 healthcare staff agreed to join the study through a convenience sampling. Due to ethical, privacy, and security concerns, the identity of these hospitals and the respondents were not disclosed in this paper. To deal with survival biases [24,45], participants who did not click the link and those who clicked the link but failed to fill out the questionnaire were contacted by phone to find out their reason for doing so.

The questionnaire instrument in this study has a social demographic section that collected attributes such as gender, position at work, and length of years of experience of the respondents. Another section collected data on the work situation such as the workload, work emergency, what the participant was engaged in, and his or her expectation prior to clicking the link. Security practice items relating to perceived barrier, perceived vulnerability, perceived severity, and perceived self-efficacy were also included in the study, as shown in Table A1. A Likert scale of five options was used. The questionnaire was crafted to cover security practice relating to internet use, email use, password management, and social media use. These aspects of security practice are mostly prone to security violations

by the human element [27,34,41]. These questionnaire items were adapted from existing questionnaire and modified for this study, as shown in Table A1 in Appendix A.

2.5. Ethical, Privacy, and Security Measures

When participants realize their behaviour is monitored, they tend to behave differently. On the other hand, when they are monitored without consent, researchers are accused of breaking the laws [40,46]. Researchers have intentionally refused to disclose some of the research procedures and purpose in order to have an unbiased study [40]. Meanwhile, studies involving deceptiveness are proven to be effective because they assess the real responses to phishing and the potential threat attacks that are yet to occur, and can effectively measure the success rate of countermeasures that are yet to be deployed [40,46].

Many ethical committees fail to approve phishing-related studies because they believe that deception in research contradicts informed consent and is potentially harmful to participants, invading privacy, breaking participants' rights, and limiting their control of risks (such as stress or psychological damage) associated with the research. However, the research community opposed this view. Various studies have stated that deception in research is not ethically wrong and the reason for withholding such information is what the ethical committee should be assessing instead [46,47]. They also explained that people in the clinical sector enjoy deception in research if it is likely to educate them. The participants were even interested in participating in similar deceptive researches [40,46].

Psychological association supported the debate and said it may be impossible to study some psychological constructs without withholding certain information about the true purpose of the study or deliberately misleading the participants [40]. The British Psychology Society also agrees with deception in research and said that the awareness of participants about some aspects of the study could likely compromise its validity [40,46].

In essence, using deception as a research method is justified to have valid inference if it has a kind of road map. The road map is as follows:

- Pre-launch of phishing: prepare fraudulent text, issue press release to administrators, and pre-inform consent;
- Launch of the attack: consider data protection, consider the well-being of the participants;
- Post-launch: consider debriefing, post informed consent and data protection.

Having followed these measures, the participants volunteered and consented to the study and also shared their phone numbers for this research. The healthcare facilities that joined this study also adopted full electronic health record systems in their operations and were elected to join the study through an invitation. Ethical clearance was obtained in Ghana. Following that, research coordinators were appointed to liaise with the management of these hospitals to facilitate the study. For instance, the facilitators identified SMS platforms and sent the phishing SMS messages together with the phishing links to the targets. Because of the high cost of internet data bundles in Ghana, the target participants who filled the questionnaire after clicking SMS received a reimbursement of their internet data amounting to GHS 10.00 each (which is about USD 1.67). Prior to filling out the form, participants were debriefed and reminded of their earlier consent to take part in the study. In addition, they were still given the opportunity to opt out if they changed their mind.

3. Findings of this Study

This section presents findings from the literature study, observation, simulated phishing attacks, and the statistical survey results.

3.1. Scoping Review Findings

As presented in Figure 5, 60 papers were initially identified from scientific databases, of which 2 were duplicates. Additionally, 16 sources of tools for phishing simulation studies were identified. Through readings, 23 records were excluded, leaving 51 records which were eligible for a full reading. In the end, 29 records were further removed because these

papers were not specifically in the healthcare domain (e.g., [48–51]), not precisely within the scope of phishing simulation (e.g., [52,53]). These were not clear in the identification stage until the full assessment stage.

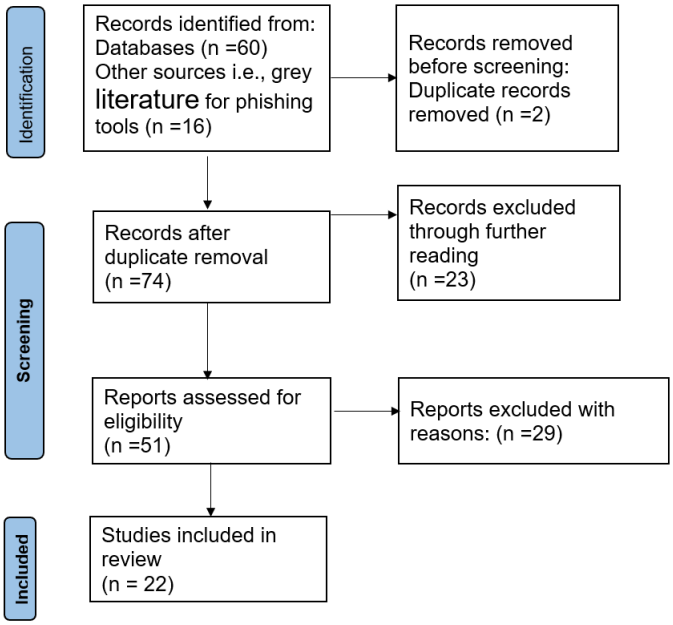

Figure 5. Report of literature: PRISMA diagram [39].

In the end, 22 studies (as shown in Figure 5) comprising 6 scientific articles (shown in Table 2) and 16 grey literature sources (shown in Table 3) were included in the study. From the six articles, one study was used only for the survey, four studies were used only in-the-wild field study with an email-based phishing attack, and one of them combined both email-based methods and literature surveys [24].

Additionally, three groups (third-party companies, custom-developed software tools, and commercial tools) emerged in the usage of a total count of five in-the-wild field phishing simulation tools. Gordon et al. [21] used commercial cloud-based phishing simulation tools (representing 20%), but [20,23] used custom-developed tools while [22,24] used third-party companies (each representing 40%) to conduct their phishing attack based on simulated studies. Out of a total of five simulated types of payloads that were used in the study, four (80%) of them simulated a malicious link, while one (20%) study [22] simulated credential harvest. The storylines that were used include health concerns [19], disposition to trust and risk-taking tendency [22], marketing, advertising potential employment position, and [23] offers of IT support services. Amidst various attack types such as email-based, voice-based and SMS-based types, all the studies (except [19] that did not indicate the attack type) used email-based attack types, as shown in Table 1. Slonka et al. further indicated that the phishing cue in the domain name type avoided the storage of clients' passwords, and used SSL to secure the interactions with clients [23] as measures towards enhancing ethics, privacy, security, and risk measures. Jalali et al. also submitted a questionnaire to those who click the link and those who did not click the link in a way to observe survival bias. In addition, the investigators did not collect contact information of the healthcare staff in an effort towards observing security and privacy measures [24].

Furthermore, out of the 16 phishing simulation tools (see in Table 3) that were identified, 7 (43.7%) were open-source, while the remaining 9 (56.3%) were commercial tools. Additionally, 6 (37.5%) could be deployed on the company network premise (premise-based), but the remaining 10 (62.5%) were cloud-based and inherited the cloud-related risks.

Table 2. Literature review categorization results.

Article	Method	Tool	Payload	Story Line	Attack Types
[24]	1.in-the-wild field study, 2. survey	third-party company	simulated malicious link		email
[19]	survey			health, concerns, disposition to trust, and risk-taking propensity	
[20]	in-the-wild field study	custom-developed software tools.	simulated malicious link		email
[21]	in-the-wild field study	Cofense, formerly PhishMe (commercial)	simulated malicious link		email
[22]	in-the-wild field study	third-party company	credential harvesting, batch files obfuscated	marketing, advertising potential employment positions	email
[23]	in-the-wild field study	custom-developed software tools	simulated malicious link	IT support request	email

Table 3. Phishing simulation tools.

No	Tool Name	Type	Cloud/On-Premise
1	GoPhish [54]	OpenSource	On-premise
2	Phishing Frenzy [55]	Open-source	On-premise
3	King Phisher [56]	Open-Source	On-premise
4	Simple Phishing Toolkit (sptoolkit) [57]	Open-source On-premise	
5	Social Engineer Toolkit (SET) [58]	Open-source	On-premise
6	SpeedPhish Framework (SPF) [59]	Open-source	On-premise
7	SpearPhisher BETA [60]	Open-source	
8	Barracuda Phishline [61]	Commercial	Cloud
9	Cofense [62]	Commercial	Cloud
10	Hoxhunt [63]	Commercial	Cloud
11	InfoSec [64]	Commercial	Cloud
12	IronScales [65]	Commercial	Cloud
13	Lucy [66]	Commercial	Both
14	Mimecast [67]		
15	KnowBe4 [68]	Commercial	Cloud
16	Proofpoint [69]	Commercial	Cloud

3.2. Observation Study

In terms of how to launch a simulated attack in the hospital, it was realised that the hospitals did not configure corporate email addresses and their network was limited to a local area network (LAN). Their healthcare staff could only access the EHR systems within the hospital premises without internet connections. The hospital's network had an internet connection to enable access to APIs and also to enable remote desktop access to the EHR. Additionally, the healthcare staff used mobile devices such as laptops and mobile phones in deliver healthcare services. Observational findings in other areas such as physical security, password management, incident reporting, and information handling were less relevant in this phishing study and were not reported in this paper.

3.3. Phishing Clicks

Out of a total of 167 healthcare staff who were targeted in the SMS-based phishing simulation study, 102 (61.1%) clicked the simulated malicious link, but 65 (38.9%) healthcare staff were not susceptible to the attack. Furthermore, 25 (24.5%) participants, out of the 102 who clicked the link, answered the questionnaire whose link was embedded in the study. So, a total of 77 (75.5%) failed to answer the questionnaire. The clicking behaviour

was high at the start of the simulation attack, but sharply decreased after the first 2 days, as shown in the graph in Figure 6. Additionally, the intended phishing security behaviours were generally lower (as shown in Figure 7) than their actual behaviour across all the roles of the healthcare staff who participated in the study.

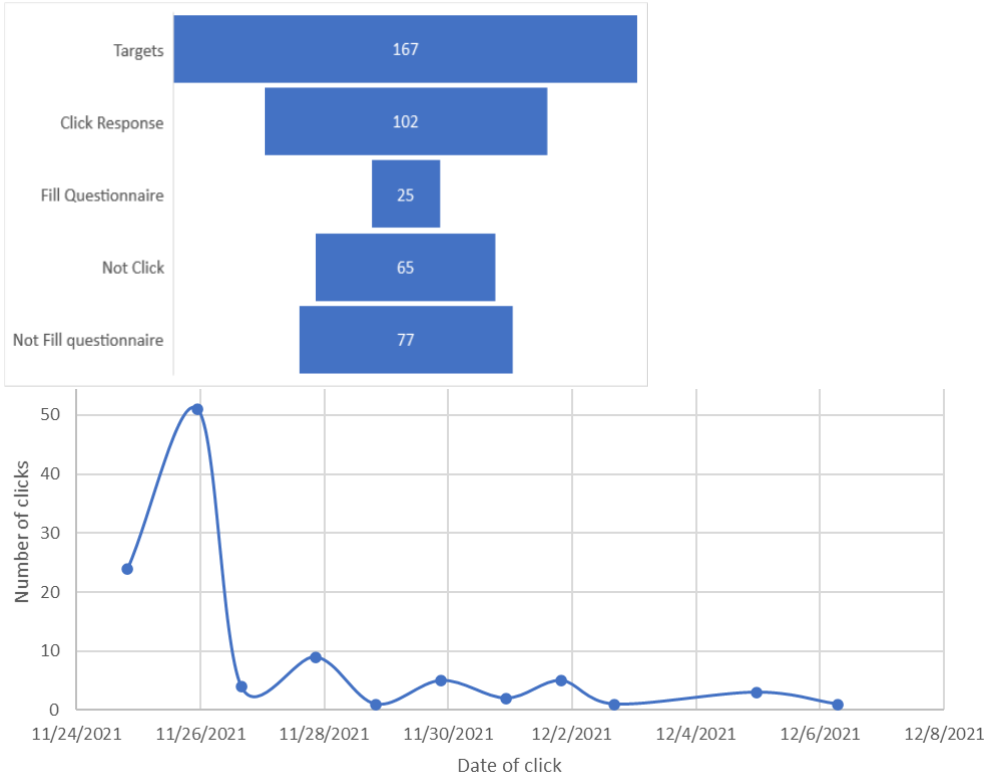

Figure 6. Phishing click statistics.

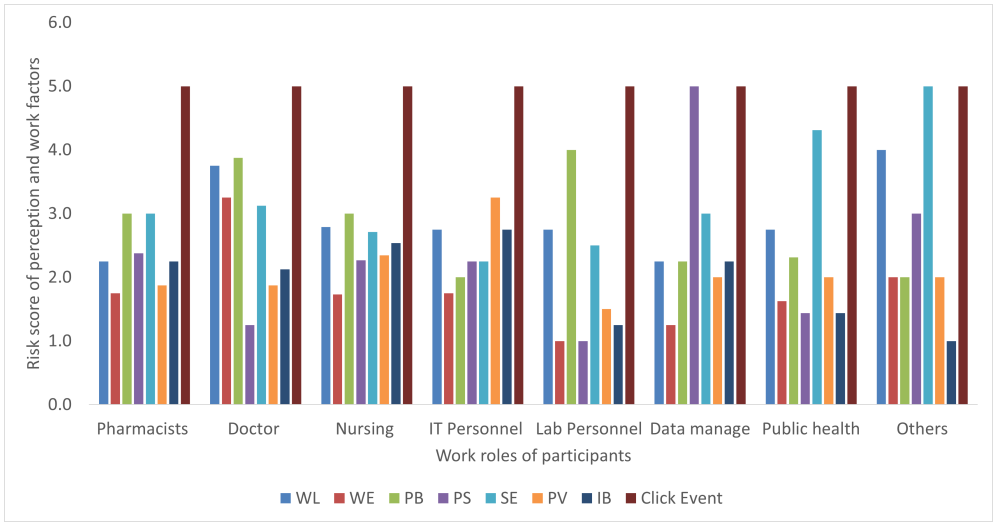

Figure 7. Comparing actual clicks with intended phishing behaviour of healthcare workers.

4. Statistical Analyses

The population profile of participants who clicked the link and answered the questionnaire is shown in Table 4. The proportion of males (44%) and females (56%) was similar, but the age range between 30 and 40 was the highest (72%). Nurses constituted the majority of the participants' population by 52%. None of the participants had less than one year of work experience. An almost-equal proportion of the participants were off-duty (56%)

and on-duty (44%), and 32% engaged in patient care and administrative duties (8%) while the rest (40%) failed to disclose what they were engaged in. A total of 17 (68%) out of the 25 participants believed in the subject of the phishing message, 6 (24%) were curious and only 2 (8%) did not disclose their expectations prior to clicking the link.

Table 4. Descriptive statistics of healthcare staff who clicked on the simulated malicious link and answered the questionnaire.

Category	Value	Freq.	%
Gender	Male	11	44.0
	Female	14	56.0
Age range	20–29	6	24.0
	30–39	18	72.0
	50–59	1	4.0
Position	Pharmacists	2	8.0
	Doctor	2	8.0
	Nurse	13	52.0
	IT personnel	1	4.
	Lab personnel	1	4.
	Data manager	1	4.0
	Public health	4	16.0
	Others	1	4.0
Work experience	<1 Year	2	8.0
	1–5 Years	11	44.0
	6–10 Years	6	24.0
	11–15 Years	5	20.0
	21–25 Years	1	4.0
	Total	25	100.0
Click location	Off-duty	14	56.0
	On-duty	11	44.0
	Total	25	100.0
Engaged in	Not disclosed	10	40.0
	Patient care	8	32.0
	Admin duties	2	8.0
	Leisure	3	12.0
	House chores	2	8.0
Expectation	Believed in the subject of the message	17	68.0
	Was curious	6	24.0
	Not disclosed	2	8.0

4.1. Reliability, Validity, Fit, Structural Model, and Correlation

The reliability of the constructs was assessed with Cronbach's alpha(CA) and composite reliability (CR), as shown in Table 5. All the CR values of the constructs were greater than 0.700. Additionally, the values of all the constructs of the average variance extracted (AVE) were greater than 0.500, which thereby met the convergence validity. The validity results are also presented in Table 5. The discriminate validity was assessed with the Fornell–Larcker criterion, the heterotrait–monotrait ratio (HTMT), and the cross factor loading of all the items. Having assessed the entire model, the values of R^2 were computed to be 0.369, 0.116, 0.086, 0.293, and 0.554 for the perceived barrier, perceived severity, perceived vulnerability, self-efficacy, and self-reported behaviour variables, respectively, while the values of Q^2 were obtained to be 0.312, 0.036, 0.003, 0.229, and 0.405 for the respective variables.

Table 5. Reliability and validity assessment.

Construct	Reliability and Validity				Discriminate Analysis: Heterotrait–Monotrait Ratio (HTMT)						
	CA	rho_A	CR	Average Variance Extracted (AVE)	IB	PB	PS	PV	SE	WE	WL
IB	0.835	0.934	0.886	0.664							
PB	0.799	0.826	0.881	0.714	0.578						
PS	0.746	1.043	0.839	0.638	0.400	0.666					
PV	0.772	0.921	0.892	0.805	0.248	0.444	0.652				
SE	0.701	0.703	0.834	0.626	0.596	0.613	0.434	0.494			
WE	0.667	0.675	0.857	0.750	0.364	0.715	0.415	0.163	0.277		
WL	0.429	0.572	0.758	0.619	0.789	0.730	0.071	0.367	0.765	0.371	

The model was then used to further test our hypothesis to determine the significance of the relationship. As shown in Figure 8 and Table 6, all hypotheses from H1 to H14 were evaluated to determine if PV, PS, PB, SE, WE, WL, and all mediating effects (from H15 to H22) have a significant effect on self-reported cyber security behaviour (IB) related to phishing among healthcare workers. Additionally, the model was used to assess the effect of gender, position, and work experience as moderating variables, as shown in Figure 8 and Table 6. The findings shown in Figure 8 and Table 6 reveal that work emergency had a significant negative effect on perceived barrier risk, as defined in the first hypothesis (H1) with a value of −0.46 at *p*-value = 0.00. Additionally, workload had a significant positive effect on perceived self-efficacy, as defined in H10 with a value of 0.50 at a *p*-value = 0.02. Aside from this, none of the constructs (PV, PS, PB, and SE) had a significant effect on IB risk. Moderating variables of gender, position, and years of work experience also showed no significant impact on IB.

Furthermore, as shown in Table 7, Pearson's correlation of the valid constructs showed that perceived barrier (PB) was positively correlated with the self-reported behaviour intention (r = 0.571, *p*-value = 0.01). Additionally, workload (WL) was also realized to have a significant positive correlation with perceived self-efficacy (r = 0.494, *p*-value = 0.05). However, perceived self-efficacy (SE) risk negatively correlated with IB (r = −0.483, *p*-value = 0.05). Similarly, work emergency had a significant negative correlation with PB risk at (r = −0.401, *p*-value = 0.05).

Views of Targets Who Did Not Click the Link

In efforts to enrich this study, we had a phone conversation with participants who clicked the link but did not answer the questionnaire and those who did not even click the link. From Figure 6, out of 167 healthcare workers who were targeted in the study, 142 failed to fill the questionnaire. Out of these, 28 provided feedback as to the reasons why they clicked the phishing simulation link without answering the questionnaire or why they did not even click the link. Eight of these respondents were males and the remaining twenty who provided the feedback were females, as shown in Figure 9.

The respondents who did not click the link said the message was malicious and some said they were busy and did not click the link. Some of those who did not click the link also claimed that there were many questionnaire items and others said they did not have time to fill out the questionnaire. Eleven individuals in total (eight females and three males) saw the message as suspicious. Two males and four females, were busy and did not click the link. Additionally, two males and four females claimed that there were many questionnaire items, while four females and two males did not fill out the questionnaire because they were busy. The female proportion was generally high (71.5%) as compared to the males (28.5%). Similarly, the proportion of females was higher in all as compared to the males.

Table 6. Structural model.

Path	Hypothesis	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	*p* Values
Work emergency -> Perceived barrier	H1	−0.46	−0.48	0.14	**0.00**
Work emergency -> Perceived vulnerability	H2	0.13	0.12	0.25	0.60
Work emergency -> Self-reported behaviour	H3	0.18	0.15	0.26	0.49
Work emergency -> Perceived severity	H4	0.35	0.35	0.26	0.18
Work emergency -> Self-efficacy	H5	0.13	0.09	0.24	0.60
Workload -> Perceived barrier	H6	−0.31	−0.32	0.19	0.10
Workload -> Perceived vulnerability	H7	−0.27	−0.20	0.30	0.38
Workload -> Self-reported behaviour	H8	−0.13	−0.17	0.30	0.66
Workload -> Perceived severity	H9	−0.03	−0.03	0.28	0.91
Workload -> Self-efficacy	H10	0.50	0.52	0.21	**0.02**
Perceived barrier -> Self-reported behaviour	H11	0.31	0.27	0.32	0.32
Perceived vulnerability -> Self-reported behaviour	H12	0.42	0.35	0.29	0.14
Perceived severity -> Self-reported behaviour	H13	−0.53	−0.45	0.34	0.12
Self-efficacy -> Self-reported behaviour	H14	−0.34	−0.34	0.32	0.29
	Indirect effect				
Work emergency -> Perceived barrier -> Self-reported behaviour	H15	−0.14	−0.13	0.16	0.37
Workload -> Perceived barrier -> Self-reported behaviour	H16	−0.10	−0.09	0.13	0.47
Work emergency -> Perceived vulnerability -> Self-reported behaviour	H17	0.05	0.05	0.12	0.66
Workload -> Perceived severity -> Self-reported behaviour	H18	0.02	0.04	0.17	0.92
Work emergency -> Self-efficacy -> Self-reported behaviour	H19	−0.04	−0.03	0.11	0.71
Workload -> Self-efficacy -> Self-reported behaviour	H20	−0.17	−0.19	0.21	0.41
Workload -> Perceived vulnerability -> Self-reported behaviour	H21	−0.11	−0.06	0.15	0.45
Work emergency -> Perceived severity -> Self-reported behaviour	H22	−0.18	−0.17	0.18	0.30
Experience -> Self-reported behaviour	H23	−0.06	−0.01	0.18	0.86
Gender -> Self-reported behaviour	H24	−0.31	−0.32	0.96	0.34
Position -> Self-reported behaviour	H25	−0.29	−0.26	0.32	0.38
	R^2	Q^2			
Perceived barrier	0.369	0.312			
Perceived severity	0.116	0.036			
Perceived vulnerability	0.086	0.003			
Self-efficacy	0.293	0.229			
Self-reported behaviour	0.554	0.405			

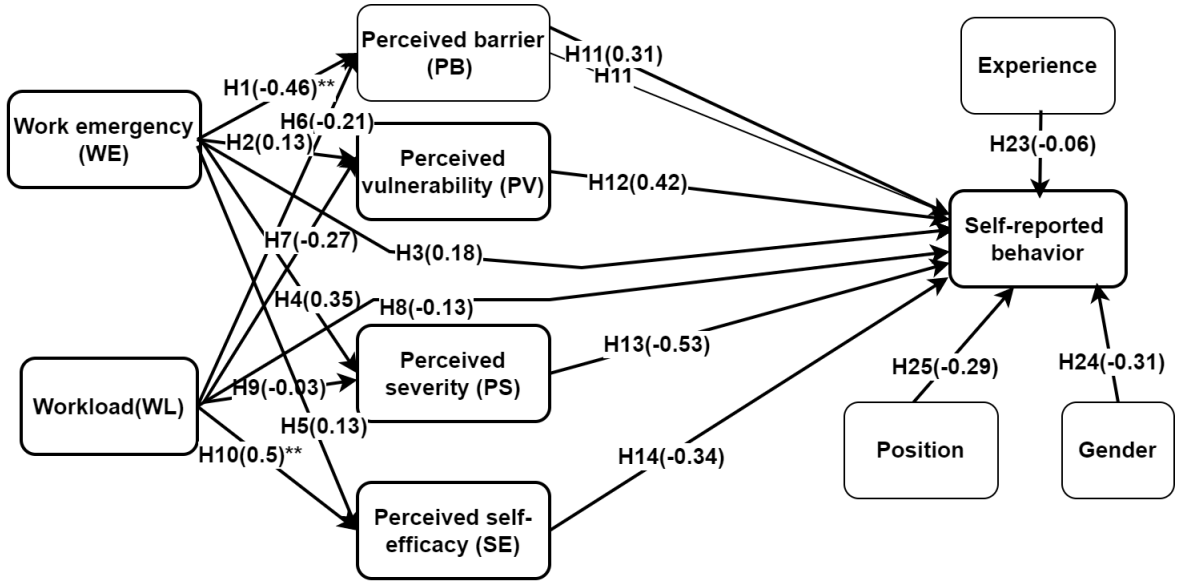

Figure 8. Research model with estimations. ** Correlation is significant at the 0.01 level (two-tailed).

Table 7. Correlation between self-reported phishing behavior (IB) perception variables and work factors.

	Correlations						
	WL	**WE**	**PB**	**PS**	**SE**	**PV**	**IB**
WL	–						
WE	0.458 *	–					
	0.021						
PB	−0.334	**−0.401 ***	–				
	0.102	0.047					
PS	0.023	0.208	−0.566 **	–			
	0.912	0.319	0.003				
SE	**0.494 ***	0.241	−0.441 *	0.038	–		
	0.012	0.245	0.027	0.857			
PV	0.003	0.291	−0.441 *	0.450 *	−0.102		
	0.987	0.157	0.027	0.024	0.627		
IB	−0.391	-0.197	0.571 **	−0.238	−0.483 *	0.015	
	0.053	0.346	0.003	0.252	0.014	0.944	

** Correlation is significant at the 0.01 level (two-tailed). * Correlation is significant at the 0.05 level (two-tailed).

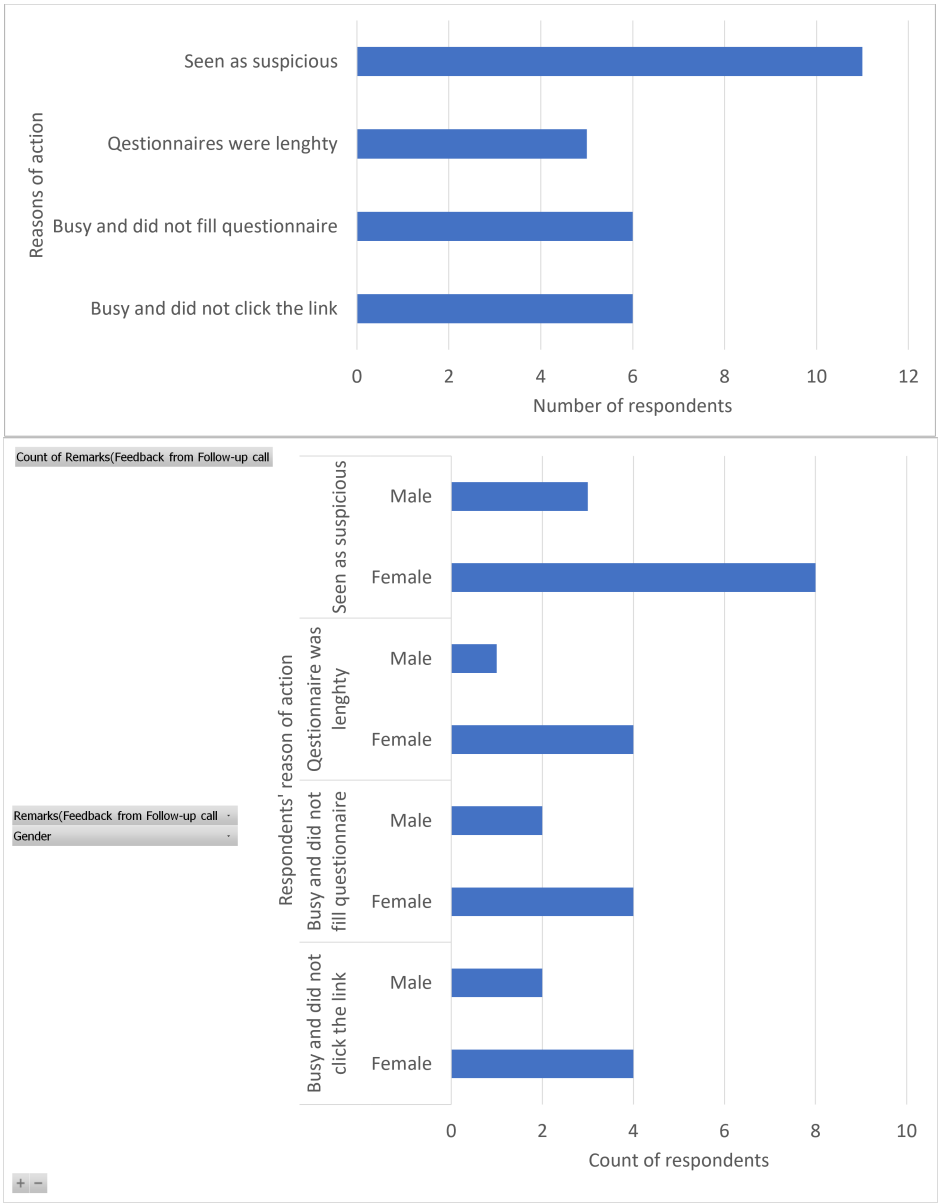

Figure 9. Feedback from respondents who fail to fill out the questionnaire and those who did not click on the link.

5. Discussion

The human aspect of cyber security practice has become a major window in recent times for cyber criminals to disturb healthcare organisations' operations through unauthorized accesses and data breaches [9]. In terms of ransomware, the human element is often baited through phishing attacks to click on malicious links. The victims may therefore compromise healthcare cyber systems if they happen to be susceptible. They may end up installing remote connection tools and malware, or may even provide their user credentials to the attackers, enabling them to move forward with their attack. Healthcare staff can fall victim to phishing attacks due to the nature of their work. They are often occupied with a heavy workload due to the high patients-to-staff ratio and their work is sometimes characterized by emergency situations, thereby increasing their cognitive load [70]. Additionally, healthcare workers may have poor information security knowledge and training and poor perception, possibly causing them to undermine better cyber security hygiene in phishing attacks [71]. Since most hospitals in Ghana are adopting EHR, many questions are being asked in the context of cyber security relating to a phishing attacks.

To provide significant answers to these questions, a smishing simulation study backed by state of-the-art studies was conducted among healthcare workers in Ghana and insight into the findings is discussed in the following sections.

5.1. Principal Findings

The principal findings in this study are shown in Table 8.

In preparation for the implementation of this phishing simulation study, the hospital's environment was physically observed to gain an understanding of its IT systems and how the healthcare workers use these tools to provide healthcare. Before that, a systematic review was conducted to provide the state-of-the-arts on various teams in a phishing simulation attack context. The attack was subsequently launched together with a statistical survey. In the scoping review, six scientific papers were identified to have been practically assessed in phishing simulation studies in healthcare. A further search for phishing simulation tools in grey literature revealed 16 different types of phishing simulation tools. Email-based phishing attacks with in-the-wild studies and surveys were the two methods being used to conduct phishing simulated studies in healthcare. Out of this in-the-wild study, email-based was the most common, as shown in Table 2. Third-party companies, custom-developed tools, and commercial tools were being used in the state-of-the-arts, of which third-party companies and custom-developed software tools were often used. A simulated malicious link was often used as the payload and storylines, including health concerns, marketing, and advertising for potential jobs, and IT support was used. Reconnaissance and intelligence gathering indicated that the hospital did not use incorporate an email system and most of the healthcare staff had not configured corporate emails. So, the hospital used mobile devices such as laptops and phones in communications and accessing EHR in their healthcare delivery.

From the 167 targeted healthcare staff who were sent the simulated phishing messages, more than half (61.1%) fell victim to the attack but only 25 (24.5%) of the victims filled a questionnaire and indicated varying reasons for their susceptibility. For instance, 7 (68%) out of the 25 participants believed in the subject of the phishing message and 6 (24%) were curious. The CA of workload and work emergency were slightly lower with CA values of 0.667 and 0.429, respectively; however, their corresponding CR values were above 0.700. It has been noted that if the number of questionnaire items measuring the construct is 10 or more, the coefficient of CA is expected to be 0.6 or higher [72,73]; otherwise, it is usual for the CA values to be around 0.5. Based on the view that just one click is needed in phishing susceptibility attack to achieve the adversary's goal, 167 participants, resulting in a 61.1% susceptibility rate, met the significant requirements. Other related phishing simulated studies have similar or lower participants [74,75].

Table 8. Principal findings.

No	Research Question (RQ) and Hypothesis (H)	Principal Finding	Remark
1	RQ1	• Six scientific papers were identified in this study, as shown in Table 2. • Five of them employed an in-the-wild field study. • One of the studies used only survey, while Jalili et al. adopted both a survey and an in-the-wild study [24] • Only Jalili et al. conducted their study based on theories i.e., PMT and collective felt truth [24]. • Five of the studies used email-based study. • Third-party tools and custom-developed tools were used in this work. • 16 phishing simulation tools were also identified, as shown in Table 3.	
2	RQ2	• Avoid collecting sensitive information from participants. • Encrypt data received from participants. • Avoid using actual malicious links.	
3	RQ3	102 (61.1%) healthcare staff clicked the simulated malicious link.	
4	RQ4	• Some staff were busy and did not click the link. • Others suspected the message to be fake. • 7 (68%) out of the 25 participants believed the subject of the phishing message. • Six (24%) were curious.	
5	RQ5	Self-reported behaviour and perception risks were generally lower than their actual behaviour, as shown in Figure 7	
6	RQ6	Deceptiveness can be used in research but certain procedures are needed. These include: • Pre-launch procedure; • Consideration of data protection; • Consideration of well-being of participants; • Perform debriefing; • Provide post-inform consent.	
7	H1	Significant estimate (value −0.46, p-value = 0.00) between work emergency and perceived barrier.	This was confirmed with Pearson's correlation coefficient (−0.494, p-value = 0.00).
8	H10	Significant estimate (value 0.5, p-value = 0.02) between workload and self-efficacy.	This was confirmed with Pearson's correlation coefficient value 0.494, p-value = 0.05).

5.2. Work Factors and Perception Risks in Relation to Self-Reported Phishing Risk Behaviour

In the report, all the factor loading values were greater than their corresponding cross-loading, indicating valid discriminate validity [76]. Moreover, the HTMT values were below the limit of 0.9, indicating the discriminate validity of the constructs [76,77]. Additionally, the variance inflation factor values were below the threshold of five, indicating no issues of multicollinearity [77].

R^2 refers to the effect or changes in the dependent variable's influenced by the independent variables, which is expected to be equal to or greater than 0.10 in order for the related construct to be adequate for predictions [78]. Aside from perceived vulnerability (PV) which recorded an R^2 of 0.086, all the dependent constructs of PB, PS, SE, and

self-reported behaviour met the 0.10 threshold, as shown in Table 6. Though the R^2 of PV is slightly lower than 0.01, other sources [79,80] indicate that such a model can be used for explaining the relationship between variables other than prediction. Q^2 measures the predictive relevance of the model, of which the value is expected to be greater than 0 in order for it to be relevant [81]. To this end, the model was generally fit and was used for the estimation, as shown in Table 6 and Figure 8 using structural equation model (SEM) of SmartPLS [82]. SEM is used for estimating causality among variables in the structures of various equations [83].

Assessing the contribution of work factors and perception variables with self-reported cyber security behaviour, the results showed that work emergency (WE) negatively predicted PB (r = 0.46, *p*-value = 0.00) and this supported H1. The remaining hypothesis were not significantly predicted with the SEM model. Furthermore, workload significantly predicted PS in the positive direction, as opposed to our hypothesis H10, as shown in Table 6 and Figure 8. Additionally, a validation with Spearman's correlation showed that workload also significantly predicted self-efficacy risk (r = 0.494, *p*-value = 0.05) and work emergency predicted perceived barrier risk in the reverse direction at the significance of r = −0.401, *p*-value = 0.05. These predictions were similar with that of the SEM.

Additionally, workload (WL) was also observed to have a significant positive correlation with perceived self-efficacy (r = 0.494, *p*-value = 0.05). This is in contradiction with our initial assertion of H10. Thus, as the workload of the healthcare staff increases, they tend to struggle to cope with additional responsibilities of security practice, thereby increasing their perceived self-ability risk of complying with security regulations. The healthcare staff could, as a result, be susceptible to phishing tricks. This also supports our initial assumption. A similar study by Jalali et al. also found a causal effect of workload on the phishing risk behaviour of healthcare staff [24]. Similarly, work emergency had a significant negative effect with PB risk. This translates that higher work emergency among healthcare staff corresponds to lower risks of PB. Consequently, a lower risk of PB is also a significant positive predictor of phishing susceptibility behaviour, as shown in Table 7. This can possibly be related to findings in Table 9, where a qualitative finding revealed that six of the healthcare staff were busy and did not click the link. Though not proven to be statistically significant, it could mean that, during an emergency, the healthcare workers tend to prioritize patient care and subsequently fail to be susceptible to a phishing attack. So, further training and awareness could possibly boost efforts of conscious care behaviour.

A further step of analysis with correlation showed that PB was positively correlated with IB at (r = 0.571, *p*-value = 0.05). This contradicts our hypothesis H11, as we originally presumed that PB negatively correlates with IB. Perceived barriers are obstacles that can inhibit secure phishing-related security behaviour. The results, therefore, suggest that higher perceptions of obstacles to secure phishing practices are related to an increase in self-reported conscious care phishing security behaviour. If the relationship was a causal effect, the removal of perceived barrier risks will improve phishing security-conscious care behaviour. Related studies on cyber security behaviour and awareness [17,25] did not show statistically significant results to support this or otherwise. Additionally, SE risk negatively correlated with IB (r = −0.483, *p*-value = 0.05), as shown in Table 7, which translates that the perceived risk of the assessment of the healthcare workers' ability to comply with phishing security policy decreases with corresponding increases in their phishing security risk behaviour. This contradicts the initial assertion (H14), as we expected SE to positively correlate with phishing-related security behaviour. This could therefore mean that healthcare workers who think they have the ability to overcome phishing tricks do not, why is why they were susceptible to this attack in the first place.

However, all mediating and moderating variables were assessed and they did not have any significant effects on the study. This indicates that the effect of those variables are statistically equal to zero. With regards to phishing simulating studies in the healthcare context, this is the first which draws specific variables from the HBM and PMT to design this model. A related study that used constructs from the theory of plan behaviour showed a positive

prediction of attitude, subjective norm, and perceived behavioural control [24]. That study further indicated that workload was positively correlated with phishing-related practice. Relating to the study, the sample size in this work was relatively small; therefore, further studies with an adequate sample size are required to arrive at a more valid conclusion.

5.3. Phishing Attack Methods, Tools, Risks Measures, Payload, and Storyline

From the state-of-the-art, six scientific studies were published on phishing practical studies in the area of healthcare. Some of the studies [20–23] used the in-the-wild study approach, but [19] used a questionnaire-based survey, while [24] combined both in-the-wild and the questionnaire survey. With these few studies, it is clear that there is a huge gap in the practical assessment of healthcare workers' phishing simulation studies. So, little knowledge has been contributed so far in the scientific community towards understanding security practices in phishing security conduct among healthcare workers. This might have possibly contributed significantly to the knowledge gap of healthcare staff and resulted in the numerous successes in ransomware attacks in healthcare. The low account of phishing simulation studies in healthcare might have been due to the critical nature of healthcare and the strict regulatory requirements needed to conduct such studies. Furthermore, according to Salah et al., the phishing simulation study consists of three types: a self-reported survey, a laboratory experiment, and an in-the-wild study [40]. Self-reported surveys are ineffective due to biases from participants and researchers. Laboratory-controlled experiments are also known to be unreliable as they create an artificial environment for participants. An in-the-wild field study is considered reliable since participants are observed in their natural environment. The challenges associated with the in-the-wild study are ethical-based, as it involves deception. Another issue involves how to collect feedback from targeted participants in a phishing simulation study. To overcome these issues, recommended road maps for safely conducting the study and survey instruments with follow-up contacts can be used as part of an effective study.

Email-based phishing is one of the preferred attack methods used by cybercriminals to launch phishing attacks [84,85]. Malicious links are usually embedded in the emails and sent to the targets with messages enticing them to click the links. The links are usually associated with payloads, such as malware installations, malicious attachments, harvesting of sensitive information (such as credit card numbers), personal identification numbers (PINs), social security numbers, and other bank details. Email-based attacks are popular in this state-of-the-art, merely due to the widespread usage of email systems among organisations. Unfortunately, the healthcare systems that were involved in this study had not begun to use corporate email systems. However, as phishing attacks include VOIP and SMS, instant messaging, and social networking sites, SMS-based phishing was therefore adapted in this study combined with a questionnaire-based survey. Both SMS-based and questionnaire studies were very essential in this work because the SMS helped to measure the susceptibility level (click/not click) of the healthcare staff, while the questionnaire helped in measuring the perception and work factors that possibly contributed to the susceptibility. Clearly, each of these methods alone would not have been able to meet the study objective and as the email system was not configured in the target hospital, it was basically not an option.

Regarding phishing simulation tools, third-party security companies, custom-developed tools, and a commercial tool were identified in the state-of-the-arts, as shown in Table 2. Appraising privacy, security, and ethical concerns, this study did not use third-party companies since the scope of the ethical clearance did not include giving out contact information to third-party companies. So, we developed custom software and hosted it with an SSL certificate to record the click events of the targets. The SMS messages were hence sent via an SMS messaging company; however, to avoid privacy and security issues, the contact phone numbers of the targets were not saved on this platform. Other phishing simulated study tools such as Gophish, Phishing frenzy, King phish, and Cofense (as shown

in Table 2) were not adopted in this study because they were all email-based systems and not associated with SMS-based attacks [13].

In terms of privacy, security, and ethical considerations, Jalili et al. avoided collecting information out of fear of privacy breaches. Similarly, Slonka et al. did not actually harvest the credentials of the targets but replaced the provided emails with some numerical values and further used SSL to secure the connection between the web server and the target participants. These were deemed safe methods; however, we encrypted the unique click events that were recorded and saved them onto the database of a website that was hosted for this exercise and followed the ethical road map proposed by Salah et al. [40]. The site was also secured with an SSL certificate to avoid data breaches. This approach was deemed reliable and valid for recording the unique click event of each respondent. To reduce the tendency of multiple recordings from one user, it was considered necessary to have reliable unique click events such that when a user happened to click the link more than once, the original click could be detected to avoid multiple recordings from one person. The SHE-256 algorithm was used based on guidelines provided in the General Data Protection Regulation of EU [86,87].

5.4. Phishing Attack Risk among Healthcare Staff

The study recorded a click rate of 61.1% (as shown in Figure 6) which would be considered very high when compared with related investigations that were performed in [23] (20.4%) and [20] (14.2%). This answered the research question RQ3, indicating that healthcare workers are susceptible to a phishing attack in the hospital. After all, the phisher may just need a single click to launch the malicious payload. Therefore, a click rate of over 50% might have even exceeded the goal of the phisher. For better understanding, and as a means of dealing with survivorship bias, those who did not click the link were contacted. With reference to Figures 6 and 9, out of 65 healthcare staff who were contacted, 17 of them provided brief feedback as to why they did not click on the link. Eleven of them regarded the message as suspicious, while six of them were busy and failed to click the link. The healthcare staff who regarded the message as fake said they were not exposed to COVID-19 risk factors and so did not believe the SMS message, implying that they would have been victims if they had been in contact with others at that time. So, their suspicion was not based on their knowledge of phishing attacks, suggesting that such healthcare staff might also need treatment together with those who click the link to improve their phishing attack resilience level. It is interesting to know that some healthcare staff (six persons) did not click the link because they were busy with patient care, as indicated in Figure 9. While a related study [24] identified that high workload contributes to phishing susceptibility, a recent study on healthcare security practice showed the reverse [88], where a higher workload has a rather negative correlation with self-reported security behaviour risks of healthcare staff. Since it was merely a correlation, the authors did not attach a causality effect to the findings. Furthermore, the study participants were relatively small, limiting the generalisation of their findings. Though this might be insignificant, our study points to a similar finding in this work, as six persons forgot to click the link simply because they were busy with patients.

To better understand the susceptibility of the victims, the location, expectations, and engagements of the victim were collected via the questionnaire. Of those who provided this information, 56% were off-duty, while 44% were on-duty. Additionally, 68% believed in the subject of the phishing message while 24% were curious. Some were engaged in patient care (32%), administrative duties (8%), leisure (12%), and house chores (8%).

According to Sonowal et al., curiosity, urgency, helpfulness, fear, trust, and greed are among the properties often baked into the phishing messages to entice prospective victims [13]. Interestingly, a higher proportion of the victims who clicked the link were curious and some also trusted the message which was crafted to have these phishing message tones. In total, 40% (10) of healthcare staff who clicked the link were also engaged in healthcare activities. On the other hand, of the 17 persons who did not click the link

(as shown in Figure 9), 6 (35.3%) of them said they were busy. During busy healthcare provision, there are still questions around who responds to the phish and who responds to the patient and why. It is possible that those healthcare staff who click the phishing link while caring for the patients were expecting such messages due to their exposure to COVID-related factors and probably did not perceive or appraise the cyber security consequences of their action. This calls for strengthening the security systems in the hospital, such that access controls and alerts to suspicious links can prompt busy healthcare staff to carefully assess a link before clicking. For those who continue to care for the patient, it is possible that they prioritized patient care over the phishing message. It could also be the case that they were not exposed to any COVID-19-related factors and felt less susceptible to the virus, and therefore had less priority for the phishing message.

5.5. Survivorship Bias and Feedback from Respondents Who Neither Clicked the Link nor Filled the Questionnaire and Those Who Clicked the Link but Failed to Fill the Questionnaire

Figure 9 shows the reasons why the healthcare staff click the link but failed to fill the questionnaire item. Apparently, five persons claimed that there were many items in the questionnaire, while six victims responded that they were too busy and did not have time to fill it in. In Ghana, the doctor–patient and nurse–patient ratios are far lower than the World Health Organisation (WHO) standard. For example, the doctor–patient ratio in Ghana is about 1:13,000 while that of the WHO limit is at 1:5000 [89,90]. This supports the findings that the healthcare staff could be busy and do not have time to fill out the questionnaire.

5.6. Implication of the Study

Our study has both practical implications and implications for the scientific community. First of all, new knowledge has been provided in the state-of-the-arts regarding phishing simulation methods, tools, payloads, ethics, privacy, and security in the context of healthcare for future consideration. Secondly, it is now known that being busy in the hospital can disturb conscious care phishing behaviour and can equally have a positive effect on conscious care behaviour. Armed with this knowledge, security professionals can find a balance of training healthcare staff to promote their conscious care phishing behaviour. Extra security layers could also be provided in healthcare to support users in their efforts of using conscious care security practice, especially in the emergency department. Additionally, as PB risk positively predicted IB risk, PB risks can then be improved towards improving conscious care behaviour if causality is established. Furthermore, workload predicted SE risk in the positive direction, while SE risk predicted IB risk in the negative direction.

Based on this study, various measures need to be taken by the leaders of healthcare and even the government in relation to phishing attacks. The leaders of the healthcare community need to provide appropriate training, awareness, learning, and eduction procedures to averse this susceptibility trend. Moreover, intrinsic incentives can be designed based on these findings to improve phishing-related conscious care behaviour. For instance, regarding educating staff on phishing attacks, healthcare staff need to know how to comprehensively identify phishing clues. This could provide them with the knowledge to avoid clicking on suspicious links. After educating the staff, training with simulation attacks needs to be conducted with healthcare staff to help them to understand the nature of real attacks. Aside from these, the perception of healthcare staff needs to improve to reduce the security behaviour risk. Social and cultural factors need to be developed to improve the conscious care behaviour of the healthcare staff. Equipping the healthcare staff with adequate knowledge and skills on phishing-related security practice could be help to reduce the perceived barrier risk in phishing attacks and other perception risks. In this regard, state-of-the-art training technologies such as virtual reality, augmented reality, or extended reality could be employed to train and inculcate longer-lasting psychological incentives towards an avoidance of phishing susceptibility. In traditional training methods, people may skip through online modules by reading the bare minimum to pass the final quiz, or attending a presentation without really paying attention or absorbing

any knowledge. Virtual realities may not only enable people to see and understand the problem of cybersecurity relating to phishing, but will engage them emotionally. Immersive technologies are deemed effective. For instance, a study by Kohn et al. showed that when students are engaged and motivated, such that they feel less stress, the understanding of what they are being thought is better and they experience better levels of cognition, develop patterns, and enjoy better long-lasting in memory.

In the simulated attack, the SMS message caption was crafted to align with the government institution responsible for healthcare. This could have also increased the click rate since some of the healthcare staff will not doubt the source. Therefore, the government should prevent SMS service provider platforms to use the names of reputable companies as sources of SMS messages. This way, adversaries will try to create similar(but not exact) names of related companies. This could increase suspicions around the source of SMS messages by the targets and can help to reduce the susceptibility level of phishing attack.

6. Conclusions

Following the huge benefits of ICT systems in healthcare, many hospitals have abandoned paper-based systems for computerized systems. However, the associated challenges include ransomware attacks and other cybersecurity-related threats. A phishing attack happens to be the most common method of ransomware attack because it targets the most vulnerable link in the security chain.

Guided with state-of-the-art and observational measures, an SMS-based phishing simulation study was performed among healthcare workers in Ghana who were elected to be part of the study. The results showed that more than half of the targeted healthcare staff (61%) were susceptible. To prevent survivorship bias, a phone call conversation showed that some of the healthcare staff were not victims in the attack because they prioritized patient care and were not susceptible to the simulated phishing attack. The self-reported phishing behaviours of healthcare workers were generally lower than their actual behaviour of having clicked the link. A correlation between work factor variables and perception variables showed that the perceived barrier is a predictor of self-reported intended behaviour among healthcare staff, that workload significantly predicted self-efficacy risk ($r = 0.494$, p-value = 0.05), and that work emergency predicted a perceived barrier risk in the reverse direction on a significant level ($r = -0.401$, p-value = 0.05). Furthermore, self-efficacy negatively predicted self-reported security behaviour related to phishing attacks. If causality was established, it basically would have meant that healthcare staff are confident in their ability to appraise and avoid phishing attacks, but do not in fact have the requisite ability to overcome them. Various suggestions have been provided to the leaders of the healthcare organization in Ghana and the government towards reducing phishing susceptibility level in the healthcare community. For instance, state-of-the-art training, using immersive technologies including virtual reality, could help to improve the psychological perceptions (such as perceived barrier and self-efficacy) that present a higher risk against cyber security practice. Some suggestions have also been provided to the government, regarding how to reduce the issue of cyber criminals being able to use the names of reputable organizations in SMS-based phishing attacks.

One of the limitations in this study includes the small number of participants who responded to the questionnaire. We pretested our questionnaire, but future studies could therefore conduct a more intensive pre-testing to increase the response rate. Additionally, further work is needed to practically assess the treatment effects with multiple clicks to practically assess various incentives, such as the perception variables in HBM, PMT, and cognitive dissonance in phishing simulation studies. Guided with these perceptions and work factors that affect the phishing security practice, better security training, awareness, and incentive measures can therefore be crafted in order to mitigate the phishing susceptibility rate.

Author Contributions: Conceptualization, P.K.Y. and B.Y.; methodology, P.K.Y.; software, P.K.Y.; validation, B.Y., M.A.F., P.N. and P.K.Y.; formal analysis, P.K.Y; investigation, P.K.Y.; resources, B.Y.; data curation, P.K.Y. and M.A.F.; writing—original draft preparation, P.K.Y.; writing—review and editing, B.Y., M.A.F. and P.N.; visualization, M.A.F. and P.K.Y.; supervision, B.Y.; project administration, B.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: This study was approved in Ghana by Kintampo health research institutional ethics committee (IEC), with the study id of KHRCIEC/2020-22.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Table A1. Questionnaire items.

No	Item	Construct	Ref
1	It is inconvenient to check the security of an email with attachment	PB	[17,25]
2	I do not have the time to check for phishing clues in an email		
3	I do not have the knowledge to check for phishing clues in an email		
4	I have not been trained properly to identify phishing related clues		
5	My hospital can not be hacked if I click on a malicious link	PV	[17,25,91]
6	Loss of data resulting from hacking is a serious problem for my hospital		
7	Giving out my password and username to external person can lead to unauthorized access in my hospital systems		
8	My hospital can be attacked by ransomware if I click on a malicious link		
9	I have the skills to identify malicious or phishing links in emails	SE	[17,92,93]
10	I am confident that I cannot download malicious attachment		
11	I am confident that I cannot share my username and password with others through phishing attack		
12	I am confident that I will not download malicious software on my computer		
13	I feel that my chance of receiving an email attachment with a virus is high	PS	[17,25]
14	I feel that I could fall victim to a malicious attack if i fail to comply with my organization's information security policy		
15	My organization's data and resources may be compromised if I don't pay adequate attention to phishing attack tricks		
16	It is not likely that an information security breach can occur at my workplace through clicking email links		
17	I check the links in my email or SMS to be sure it is not harmful before clicking	IB	[17,25,94]
18	I do not open email attachments from people whom I do not know		
19	I do not enter usernames, passwords and other sensitive information on pop-up windows		
20	I always verify the source of the email or SMS before accessing its content		
21	I was called to attend to urgent issues prior to clicking the link	WE	
22	Prior to clicking the link, the work i was performing required URGENT or IMMEDIATE intervention to prevent a worsening condition which poses an immediate risk to health and life		
23	I was called outside my shift time to attend to urgent issues prior to clicking the link		
24	I was preparing to receive an emergency case prior to clicking the link		
25	In my workplace, I SKIPPED my daily break or I was in a hurry in order to keep up with my workload prior to clicking the link		
26	I was at work early or I stayed late outside of my regular or normal working hours in order to keep up with my workload prior to clicking the link		
27	Prior to clicking this link, I had performed some mind draining activities (thinking, deciding, calculating, remembering, looking, searching, etc.) which affected my ability to pay much attention to the message details and the SMS links before clicking.	WL	[24]
28	Prior to clicking this link, I had performed some amount of physical activities (e.g., pushing, pulling,turning, controlling, activating, etc.) which affected my ability to pay much attention to message details and the SMS link before clicking.		

References

1. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef] [PubMed]
2. Faddis, A. The digital transformation of healthcare technology management. *Biomed. Instrum. Technol.* **2018**, *52*, 34–38. [CrossRef] [PubMed]
3. WHO. *Technical Series on Primary Healthcare*; WHO: Geneva, Switzerland, 2021.
4. Yeng, P.; Yang, B.; Wolthusen, S.D. Legal Requirements towards Enhancing the Security of Medical Devices. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 666–675. [CrossRef]
5. Yeng, P.K.; Woldaregay, A.Z.; Hartvigsen, G. *K-CUSUM: Cluster Detection Mechanism in EDMON*; Linköping University Electronic Press: Linköping, Sweden, 2019.
6. Adu, E.K.; Mills, A.; Todorova, N. Factors influencing individuals' personal health information privacy concerns. A study in Ghana. *Inf. Technol. Dev.* **2021**, *27*, 208–234. [CrossRef]
7. Osei, E.; Agyei, K.; Tlou, B.; Mashamba-Thompson, T.P. Availability and Use of Mobile Health Technology for Disease Diagnosis and Treatment Support by Health Workers in the Ashanti Region of Ghana: A Cross-sectional Survey. *Diagnostics* **2021**, *11*, 1233. [CrossRef]
8. Ayakwah, A.; Damoah, I.S.; Osabutey, E.L. Digitalization in Africa: The Case of Public Programs in Ghana. In *Business in Africa in the Era of Digital Technology*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 7–25.
9. Verizon2021. *2021 Data Breach Investigations Report*; Verizon: New York, NY, USA, 2021.
10. Ransomware Is Leading Hospital Boards to Pour More Money into Cybersecurity. Available online: https://www.healthcareitnews.com/news/ransomware-leading-hospital-boards-pour-more-money-cybersecurity (accessed on 4 August 2022).
11. Chernyshev, M.; Zeadally, S.; Baig, Z. Healthcare data breaches: Implications for digital forensic readiness. *J. Med. Syst.* **2019**, *43*, 7. [CrossRef]
12. Spence, N.; Paul, D.P.; Coustasse, A. Ransomware in Healthcare Facilities: The Future is Now. Available online: https://mds.marshall.edu/mgmt_faculty/185/ (accessed on 4 August 2022).
13. Sonowal, G. Phishing Kits. In *Phishing and Communication Channels*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 115–135.
14. Mishra, S.; Soni, D. SMS Phishing and Mitigation Approaches. In Proceedings of the 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 8–10 August 2019, pp. 1–5. [CrossRef]
15. Ulfath, R.E.; Sarker, I.H.; Chowdhury, M.J.M.; Hammoudeh, M. Detecting Smishing Attacks Using Feature Extraction and Classification Techniques. In Proceedings of the International Conference on Big Data, IoT, and Machine Learning, Sydney, NSW, Australia, 22–23 October 2022; pp. 677–689.
16. Wayne W. LaMorte. Behaviour Change Models: The Health Belief Model. Available online: https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/#headingtaglink_1 (accessed on 4 August 2022).
17. Ng, B.Y.; Kankanhalli, A.; Xu, Y.C. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
18. Cazares, M.F.; Arévalo, D.; Andrade, R.O.; Fuertes, W.; Sánchez-Rubio, M. A Training Web Platform to Improve Cognitive Skills for Phishing Attacks Detection. In *Intelligent Sustainable Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 33–42.
19. Abdelhamid, M. The role of health concerns in phishing susceptibility: Survey design study. *J. Med. Internet Res.* **2020**, *22*, e18394. [CrossRef] [PubMed]
20. Gordon, W.J.; Wright, A.; Aiyagari, R.; Corbo, L.; Glynn, R.J.; Kadakia, J.; Kufahl, J.; Mazzone, C.; Noga, J.; Parkulo, M.; et al. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Netw. Open* **2019**, *2*, e190393. [CrossRef]
21. Gordon, W.J.; Wright, A.; Glynn, R.J.; Kadakia, J.; Mazzone, C.; Leinbach, E.; Landman, A. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *J. Am. Med. Inform. Assoc.* **2019**, *26*, 547–552. [CrossRef] [PubMed]
22. Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inform.* **2019**, *26*, e100031. [CrossRef] [PubMed]
23. Slonka, K.J.; Shrift, B.F. Phishing our clients: A Step toward improving training via social engineering. *Issues Inf. Syst.* **2016**, *17*, 231–241.
24. Jalali, M.S.; Bruckes, M.; Westmattelmann, D.; Schewe, G. Why employees (still) click on phishing links: Investigation in hospitals. *J. Med. Internet Res.* **2020**, *22*, e16775. [CrossRef] [PubMed]
25. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. [CrossRef]
26. Humaidi, N.; Balakrishnan, V. The influence of security awareness and security technology on users' behavior towards the implementation of health information system: A conceptual framework. In Proceedings of the 2nd International Conference on Management and Artificial Intelligence IPEDR, Bangkok, Thailand, 7–8 April 2012; IACSIT Press: Singapore, 2012; Volume 35, pp. 1–6.
27. Yeng, P.K.; Szekeres, A.; Yang, B.; Snekkenes, E.A. Mapping the Psychosocialcultural Aspects of Healthcare Professionals' Information Security Practices: Systematic Mapping Study. *JMIR Hum. Factors* **2021**, *8*, e17604. [CrossRef]

28. Chen, Y.; Ramamurthy, K.; Wen, K.W. Organizations' information security policy compliance: Stick or carrot approach? *J. Manag. Inf. Syst.* **2012**, *29*, 157–188. [CrossRef]
29. Chen, Y.; Xia, W.; Cousins, K. Voluntary and instrumental information security policy compliance: An integrated view of prosocial motivation, self-regulation and deterrence. *Comput. Secur.* **2022**, *113*, 102568. [CrossRef]
30. Champion, V.L.; Skinner, C.S. The health belief model. *Health Behav. Health Educ. Theory Res. Pract.* **2008**, *4*, 45–65.
31. Humaidi, N.; Balakrishnan, V.; Shahrom, M. Exploring user's compliance behavior towards Health Information System security policies based on extended Health Belief Model. In Proceedings of the 2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), Hawthorne, VIC, Australia, 10–12 December 2014; pp. 30–35.
32. Mou, J.; Cohen, J.F.; Bhattacherjee, A.; Kim, J. A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *J. Assoc. Inf. Syst.* **2022**, *23*, 196–236. [CrossRef]
33. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [CrossRef]
34. Yeng, P.K.; Yang, B.; Snekkenes, E.A. Healthcare Staffs' Information Security Practices Towards Mitigating Data Breaches: A Literature Survey. *Stud. Health Technol. Inform.* **2019**, *261*, 239–245. [PubMed]
35. Ansari, Z.M.; Yasin, H.; Zehra, N.; Faisal, A. Occupational stress among emergency department (ED) staff and the need for investment in health care; a view from Pakistan. *J. Adv. Med. Med. Res.* **2015**, *10*, 1–9. [CrossRef]
36. Yeng, P.K.; Yang, B.; Snekkenes, E.A. Framework for healthcare security practice analysis, modeling and incentivization. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 3242–3251.
37. Cocker, F.; Joss, N. Compassion fatigue among healthcare, emergency and community service workers: A systematic review. *Int. J. Environ. Res. Public Health* **2016**, *13*, 618. [CrossRef]
38. Safa, N.S.; Sookhak, M.; Von Solms, R.; Furnell, S.; Ghani, N.A.; Herawan, T. Information security conscious care behaviour formation in organizations. *Comput. Secur.* **2015**, *53*, 65–78. [CrossRef]
39. PRISMA. *PRISMA:Preferred Reporting Items for Systematic Reviews and Meta-Analyses*; Available online: http://www.prisma-statement.org (accessed on 4 August 2022).
40. Salah El-Din, R. *To Deceive or Not to Deceive! Ethical Questions in Phishing Research*.In Proceedings of the HCI Research in Sensitive Contexts: Ethical Considerations workshop at HCI 2012, Birmingham, UK, 10–14 September 2012.
41. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. *The Development of the Human Aspects of Information Security Questionnaire (HAIS-Q)*; RMIT University: Melbourne, VIC, Australia, 2013.
42. Parsons, K.; Calic, D.; Pattinson, M.; Butavicius, M.; McCormac, A.; Zwaans, T. The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Comput. Secur.* **2017**, *66*, 40–51. [CrossRef]
43. Yeng, P.; Yang, B.; Snekkenes, E. Observational Measures for Effective Profiling of Healthcare StaffsŚecurity Practices. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; Volume 2, pp. 397–404.
44. The University of Oslo. *Web Form for Questionnaire Registrations*; The University of Oslo: Oslo, Norway, 2022.
45. Ball, R.; Watts, R. Some additional evidence on survival biases. *J. Financ.* **1979**, *34*, 197–206. [CrossRef]
46. Athanassoulis, N.; Wilson, J. When is deception in research ethical? *Clin. Ethics* **2009**, *4*, 44–49. [CrossRef]
47. Sieber, J.E. Deception in social research I: Kinds of deception and the wrongs they may involve. *IRB Ethics Hum. Res.* **1982**, *4*, 1–5. [CrossRef]
48. McElwee, S.; Murphy, G.; Shelton, P. Influencing outcomes and behaviors in simulated phishing exercises. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–6.
49. Rakhra, M.; Kaur, D. Studying user's computer security behaviour in developing an effective antiphishing educational framework. In Proceedings of the 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2018; pp. 832–836.
50. Li, Y.; Xiong, K.; Li, X. Understanding user behaviors when phishing attacks occur. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019; p. 222.
51. Flores, W.R.; Holm, H.; Svensson, G.; Ericsson, G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Inf. Manag. Comput. Secur.* **2014**, *22*, 393–406. [CrossRef]
52. Öğütçü, G.; Testik, Ö.M.; Chouseinoglou, O. Analysis of personal information security behavior and awareness. *Comput. Secur.* **2016**, *56*, 83–93. [CrossRef]
53. Campbell, C.C. Solutions for counteracting human deception in social engineering attacks. *Inf. Technol. People* **2019**, *32*, 1130–1152. [CrossRef]
54. Open-Source Phishing Framework. Available online: https://getgophish.com/ (accessed on 4 August 2022).
55. Phishing All the Chings. Available online: https://www.phishingfrenzy.com (accessed on 4 August 2022).
56. King-Phisher. Available online: https://www.kali.org/tools/king-phisher/ (accessed on 4 August 2022).
57. sptoolkit. sptoolkit Rebirth–Simple Phishing Toolki. Available online: https://www.darknet.org.uk/2015/04/sptoolkit-rebirth-simple-phishing-toolkit/ (accessed on 4 August 2022).
58. TrustedSec. The Social-Engineer Toolkit (SET). Available online: https://www.trustedsec.com/tools/the-social-engineer-toolkit-set/ (accessed on 4 August 2022).

59. SPF. SPF–Speed Phishing Framework. Available online: https://sectechno.com/spf-speedphishing-framework/ (accessed on 4 August 2022).
60. Kennedy, D. Introducing Spearphisher—A Simple Phishing Email Generation Tool. Available online: https://www.faqlogin.com/login/spearphisher-a-simple-phishing-email-generation-tool (accessed on 4 August 2022).
61. Barracuda. Barracuda PhishLine:Fight Phishing with Continuous Simulation and Training. Available online: https://www.barracuda.com/resource/data_sheets/Barracuda_PhishLine_DS_US (accessed on 4 August 2022).
62. Cofense. Security Solutions Built to Stop Phish. Available online: https://cofense.com/ (accessed on 4 August 2022).
63. Hoxhunt. Enterprise Security Awareness, Re-Invented. Available online: https://www.hoxhunt.com/ (accessed on 4 August 2022).
64. Infosecinstitute. Prepare Every Employee with Phishing Simulations & Training. Available online: https://www.infosecinstitute.com/iq/phishing-simulations/ (accessed on 4 August 2022).
65. IronScales. Phishing Simulation & Training: Anti Phishing Simulations and Customized Training Based on Real-Time Data and Real World Situations. Available online: https://ironscales.com/ (accessed on 4 August 2022).
66. Lucy. Cyber Security Training Solutions. Available online: https://lucysecurity.com/ (accessed on 4 August 2022).
67. Mimecast. Relentless Protection Starts Here. Available online: https://www.mimecast.com/ (accessed on 4 August 2022).
68. KnowBe4. Phishing. Available online: https://www.knowbe4.com/ (accessed on 4 August 2022).
69. proofpoint. Attackers Start with People. Your Cybersecurity Strategy Should too. Available online: https://www.proofpoint.com/us (accessed on 4 August 2022).
70. Nasser, G.; Morrison, B.W.; Bayl-Smith, P.; Taib, R.; Gayed, M.; Wiggins, M.W. The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails. *Front. Big Data* **2020**, *3*, 33. [CrossRef]
71. Stewart, H.; Jürjens, J. Information security management and the human aspect in organizations. *Inf. Comput. Secur.* **2017**, *25*, 494–534. [CrossRef]
72. Shah, M. Perception of Managers on the Effectiveness of the Internal Audit Functions: A Case Study in Tnb. Available online: https://www.semanticscholar.org/paper/PERCEPTION-OF-MANAGERS-ON-THE-EFFECTIVENESS-OF-THE-Shamsuddin-Shah/fe1a47ff6304041398376b1e7fefe0021d21dd6e (accessed on 4 August 2022).
73. Hair, J.F.; Page, M.; Brunsveld, N. *Essentials of Business Research Methods*; Routledge: London, UK, 2019.
74. Anawar, S.; Kunasegaran, D.L.; Mas'ud, M.Z.; Zakaria, N.A. Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. *J. Eng. Sci. Technol.* **2019**, *14*, 2865–2882.
75. Goel, S.; Williams, K.; Huang, J.; Warkentin, M. Understanding the Role of Incentives in Security Behavior. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 7–10 January 2020.
76. Leguina, A. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). *Int. J. Res. Method Educ.* **2015**, *38*, 220–221. [CrossRef]
77. Henseler, J.; Ringle, C.M.; Sarstedt, M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J. Acad. Mark. Sci.* **2015**, *43*, 115–135. [CrossRef]
78. Falk, R.F.; Miller, N.B. *A Primer for Soft Modeling*; University of Akron Press: Akron, OH, USA, 1992.
79. Statology. What is a Good R-Squared Value? Available online: https://www.statology.org/good-r-squared-value/ (accessed on 4 August 2022).
80. Houle, D. High Enthusiasm and Low R-Squared. *Evolution* **1998**, *52*, 1872–1876. [CrossRef]
81. Anderson, J.C.; Gerbing, D.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychol. Bull.* **1988**, *103*, 411. [CrossRef]
82. Ringle, C.M.; Becker, V. "SmartPLS 3" . Available online: http://www.smartpls.com (accessed on 4 August 2022).
83. Bollen, K.A.; Pearl, J. Eight myths about causality and structural equation models. In *Handbook of Causal Analysis for Social Research*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 301–328.
84. Morolong, M.P.; Shava, F.B.; Shilongo, V.G. Designing an Email Security Awareness Program for State-Owned Enterprises in Namibia. In *IOT with Smart Systems*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 679–688.
85. Chaudhry, J.A.; Chaudhry, S.A.; Rittenhouse, R.G. Phishing attacks and defenses. *Int. J. Secur. Its Appl.* **2016**, *10*, 247–256. [CrossRef]
86. Yeng, P.; Woldaregay, A.Z.; Hartvigsen, G. K-cusum: Cluster detection mechanism in edmon. In Proceedings of the 17th Scandinavian Conference on Health Informatics, Oslo, Norway, 12–13 November 2019; Linköping University Electronic Press, Linköpings Universitet, LiU: Linkopings, Sweden, 2019; pp. 141–147.
87. Baig, A. Understanding Data Encryption Requirements for GDPR, CCPA, LGPD & HIPAA. Available online: https://www.thesslstore.com/blog/understanding-data-encryption-requirements-for-gdpr-ccpa-lgpd-hipaa/ (accessed on 4 August 2022).
88. Prosper Kandabongee Yeng, M.A.F.; Yang, B. Assessing the effect of human factors in healthcare cybersecurity practice: An empirical study. In Proceedings of the Volos '21: Volos '2021: 25th Pan-Hellenic Conference on Informatics, Volos, Greece, 26–28 November 2021; ACM: New York, NY, USA, 2021.
89. Opoku, S.Y.; Benwell, M.; Yarney, J. Knowledge, attitudes, beliefs, behaviour and breast cancer screening practices in Ghana, West Africa. *Pan Afr. Med. J.* **2012**, *11*, 1–10.
90. Atinga, R.A.; Abekah-Nkrumah, G.; Domfeh, K.A. Managing healthcare quality in Ghana: A necessity of patient satisfaction. *Int. J. Health Care Qual. Assur.* **2011**, *24*, 548–563. [CrossRef] [PubMed]

91. Mohamed, N.; Ahmad, I.H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Comput. Hum. Behav.* **2012**, *28*, 2366–2375. [CrossRef]
92. Rhee, H.S.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Comput. Secur.* **2009**, *28*, 816–826. [CrossRef]
93. Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inf. Manag.* **2014**, *51*, 69–79. [CrossRef]
94. Shih, D.H.; Lin, B.; Chiang, H.S.; Shih, M.H. Security aspects of mobile phone virus: A critical survey. *Ind. Manag. Data Syst.* **2008**, *108*, 478–494. [CrossRef]