Journal of
Cyber Security

Tech Science Press

https://doi.org/10.32604/jcs.2026.079750

ARTICLE

The Impact of Cybersecurity Awareness on Phishing Attack Vulnerability

Darlington Chigozie Okeke*

Department of Computing and Engineering, University of Gloucestershire, Cheltenham, UK

*Corresponding Author: Darlington Chigozie Okeke. Email: okekechigozied2023@gmail.com

Received: 27 January 2026; Accepted: 16 March 2026; Published: 29 May 2026

ABSTRACT: Phishing has become the most common cybersecurity threat and increasingly exploits human factors rather than technical vulnerabilities. This study examined the relationships between cybersecurity awareness, training frequency, user cyber-hygiene behaviour, organisational culture, risk perception, and self-reported phishing vulnerability and the theoretical basis of this research is the Technology Threat Avoidance Theory (TTAT). A quantitative correlational design was used for data collection and analysis with Pearson correlation in structured questionnaires. The results indicated that the five independent variables have a significant positive relationship with phishing vulnerability. The increased awareness and regular training correlate with greater recognition of the vulnerability, suggesting improved self-observation but not an increased risk. On the same note, users with high cyber-hygiene practices also perceived themselves as more vulnerable, suggesting that protective measures can be driven by risk perception. An organisational culture also significantly correlated with vulnerability, which requires institutions that are supportive to provide a key role in threat perception. Vulnerability was also impacted by risk perception, with those who perceived phishing to be serious and personalised tending to agree that they were vulnerable. The findings, in general, support the idea that phishing vulnerability is a multidimensional phenomenon shaped by cognitive, behavioural, and organisational factors.

KEYWORDS: Cyber security awareness; phishing attacks; training frequency; cyber hygiene; organisational culture; risk perception; phishing vulnerability; security behaviour

1 Introduction

1.1 Background

Phishing is one of the most prevalent and harmful types of cyberattacks that exploit cognitive and behavioral shortcomings in humans and is not based on a technical vulnerability of the system. Phishing attacks have become a significant cybersecurity issue their sophistication and frequency over the last 10 years affecting governments, organisations, and individuals all over the world. New phishing campaigns no longer rely on overly primitive mass-emailed campaigns but more on social engineering, predictive profiling, and the manipulation of behaviour to trick users into revealing confidential information or installing harmful software [1,2]. Since cybercriminals keep perfecting their tactics and exploiting social and psychological opportunities, phishing is one of the most popular facilitators of identity theft, monetary fraud, account hijacking, and system intrusion [3]. The replacement of purely technical vulnerabilities with human-oriented attack vectors has consequently redefined users as the primary target of the cybersecurity ecosystem.

It is also due to the growing digitalisation of personal, financial, and organisational activities, which leads to a global increase in phishing threats. In the modern digital setting, people are used to doing banking,

shopping, communications, and work-related activities online, exposing them more to cyber threats [4,5]. This sensitivity is also enhanced by the fact that email and instant messaging systems are widespread and are the main delivery mediums in phishing campaigns. The ease with which phishing can be scaled and evade sophisticated security systems through false user trust makes it a favourite among cybercriminals. The latest sources state that to increase persuasion and minimize suspicion, cybercriminals increasingly use contextual cues (branding, financial urgency, and portrayals of legitimate institutions) to persuade people [3]. Such tendencies indicate that human factors, rather than technological inadequacies, are the primary vulnerability in the contemporary cybersecurity setting.

Due to the increase in the user-centred nature of cybersecurity threats, cybersecurity awareness has become a significant factor in mitigating phishing attacks. It has been found that awareness determines how the user recognises suspicious content and the malicious intent, and makes an informed decision when they come into contact with digital communications [6,7]. Research analysing the concept of cybersecurity awareness has shown that the level of knowledge pertaining to cyber threats has a huge influence on risk perceptions and behavioural reactions among users in situations where phishing is involved [8]. A lower level of user awareness of cyber threats will result in diminished detection ability and increased vulnerability to manipulation. On the other hand, the greater the awareness levels, the higher the security consciousness and the promotion of defensive digital behaviors, such as checking the origin of messages, taking a second look at hyperlinks, and avoiding unsolicited communication [2,9,10]. Thus, enhancing cybersecurity awareness has emerged as a strategic approach to minimise phishing vulnerability across various user groups.

Nevertheless, awareness might not be sufficient without organised training interventions that strengthen learning and induce behavioural change. Experimental evidence indicates that cybersecurity training helps users to identify phishing attacks and engage in more secure online behaviours [11,12]. The training programs are designed to recreate phishing scenarios, train users on the security policy, and provide practical training on how to detect the use of social engineering techniques. The effectiveness of training is largely reported, and it has been indicated that trained users have much lower click-through rates in simulated phishing campaigns [13]. In addition, modern training models are increasingly integrated with artificial intelligence and adaptive learning to make the content more personalized and engaging [14]. Regardless of these developments, the literature recognizes variability in the frequency, quality, and institutional uptake of cybersecurity training programs, as a large proportion of users have insufficient exposure to systematic cybersecurity training.

In addition to awareness and training, there is a concept called cybersecurity behaviour, also known as cyber-hygiene, which is significant in reducing phishing risks. Cyber-hygiene refers to regular activities that facilitate the use of secure systems, including software updates, the use of strong passwords, multifactor authentication, and avoiding suspicious links [4]. Studies show that even users who are aware of cybersecurity risks might fall into risky practices because of habit, convenience, or even cognitive overload [15]. These results indicate that behavioural compliance is not entirely knowledge-based but also influenced by psychological, motivational, and contextual factors.

Organisational culture has also been found to predict cybersecurity outcomes, especially in institutional contexts where compliance with security policies is mediated by organisational norms, communication patterns, and attitudes of the leadership and enforcement of the policy. Research shows that the lower the levels of phishing vulnerability among employees in an organisation, the more the organisation has invested in cybersecurity policy, encouraged safe behaviour, and reported an incident [16,17]. Positive organisational cultures help to create a sense of collective responsibility, which is why employees can see cybersecurity as a group issue rather than to an IT-limited problem. On the other hand, negligence, breaches of policies, and low reporting rates of phishing cases are caused by weak organisational cultures, where poor communication,

security is not prioritised, and a lack of resources [18]. These cultural aspects demonstrate that cybersecurity cannot be effectively addressed without the understanding the social environment in which users work.

Another important element that plays a critical role in phishing vulnerability is the perception of risk. Risk perception is the personal evaluation of the potential risks and threats to cybersecurity. When phishing is perceived as a significant threat, users tend to employ defensive strategies, including verifying their messages and being careful when interacting with links [19,20]. On the other hand, when perceived risk is low, users can misjudge the effects of phishing attacks, thus becoming complacent and more vulnerable. Research on behavioral cybersecurity has shown that risk perception mediates the relationship between behavioral awareness and behavior, suggesting that risk awareness does not necessarily lead to protective behavior without proper risk appraisal [4]. This supports existing theories in the psychology of cybersecurity that propose cognitive and motivational premises underlying users' decision-making regarding cyber threats.

Although there have been advancements in understanding these determinants, the continued increase in the number of phishing attacks across the world indicates that there is a lack of comprehensive measures to ensure that human susceptibility is properly tackled. According to the literature, cybercriminals are evolving faster than users are learning, thus the security gap is increasing. Therefore, there has been increased interest in studying the relationships among cyber security awareness, training frequency, behavioural practices, organisational culture, and risk perception, and their combined effects on user susceptibility to phishing attacks. It is on this basis that such research is required to inform more sophisticated and efficient cybersecurity interventions that can bolster human defences in an ever-more-complicated digital threat environment.

1.2 Research Gap

Whereas phishing has been an area of extensive research due to its escalating cybersecurity risk, the body of existing research has focused primarily on technological mitigation measures, threat detection, and machine learning algorithms, and the relative lack of studies that explore the human and behavioural factors of phishing vulnerability at a worldwide level. According to recent research, phishing attacks target psychological and behavioural vulnerabilities, and users are the primary attack vector [1,3]. Nonetheless, the studies are still incomplete on the influence of various user-related variables as a collectively defined vulnerability [1]. As an example, there is a range of empirical studies on cybersecurity awareness. Still, many of them consider only a specific group within the population, including students [2,21], or organisational employees in industry-specific settings, such as finance [19], which does not reflect the general user environment.

Also, cybersecurity training has been proven to reduce phishing success rates. Yet, there are still inconsistencies in the frequency of training, delivery method, and user engagement, which indicate that training results may be mediated by the users and the context [14]. Behavioural aspects such as cyber-hygiene are also currently being independently identified as critical, but behavioural constructs have not been comprehensively included in the models of research on phishing vulnerability [4]. On the same note, the organizational culture has been addressed in terms of the policy implementation and adherence [16,18]. Still, the effects of culture on the phishing vulnerability are under-researched in non-workplace settings.

Moreover, the risk perception is a significant cognitive factor that has not been well researched in the phishing literature despite its proven role in protective cybersecurity behaviour [19]. The available studies tend to investigate these aspects separately rather than within a human factors multilayer framework. Hence, there is still a missing piece of the puzzle in the overall investigation of how the combination of cyber security awareness, training rate, cyber-hygiene behavior, organizational culture, and risk perception affects user vulnerability to phishing attacks in a less sector-specific context. The fact that phishing attacks continue to

occur worldwide, even despite the significant number of investments in cybersecurity systems, only confirms the importance of bridging this gap in human-centred research.

1.3 Study Purpose

This research paper aims to explore how critical human-related cybersecurity variables affect the vulnerability of users against phishing attacks in an international environment. In particular, the research is expected to investigate the influence of cybersecurity awareness, the frequency of training, and cyber-hygiene behaviour, organisational culture, and risk perception on the vulnerability to phishing threats among users. The study is aimed at offering a more in-depth view of the human determinants of phishing vulnerability beyond the technical factors, as well as by incorporating these five constructs into one empirical model. It is assumed that the results of the research will be relevant to the field of cybersecurity and that they will improve behavioural and organisational approaches, guide the creation of more efficient awareness-raising strategies, training, and user-centred defence techniques that will be able to reduce the threat of phishing in various online settings.

1.4 Research Objectives (ROs)

RO1: To examine the relationship between cybersecurity awareness level and self-reported vulnerability to phishing attacks.

RO2: To determine the relationship between training frequency and self-reported vulnerability to phishing attacks.

RO3: To analyse the relationship between user cyber-hygiene behaviour and self-reported vulnerability to phishing attacks.

RO4: To assess the relationship between organizational culture and self-reported vulnerability to phishing attacks.

RO5: To evaluate the relationship between risk perception and self-reported vulnerability to phishing attacks.

1.5 Research Questions (RQs)

RQ1: What is the relationship between the level of cybersecurity awareness and self-reported vulnerability to phishing attacks?

RQ2: What is the relationship between training frequency and self-reported vulnerability to phishing attacks?

RQ3: What is the relationship between user cyber-hygiene behavior and self-reported vulnerability to phishing attacks?

RQ4: What is the relationship between organizational culture and self-reported vulnerability to phishing attacks?

RQ5: What is the relationship between risk perception and self-reported vulnerability to phishing attacks?

1.6 Hypotheses (Hs)

H1: *There is a significantly positive relationship between cybersecurity awareness level and self-reported vulnerability to phishing attacks.*

H2: *There is a significantly positive relationship between training frequency and self-reported vulnerability to phishing attacks.*

H3: *There is a significantly positive relationship between user cyber-hygiene behaviour and self-reported vulnerability to phishing attacks.*

H4: *There is a significantly positive relationship between organisational culture and self-reported vulnerability to phishing attacks.*

H5: *There is a significantly positive relationship between risk perception and self-reported vulnerability to phishing attacks.*

2 Literature Review

2.1 Phishing and Cybersecurity Threat Landscape

Phishing has become one of the most common and harmful cybersecurity risks in the modern digital world, involving attempts to obtain confidential information by deceiving unaware users. Phishing has evolved beyond simple email fraud, incorporating advanced social engineering tactics that exploit the psychological prejudice of the human brain [1]. This change is symptomatic of a broader shift in the cybersecurity environment, whereby intruders have begun to focus less on systems and more on people, as the human operator is the most vulnerable point in digital security systems. Phishing schemes have acquired contextual relevance, brand impersonation, and spear-phishing, which have elevated the rates of deception to high levels [3]. Phishing is a promising cybercrime tool that enables criminals to illegally access personal information, financial resources, and corporate networks because of its low operational costs, scalability, and high reward capability.

As noted in recent literature, phishing can be defined not merely as a technical attack but also as a psychological manipulation tool aimed at influencing users' actions. Cognitive and emotional manipulation, fear, urgency, curiosity, and perceived authority are often the determinants of the success of phishing campaigns [4]. An example is the use of phishing messages that impersonate reputable financial institutions, government agencies, or workplace departments to manipulate compliance. With digital communication platforms still facilitating financial, academic, social, and corporate transactions, the likelihood of attackers infiltrating communication channels with fraudulent information increases significantly. This has been accompanied by an increase in awareness that technological solutions are inadequate to counter phishing threats unless accompanied by behavioral and educational interventions.

Phishing attacks present a particular challenge to the overall cybersecurity threat landscape, as they do not rely on any more conventional technical solutions; they directly involve human participants. The organisations have invested heavily in firewalls, intrusion detection, and endpoint protection, yet they have failed to ensure that the users do not access malicious links on their own will or share sensitive data [15]. This creates a paradox: technology security systems that are safe in technology but insecure in an organisation due to human vulnerability. In the modern environment, the major causes of breaches include insufficient cybersecurity awareness, human error, and negligence [8]. Phishing is thus becoming a first step in bigger cyber-attacks, such as ransomware, credit theft, and business email compromise schemes.

The cybersecurity environment globally has become increasingly fearful as the sophistication of phishing techniques has increased. The digital transformation initiatives have also spread to the banking, education, healthcare, and government sectors, expanding the digital attack surface and amplifying the risk of data exposure. Banks have been a particular target because financial institutions possess not only financial resources but also personal customer data [19]. Similarly, academic settings have been shown to be more vulnerable as student bodies do not tend to be cybersecurity conscious and cautious [2]. These

sector differences reflect the point that phishing is a global menace but has various shades in various sectors depending on the level of digital maturity, regulatory, and user competency levels.

The topography is also made more difficult by increased global connectivity and digital communication media. The use of the internet and the prevalence of email as a communication tool have given cybercriminals a wide reach [4]. In addition, cyberspace is anonymised and borderless, which also makes it difficult to conduct attribution and prosecution and allows criminals to act with relative impunity. Phishing schemes keep up with the new trends in technology, such as cloud services, remote working environments, and mobile applications [14]. Remote working conditions, as a result of global disruptions, have also expanded the cybersecurity boundary, both exposing users to more phishing threats and reducing organisational control.

The training and awareness interventions have been actively discussed as a way to deal with the threats of phishing. Studies have also shown that cybersecurity awareness training is a strong measure that reduces user vulnerability by increasing their awareness of phishing indicators and decision-making under conditions of deception. Organised training can lower click-through rates and promote behavioural changes in the case of phishing simulations [11]. On the same note, simulations of cybersecurity attacks are useful pedagogical tools that enhance experiential learning and user threat-detection abilities [13,20]. Nevertheless, conventional training methods may to be effective unless they are supplemented by novel and interactive training designs that can maintain user attention and long-term knowledge retention [14]. These findings suggest the need for dynamic, continuous training models to keep abreast of evolving phishing methods.

Irrespective of efforts to instill user competencies, phishing cases are increasing globally, indicating a vulnerability- and threat-based landscape. Regular user accountability and organisational participation in cybersecurity is not very likely to be practised, particularly having cybersecurity as an IT-related, but not an organisational-wide activity [16]. Organizational culture, therefore, is a significant intermediary in the defensive cybersecurity posture, making cybersecurity internalized as part of day-to-day activity in cyberspace. The cybersecurity skills among demographic groups, such as age, education level, and digital experience, are very diverse, which complicates the development of generalised preventive measures [18].

The contemporary cybersecurity threat environment across the world depicts that phishing attacks are going to continue being a leading cyber threat, as they have behavioral, economic, and strategic strengths for the attackers. As noted in the existing literature, human-level exploits are always better than technical ones, and thus, the end user is the key point of vulnerability [1,22]. As a result, reducing phishing risks is a complex task that involves a combination of awareness, training, behavioral adjustments, organizational culture, and risk perception. With their ability to improve fraudulent procedures, the need to enhance human-focused cybersecurity defense grows more urgent by the day.

2.2 Theoretical Framework: Technology Threat Avoidance Theory

The Technology Threat Avoidance Theory (TTAT) is a suitable theoretical framework for analyzing individual perceptions and reactions to cybersecurity threats, including phishing attacks. TTAT was proposed by Ghelani [23], describing user action in the light of the threat appraisal and the coping behaviour affecting the use of protective technology and the defensive behaviour. This theory presumes that users will be motivated to prevent the threat posed by malicious information technologies when they judge the threat as potentially harmful and personally relevant, and when they believe they have the ability and coping resources to avert adverse effects. In the framework of the phishing phenomenon, it is the TTAT that becomes especially helpful since phishing campaigns are based on the inability of users to identify the threat and implement protective actions in online surroundings.

The main idea of TTAT is that, in the face of cybersecurity threats, people engage in two cognitive processes: threat appraisal and coping appraisal. Threat appraisal entails the perceived susceptibility and perceived severity. Perceived severity is an individual's attitude toward the extent of harm associated with a threat. In contrast, perceived susceptibility is the attitude of an individual with regard to the probability that he will experience the threat. These elements are applicable in the context of phishing since users form perceptions of the extent to which phishing is dangerous and whether they may become victims of phishing attacks themselves. Users who believe that phishing is a serious and personal threat will employ protective strategies, such as questioning email sources, confirming hyperlinks, or even avoiding interaction with a suspicious item [19,24]. On the other hand, users who do not perceive the risk or likelihood of a phishing attack will not trigger timely defensive measures.

After threat appraisal, TTAT assumes that the user undertakes a coping appraisal, in which they evaluate the effectiveness of protective actions, their self-efficacy to carry them out, and the costs involved in the response. Coping appraisal in the case of cybersecurity is essential since awareness is not sufficient to take any protection measures. Despite being aware of phishing threats, users can forget about safe practices, be inconvenienced, or cognitively overloaded, or have a lack of perceived self-efficacy [4]. For example, implementing multi-factor authentication or verifying message authenticity could be time-consuming or technically complex. TTAT, thus, emphasize that perceived response costs are to be minimised and self-efficacy is to be trained, the policy communicated, and favourable organisational cultures promoted, which may raise the prospects of security compliance.

The applicability of TTAT to phishing research is also supported by the current body of behavioural cybersecurity research prioritising the interaction between awareness, behavioural intentions, and actual cybersecurity behaviour. Training interventions promoting user competence and confidence enhance cybersecurity self-efficacy and positively influence the threat avoidance behaviours of the users [11]. Correspondingly, organisational culture and educational engagement strategies can increase the involvement of users in cybersecurity activities, which corresponds to the coping appraisal factors of TTAT [16]. All these studies demonstrate that, in addition to awareness of threats, users should feel they have the capacity and means to reduce risks, which resonates with the main propositions of TTAT.

Regarding the phishing vulnerability, TTAT provides explanatory power for several constructs studied in this paper. Cybersecurity awareness involves aspects of threat appraisal and coping appraisal, as it increases users' awareness of phishing severity, probability, and mitigation measures. The frequency of training is linked with improvements in coping appraisal through enhancing the confidence of users and competency in coping with phishing threats. The concept of cyber-hygiene behaviours should be included in the category of avoidance behaviours since they imply proactive behaviours that users implement to reduce their exposure to threats. The organisational culture can minimise the costs of response through the structural and institutional support that can enhance the chances of ensuring security compliance. Risk perception closely aligns with perceived susceptibility and perceived severity, key components of the threat appraisal process in TTAT. Connecting these constructs, TTAT offers a consistent theoretical prism of explanation regarding how cognitive judgments could be transformed into defensive or careless cybersecurity practices.

In addition, the focus on behavioral intention in TTAT is especially useful, as a phishing attack is a psychological phenomenon. Studies have also shown that cyber criminals use cognitive biases and decision-making shortcuts to overcome rational threat appraisals [1,3]. Users in such settings might end up making the wrong decision of clicking on malicious links, even though they have the knowledge of cyber threats, since heuristic reactions prevail over cognitive evaluation when faced with urgency or distraction. TTAT postulates that the heuristic vulnerabilities may be offset by enhancing coping resources through training/awareness to

counter systematic threat assessment. This interpretation of behaviour supports the applicability of TTAT in the phishing environment, where human thinking is often controlled.

All in all, TTAT provides a strong theoretical basis to examine phishing vulnerability since it frames cybersecurity as a process that is based on human behaviour and cognition and is motivated and contextual instead of a technical defence only. The theory acknowledges that users are proactive decision-makers who balance perceived threats and perceived coping capacity, then engage in avoidance behavior. With phishing attacks becoming more prevalent across the world despite the amount of investment in technology, TTAT presented the need to focus on humanistic aspects of cybersecurity. With the help of the application of TTAT to the present study, one will be able to determine how awareness, training, cyber-hygiene, organisational culture, and risk perception affect phishing vulnerability, which will help understand the user-centred cyber defence mechanisms more holistically.

2.3 Variable-Based Review

2.3.1 Cyber Security Awareness → Phishing Vulnerability

The issue of cybersecurity awareness has been generally identified as a key factor in defining the relationship between people and the internet space, especially when they face fraudulent online dangers like phishing. The concept of cyber security awareness is very broad, and it is understood to refer to the knowledge, the understanding, and the cognitive preparedness of a user about cyber threats, attacks, and preventive measures. As detailed in the literature, cybersecurity awareness is formed by the user behaviour, attitude, and threat comprehension, which have an impact on how people are aware and responsive to phishing attacks [14,24]. Awareness in this respect can be viewed not only as access to information but also as a sense-making that users exercise in relation to digital stimuli, risk perception, and warning messages. Cyber security awareness, in turn, can be related to the levels of phishing vulnerability, as lowly-aware users will not notice dangerous messages or mistakenly assess the intent of the threat [8].

Several surveys have reported that phishing attacks use cognitive and informational loopholes in users. People having weak awareness of phishing tricks are more likely to be convinced of the fraudulent messages that have the appearance of official messages of the organisation [15]. These users often ignore such inconspicuous signs, like inconsistencies in the sender, to give out false URLs, or unusual language patterns, which contribute to successful phishing attacks. In addition, internet users with little or no knowledge of changing cyber threats have lower decision-making approaches when they operate in internet spaces, particularly where money or credential validation is involved [4]. These results imply that awareness can define a user's interpretive framework, which can exacerbate weaknesses in a high-pressure or time-sensitive context that is often designed by attackers.

It is also clear that phishing attackers openly exploit informational asymmetries, using social engineering, situational mimicry, and psychological persuasion. Self-regulation, the ability to process information, and personal knowledge have significant effects on how users react to deceptive cues that come with phishing messages [4,25]. Users with better cybersecurity awareness report a more strategic and analytical approach to assessing suspicious material, whereas unaware users rely heavily on heuristics. When applied to education, less knowledgeable university students showed greater vulnerability to phishing because they lacked the knowledge of the kinds of attacks and the safeguards against them [21], and this relationship is obvious because of the difference in awareness levels, resulting in the difference in the distribution of vulnerabilities.

Second, cybersecurity awareness can also have an indirect relationship with other cognitive variables, including threat perception, risk evaluation, and response efficacy. Awareness and cybersecurity education would help to achieve higher levels of accountability and vigilance among the employees so that they more

actively internalise security norms and practices [16,26]. This view presents a perspective in which awareness helps users not only identify cyber threats but also understand how they work and develop [1]. This mental expression can determine whether one disregards, researches, or interacts with the suspicious information, and thus vulnerability is not a product of knowledge deficits but rather a product of knowledge mobilization during real-time exposure to internet danger.

Though the literature suggests a general trend that relates a low level of cybersecurity awareness to an increased level of phishing vulnerability, researchers have observed that the manifestation of awareness varies significantly across demographic, organisational, and contextual lines. The level of awareness among university students varies depending on their academic discipline, training exposure, and background in digital literacy [18,27]. On the same note, workplace communities have diverging awareness as a result of different organisational focus, communication tactics, and behavioural reinforcement systems [15]. These results indicate that cybersecurity awareness is not a fixed concept but evolves through the social, educational, and experiential channels. As a result, awareness has a determining effect on susceptibility to phishing, shaped by personal learning processes and context-related affordances.

Lastly, it is worth noting that the notion of vulnerability can depend on awareness, though awareness cannot ensure safe behaviour. Most users with sufficient cybersecurity knowledge will still appear to take on risky digital behaviours because of cognitive overload, convenience bias, or because attackers are able to manipulate their emotions [15,28]. This effect means that awareness is not a protective determinant but one among several forms of interdependent variables that lead to vulnerability. Thus, cyber security awareness is a complex cognitive tool whose impact on vulnerability to phishing should be viewed through a multidimensional behavioral lens.

2.3.2 Training Vulnerability and Phishing Frequency

Cyber security training is an institutionalised organisational process of improving the knowledge, skills, and adaptive reaction of users to changing cyber threats. Training frequency specifically refers to the frequency of such educational interventions as a whole and to the consistency of employee exposure to updated cybersecurity material. Regular cybersecurity awareness training is efficient in increasing the workforce preparedness because it provides users with current information on phishing and the mechanisms used by the attackers to defraud targets [11,29].

Organisational research proved that the effectiveness of irregular, outdated, or one-time training cannot achieve long-term behaviour change. Current phishing threats are changing at a rapid rate, which tends to combine artificial intelligence and psychological profiling, and therefore makes the existing training material inadequate [14]. Since phishing uses novelty and poses as a strong strategy, the employees who are not updated regularly would be unaware of new tricks or new patterns of attack and would become more prone to misclassification and contact with malware. To reinforce this, spear phishing, which is a more specific and individualised form of phishing, needs sustained training interventions to ensure that the financial employees can identify subtle manipulation tactics that are used to exploit trust relations in the organisations [19].

Studies have also indicated that regular training increases the acquisition of knowledge as well as the normalization of behaviors in which safe behaviors become part of organizational culture. Companies that institutionalise frequent cybersecurity training inculcate responsibilities, attentiveness, and proactive reporting of threats among their staff members [16]. According to this trend, the vulnerability may also be determined by how often training takes place through cognitive processes, normative reinforcement, and practice. In the meantime, the training helps raise policy compliance and cybersecurity posture, making

people more willing to communicate with digital systems and less hesitant and suspicious when making cybersecurity decisions [15].

Affective and perceptual processes are also important to consider, as they may influence vulnerability. Even untrained users are likely to overrate their own security and underrate the dangers of phishing or overestimate the consequences of their own risky relationship with rogue online users [1,30]. Conversely, frequently trained employees experience greater skepticism, heightened risk perception, and greater threat potential evaluation. Moreover, cyber-attack simulation may be used as an engaging learning experience where the learners would be able to practice their response to the dangers within a controlled environment [13]. These kinds of simulations enhance reality preparation by exposing users to attacker techniques without damaging any organisational resources.

Whereas the literature confirms that training frequency affects phishing vulnerability, research indicates that training can be effective among different demographic and professional groups. Academic populations do not react to cybersecurity training as financial or government employees, where attack vectors and operational stakes have different values [21]. Also, training should be effective and take into account differences in cognitive diversity and processing, implying that the frequency of training is not necessarily the sole determinant of vulnerability unless it is provided with pedagogical differentiation, motivation, and involvement [4].

The combined analysis of the reviewed literature suggests that training frequency can affect susceptibility to phishing attacks, and the mechanisms underlying this effect can be explained by the reinforcement of knowledge, conditioning of behaviour, the improvement of perception, and the formation of organisational norms. Nevertheless, just as with cybersecurity awareness, training is merely part of a larger sociotechnical ecosystem that conditions user vulnerability, meaning that training does not eliminate phishing risks but helps them to be managed through ongoing cognitive and behavioral interventions.

2.3.3 Cyber-Hygiene Behaviors and Phishing Vulnerability

The concept of cyber-hygiene behaviours can be explained as the common habits, behavioural decisions, and preventive measures that users use to ensure that their cyber-spaces, accounts, and information are not vulnerable to cyber-attacks. The actions that can be considered as cyber-hygiene in the context of phishing are staying suspicious of untrustworthy links, using passwords that are difficult to crack, enabling multi-factor authentication, updating software, and reporting suspicious messages to the corresponding authorities. Self-regulation, information processing, and knowledge mobilization are key psychological attributes of cyber-hygiene, defining the manner in which users assess, react to, and overcome phishing threats [4,30]. Individuals who practice cyber-hygiene regularly would be better positioned to examine external stimuli, identify anomalies, and apply security measures to mitigate phishing attacks.

The literature indicates that a lack of sufficient cyber-hygiene habits is becoming a powerful tool that is used by many phishing attacks, instead of ignorance alone. Phishing attacks are becoming more and more advanced in terms of mimicry and manipulation of context, and conventional knowledge-based defences are no longer sufficient unless users use behavioural countermeasures [1]. Such countermeasures as password rotation, defensive authentication regimes, and device-level updating are collectively behavioural defences, upon which phishing is dependent to evade. Consistent with this opinion, organisations that inculcate the cyber-hygiene expectations into the duties of their employees are more likely to create a setting whereby the vulnerability to phishing can be shaped by the general behavioural norms instead of being dependent on individual discretion [16].

In addition, the results of a series of empirical studies have demonstrated that some of the practices expected to enhance cyber-hygiene weaken the options available to attackers to develop simple phishing attacks into more comprehensive exploit chains. AI-based cybersecurity raising awareness programs tend to focus on cyber-hygiene behaviour as a teaching area because the phishing attack is often the entry point to more comprehensive cyber intrusions [14]. In comparison, the users and dangerous agents who do not follow these preventive measures can facilitate a chain of security violations, including the theft of credentials, unauthorized access, or data leakage, completely unaware of it. Knowledge vs. action, the difference between knowledge and action is thus rather prominent. In contrast, knowledge about phishing gives users awareness, cyber-hygiene puts that awareness into action, and translates it into beneficial, defensive actions.

In addition, cyber-hygiene practices can affect phishing vulnerability through reporting and incident response systems. The timely reporting and escalation of phishing incidents play a significant role in the resilience of the organization to these attacks, with the most significant role played by the large organizations with high communication flows during cybersecurity simulations [13]. By users reporting suspicious emails, organizations can take containment measures, conduct forensic tests, and inform other workers to prevent them from interacting with such phishing emails. On the other hand, undocumented cases give rise to information gaps in which phishing activities thrive without detection. Therefore, cyber-hygiene behavior is preventive, but also communicative and collaborative.

Researchers have also been keen to note the differences in cyber-hygiene practices between demographic and sectoral lines. University students exhibited disproportionate patterns in cyber-hygiene practices, which were predominantly determined by individual digital literacy, exposure to courses in the field, and perceived risk [18,31]. In the meantime, students who lacked cyber-hygiene discipline were more likely to demonstrate increased vulnerability to phishing, particularly when communicating through academic platforms, email systems, and financial aid portals [21]. These results highlight that cyber-hygiene behavior might not consistently affect vulnerability; instead, it depends on context.

Although the literature suggests that cyber-hygiene can determine phishing vulnerability, researchers warn that behavioral compliance can vary depending on situational factors, emotional manipulation, or institutional support. Convenience and efficiency are usually highlighted by the user in navigating the digital platforms, despite being conscious of best practices, and a behavioral-intent gap commonly complicates the cybersecurity results [4]. The tendency to induce a sense of urgency, curiosity, or fear is the basis on which phishing attackers create messages that trigger these emotions, thereby bypassing cyber-hygiene behavior. For these reasons that cyber-hygiene behaviors remain fundamental aspects that affect phishing vulnerability, even though their effects are inherent in larger behavioral and psychological ecologies.

2.3.4 Organizational Culture → Phishing Vulnerability

Organizational culture is one of the determinants of context that is critical to how individuals view cybersecurity responsibilities, embrace secure digital practices, and respond to cyber risks like phishing. Organizational culture refers to the shared values, norms, expectations, policies, leadership priorities, and informal practices that shape how employees behave in the workplace. The probability of cybersecurity awareness and educational programs is far more effective when incorporated in cultures that encourage engagement, accountability, and collective responsibility [16,32]. These cultures contribute to the normalization of secure practices and to reduced individual differences in cybersecurity outcomes among employees with different technical backgrounds.

Phishing vulnerability could be moderated by organizational culture that determines the frame, communication, and prioritization of cyber threats. Employee compliance with cybersecurity policies is

more likely to be high in organizations with clear policies and a regular communication channel [15]. The probability of vague or inconsistent enforcement of security policies is that employees tend to apply informal judgments, which can easily be exploited in phishing campaigns. In addition, the focus on leadership is critical to mark the significance of cybersecurity. Financial institutions in which phishing prevention became a strategic priority saw higher levels of training participation, incident reporting, and vigilance, indicating that cultural alignment has an indirect impact on vulnerability by reinforcing behaviors [19].

Support mechanisms in an organisation can also predispose employee behavior in a phishing attack. Social environments at the workplace determine how people perceive cybersecurity risks and feel confident enough to disrupt suspicious interactions [14,33]. When employees are afraid of being punitive in cases of reporting incidents, they can engage in concealment behaviors, thereby making systems vulnerable. However, cultures that enable reporting but do not blame will learn about threats faster and minimize phishing. This communication indicates that communication flow, trust, and coordination are part of people`s response to phishing [13].

Moreover, there are variations in how cybersecurity is implemented across organizations. Human weaknesses have been known to cause organizational breaches, unlike system weaknesses, which suggests that organizational responses that view cybersecurity as an IT function alone might be indirectly dependent on high phishing vulnerability [8]. On the other hand, holistic cultures divide responsibility among road staff, managers, and technical units, which makes them alert. Responsibility systems among workers improve security positioning by intensifying behavioral expectations and reducing uncertainty [16].

Investment in an organization also contributes to the formation of a culture that shapes the phishing vulnerability. Phishing attacks are becoming more and more intensive based on the high-level social engineering, requiring education and the implementation of technological solutions, including email filters, authentication procedures, and intrusion detection systems [1,34]. Companies that fail to invest significantly in these tools unwillingly place the responsibility for identifying threats in the hands of individual workers who might lack the required skills to assess the level of sophistication of attackers. These environments introduce structural weaknesses that manifest in higher phishing success rates, showing that cultural variables touch on technical systems.

Lastly, the difference in organizational culture across industries means that phishing vulnerability is not evenly spread throughout the institutional areas. Financial institutions have considered phishing as a strategic risk because of financial exposure, but academic settings have considered it an educational or IT inconvenience, and thus, there is a disparity in the allocation of resources [19,35]. Higher phishing vulnerability has also been reported in academic environments because users did not face institutional pressure to internalize security behaviors [21]. Therefore, organizational culture can be used to affect vulnerability to phishing through strategic prioritization, resource allocation, normative messaging, and behavior reinforcement.

2.3.5 Risk Perception-Phishing Vulnerability

Risk perception is an individual's subjective evaluation of the probability, magnitude, and impacts of cyber threats, such as phishing. In a phishing situation, risk perception will involve beliefs on how much one can be a victim, how severe harm can be (financially or reputational), and how much perceived prevalence there is of phishing attacks in the digital ecosystem. Risk perception is a cognitive process that can guide a user in the way they process information and make judgments when interacting in the online environment [4,34,36]. Perceived seriousness and perceived personal relevance of phishing will contribute

to the formation of safeguarding behaviors when individuals take the threats seriously and perceive them as important to them. Still, low perceived risk may be associated with complacency and high susceptibility.

According to the latest literature, phishing attackers tend to utilize gaps in perception of risk by either presenting messages in a manner that minimizes the threat perception or by having heuristic judgments. Phishing attacks are executed by combining anonymity, social engineering, and psychological manipulation to present fraudulent messages as normal or non-dangerous [1]. These tricks are designed to reduce the perceived risk, enabling users to access malicious links or data requests without evoking systematic threat appraisal. The importance of emotional triggers should not be ignored as well. Spear-phishing attacks frequently create a sense of urgency or fear within financial institutions by making the request seem time-sensitive, which temporarily represses rational risk assessments [19].

Research findings also indicate that risk perception is a variable with respect to cyber experience, training exposure, demographics, and organisational environment. General risk perception was significantly higher than perceived personal risk among university students, who did not perceive a high likelihood of being victims of phishing attacks despite reporting general cybercrime risks [14]. Equally, academic users often viewed phishing as a distant or theoretical problem rather than a personal issue of concern [21]. These observations indicate that risk perception does not necessarily apply to defensive reactions unless users assimilate the significance of the hazard.

Financial and privacy implications are also identified as a main focus of research on phishing risk perception. Sensitive personal and financial information is now being targeted with increasing of sophistication, expanding the scale of damages that successful phishing attacks can cause, and making the consequences of such attacks more significant [3]. Online users who are aware of such outcomes can modify their online activities. However, those who do not realize the threats to privacy and finances can still use online platforms without sufficient precautions. Moreover, the training methods emphasizing individual and corporate results are more effective at increasing risk perceptions than technical descriptions of phishing attacks [14].

User characteristics also mediate risk perception through contextual factors, including media exposure and institutional communication. The standard of consciousness concerning threats among the population is impacted by the discourse on cyber events on the public internet, especially in the case of high-profile phishing attacks that are highly discussed in the media [14]. Organizations can also influence the perception of risk in a proactive manner. Organizations that submit cybersecurity warning messages and reports of cybersecurity incidents raise employees' awareness of the high rate of phishing, which reduces laxity in behavior [15]. On the other hand, conditions in which limited information on cyber incidents is reported unintentionally lead to low risk perception, which exposes vulnerability.

However, scholars caution that there may be excessive risk perception. In situations where people view risk as being ubiquitous and inescapable, they might turn to avoidance or resignation behaviour instead of defensive actions [16,37]. This means that phishing mitigation will need a measured risk communication that helps foster awareness without causing death. Good risk perception; hence, it falls between dismissal and panic, which promotes vigilance and active action.

Overall, the literature demonstrates that risk perception influences phishing vulnerability using user motivation, behavioral intention, focus of attention, and decision-making. Having correct and internalised risk perception can make a user more inclined to doubt and challenge digital interactions, adopt cyber-hygiene practices, participate in training programs, and report suspicious behavior. On the contrary, people with a low or distorted perception of the risk will ignore organizational policies, neglect safe practices, and underestimate their risks of becoming a victim of phishing. Given the increased intensity and complexity of

phishing attacks, risk perception is also a highly important human-factor variable that defines vulnerability at both organizational and individual cybersecurity levels.

2.3.6 Outcome Variable: Phishing Vulnerability

Phishing vulnerability is the extent to which people are manipulated, defrauded, and abused in a phishing attack. Phishing vulnerability as an outcome variable in cybersecurity research is not merely a behavioral (i.e., clicking suspicious links or disclosing sensitive information); it also involves a cognitive disorientation, ambiguity, and failure to differentiate genuine and malicious messages are also present in this outcome variable. The Phishing vulnerability is intrinsically multidimensional because internal cognitive as well as external contextual factors play a role in creating it [4]. In part, this multidimensionality explains why phishing has become one of the most widespread and effective forms of cybercrime worldwide, despite heightened awareness and technological protections.

The literature indicates that phishing vulnerability is affected by psychological, informational, organizational, and behavioral factors, but not by technical deficiencies. Phishing criminals are constantly improving themselves through human heuristics, emotional responses, and social trust systems rather than relying solely on technical exploits [1,38]. This framing positions users as the primary targets of phishing ecosystems. Similarly, phishing has been described as a social engineering process that uses communication, not code, to weaponize, and the user cognition mediation of vulnerability has been identified [3]. The tactical application of persuasion, imitation, and familiarity is why the phishing vulnerability cannot be perceived as a technological failure.

Empirical studies also prove that the vulnerability to phishing is contextual and population-specific. Scholars have been found to be more susceptible to this because they are less exposed to mandatory cybersecurity education, and the instability of security is less of a priority on the institutional level [3]. Workers in financial institutions, on the other hand, are less prone to this due to increased regulatory oversight, awareness of risk, and the inculcation of security-related education [19]. These results suggest that the phishing vulnerability is not distributed equally across sectors depending on the institutional expectations, resource distribution, and cultural priorities.

Moreover, phishing weakness could remain even in cognitively conscious users. The practice of cyber security awareness does not eliminate the vulnerability, as users can still interact with malicious content due to distraction, habituation, and situational pressure [11,39]. This aligns with the overall behavioral decision-making studies that found that cognitive overload, time constraints, and emotional manipulation have implications for reactions to cyber threats. The phishing vulnerability is consequently presented at the border of knowledge, perception, behavior, and context.

Technological mediation may also determine the vulnerability outcomes. Companies that do not invest in protective technologies such as state-of-the-art email filters, anti-phishing gateways, and automated alerts risk overloading individual workers with the task of detection [15]. The absence of institutionalized support and adequate resources to cope disposes individuals to phishing vulnerability, irrespective of the training or awareness. It supports the idea that vulnerability is produced in social-technical systems.

Lastly, the phishing vulnerability is enhanced by the sophistication of attackers. Modern phishing programs involve specific operations, such as spear phishing, cloning phishing, and credential harvesting that replicate official institutional messages [8]. Users are increasingly finding it hard to spot ill motives as malicious intent is enhanced by attackers through increasingly personalizing, linguistic matching, and contextual realism. This development means that the phishing vulnerability is dynamic and constantly retooled by antagonistic innovation.

On the whole, one essential outcome variable in cybersecurity studies is phishing vulnerability, which summarizes the behavioral expression of the complex upstream variables of awareness, training, cyber-hygiene, organizational culture, and risk perception. The multi-layered view of phishing vulnerability facilitates the formulation of multi-layered intervention strategies that go beyond technical controls to encompass the behavioral and organizational interventions. Given that phishing remains one of the primary vectors of cyber threats to this day, a human-centered vulnerability analysis can be used to enhance cybersecurity resilience and threat management.

2.4 Empirical Studies Review

Empirical research on phishing has experienced a remarkable increase during the last few years, with organizations and researchers seeking to understand human factors of vulnerability and protection. The relationship between phishing outcomes and cybersecurity awareness has been studied by other researchers. The effects of user behavior on cybersecurity awareness, for example, indicate that the higher the level of awareness, the more behavioral resistance towards exposure to the threat was observed. However, behavioral inconsistency was also exhibited between sets of users [14]. Similarly, investigations carried out on phishing vulnerability on students indicated that the students who had less awareness were more susceptible, which proves the importance of awareness as a mitigation variable [21]. In a follow-up study, it was found that the level of awareness significantly differed between the demographic segments. Therefore, that vulnerability could be influenced by both personal and situational factors.

Empirical studies of training interventions have also been conducted. It has been demonstrated that formal cybersecurity awareness training reduces vulnerability to phishing due to increased detection and user confidence [11]. A study conducted within financial institutions demonstrated that social engineering training on awareness of phishing resistance enhanced the operational environments that are at risk [19]. It was also demonstrated that AI-based cybersecurity awareness training is more efficient at detecting phishing, meaning that the frequency and modality of training have an impact on the results [14,39]. Combined, these studies suggest that training is a behavioral and cognitive intervention that can change susceptibility.

Some empirical studies have focused on cyber-hygiene practices alongside training and awareness. Self-regulation and making informed decisions were found to be key predictors of anti-phishing behaviors, and behavioral practices are protective factors [4]. Through cyber-attack simulation, the participants who had good hygiene behaviors, like reporting suspicious items and checking the authenticity of the communications, were identified to be more resistant to phishing [13]. These findings indicate that vulnerability outcomes are determined by behavioural performance, not by awareness.

Phishing vulnerability has also been identified as a result of organizational culture in the empirical literature. Companies that periodically have established cybersecurity policies are more compliant and less affected by phishing [15]. The cultural aspects of employee involvement and responsibility can enhance defense capabilities [16], and supportive environments make users treat cyber threats seriously and take proactive security measures [14]. Such results are consistent with the broader discussion that institutional environments determine cybersecurity outcomes through norms, support networks, and risk communication.

Finally, as an outcome variable, empirical studies have investigated phishing vulnerability. Changing trends in phishing reveal a persistent vulnerability despite technological advancements, driven by increasing attack sophistication and behavioral exploitation [1]. Phishing has also been characterized as a pervasive cybersecurity issue because social engineering techniques bypass technical protections by manipulating human cognition [3].

2.5 Conceptual Framework

This paper investigates factors that influence self-reported vulnerability to phishing, including cybersecurity awareness level, training frequency, user cyber-hygiene behavior, organizational culture, and risk perception. Therefore, the association of these variables can be presented in Fig. 1 below:

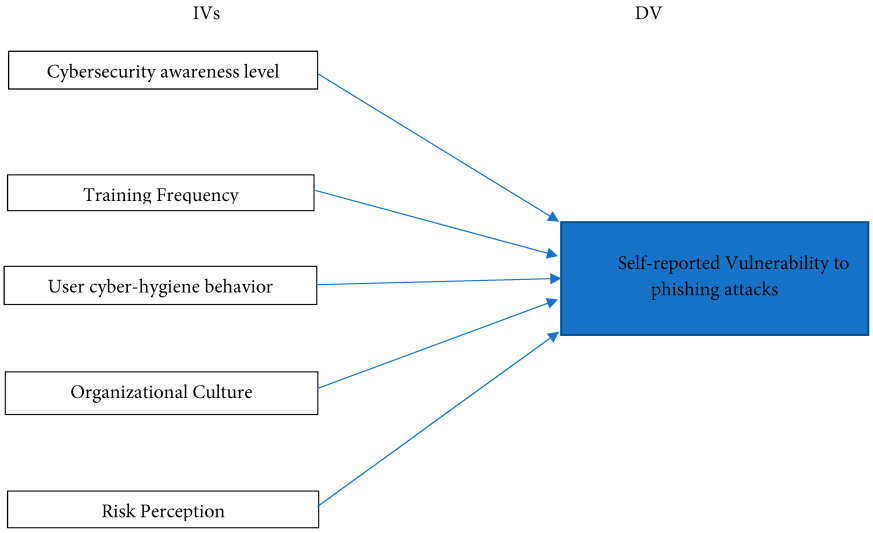

Figure 1: Conceptual framework on different factors and phishing attacks [4].

3 Methods

3.1 Research Design

This research took a quantitative research methodology where the correlational research design was applied to test the hypothesis that the independent variables, with phishing vulnerability as a dependent variable, included the level of cybersecurity awareness, the frequency of training, the cyber-hygiene behavior of the user, the organizational culture, and perception of risk. The quantitative methodology was suitable since the study's purpose was to quantify the constructs, to test the relationship among the variables, and to extrapolate the sample results to the broader population. A correlational research design was particularly appropriate to this effect since the study aimed at establishing whether and to what degree differences in the predictor variables were statistically related to differences in phishing vulnerability without controlling the variables experimentally. Unlike experimental designs where variables are controlled, a correlational design can be used to study such variables in a natural setting and takes the form of predictive modelling, which is in line with the practical setting of cybersecurity behaviors within an organizational and user setting. The quantitative framework based on the survey method allowed data collection from more respondents in a time-saving manner. It made the results more comparable by standardizing measurement scales.

3.2 Population and Sampling

The sample population of this study was the people who are involved in computer-mediated communications and use email or digital media in work or academic settings, since these users are the main victims of phishing attacks. The population of 400 individuals was described as comprising working professionals from various branches of organizations, students, and specialists who regularly work with digital systems. Since the phishing attacks happen among demographic and professional groups, this population frame was

appropriate to attain a variance in cybersecurity awareness, training exposure, behavioral practices, and cultural factors that can determine vulnerability to phishing.

This choice of a population of 400 people has been made based on relevance, statistical adequacy, and diversity considerations. The research focused on people who are active users of computer-based communication, who are frequent users of email and other digital platforms in the workplace or academia, since they are the direct victims of phishing. The size of 400 is large enough, and it improves the power of the statistics, minimises sampling error, and the power of the parametric tests: the correlation. Also, the presence of working professionals representing different branches of the organizations, students, and experts in digital systems makes it more varied to achieve cyber security awareness, training exposure, cyber-hygiene behavior, organizational culture, and risk perception. This heterogeneity enhances the generalizability and reliability of the results, as the chosen population would be suitable to investigate the factors regarding self-reported vulnerability to phishing attacks.

Simple random sampling was used to identify the respondents to participate. This sampling strategy meant that every individual of the identified population was equally likely to be chosen and therefore reduced sampling bias and made the sample more representative. The initial sampling method used was simple random sampling, and this was especially suitable since the study was to offer inferential statistical generalizations concerning the relationships between the variables. In addition, random selection contributed to increasing the methodological rigor of the study because it minimized systematic bias that could otherwise be present in the study due to convenience or purposive sampling. A total of 200 participants were identified to constitute a final sample, which was adequate enough to carry out both the correlational analysis and maintain statistical power.

3.3 Sample Size Determination

The determination of sample size was done using a smaple size was done using Yamane's formula from a population of 400 respondents. Given a population of 400 participants, Yamane's (1967) formula for sample size calculation is expressed as:

$$n = N/(1 + N(e^2))$$

where:

- n = required sample size
- N = total population
- e = margin of error, commonly 0.05 (5%)

Applying the formula with N = 400 and a precision level of e = 0.05:

$$n = 400/(1 + 400(0.05^2)) = 200$$

Therefore, the required sample size is:

n = 200 participants.

Therefore, the sample size involved in this particular study was 200 participants.

3.4 Data Collection Instrument

The structured questionnaire was a self-administered questionnaire, which was created to collect data used in this study. The questionnaire was classified into sections of demographic characteristics and the main variables of the study. The tool was the one that would be used to assess cybersecurity awareness and

training frequencies, user behavior related to cyber-hygiene, organizational culture, perception of risks, and phishing vulnerability with the help of standardized statements. The administration of the questionnaire was beneficial as it made it easier to collect data from a number of respondents efficiently and consistently presented items, which meant that the responses could be compared statistically. The questionnaire was distributed electronically to the participants to promote ease of access, minimize logistic limitations, and preserve anonymity, which is crucial in cybersecurity-related studies, in which behavioral disclosures can be sensitive. The Items of the questionnaire of the collected dataset are presented in Appendix A.

3.5 Validity and Reliability

In order to make the questionnaire instrument valid, the content validation was conducted by subject matter experts in the field of cybersecurity, behavioral information systems, and research methodology. The instrument was reviewed by experts on their clarity, relevance, and correspondence to the constructs under measurement. Their feedback led to slight changes to question wording and structure to make them more interpretable and less ambiguous. Pilot testing was also conducted on the instrument among 20 respondents selected from the target population to establish any possible problems associated with the understanding of the items and the pattern of response. The responses of the pilot study were not incorporated into the final dataset, but were utilized to narrow down the instrument before implementation.

Internal consistency was used to evaluate the reliability of the instrument using Cronbach's Alpha coefficients. Cronbach's alpha is used to examine how much the items used to measure the same construct can give consistent answers. Any alpha values over 0.70 are normally deemed as satisfactory in exploratory research. The internal consistency items derived from the five independent variables and a dependent variable lie between a range of 0.800 and 0.877 in the five-item latent constructs, which are very strong; thus, they support a high score in reliability and show that the items had high cohesion in measuring the constructs they were intended to measure. The application of Cronbach's alpha was in line with the reliability assessment criteria in behavioral research on cybersecurity.

3.6 Measurement of Variables

The five-point Likert scales were used to operationalize all variables of the study to encompass the level of agreement with the statements regarding cybersecurity behaviors, perceptions, and vulnerabilities of the respondents. The Likert scale was on the basis of 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. Cyber security awareness, training frequency, user cyber-hygiene behavior, organizational culture, and risk perception were independent variables with five items used to measure each. Five items were also created to measure the dependent variable, which is the phishing vulnerability, to determine the susceptibility indicators, including the challenge to detect phishing scams, suspicious links, and perceived probability of becoming a victim. The Likert format was chosen because it is suitable for the measurement of latent constructs, and it is widely used in literature related to behavioral cybersecurity.

3.7 Data Analysis Techniques

The analysis of the data collected in the study used descriptive and inferential statistical methods. The summarisation of demographics and characterization of response patterns in the variables of study were summarized using descriptive statistics, including the mean, standard deviation, and frequency distributions. Inferential analysis was aimed at the investigation of the correlation between the independent variables and phishing vulnerability by means of Pearson correlation coefficient analysis. The entire analysis was performed with the help of the Statistical Package for the Social Sciences (SPSS), which offered standardized computational routines that are applicable to conduct quantitative behavioral research. The level of statistical

significance was taken to be $p < 0.05$, which is in line with general levels of statistical significance in social science research.

4 Results

4.1 Demographic Characteristics

Table 1 is the demographic distribution of the participants and offers the necessary background details regarding the nature of the sample and its applicability to the study of phishing vulnerability. Regarding age, most of the respondents were in the range of 25 to 29 years (50.5%), others in the range of 18 to 24 years (20.0%) and 30 to 34 years (19.5%), with the highest percentage in respondents aged 35 years and above (10.0%). This age group shows that the sample consisted mostly of young adults who are generally hyperactive and who use digital technologies at work, school, and while socialising. This age group is a very important group to conduct a study on phishing vulnerability since they are often exposed to online platforms and other digital communication tools. Nevertheless, younger users are more frequently assumed to be more digitally literate. However, previous research indicates that high levels of online activity can also put a person in the spotlight for phishing. Hence, age is also a significant contextual factor in exploring patterns of susceptibility.

Table 1: Participant's demographic distribution.

	N	%
AGE		
18 to 24 years	40	20.0%
25 to 29 years	101	50.5%
30 to 34 years	39	19.5%
35 years and above	20	10.0%
LEVEL OF EDUCATION		
High School	42	21.0%
Diploma	104	52.0%
Bachelor's Degree	34	17.0%
Others	20	10.0%
YEARS OF EXPERIENCE IN COMPUTER USAGE		
Less than 1 year	40	20.0%
1–3 Years	97	48.5%
4–6 years	43	21.5%
More than 6 years	20	10.0%
GENDER		
Male	74	37.0%
Female	126	63.0%

As far as educational background is concerned, the majority of respondents had a diploma (52.0%), followed by high school education (21.0%) and bachelor's degrees (17.0%). A lower percentage (10.0%) gave other types of education. This distribution indicates a sample of moderate education level with different levels of formal exposure to cybersecurity. Individuals who have a diploma and a high school education might have

received little formal training on cybersecurity, which may affect their awareness and behavioral response towards phishing attacks. The fact that respondents with higher education were a smaller proportion but still present in the sample increases the applicability of the results to the sample and, by implication, to other levels of education.

The outcome also indicates that one out of five respondents (48.5) had one to three years' experience of using the computer, with the other 21.5 having four to six years of computer usage experience. Those with less than one year of experience and over six years of experience, respectively, constituted 20.0% and 10.0% of the participants. This implies that the majority of the respondents could have moderate experience with computers, and this is pertinent since limited or moderate experience could be linked to a certain degree of confidence and vulnerability when engaging with digital data. Lastly, the gender distribution shows that the female participants are more (63.0) than the males (37.0). This disparity can be seen in a higher number of survey respondents being female, and it offers a chance to investigate the phishing vulnerability between the sexes, which will enable wider inclusivity in the field of cybersecurity studies. The pie charts and graphs support the distribution of demographic factors in Figs. 2–5.

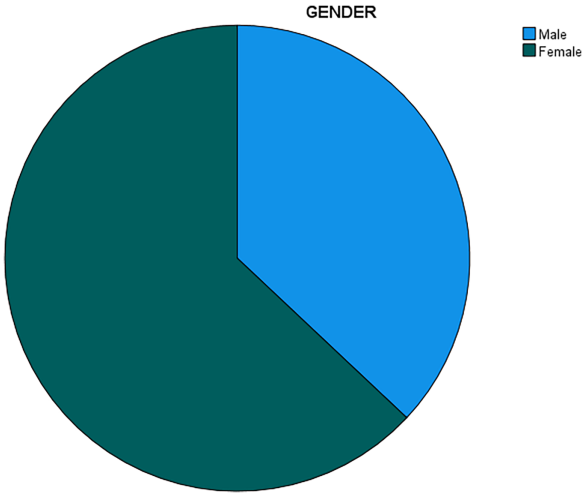

Figure 2: Participant's gender distribution.

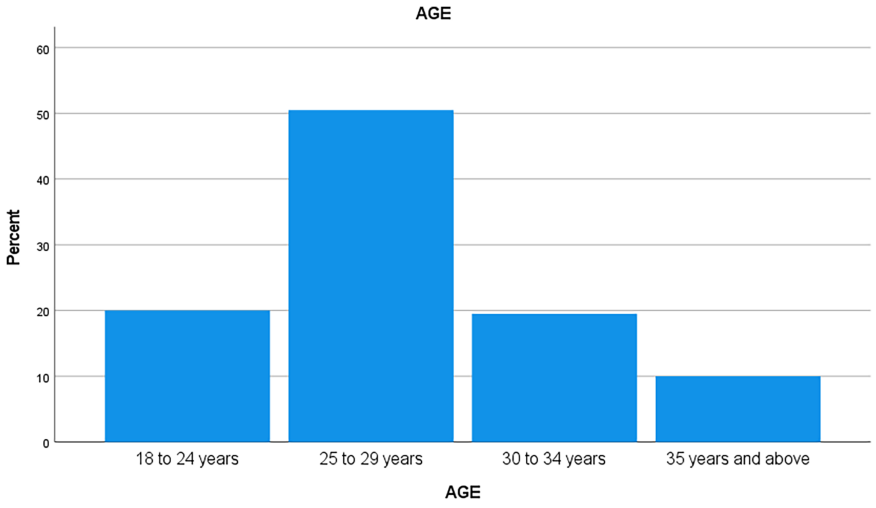

Figure 3: Participant's age distribution.

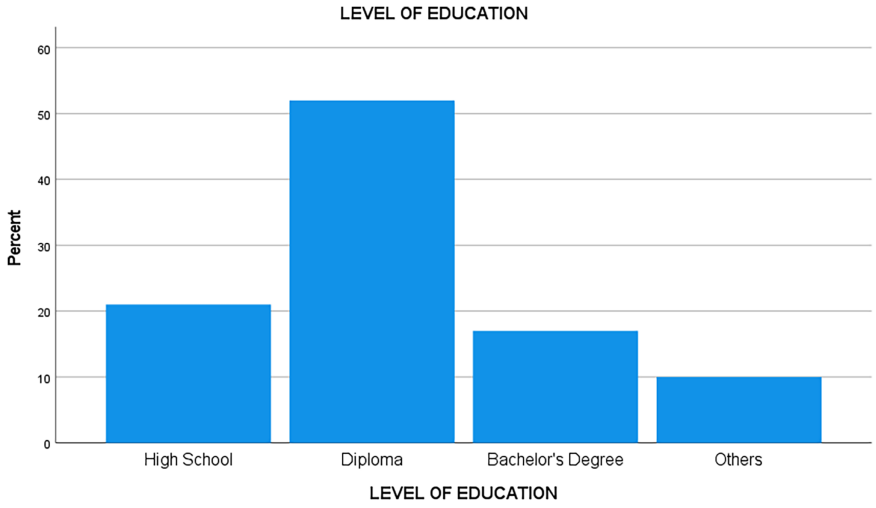

Figure 4: Participant's distribution on level of education.

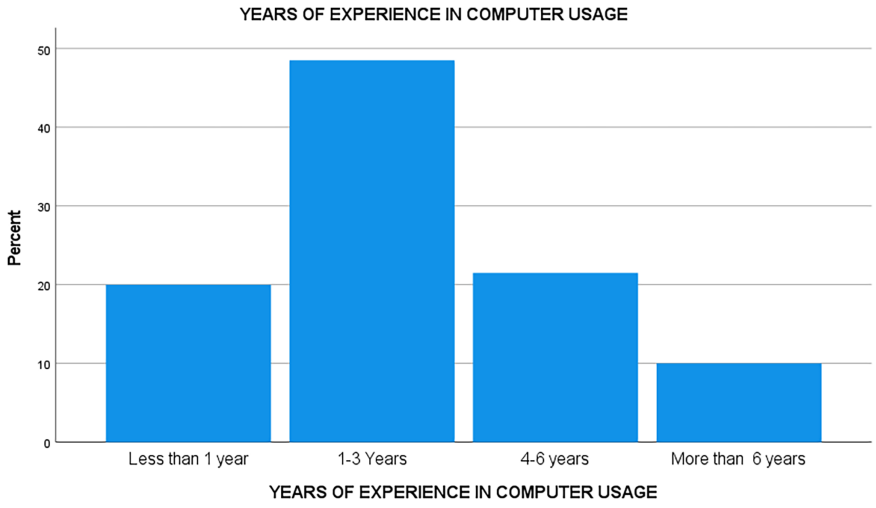

Figure 5: Participants' distribution on computer usage.

4.2 Descriptive Statistics

The descriptive statistics used in Table 2 give a good idea of the perception of respondents, their behaviors, and their experience concerning cyber security awareness, training, cyber-hygiene, organizational culture, perception of risk, and vulnerability to phishing. The general response rates for the majority of items were 3.59 to 3.85 on a five-point Likert scale, which was moderately high and moderately high agreement among respondents. In the case of cyber security awareness items (B1.1–B1.5), mean values greater than 3.69 indicate that most respondents tend to have a fair degree of awareness about phishing threats and meanings, as well as ways of confirming the authenticity of email or websites. The standard deviations are relatively moderate, which implies that there is some variability in the levels of awareness, as there is a difference in the level of exposure, education, and experience of individuals.

Table 2: Descriptive statistics (own work).

Item	N	Mean	Std. Deviation	Skewness	SE	Kurtosis	SE
B1.1 I have heard about common cybersecurity threats, such as phishing.	200	3.7150	0.73926	−0.545	0.172	1.484	0.342
B1.2 I can detect suspicious emails or links.	200	3.6900	0.75282	−0.418	0.172	1.171	0.342
B1.3 I am aware of the implications of cybersecurity attacks.	200	3.8450	0.80885	−0.112	0.172	−0.712	0.342
B1.4 I maintain awareness of cybersecurity matters.	200	3.7450	0.82668	0.075	0.172	−0.832	0.342
B1.5 I am aware of how to check the authenticity of websites or emails.	200	3.7150	0.73926	−0.545	0.172	1.484	0.342
C1.1 My company has frequent cybersecurity training programs.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
C1.2 The cybersecurity training that I get is current.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
C1.3 I attend cybersecurity awareness seminars or workshops.	200	3.5900	0.77128	−0.007	0.172	−0.383	0.342
C1.4 I have been educated about how to identify phishing attacks.	200	3.6050	0.80761	0.030	0.172	−0.519	0.342
C1.5 In my organization, cybersecurity training is not an option.	200	3.7250	0.61476	−0.119	0.172	−0.563	0.342
D1.1 I will not open links that have unrecognized authors.	200	3.6983	0.62571	−0.217	0.172	−0.496	0.342
D1.2 I use hard and memorable passwords for various accounts.	200	3.6900	0.75282	−0.418	0.172	1.171	0.342
D1.3 I allow two-factor authentication where it can be done.	200	3.7700	0.76158	0.001	0.172	−0.569	0.342
D1.4 I will update software and applications on my devices regularly.	200	3.7450	0.82668	0.075	0.172	−0.832	0.342
D1.5 I would submit suspicious emails to the concerned personnel or departments.	200	3.7150	0.73926	−0.545	0.172	1.484	0.342
E1.1 My organization promotes safe online behavior among its employees.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342

(Continued)

Table 2 (continued)

Item	N	Mean	Std. Deviation	Skewness	SE	Kurtosis	SE
E1.2 The management places cybersecurity as a priority in the organisational strategy.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
E1.3 Security policies are well stated in the organization.	200	3.5900	0.77128	−0.007	0.172	−0.383	0.342
E1.4 Workers will have a sense of support when reporting security issues or incidents.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
E1.5 The organization invests in cybersecurity enhancing tools.	200	3.5900	0.77128	−0.007	0.172	−0.383	0.342
F1.1 I am of the belief that phishing attacks are dangerous to people.	200	3.6050	0.80761	0.030	0.172	−0.519	0.342
F1.2 I believe that I can be a victim of phishing.	200	3.7250	0.61476	−0.119	0.172	−0.563	0.342
F1.3 I think phishing attacks may bring about the loss of a lot of money.	200	3.6983	0.62571	−0.217	0.172	−0.496	0.342
F1.4 I suppose that phishing activities are on the rise.	200	3.6900	0.75282	−0.418	0.172	1.171	0.342
F1.5 I think the results of falling into a phishing trap can be long-term.	200	3.7700	0.76158	0.001	0.172	−0.569	0.342
G1.1 I am occasionally confused about the authenticity of messages that come to me via email.	200	3.7450	0.82668	0.075	0.172	−0.832	0.342
G1.2 I have previously used suspicious links.	200	3.7150	0.73926	−0.545	0.172	1.484	0.342
G1.3 I struggle to differentiate between a genuine email and a phishing email.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
G1.4 I tend to believe phishing messages.	200	3.7000	0.83876	−0.315	0.172	0.102	0.342
G1.5 I reckon that I would accidentally fall into a trap of phishing.	200	3.6950	0.83994	−0.299	0.172	0.080	0.342

Mean scores for the frequency items (C1.1–C1.5) were also moderate, indicating that the respondents were aware of cyber security training as existing, but not always strong and inclusive. As participants tended to agree that training programs are indeed present and timely, the mean scores of attending seminars and

learning about phishing identification are slightly lower, indicating a lack of consistency in regular attendance and the level of training.

The behavioral aspect of cyber-hygiene (D1.1–D1.5) showed fair to good mean scores, especially for turning on two-factor authentication and avoiding unfamiliar links. These findings indicate that respondents engage in basic protective behaviors, though moderate deviations suggest they are not applied consistently. Organizational culture (E1.1–E1.5) items showed moderate views on institutional support, policy clearance, and investment in cyber security tools, which implies that, although organizations recognize the importance of cyber security, their actual implementation might not yet be complete and uniform.

The risk perception questions (F1.1–F1.5) revealed that the risk of phishing is generally perceived as harmful (financially) and is on the rise, meaning that there is an increased awareness of the danger. Vulnerability indicators (G1.1–G1.5), however, were also moderate in agreement and indicate that despite the awareness and the perceived risk, the respondents are still confused, uncertain, and sometimes exposed to suspicious material.

The normality assumption has been evaluated using skewness and kurtosis. The skewness values were between −0.545 and 0.075, whereas the kurtosis values were between −0.832 and 1.484. The values are within the acceptable limits of ±1 of skewness and ±2 of kurtosis, which state that there are no significant deviations from normality. Even though the majority of items had minor negative skewness, the deviations were not large. Thus, the data set is reasonably well-distributed and fits the parametric statistical tests.

Q-Q plot

The detrended normal Q-Q plot (Fig. 6) indicates that the measured values are randomly distributed around the zero reference line with no visible pattern and no extreme values. The dispersion of points only indicates insignificant deviations from normality. Hence, the normality assumption on the vulnerability to phishing attacks, which are self-reported, is assumed to be met.

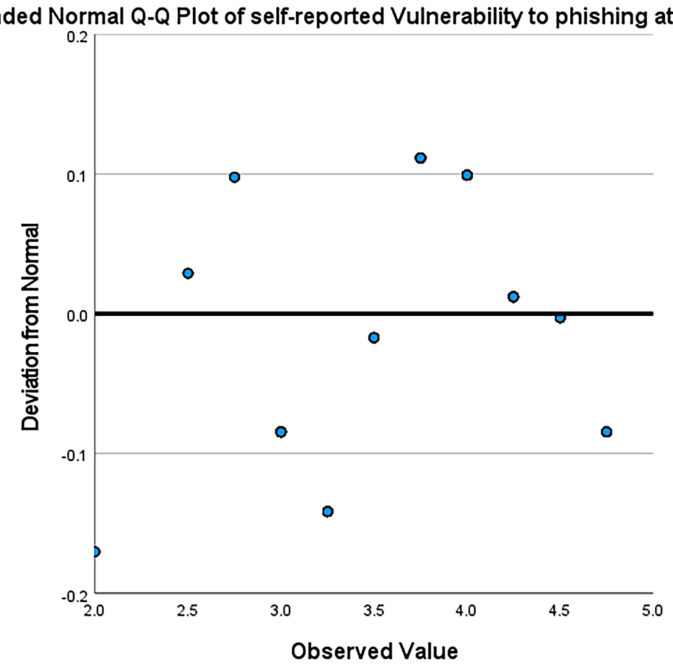

Figure 6: Q-Q plot of self-reported vulnerability to phishing attacks (IBM SPSS version 27).

4.3 Reliability Test

The reliability test findings in Table 3 demonstrate that the measurement instruments employed in this study have a high level of internal consistency and could be further used in the statistical analysis. The alpha coefficients of all constructs were a lot higher than the generally accepted alpha of 0.70, meaning that the items in each scale were a reliable measure of the various variables being measured. The most reliable coefficient was obtained for the cyber security awareness level (a = 0.877), indicating that there is a high level of consistency between the five items that measure the knowledge and awareness of cyber security and phishing-related threats among the respondents. This means that the awareness dimension was adequately measured using the items. The alpha of training frequency and user cyber-hygiene behavior was 0.825, which is a strong level of reliability and indicates that the items used to measure exposure to cybersecurity training and routine protective behavior are correlated with each other. Equally, organizational culture had a coefficient of reliability of 0.831, which implied that the items that measured institutional support, policy clarity, and commitment by management to cybersecurity were consistent. The Cronbach's alpha for risk perception was 0.800; this is acceptable, indicating consistency in the scale in measuring the perceived severity and vulnerability to phishing threats. Lastly, the dependent variable, which is vulnerability to phishing attacks, had a reliability coefficient of 0.832, which proved that the items employed to measure the susceptibility and confusion to phishing were reliable.

Table 3: Cronbach's reliability test.

Variable	Cronbach's Alpha	Number of Items
Cyber Security Awareness Level (IV1)	0.877	5
Training Frequency (IV2)	0.825	5
User Cyber-Hygiene Behavior (IV3)	0.825	5
Organizational Culture (IV4)	0.831	5
Risk Perception (IV5)	0.800	5
Vulnerability to Phishing Attacks (DV)	0.832	5

4.4 Normality Test

The histogram (Fig. 7) shows the probability of the respondents being victims of phishing attacks, and offers documentation through a visual evidence of normality assessment. Its distribution is bell-shaped, with most of the observations centered on the mean value of 3.71. This implies that, on average, respondents reported moderate vulnerability to phishing attacks. The overlaying normal curve is in the same line with the bars, implying that the observed data is, in essence, a good approximation of a normal distribution. Even though there is a slight deviation at the lower and upper ends of the scale, there are no extreme deviations or high skewness that would indicate a severe violation of normality. The standard deviation of 0.609 also indicates that the responses are not highly dispersed around the mean. Thus, most participants do not have their vulnerability levels too far from the central tendency. With a sample of 200 respondents, small departures from normality are statistically tolerable, as the central limit theorem supports the use of parametric tests.

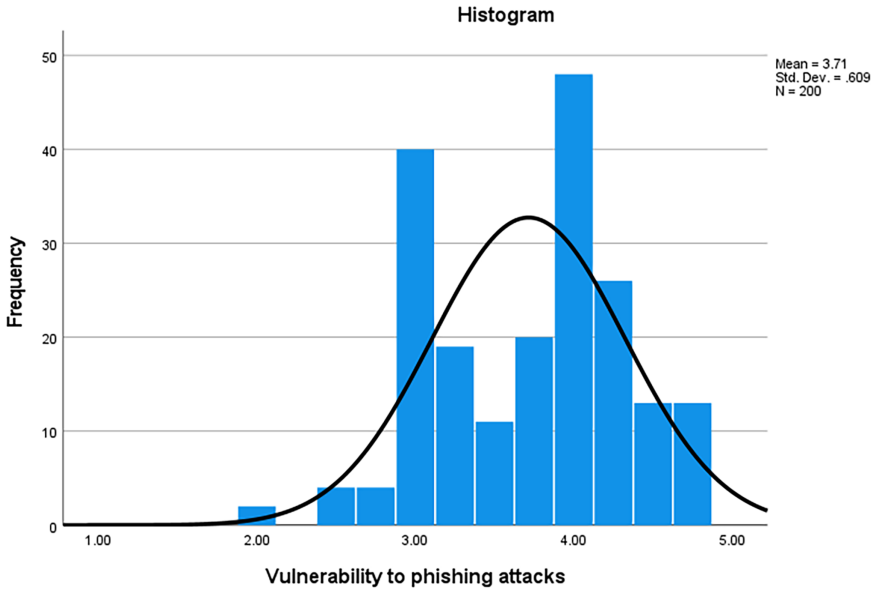

Figure 7: Normal distribution of phishing attacks (IBM SPSS version 27).

4.5 Inferential Statistics

Correlation Analysis

The Pearson correlation outcomes, illustrated in Table 4, prove that the awareness of cybersecurity is strongly, positively, and statistically significantly correlated with self-reported vulnerability to phishing ($r = 0.733$, $p < 0.01$). This means that the greater the level of awareness that respondents have of phishing threats, detection strategies, and implications of cybersecurity, the greater they report their vulnerability. Instead of indicating that awareness has a risk-enhancing effect, this relationship can indicate increased self-awareness of vulnerability. The better-informed people are regarding phishing tricks, the better they can judge how advanced and tricky such tricks can be, and thus admit that they can be exposed to them. Accordingly, vulnerability is influenced by awareness, including cognitive recognition and informed self-evaluation.

Table 4: Pearson correlation matrix for study variables.

Correlations							
		Cybersecurity Awareness Level	**Training Frequency**	**User Cyber-Hygiene Behavior**	**Organizational Culture**	**Risk Perception**	**Self-Reported Vulnerability to Phishing Attacks**
Cybersecurity awareness level	Pearson Correlation	1	0.523**	0.918**	0.373**	0.793**	0.733**
	Sig. (2-tailed)		0.000	0.000	0.000	0.000	0.000
	N	200	200	200	200	200	200
Training frequency	Pearson Correlation	0.523**	1	0.672**	0.942**	0.800**	0.893**
	Sig. (2-tailed)	0.000		0.000	0.000	0.000	0.000
	N	200	200	200	200	200	200

(Continued)

Table 4 (continued)

Correlations							
		Cybersecurity Awareness Level	**Training Frequency**	**User Cyber-Hygiene Behavior**	**Organizational Culture**	**Risk Perception**	**Self-Reported Vulnerability to Phishing Attacks**
User cyber-hygiene behavior	Pearson Correlation	0.918**	0.672**	1	0.520**	0.930**	0.855**
	Sig. (2-tailed)	0.000	0.000		0.000	0.000	0.000
	N	200	200	200	200	200	200
Organizational culture	Pearson Correlation	0.373**	0.942**	0.520**	1	0.607**	0.843**
	Sig. (2-tailed)	0.000	0.000	0.000		0.000	0.000
	N	200	200	200	200	200	200
Risk perception	Pearson Correlation	0.793**	0.800**	0.930**	0.607**	1	0.832**
	Sig. (2-tailed)	0.000	0.000	0.000	0.000		0.000
	N	200	200	200	200	200	200
Self-reported Vulnerability to phishing attacks	Pearson Correlation	0.733**	0.893**	0.855**	0.843**	0.832**	1
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	
	N	200	200	200	200	200	200

Note: **Correlation is statistically significant at the 0.01 level (2-tailed), $p < 0.01$.

One of the strongest relationships among the independent variables is observed between training frequency and self-reported phishing vulnerability (r = 0.893, $p < 0.01$), which is a very strong and positive relationship. This is an indication that people who are regularly engaged in cybersecurity training programs are prone to being vulnerable to phishing attacks. Regular training can bring more exposure to real-life phishing simulations and case studies, which will support the idea that phishing threats are not simple (and hard to remove completely). As a result, training can lead to more realistic judgments of personal susceptibility and not to the development of overconfidence. The strength of this relationship supports the key role of ongoing training in shaping the idea of vulnerability.

The cyber-hygiene behavior of the users is also positively related to phishing vulnerability (r = 0.855, $p < 0.01$). Those respondents who hold a regular practice of using protective measures are also the ones who report high levels of vulnerability, and they include virus avoidance of unknown links, two-factor authentication, updates in software, and reporting of suspicious emails. This connection implies that persons who take proactive measures can be motivated by the fact that they are vulnerable to phishing attacks. That is, protective measures might be based on risk awareness, not risk immunity. High association indicates that behavioral vigilance and perceived vulnerability are two things that co-exist within the environment of cybersecurity.

The organizational culture also shows a positive and significant correlation with phishing vulnerability (r = 0.843, $p < 0.01$). In companies where cybersecurity is a priority, policies are clear, management support is high, and online behavior is safe, the proportion of those who report being more aware of the risks of phishing is higher. An effective cybersecurity culture can lead to more talk on threats, more incidents reported, and more about risks discussed and disclosed, which, in turn, can elevate the level of confidence of people in themselves as exposed to risks. This result implies that phishing risks are perceived and interpreted in institutional settings.

Lastly, self-reported phishing vulnerability has a strong and positive correlation with risk perception (r = 0.832, $p < 0.01$). People whose opinion is that phishing attacks are hazardous, rising in number, harmful to the budget, and to their personal well-being will vote in favor of the possibility of falling prey to them. This connection can be theoretically consistent because first impressions of severity and vulnerability immediately affect the sense of vulnerability. Generally speaking, the Pearson correlation analysis indicates that self-reported phishing vulnerability is closely related to cognitive awareness, training, behavioral practices, organization, and perceived risk, which confirms that vulnerability to phishing is a multidimensional outcome of human and contextual factors. The hypothesis testing summary for H1 to H5 is presented in Table 5.

Table 5: Summary of hypothesis testing.

Hypothesis	Independent Variable	r	*p*-Value	Decision	Interpretation
H1	Cyber Security Awareness	0.733**	<0.01	Accepted	Significant positive relationship
H2	Training Frequency	0.893**	<0.01	Accepted	Significant positive relationship
H3	User Cyber-Hygiene Behavior	0.855**	<0.01	Accepted	Significant positive relationship
H4	Organizational Culture	0.843**	<0.01	Accepted	Significant positive relationship
H5	Risk Perception	0.832**	<0.01	Accepted	Significant positive relationship

Note: ** = statistically significant at the 0.01 level ($p < 0.01$).

5 Discussion

This paper discussed the connections among cybersecurity awareness, training frequency, cyber-hygiene behavior, organizational culture, perceptions of risk, and self-reported phishing vulnerability. Results from Pearson correlation reveal that all five independent variables have statistically significant correlations with phishing vulnerability and strengthening the argument that phishing is more of a human-centered cybersecurity issue, and not a solely technical vulnerability. These results are consistent with the general literature highlighting that attackers are progressively using cognitive biases, behavior patterns, and contextual trust rather than bugs in the system [1,3]. The findings thus substantiate the claim that phishing vulnerability is a product of the combination of knowledge, perception, behavior, and organizational environment.

The high correlation between cybersecurity awareness and phishing vulnerability indicates that the more a person matures in understanding phishing, the more they will admit to being vulnerable. However, the conventional wisdom is that the greater the awareness, the lesser the vulnerability; it is evident that greater awareness can lead to a better perception of exposure in this case. This interpretation is in line with research showing that awareness enhances users' ability to detect deceptive messages and interpret the consequences of cyber-attacks [2,15]. Moreover, it has been demonstrated that awareness influences threat appraisal procedures and impacts the way users interpret suspicious communication over the Internet [7]. Consistent with the Technology Threat Avoidance Theory (TTAT), better awareness will enhance the perceived severity and vulnerability, which can provide an individual with a greater awareness of risk instead of eradicating it.

Phishing vulnerability was also strongly related to training frequency. Those who received frequent cybersecurity training were more likely to report being aware of their vulnerability. This result confirms the previous studies, which have already shown that formatted and ongoing training can increase user awareness about phishing tactics and elevate threat detection skills [11,13]. It has also been found that phishing simulations and adaptive training programs enhance experiential learning and decrease complacency [12]. Instead of making users less safe, the common training can help decrease overconfidence by showing users the ever-changing complexity of phishing campaigns. Organizational experiments also have demonstrated

that trained employees are much more skeptical and mechanisms of response are better developed when suspicious communications are received [19]. Therefore, training increases realistic self-evaluation of vulnerable conditions and reinforces coping skills.

Phishing vulnerability was also found to have a significant relationship with the user's cyber-hygiene behavior. Persons who had habitually engaged in protective activities like checking links, using multi-factor authentication, and software updating were found to report vulnerability more. This trend is consistent with the findings of studies that suggest that protective behaviors are usually the result of an increased attentional devotion to digital threats [4]. Cognitive overload, emotional manipulation, or contextual pressure might make even educated users vulnerable [28]. Consequently, the behavior of security is not always evidence of immunity, but rather a continued vigilance in response to identified risk. Empirical data have demonstrated that active reporting of suspicious messages along with strong user authentication practices by users will lead to greater organizational resilience [13]. The presence of behavioral discipline and perceived vulnerability confirms the assumption that phishing vulnerability is dynamic and constantly negotiated through users' actions.

Phishing vulnerability was also found to have a strong association with organizational culture, highlighting the significance of the institutional context. It has been proven that positive cultures of cybersecurity, defined by well-articulated policies, dedication by leaders, and unrestricted reporting mechanisms, increase awareness of the risks among the community [17]. Employees would internalize the risk and admit the exposure when cybersecurity is part of organizational strategy and communication. On the other hand, poor cultural environments can lead to complacency and underreporting [18]. The results in this case indicate that powerful cybersecurity cultures can increase perceived vulnerability by promoting transparency and discussing threats. This explanation is justified by the literature, which shows that organizational investment in policy reinforcement and communication is a strong force in enhancing user participation in security responsibilities [16]. Thus, the institutional climate is very important in the way phishing risks are viewed and understood.

Lastly, phishing vulnerability was strongly associated with risk perception. Those with the cognition of phishing as serious, economically harmful, and more common were more apt to report vulnerability. The finding is conceptually compatible with TTAT, which emphasizes perceived severity and susceptibility as the primary elements of threat appraisal [14]. Previous research has verified that increased perceived risk is an incentive to protective behavior and a determinant in decision making concerning digital settings [20]. Simultaneously, it has been demonstrated that the perceived risk is low, thereby contributing to complacency and increased exposure to phishing manipulation [4]. The current results support the notion that a valid and internalized perception of risk enhances vigilance without a total concentration on risk vulnerability, considering the increasing level of sophistication in phishing methods.

In general, the discussion demonstrates the multidimensional nature of phishing vulnerability, which is influenced by awareness, training, behavior, organizational culture, and perceived risk. In line with previous works, the results indicate that prevention of phishing would not be achieved through a single technical control, but would be a human-centered approach. Both the threat appraisal and coping mechanisms should be strengthened in response to the contemporary risks posed by phishing.

6 Conclusions

6.1 Summary of Findings

The paper examined the correlation between cybersecurity awareness, training frequency, user cyber-hygiene behavior, organizational culture, risk perception, and self-reported phishing vulnerability. The

results showed a significant relationship between phishing vulnerability and all five independent variables. The relationship between vulnerability and cybersecurity awareness was positive, suggesting that the more people know about phishing threats, the higher the chances that they will be able to realize and admit that they are vulnerable. The extent of training was also found to be strongly related; that is, constant exposure to cybersecurity training enhances users` knowledge of phishing dangers and improves realistic self-evaluation among users.

Cyber-hygiene behavior among users was also associated with vulnerability, indicating that people who are proactive in taking protective actions do so when they perceive themselves to be at threat. Culture within the organization was also a significant factor, since the environments that supported cybersecurity and emphasized it were associated with a higher perceived phishing threat. Lastly, vulnerability was also largely affected by risk perception in that people who viewed phishing as dangerous and close to them were more likely to declare vulnerability. In general, the results validate the idea that vulnerability to phishing is preconditioned by the combined cognitive, behavioral, and organizational factors.

6.2 Practical Implications

The results of this research have significant practical implications for organizations seeking to minimize their vulnerability to phishing. Since awareness, training, cyber-hygiene behavior, organizational culture, and risk perception are closely linked to vulnerability, the interventions should be designed and combined in a behaviour-oriented manner rather than being dependent on technical protection. The implications could be addressed across three main domains, including organizational policies, training design, and behavioral nudges.

6.2.1 Organizational Policies

Those organizations need to make cybersecurity a formal strategy, not just a technical or IT operation. The cybersecurity policy should also be clear, accessible, and regularly updated to provide a sense of direction for the behavior of the employees. Policies should define acceptable digital practices, reporting procedures, and accountability mechanisms. Notably, the leadership should be seen to support cybersecurity efforts to underscore their significance.

An organizational culture of non-punitive reporting is also important. The employees must be psychologically safe enough to report suspicious emails or near-miss cases without fearing being blamed. The communication of phishing cases clearly will raise the awareness of the group and strengthen the vigilance. Also, organizations are advised to incorporate cybersecurity goals in performance appraisals as well as in operational systems to guarantee long-term commitment.

6.2.2 Training Design

The close correlation between training frequency and vulnerability recognition indicates that training ought to be incessant, adaptive, and experiential. Awareness programs cannot be done once. In their place, organizations ought to introduce regular phishing drills, simulation-based learning, and interactive workshops that mirror emerging attack trends.

The training content must progress beyond technical explanations and encompass psychological concepts of phishing, such as the manipulation of urgency, the use of authority, and the manipulation of emotions. This aids users in knowing the reason why they can be weak even though informed. Engagement

and retention can be ensured through microlearning modules and brief refresher courses. Moreover, post-phishing simulation feedback must be positive and informative rather than disciplinary and aimed at the learning curve.

6.2.3 Behavioral Nudges

Protective behaviors and perceived vulnerability are present simultaneously, and this means that small-scale behavioral interventions could reinforce daily cybersecurity behavior. Behavioral nudges include warning messages shown upon clicking on external links, a reminder banner on phishing, or frequent security information integrated with communication tools.

Default security options should be streamlined, such as automatically enabling multi-factor authentication and requiring stronger passwords. Graphical messages, such as marking extra external email addresses or warning that an attachment is suspicious, can help users take a moment and re-evaluate. Timely reminders can further improve vigilance during high-risk times (e.g., tax season or organizational changes).

All in all, the results indicate that phishing prevention should be a holistic process that incorporates established policy enforcement schemes, well-designed training programs, and strategically positioned behavioural cues. Organizations can develop sustainable resilience against phishing attacks by focusing on cognitive awareness and environmental reinforcement at the same time as routine behavior.

6.3 Theoretical Contribution

This research paper is relevant to the cybersecurity literature as it empirically confirms the relevance of the Technology Threat Avoidance Theory (TTAT) in the case of phishing vulnerability. The study integrates awareness, training frequency, cyber-hygiene behavior, organizational culture, and risk perception into a single model, thereby generalizing TTAT to both behavioral and organizational aspects. The results illustrate the combination of threat appraisal and coping appraisal processes that lead to a vulnerability outcome. Further, the research fills a gap in the existing literature by taking a holistic human-centered approach rather than analyzing individual predictors, thus providing a better understanding of phishing vulnerability.

6.4 Limitations

Although this study has made contributions, it is limited in several ways. To begin with, the cross-sectional survey design does not allow for a causal conclusion between the variables. Second, the study is based on self-reported information, which can impact the bias of respondents since respondents can overrate their behaviors towards awareness or security. Third, the statistical analysis was based on a large sample size, but the study did not consider sector or cultural variations that can affect phishing vulnerability. Finally, the research focused on general phishing contexts. It was not oriented on isolating the various types of phishing, such as spear phishing or smishing, that might be equipped with different degrees of sophistication.

6.5 Future Research Recommendations

Future research should adopt a longitudinal design to identify more precise causal relationships between cybersecurity awareness, frequency of training, user cyber-hygiene behavior, organizational culture, risk perception, and phishing vulnerability. Although the current study revealed strong correlations among these variables, the cross-sectional research design does not allow for determining directionality. The question of whether awareness and training can result in a change in vulnerability over time, or whether the already vulnerable people are more inclined to pursue knowledge and protection-related actions, has yet to be answered.

The longitudinal design would help the researchers monitor participants over a series of time periods, enabling them to observe how the evolution of awareness, training exposure, or organizational culture affects the trajectory of vulnerability. For example, pre- and post-training intervention measures of phishing susceptibility would be more convincing evidence of causal implications. Similarly, recurrent measurements would establish whether any improvement in cyber-hygiene behavior would lead to a long-lasting decrease in real phishing cases or simply changes in perceived susceptibility.

Longitudinal studies would also be useful for determining the delayed effects and the pattern of behavioral adaptation. Phishing techniques evolve quickly, and users' reactions can change as new threats emerge. The ability to monitor these dynamics with time would be more insightful into the interactions between cognitive and behavioral factors and changes in threat environments. In general, longitudinal designs would increase the strength of theoretical validation, practical recommendations, and provide more solid evidence in building effective phishing prevention strategies.

Acknowledgement: Not applicable.

Funding Statement: The author received no specific funding for this study.

Data and Materials Availability: The SPSS dataset and analysis output supporting the findings of this study are provided as a research data file (PhishingAwareness_ResearchData.zip) uploaded with this submission.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A

Questionnaire

SECTION A: Demographic Information

(Please tick or fill where applicable)

A1. Age:

□ 18–24 □ 25–34 □ 35–44 □ 45–54 □ 55+

A2. Gender:

□ Male □ Female □ Prefer not to say

A3. Education Level:

□ High School

□ Diploma/Certificate

□ Bachelor's Degree

□ Other: _____

A4. Years of Experience with Computer Use:

□ Less than 1 year □ 1–3 years □ 4–6 years □ 7–10 years □ 10+ years

SECTION B: Cyber Security Awareness Level (IV1)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
B1.1	I have heard about such common cyber security threats as phishing.	□	□	□	□	□
B1.2	I am able to detect suspicious emails or links.	□	□	□	□	□
B1.3	I am aware of the implications of cyber security attacks.	□	□	□	□	□
B1.4	I maintain awareness of cyber security matters.	□	□	□	□	□
B1.5	I am aware of how to check the authenticity of websites or emails.	□	□	□	□	□

SECTION C: Training Frequency (IV2)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
C1.1	My company has frequent cyber security training programs.	□	□	□	□	□
C1.2	The cyber security training that I get is current.	□	□	□	□	□
C1.3	I attend cyber security awareness seminars or workshops.	□	□	□	□	□
C1.4	I have been educated about how to identify phishing attacks.	□	□	□	□	□
C1.5	In my organization, cyber security training is not an option.	□	□	□	□	□

SECTION D: User Cyber-Hygiene Behavior (IV3)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
D1.1	I will not open links that have unrecognized authors.	□	□	□	□	□
D1.2	I use hard and memorable passwords to various accounts.	□	□	□	□	□
D1.3	I allow two-factor authentication where it can be done.	□	□	□	□	□
D1.4	I will update software and applications on my devices on a regular basis.	□	□	□	□	□
D1.5	I would submit suspicious emails to the concerned personnel or departments.	□	□	□	□	□

SECTION E: Organizational Culture (IV4)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
E1.1	My organization promotes safe online behavior among its employees.	□	□	□	□	□
E1.2	The management places cyber security as a priority in the organizational strategy.	□	□	□	□	□
E1.3	Security policies are well stated in the organization.	□	□	□	□	□
E1.4	Workers will have a sense of support when reporting security issues or incidences.	□	□	□	□	□
E1.5	The organization invests in cyber security enhancing tools.	□	□	□	□	□

SECTION F: Risk Perception (IV5)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
F1.1	I am of the belief that phishing attacks are dangerous to people.	□	□	□	□	□
F1.2	I believe that I can be a victim of phishing.	□	□	□	□	□
F1.3	I think phishing attacks may bring about the loss of a lot of money.	□	□	□	□	□
F1.4	I suppose that phishing activities are on the rise.	□	□	□	□	□
F1.5	I think the results of falling into a phishing trap can be long-term.	□	□	□	□	□

SECTION G: Vulnerability to Phishing Attacks (DV)

Statement Code	Statement	1 = Strongly Disagree	2 = Disagree	3 = Neutral	4 = Agree	5 = Strongly Agree
G1.1	I am occasionally confused about the authenticity of messages that come to me via email.	□	□	□	□	□
G1.2	I have previously used suspicious links.	□	□	□	□	□
G1.3	I struggle to differentiate between genuine email and phishing email.	□	□	□	□	□
G1.4	I tend to believe phishing messages.	□	□	□	□	□
G1.5	I reckon that I would accidentally fall into a trap of phishing.	□	□	□	□	□

References

1. Putra FPE, Ubaidi U, Zulfikri A, Arifin G, Ilhamsyah RM. Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance. 2024;4(1):413–21. doi:10.47709/brilliance.v4i1.4357.
2. Alqahtani MA. Factors affecting cybersecurity awareness among university students. Appl Sci. 2022;12(5):2589. doi:10.3390/app12052589.
3. Kheruddin MS, Zuber MAEM, Radzai MMM. Phishing attacks: unraveling tactics, threats, and defenses in the cybersecurity landscape. 2024 [cited 2026 Mar 15]. Available from: https://www.researchgate.net/publication/377434394_Phishing_Attacks_Unraveling_Tactics_Threats_and_Defenses_in_the_Cybersecurity_Landscape.

4. Waqas M, Hania A, Yahya F, Malik I. Enhancing cybersecurity: the crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. Sage Open. 2023;13(4):21582440231217720. doi:10.1177/21582440231217720.
5. Safitra MF, Lubis M, Fakhrurroja H. Counterattacking cyber threats: a framework for the future of cybersecurity. Sustainability. 2023;15(18):13369. doi:10.3390/su151813369.
6. Kuraku S, Kalla D, Smith N, Samaah F. Exploring how user behavior shapes cybersecurity awareness in the face of phishing attacks. Int J Comput Trends Technol. 2023;71:74–9.
7. Savaş S, Karataş S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. Int Cybersecur Law Rev. 2022;3(1):7–34. doi:10.1365/s43439-021-00045-4.
8. Kuraku DS, Kalla D, Samaah F. Navigating the link between internet user attitudes and cybersecurity awareness in the era of phishing challenges. Int Adv Res J Sci Eng Technol. 2023;9(12):116–24. doi:10.17148/IARJSET.2022.91224.
9. Admass WS, Munaye YY, Diro AA. Cyber security: state of the art, challenges and future directions. Cyber Secur Appl. 2024;2(1):100031. doi:10.1016/j.csa.2023.100031.
10. Zhang J, Bu H, Wen H, Liu Y, Fei H, Xi R, et al. When LLMs meet cybersecurity: a systematic literature review. Cybersecurity. 2025;8(1):55. doi:10.1186/s42400-025-00361-w.
11. Iqbal F, Yusof ZB. Efficacy of cybersecurity awareness training in reducing phishing vulnerabilities in organizations. J Adv Cybersecur Sci Threat Intell Countermeas. 2024;8:10–21.
12. Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023;12(6):1333. doi:10.3390/electronics12061333.
13. Scherb C, Heitz LB, Grimberg F, Grieder H, Maurer M. A cyber attack simulation for teaching cybersecurity. In: Gerber A, Hinkelmann K, editors. Proceedings of Society 5.0 Conference 2023. Stockport, UK: EasyChair; 2023. Vol. 93, p. 129–40. doi:10.29007/dkdw.
14. Ansari MF, Sharma PK, Dash B. Prevention of phishing attacks using AI-based cybersecurity awareness training. Prevention. 2022;3(6):61–72. doi:10.47893/IJSSAN.2022.1221.
15. Alsharif M, Mishra S, AlShehri M. Impact of human vulnerabilities on cybersecurity. Comput Syst Sci Eng. 2022;40(3):1153–66. doi:10.32604/csse.2022.019938.
16. Abrahams TO, Farayola OA, Kaggwa S, Uwaoma PU, Hassan AO, Dawodu SO. Cybersecurity awareness and education programs: a review of employee engagement and accountability. Comput Sci IT Res J. 2024;5(1):100–19. doi:10.51594/csitrj.v5i1.708.
17. Jada I, Mayayise TO. The impact of artificial intelligence on organisational cyber security: an outcome of a systematic literature review. Data Inf Manag. 2024;8(2):100063. doi:10.1016/j.dim.2023.100063.
18. Pinto L. Assessing the relevance of cybersecurity training and policies to prevent and mitigate the impact of phishing attacks. J Internet Serv Inf Secur. 2022;12(4):23–38. doi:10.58346/JISIS.2022.I4.002.
19. Ayoola VB, James UU, Idoko IP, Ijiga OM, Olola TM. Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective. Global J Eng Technol Adv. 2024;20(3):094–117. doi:10.30574/gjeta.2024.20.3.0164.
20. Sai S, Yashvardhan U, Chamola V, Sikdar B. Generative AI for cyber security: analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space. IEEE Access. 2024;12(4):53497–516. doi:10.1109/ACCESS.2024.3385107.
21. Okokpujie K, Kennedy CG, Nnodu K, Noma-Osaghae E. Cybersecurity Awareness: investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a Nigerian leading university). Int J Sustain Dev Plan. 2023;18(1):255–63. doi:10.18280/ijsdp.180127.
22. De Azambuja AJG, Plesker C, Schützer K, Anderl R, Schleich B, Almeida VR. Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics. 2023;12(8):1920. doi:10.3390/electronics12081920.
23. Ghelani D. Cyber security, cyber threats, implications and future perspectives: a review. Authorea Prepr. 2022. doi:10.22541/au.166385207.73483369/v1.
24. Xu H, Wang S, Li N, Wang K, Zhao Y, Chen K, et al. Large language models for cyber security: a systematic literature review. ACM Trans Softw Eng Methodol. 2025;2025:3769676. doi:10.1145/3769676.

25. Safaei Pour M, Nader C, Friday K, Bou-Harb E. A comprehensive survey of recent internet measurement techniques for cyber security. Comput Secur. 2023;128(5):103123. doi:10.1016/j.cose.2023.103123.
26. Fernandez De Arroyabe I, Arranz CFA, Arroyabe MF, Fernandez De Arroyabe JC. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019. Comput Secur. 2023;124(2):102954. doi:10.1016/j.cose.2022.102954.
27. Abdullayeva F. Cyber resilience and cyber security issues of intelligent cloud computing systems. Results Control Optim. 2023;12(1):100268. doi:10.1016/j.rico.2023.100268.
28. Rademaker M. Assessing cyber security 2015. Inf Secur. 2016;34(2):93–104. doi:10.11610/isij.3407.
29. Yamin MM, Katt B. Modeling and executing cyber security exercise scenarios in cyber ranges. Comput Secur. 2022;116(1):102635. doi:10.1016/j.cose.2022.102635.
30. Lee YY, Gan CL, Liew TW. Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. Int J Environ Res Public Health. 2023;20(4):3514. doi:10.3390/ijerph20043514.
31. Petcu I, Barbu D-C. The new challenges of Romania's cyber security policy. Rom Cyber Secur J. 2022;4(1):57–67. doi:10.54851/v4i1y202207.
32. Albladi SM, Weir GRS. User characteristics that influence judgment of social engineering attacks in social networks. Hum Cent Comput Inf Sci. 2018;8(1):5. doi:10.1186/s13673-018-0128-7.
33. Chirra DR. AI-enabled cybersecurity solutions for protecting smart cities against emerging threats. 2025 [cited 2026 Mar 15]. Available from: https://www.academia.edu/125039298/AI_Enabled_Cybersecurity_Solutions_for_Protecting_Smart_Cities_Against_Emerging_Threats.
34. Ismail M, Madathil NT, Alalawi M, Alrabaee S, Al Bataineh M, Melhem S, et al. Cybersecurity activities for education and curriculum design: a survey. Comput Hum Behav Rep. 2024;16(1):100501. doi:10.1016/j.chbr.2024.100501.
35. Hamlet C, Straub J, Russell M, Kerlin S. An incremental and approximate local outlier probability algorithm for intrusion detection and its evaluation. J Cyber Secur Technol. 2017;1(2):75–87. doi:10.1080/23742917.2016.1226651.
36. DCMS: cyber security breaches survey 2019. Netw Secur. 2019;2019(4):4. doi:10.1016/S1353-4858(19)30044-3.
37. Horowitz BM, Lucero DS. System-aware cyber security: a systems engineering approach for enhancing cyber security. Insight. 2017;20(3):66–8. doi:10.1002/inst.12165.
38. Mohammed A. Protecting space assets: cybersecurity challenges and solutions for the final frontier. Balt J Eng Technol. 2023;2(1):55–61.
39. Wazid M, Das AK, Chamola V, Park Y. Uniting cyber security and machine learning: advantages, challenges and future research. ICT Express. 2022;8(3):313–21. doi:10.1016/j.icte.2022.04.007.