







Evaluating Students' Vulnerability and Awareness to Phishing Attacks in Educational Institutions

Kennedy Okokpujie^{1,2*}, Michael Ayomide Ariyo¹, Funmilayo S. Moninuola¹, Matthew Boladele Akanle^{1,2},
Imhade P. Okokpujie^{3,4}

¹ Department of Electrical and Information Engineering, Covenant University, Ota 112101, Nigeria

² Africa Centre of Excellence for Innovative & Transformative STEM Education, Lagos State University, Ojo 102101, Nigeria

³ Department of Mechanical and Mechatronics Engineering, Afe Babalola University, Ado Ekiti 360001, Nigeria

⁴ Department of Mechanical and Industrial Engineering Technology, University of Johannesburg, Johannesburg 2028, South Africa

Corresponding Author Email: kennedy.okokpujie@covenantuniversity.edu.ng

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijss.150320>

ABSTRACT

Received: 1 June 2024

Revised: 15 September 2024

Accepted: 12 October 2024

Available online: 31 March 2025

Keywords:

phishing, email phishing, cybersecurity, identity theft, education institutions, cyber-attack, research security awareness, information security

The rapid growth of the internet has made students increasingly susceptible to phishing attacks, posing risks such as identity theft, financial fraud, and other cybercrimes. Reports indicate that these phishing attacks increasingly target universities and students in higher education institutions (a case study of final engineering students). The objective of this study is to assess the susceptibility and knowledge of students towards phishing attacks through the configuration and analysis of a phishing framework. The methodology encompassed the establishment of a phishing campaign specifically designed to target the academic setting of the students, followed by an assessment of their reactions to the phishing emails. An online survey was conducted to assess students' cyber security comprehension level and their responses to phishing emails. The findings of this study indicate that a significant proportion of students' exhibit susceptibility to phishing attacks and demonstrate a lack of awareness regarding the nature of phishing emails. In conclusion the study enhanced students' awareness of cyber security concerns and equip them with the necessary knowledge to safeguard themselves against phishing attacks in both educational settings and real-world scenarios.

1. INTRODUCTION

In recent times, the escalating dependence on technology and the extensive integration of digital tools within educational establishments have rendered them susceptible to cyberattacks, thereby making them alluring targets. Due to their comprehensive repositories of sensitive information such as student records, research data, financial details, and intellectual property, educational institutions have emerged as prominent targets for cybercriminals who aim to exploit vulnerabilities for monetary gain or disrupt operational activities. The increasing significance of cybersecurity in educational institutions can be ascribed to various pivotal factors.

Educational institutions are responsible for managing diverse sensitive information, including personally identifiable information of students, faculty members, and administrative personnel [1]. Ensuring the security of this data against unauthorised access, data breaches, and identity theft is of utmost importance to uphold trust and adhere to data protection regulations [2].

Universities engage in advanced research endeavours, foster the creation of groundbreaking technologies, and yield significant intellectual assets. Cyberattacks targeting the theft

of research data or intellectual property can result in significant repercussions, compromising the competitive edge and reputations of the affected institutions.

The emergence of e-learning and remote education has significantly broadened the scope of vulnerability for cybercriminals. In light of the growing dependence on online platforms, virtual classrooms, and cloud-based services, it has become imperative for educational institutions to fortify their digital infrastructure in order to safeguard against various forms of cyber threats, including ransomware, phishing, and denial-of-service attacks.

Cyberattacks have the potential to cause significant disruption in the financial and operational aspects of educational institutions, resulting in monetary setbacks and harm to their reputation. An illustration of the impact of ransomware attacks is the potential for rendering critical systems inoperable, resulting in substantial periods of unavailability and impeding the institution's capacity to provide educational services effectively.

Integrating internet-connected devices and smart technologies in educational environments poses security risks that may compromise the safety of students and staff. Implementing cybersecurity measures is imperative to protect students, staff, and physical infrastructure from the risks posed

by cyber threats and potential attacks that specifically target Internet of Things (IoT) devices [3].

Evaluating the vulnerability and level of awareness among students regarding phishing attacks is of utmost importance for educational institutions and the broader cybersecurity landscape. There are several significant reasons why this assessment holds excellent importance.

Identifying weak points in security awareness is crucial in addressing the ongoing threat of phishing attacks, which are prominent methods cybercriminals employ to gain unauthorised access to networks. By evaluating students' susceptibility to phishing attempts, institutions can identify areas of weakness within their security awareness programmes. This capability allows organisations to customise training and educational programmes to target specific areas of vulnerability, thereby improving the overall cybersecurity stance.

The enhancement of cybersecurity education can be achieved by implementing phishing assessments. These assessments offer a valuable opportunity to educate students about the most recent phishing techniques and tactics employed by cyber attackers. Using simulated phishing attempts, students can acquire a direct experiential understanding of the threats they may encounter in real-world scenarios. This results in heightened awareness and improved decision-making abilities when faced with real phishing emails.

The promotion of a security-conscious culture within the educational institution can be achieved through the implementation of phishing simulations and awareness campaigns. These initiatives aim to enhance the institution's members' overall understanding and vigilance towards security measures. Students and faculty should enhance their vigilance in identifying potential cyber threats, promptly reporting suspicious activities, and actively engaging in initiatives to safeguard sensitive data and resources.

In the context of mitigating cyber risks and data breaches, it is common for students to be entrusted with handling sensitive data, including personal information and research data. The occurrence of a successful phishing attack on a student's account has the potential to result in data breaches, thereby exposing sensitive information. The assessment of students' susceptibility to phishing aids in the mitigation of these risks, thereby decreasing the probability of data breaches and the resulting legal and reputational ramifications.

In order to adequately equip students for real-world situations, it is crucial to address the prevalence of phishing attacks beyond educational institutions. By exposing students to simulated phishing attempts within an educational setting, they acquire crucial abilities to identify and effectively handle phishing attempts they may encounter in their future professional endeavours or personal circumstances.

Assessing the susceptibility and knowledge of students towards phishing attacks is a proactive and crucial measure in cultivating a cybersecurity-conscious environment within educational institutions [4]. This process aids in the identification of areas that require improvement, enhances security measures, and provides students and faculty with the necessary knowledge and skills to safeguard themselves and the institution against cyber threats.

In the past few years, there has been a notable increase in cyberattacks aimed explicitly at educational institutions. These attacks involve hackers using advanced methods to

breach security systems and obtain unauthorised access to valuable and confidential information. These cyberattacks not only present a substantial risk to the confidentiality and integrity of students and faculty members but can also cause significant disruption to the entire educational infrastructure. Moreover, the heightened dependence on online learning platforms and digital tools amidst the COVID-19 pandemic has exacerbated the susceptibility of educational institutions, underscoring the pressing requirement for resilient cybersecurity protocols to protect against cyber risks.

2. LITERATURE REVIEW

This session consists of the types and related works of phishing attacks.

2.1 Types of phishing attacks

i. Email Phishing

The umbrella term used to describe any malicious email communication intended to coerce recipients into disclosing personal information. Account credentials, personally identifiable information (PII), and business trade secrets are the usual targets of attacks. Attackers may, however, be acting for other reasons when they target a particular company [5].

ii. Spear Phishing

In order to deceive them into disclosing critical information, giving the attacker money, or installing malware, these email messages are typically addressed to high-privilege account holders within an organization [6].

iii. Link Manipulation

Messages include a link to a malicious website that impersonates the legitimate company but really directs recipients to a server under the control of the attacker. There, users are tricked into authenticating through a fake login page, which then delivers their credentials to the attacker.

iv. Whaling (CEO Fraud)

These messages are frequently addressed to prominent workers of a firm in an effort to deceive them into thinking the CEO or another executive has authorized a money transfer. CEO fraud falls under the phishing category, except instead of a hacker impersonating a well-known website, they impersonate the CEO of the organization being attacked.

v. Malware

Users who have been duped into opening a file or clicking on a link might have malware installed on their devices. Common malware attachments that steal data and demand money from intended victims include ransomware, rootkits, and keyloggers.

vi. Smishing

Attackers use SMS messages to deceive consumers into visiting malicious websites on their cellphones. Attackers send a selected victim a text message that contains a malicious link that offers discounts, incentives, or free gifts.

vii. Vishing

Attackers can trick victims into calling a phone number where they can be defrauded by using voice-changing software to leave a message for them. Voice changers can also be used to modify an attacker's accent or gender when interacting with a target in order to make them appear to be a fake.

viii. “Evil Twin” Wi-Fi

Attackers deceive users into connecting to a malicious hotspot by faking free Wi-Fi in order to carry out man-in-the-middle vulnerabilities.

ix. Pharming

Pharming is a two-stage assault that is used to obtain login information. In the first stage, a victim is selected, malware is installed on them, and they are then forcibly taken to a browser and a fake website where they are duped into providing login information. Users are also redirected to fake domains via DNS poisoning.

x. Angler Phishing

Attackers utilize social media to respond to postings while posing as representatives of legitimate companies to deceive users into disclosing login information and personal data.

xi. Watering Hole

An attacker chooses a website that is often visited by their target audience, finds a weakness on the website, and utilizes it to deceive visitors into downloading malware since a hacked site offers countless possibilities. An attacker can drive users to fake websites or send a payload to the local network to steal data by installing malware on the targeted user workstations.

2.2 Review of related works

Chandarman and Van Niekerk [7] used an adapted version of the theory of planned behavior (TPB) framework to assess the levels of Cyber security awareness among students at a private tertiary education institution in South Africa. This research uses the adapted version of the Theory of Planned Behavior to investigate the Cyber security awareness amongst students with focus on the relationships among four core variables which are; Knowledge, Self-perception skills, actual skills and behavior and attitude. The cognitive dissonance shown in students who took part of this research is a phenomenon targeted by cyber criminals showing that students are vulnerable to cyber-attacks.

Okokpujie et al. [8] carried out research to investigate the susceptibility of students to phishing attacks in an academic environment and understand how they react to phish emails. The result of this research shows that 70.6% of students who participated are susceptible to this form of phishing attack due to the lack of cyber security awareness and also the research was able to show vulnerabilities in the school's resources such as the ability for the school website to be successfully cloned. Therefore, it shows there is a need to educate students, staffs and even stakeholders on the dangers of phishing attacks and put in place activities to increase the level of cyber security awareness.

Garba et al. [9] showed us that educating students through classroom is a more effective way to increase awareness and reduce risk of students falling victim to email phishing. This research was conducted across three years using two types of assessment, the formative assessment which phishing emails and online phishing awareness quizzes. The result of the first formative assessment show that more than half of the students clicked on the phishing email and about 80% of them had low scores in the quiz, the second formative assessment shows an improvement with about half of the students ignoring the phishing email and about 43% getting low scores in the quiz and the result for the summative assessment shows that about 87% of students ignored the phishing email and about 71% got high scores in the quiz. The results of the assessment show the decrease in the risk of phishing emails and also shows that

students were able to distinguish between phishing and legitimate emails and this shows the effectiveness of education through classes to increase awareness amongst students.

Alharbi and Tassaddiq [10] carried out an assessment of cybersecurity awareness among students of a university in Saudi Arabia. This research used a scientific questionnaire based on safety factors for the use of the internet to assess the level of cyber security awareness among students. The result of the questionnaire shows that even though 92% had attended a security awareness program most of the participants of the research were still lacking fundamental cyber security knowledge and did not know how to manage their personal data. Using multiple statistical tests this research has been able to prove that a cyber security awareness program and training is strongly needed among students to ensure they know how to identify the most common cyber security threats.

Aljeaid et al. [11] carried out research on the assessment of end user susceptibility to cyber security threats in Saudi Arabia. This research is aimed at assessing end user susceptibility and evaluating their level of cyber security knowledge and awareness by using 3 different phishing attack simulations which are clone phishing, email phishing and SNP. The result of this experiment shows that 77% of the participants were susceptible to the clone phishing attack, 27% were susceptible to the email phishing attack and 47% were susceptible to the SNP attack. The results of this research shows that users can easily fall victim to cyber-attacks and there is need to improve cyber security knowledge and establish cyber security awareness programs to reduce risk and allow users to be aware and better understand cyber security risk and manage their private data better.

Daengsi et al. [12] carried out research to see the effect of gender and age of Thai employees associated with phishing attacks. This result of this research tells us the female than employees have a higher level of cyber security awareness than male than male employees and it shows that after analysis there are no significant differences between the different age groups. In the study, after the use of the transfer knowledge processes in phase 2 and its effectiveness, it shows how the concept of the cyber-attack simulation and knowledge work effectively and helps it reduce risk and should be recommended in other organizations to reduce of falling victim to phishing attacks.

Gordon et al. [13] carried out an assessment of employment susceptibility to phishing attacks at US health care institutions. This research included 6 US health care institutions which was anonymized and the phishing simulations ran from 2011 to 2018. This research shows that after repeated simulations there were improved number of phishing email click rates which proves that the email phishing simulation is an important approach in educating and giving awareness on cyber security.

Althobaiti [14] carried research to investigate user's susceptibility and awareness of cyber security threats relating to students in a university. This research was carried out with 20 students from Taif University and it used an experimental approach known as the think aloud protocol, this approach allows the students to express their thoughts through the performance of the experiment. This research showed that certain demographic factors such as age, gender and knowledge field do not really affect susceptibility to phishing attacks and there is no fixed cause for a person to fall victim. This research shows how there's decrease in link click rates between the first and second simulation which shows that

awareness in an important factor to prevent people from falling victim.

Diaz et al. [15] carried out research on phishing in an academic environment. This research focused on the relationship between demographic factors and phishing susceptibility at a university in USA. The result of the experiment shows 59% of students clicked the phishing link and 70% of those students who took the demographic survey also clicked the phishing link, this research shows that phishing awareness, hours spent on the computer, academic year, age and college affiliations are variables to student susceptibility meaning there is a relationship between demographic factors and susceptibility to phishing.

Nicholson et al. [16] carried out research investigating teenagers' ability in detecting phishing messages. This research investigates their ability to detect phishing messages at the same time checking if their familiarity with a service affects their ability to detect phishing messages. This research also shows that educating teachers through training is a key aspect in integrating phishing training into education to better help students identify phishing emails.

Broadhurst et al. [17] carried out an experiment on phishing cybercrime risks in a university community. This research is aimed at identifying the risk of cybercrime to students by observing their responses to social engineering and observing their behavior to cybercrime risks before and after the phishing phase. Result of this experiment show participants are more likely to be deceived by scams that are personal rather than generic meaning the specificity of a scam influences susceptibility of individuals, results also show that participants in the hunter condition were still susceptible to scam despite being warned to be vigilant meaning cyber security awareness would need constant effort than general warnings.

Alwanain [18] carried out an experiment to identify the effects of user-awareness and phishing knowledge on individuals in detecting phishing emails and phishing websites. This research was carried out using 2 experiments to assess the behavior of users when involved in phishing attacks. The results of this experiment also show that theoretical knowledge is not enough in detecting phishing emails and websites and shows the need for more practical training in enhancing phishing awareness and knowledge.

Abroshan et al. [19] carried out an experiment to identify the effects of human behaviors and demographics on each step of a phishing process. The experiment uses 3 specific phishing steps to investigate to what level individual risk taking and decision-making styles and demographic factors such as age, gender and education influence the likelihood of becoming victim to phishing. The results also show that participants risk taking behavior in specific domains and decision-making styles had no effect in their level of susceptibility to phishing attacks. Some other related works [20-23] emphasized on cybersecurity education; the skill gap hurdle etc.

3. RESEARCH METHODOLOGY

3.1 Introduction

This section presents the methodology for configuring and analyzing a phishing framework to evaluate the vulnerability and awareness of 500 level engineering students in Covenant University to a phishing attack. Figure 1 depicts the research

methodology conceptual framework. The rest subsections follow the outline of the Figure 1 sequentially.

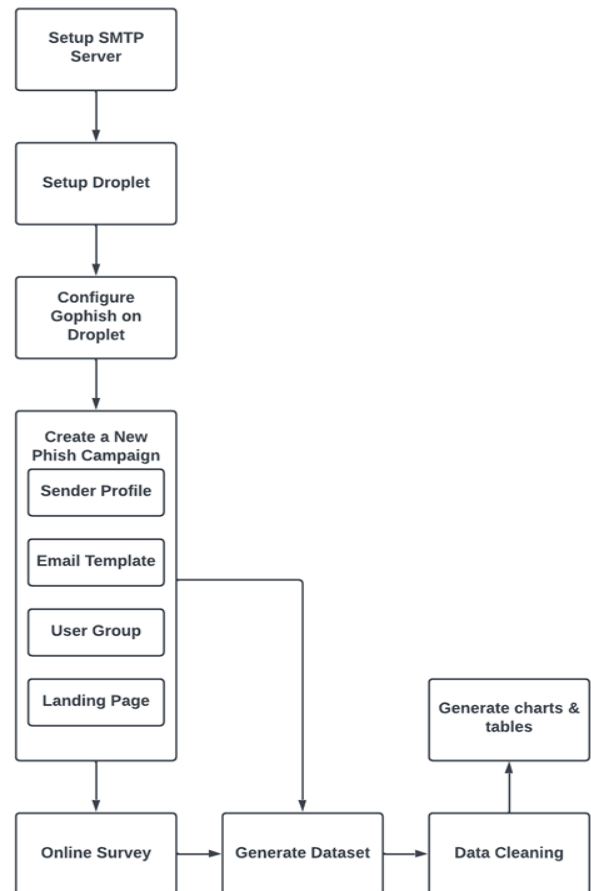


Figure 1. Research methodology conceptual framework

3.2 Phishing framework requirements

A simulated phishing campaign was conducted using a phishing framework to assess the susceptibility and awareness of students towards phishing attacks. The objective was to gain insights into individuals' reactions to phishing emails specifically customised to reflect current events in their student lives. The campaign was active for 53 hours, following which a digital survey was distributed to the engineering students enrolled in the 500 level. In order to successfully configure the phishing framework, the following prerequisites were necessary:

- i. A Simple Mail Transfer Protocol (SMTP) server was developed to enable the spoofing of the sender domain '@covenantuniversity.cu.edu.ng' and facilitate the simultaneous delivery of emails to all engineering students in the 500 level. The objective was to ensure the emails were successfully delivered to each student's inbox without being flagged as spam.
- ii. A software application was necessary to generate phishing emails, disseminate them, capture the interactions between specific students and these emails, and serve as the hosting platform for the phishing campaign's landing page. The software must be able to store and generate a comprehensive report documenting all instances of student interactions with phishing emails. Interactions, such as:

- 1) Email Opened: The recipient accessed the email but did not interact with the embedded hyperlink.
 - 2) User Action: The students initiated a click event on the hyperlink but did not submit any data.
 - 3) Submitted Data: The user has attempted to authenticate using their educational institution's login credentials.
- iii. A server was required to host and manage the campaign software and serve as a centralised platform.

3.3 Software setup

The Software used to carry out the phishing campaign was GoPhish. GoPhish is an open-source phishing framework used to test the exposure of individuals or organizations to phishing. The software offers a user interface that enables users to design email templates and landing pages, enter and store participant emails in various categories, connect to SMTP mail servers for email sending, and view an attractive real-time display of activity.

GoPhish can be used on a variety of operating systems, including Mac, Linux, Windows, and Unix. The program also specifies two ports on which it will independently listen for participant interactions and administrative directives.

3.4 Server setup

The phishing campaign employed a Linux-based virtual machine, commonly called a droplet hosted by Digital Ocean, to act as the platform for the Gophish software. Upon accessing the Digital Ocean platform and opting for the "Create a Droplet" feature. The droplet was configured using Ubuntu 22.10 x64 as the chosen operating system. The Frankfurt region was picked, along with a droplet size of 1gb/1 CPU, a 25GB SSD disc, and 1000GB transfer.

The authentication method chosen was password-based, requiring creating a root password. The hostname employed for this droplet corresponded to the domain designated to serve as the landing page for the phishing campaign, namely 'moodlecu.com'.

3.5 GoPhish setup

Upon the successful creation of the droplet, the server was remotely configured using the Bitwise SSH client. The Bitwise SSH client successfully established a connection on port 22, utilising the IP address of the droplet and authenticating it with the root password.

The Gophish software was configured. The Gophish file was downloaded using the 'wget' command in the Bitwise SSH client's terminal. The URL address for the Gophish download file was obtained from GitHub. Once the download process has concluded, we install the unzip command by executing the 'apt install unzip' command. Subsequently, we proceed to extract the contents of the downloaded file.

Following the installation process, it is necessary to proceed with configuring the Gophish software. However, it is necessary to assign executable rights to the gophish file by utilising the command 'chmod+x gophish' beforehand. The colour of the text displayed for the 'gophish' command when executing the 'ls' command should be green.

Prior to executing Gophish, the 'screen' command is

employed. 'Screen' is a utility that facilitates the ability to close the terminal while simultaneously running Gophish in the background or sustaining the session in the event of disconnection from the server or the client. To execute the Gophish programme, enter the command '/gophish'.

In order to access the Gophish admin page using the domain name, it is necessary to establish a connection between the droplet IP address and the domain. In order to accomplish this task, the user should navigate to the domain administration page provided by Namecheap. Once there, they should modify the domain nameservers by replacing the default ones with custom ones. Specifically, the custom nameservers to be entered are ns1.digitalocean.com, ns2.digitalocean.com, and ns3.digitalocean.com.

Upon establishing the domain name, it becomes imperative to ensure the website's security by procuring an SSL certificate. The SSL certificate was generated using the website 'zerossl.com'. The necessary information was provided, and the domain was verified using DNS verification. This involved generating DNS records on Digital Ocean for the shown CNAME record. Once the CNAME has been established, proceed to obtain the SSL certificates.

Upon the successful installation and subsequent examination of our certificate and private key. The files 'gophish_admin.crt' and 'gophish_admin.key' were successfully configured. The data contained within the private key and certificate files were transferred to the respective files named 'gophish_admin.crt' and 'gophish_admin.key'.

The certificate and essential files have been modified, necessitating reconfiguring the 'config.json' file.

In configuring the phishing server, it is necessary to modify the values of 'cert_path' and 'key_path' to 'gophish_admin.crt' and 'gophish_admin.key', respectively. Additionally, the 'use_tls' parameter should be set to true, and the port should be changed from 80 to 443 to enable communication over the secure 'https://' protocol. In the context of the administrative server, it is recommended to modify the port configuration to 7040. Terminate the 'nano config.json' command. Execute the screen command and initiate the execution of the gophish programme.

3.6 Phishing campaign

A successful phishing campaign requires several key components: a sender, an email, recipients, and a landing page. A well-designed landing page is crucial if recipients engage with the campaign by clicking on the provided link. The subsequent sections provide a detailed explanation of formulating and assembling these requirements.

3.6.1 Creating sender profile

Possessing an email address that closely mirrors that of a reputable company is vital. Ensuring the efficacy of the test is of utmost importance. In order to safeguard the anonymity of the sender, it is imperative to conceal any details that may reveal their identity. SMTP is an effective technique in this context, as it provides adequate levels of anonymity for this specific use case. The email address designated for this campaign on the Simple Mail Transfer Protocol (SMTP) server is 'anthony.ede@covenantuniversity.com'. To configure the sender email as Simple Mail Transfer Protocol (SMTP) on Gophish, the necessary information includes the email address, password, host, and the required port number. This enables the software to send emails using the specified

SMTP server. The designated port number for transmitting emails over the established SMTP server is 465, incorporating SSL encryption for enhanced security.

3.6.2 Creating an email template

A sample email template was acquired from a prior email dispatched through a legitimate school account. GoPhish successfully generated a novel email that allows for customisation by utilising the source code of the original email. This functionality also allows email formatting modification according to the preferred style. The GoPhish platform promptly modifies the destination of each hyperlink to our designated landing page. The primary distinctions between the recently generated email templates and the exemplar email are the placement of each URL and the information inside the email. Reducing recipients' scepticism and promoting enhancements in interactions that may lead to data submission is imperative.

3.6.3 Creating a user group

In order to execute this phishing effort, it was determined that the target audience would consist exclusively of engineering students enrolled in courses at the 500 level. Four hundred sixty students enrolled in the 500-level Computer Engineering, Information & Communication Engineering, Electrical Electronics Engineering, Chemical Engineering, Petroleum Engineering, Mechanical Engineering, and Civil Engineering courses were chosen to participate in this phishing effort. A formal request was sent to the Director of the CSIS (Computer Science and Information Systems) department, proposing implementing a phishing campaign targeting 500-level Engineering students. Subsequently, authorization was granted to experiment and access the students' email accounts. The emails were stored in a Comma-Separated Values (CSV) file format and uploaded to the Gohish platform. Additionally, a user group was established specifically to conduct the phishing campaign.

3.6.4 Creating a landing page

In a manner analogous to creating an email template, we proceeded to import the target website, which serves as the online learning platform for the school, by utilising its URL. Subsequently, the cloned version of the website was hosted on the droplet. A distinct identification (ID) was assigned to every recipient, which was subsequently documented in the database and employed by the web server as a point of reference. The destination address of each email consists of the domain name hosted on the droplet, port 443 for secure sites, a query string containing the parameter "rid", and the unique ID of the specific recipient as its corresponding value. The following depicts a Uniform Resource Locator (URL) for a landing page.

3.6.5 Creating a new phish campaign

The phishing campaigns were launched after the completion of all necessary prerequisites. Phishing remained operational for fifty-three hours.

In the GoPhish platform, a comprehensive campaign necessitates the inclusion of several key components. These components consist of a designated campaign name, an email template, a landing page, a URL adhering to the HTTP protocol, a specified launch date, a sending profile, and the incorporation of one or more user groups. The campaign's email distribution was not dispersed; all emails were delivered simultaneously.

3.7 Monitoring recipient interaction

The GoPhish platform effectively monitors and records the activities of individual recipients, encompassing email openings, hyperlink interactions, and data submissions. The system presents a graphical representation that illustrates the effectiveness of each campaign and provides a visual timeline of the various interactions.

The campaign incorporates a chronological sequence of events that organises time-related information for the recipients. Every recipient is associated with a chronological sequence of encounters, forming a history of events. Furthermore, the email tracking feature provides specific information regarding the recipient's computer and web browser utilised to access the email.

3.8 Generating phishing campaign result

The reports of the phishing effort were generated and stored in a Comma-Separated Values (CSV) file. The campaign's result file has comprehensive data on each beneficiary. The distinct identifiers allocated to individual users and events are utilised to arrange them in a specific sequence.

The file is ordered by recipient ID in GoPhish. The dataset comprises the following components:

- The final recipient interaction,
- An IP address,
- Recipient longitude and latitude,
- The time the email was sent,
- A reported field for if emails were reported as phish,
- The last interaction time with the email,
- Recipient email,
- Recipient name and program.

3.9 Data cleaning

The resultant CSV file contained multiple extraneous fields deemed unnecessary for the datasets and subsequent graph and chart generation. These fields were promptly removed to prevent any compromise of students' information. The following fields were removed from the dataset as they were deemed unnecessary.

- i. First name,
- ii. Email,
- iii. Longitude and latitude,
- iv. IP Address.

3.10 Datasets

In order to effectively monitor the recipients and their engagements, Interaction datasets were created. The charts and graphs presented in the results section were generated utilising the Interaction datasets derived from the phishing campaign result file.

3.10.1 Survey dataset

A survey was conducted among recipients to gain insights into the specific circumstances surrounding their interactions with phishing emails. A dataset was formulated using the collected survey data, and subsequent charts were generated from this dataset to facilitate a more comprehensive analysis of the results. The dataset comprises various fields, encompassing the respondents' expertise in cyber security, inquiries about their email communication, the measures they

have undertaken, their familiarity with Gmail's phish protection feature, and their level of suspicion.

4. RESULTS AND DISCUSSION

This section presents an overview of the outcomes derived from the interaction with the phishing email within the context of the phishing campaign. The dataset provided by the student offered multiple analytical approaches for examining the interplay between phishing emails in a phishing campaign and their correlation with the participant's diverse programmes. This dataset was subsequently utilised to assess the level of cyber security awareness and safe practises, actions performed, familiarity with Gmail's phish protection function, and the degree of suspicion exhibited by 500-level students towards phishing emails.

4.1 Phishing email interactions

In Figure 2, the data illustrates the aggregate count of engagements initiated by engineering students enrolled in the 500-level courses in response to the phishing email. A total of 183 students were found to have accessed the phishing email. Out of these, 36 students proceeded to click on the embedded link within the email, while a subset of 8 students went on to submit their personal information.

In Figure 3, the data illustrates the count of 500-level students enrolled in each engineering programmes which engaged with phishing emails. This engagement includes opening the email, clicking the embedded link, or submitting personal information. Additionally, the figure presents the total number of 500-level engineering students in each respective programme.

These below abbreviations were used to represent the programmes:

CHE - Chemical Engineering,
CEN - Computer Engineering,
CVE - Civil Engineering,
MCE - Mechanical Engineering,
PET - Petroleum Engineering,
ICE - Information and Communication Engineering, and
EEE - Electrical Electronics Engineering.

According to Figure 3, the data indicates that students enrolled in the 500-level EEE had the highest number of interactions with a phishing email, with a total of thirty-one students engaging with the email. Conversely, students in the 500-level PET had the lowest number of interactions, with only twenty-one students interacting with the phishing email.

Figure 4 presents a comprehensive breakdown, illustrating the interactions made by students enrolled in engineering programmes at the 500 level with phishing emails. The interactions were categorised into three groups based on the actions taken by 500-level students. The first group consisted of students who only opened the email. The second group comprised students who clicked the link provided in the email but did not submit any data. The third group included students who both clicked the link and submitted data.

According to Figure 4, it can be observed that MCE had the highest count of 500 level students who exclusively opened the email, with a total of twenty-five students. On the other hand, PET had the lowest count of 500-level students who exclusively opened the email, totalling seventeen students.

Also, in Figure 4, the disciplines of ICE and EEE exhibited the highest count of 500 level students who clicked on the provided link but failed to submit their data, with each discipline having six students. Conversely, CHE had the lowest count of 500-level students who clicked on the link but did not submit, with only one student.

Figure 4 also displays that CEN and CVE had the maximum number of students at the 500 level who provided their personal data, with two students each. On the other hand, CHE had the minimum number of 500-level students who submitted their personal data, with zero students.

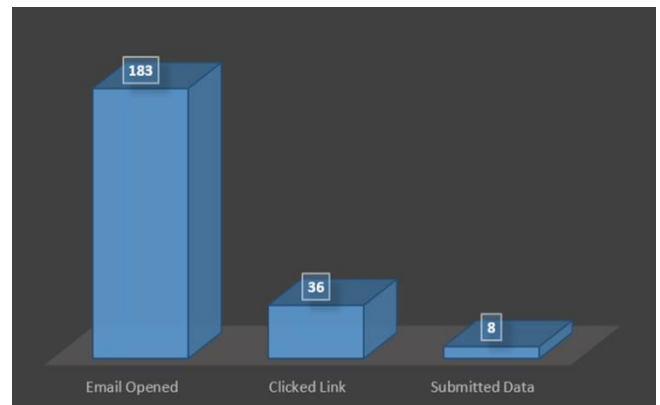


Figure 2. Total number of email interactions

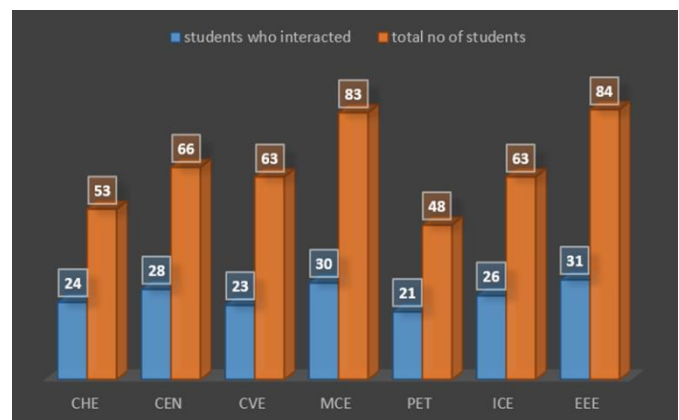


Figure 3. Total number of students in each program that Interacted with the phishing email

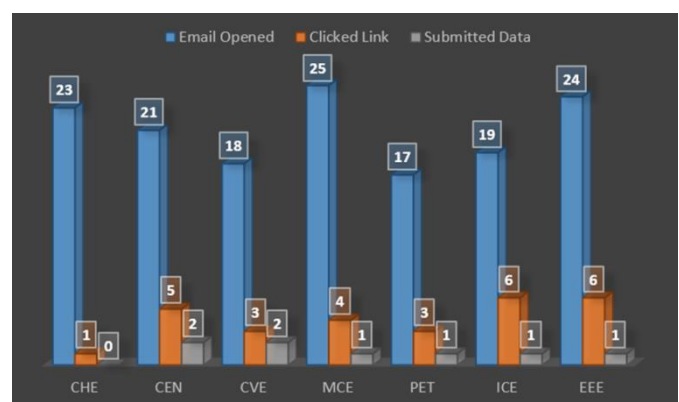


Figure 4. Breakdown of email interactions for each programme

Table 1. Percentage of students' interaction per programme with the phishing email

	CHE	CEN	CVE	MCE	PET	ICE	EEE	Total
Total no of students	53	66	63	83	48	63	84	460
No. of Students interaction	24	28	23	30	21	26	31	183
% of Students interaction	45	42	37	36	44	41	37	40

Table 1 shows the percentage of students' interaction per programme with the phishing email. The chemical engineering been the highest with 45% susceptible. On the average 40% of the entire students are susceptible to phishing attached. Thus, the need to create awareness and mitigate the effects.

4.2 Survey results

Figure 5 illustrates the proportion of Engineering students at the 500-level who have engaged in cybersecurity activities prior to the occurrence of the phishing campaign. According to the survey results, 66% of the student population reported not engaging in any previous cybersecurity exercise, while 34% confirmed their participation.

Figure 6 illustrates the percentage of Engineering students at the 500 level who possess knowledge of Cybersecurity and adhere to Cybersecurity safe practises. 68% of the surveyed students indicated possessing knowledge of Cybersecurity and Cybersecurity safe practices, while the remaining 32% reported lacking such knowledge.

Figure 7 illustrates the percentage of awareness among Engineering students at the 500 level regarding phishing emails. 5% of students were informed about the email through personal acquaintances, while another 5% remained unaware of its existence. Approximately 43% of students became aware of the email by disseminating screenshots and related information on the Telegram platform. The remaining 48% of students became aware of the email by directly encountering it in their email inbox.

Figure 8 illustrates the proportion of Engineering students at the 500 level who possessed knowledge regarding the phishing email employed in the phishing campaign. 93% of the surveyed students indicated they knew about the phishing email, while the remaining 7% reported lacking awareness of the email.

Figure 9 illustrates the proportion of Engineering students at the 500 level who attempted to access the Moodle platform after becoming informed about the phishing email and its contents. According to the survey results, 43% of students responded affirmatively when asked if they had attempted to log into the Moodle platform. Conversely, 57% of students indicated they had not attempted to log into the Moodle platform.

Figure 10 depicts the percentage of attempts made by Engineering students at the 500 level to access the Moodle platform after their awareness of a phishing email. 9% of students attempted to access the Moodle platform by clicking the hyperlink in the phishing email. Conversely, 48% of students refrained from attempting to access the Moodle platform altogether. Additionally, 43% of students opted to access the Moodle platform through alternative means, such as

manually searching for the original Moodle link via a web browser.

Figure 11 illustrates the proportion of Engineering students at the 500 level who exhibited suspicion towards the phishing email. 52% of the student population responded affirmatively when asked about their level of suspicion towards the phishing email, while the remaining 48% responded negatively.

Figure 12 illustrates the percentage of Engineering students at the 500 level who know about the existence of the 'Report Phish' functionality on their email service provider. According to the survey results, 20% of the student population indicated their awareness of the 'Report Phish' feature, while 80% reported being unaware of it.

PRIOR PARTICIPATION IN CYBER SECURITY EXERCISES

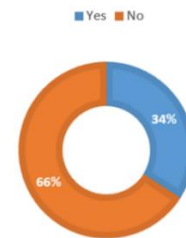


Figure 5. Participation in cyber security exercises

KNOWLEDGE ON CYBER SECURITY & SAFE PRACTICES

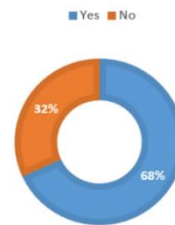


Figure 6. Knowledge on cyber security and safe practices

HOW DID STUDENTS KNOW ABOUT THE EMAIL

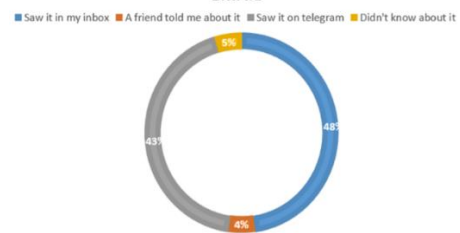


Figure 7. How students aware of the email

AWARENESS OF EMAIL

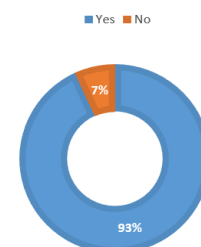


Figure 8. Awareness of email survey

MOODLE LOG IN ATTEMPT

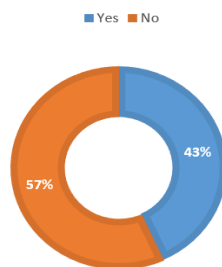


Figure 9. Moodle Log in attempt

HOW WAS MOODLE ACCESSED

■ through the link ■ elsewhere ■ I didn't open moodle

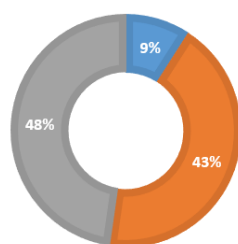


Figure 10. How did students access Moodle

PHISH SUSPICION

■ Yes ■ No

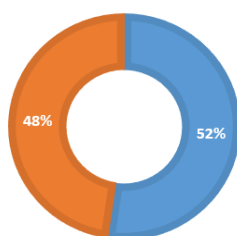


Figure 11. Phishing email Suspicion

AWARENESS OF 'REPORT PHISH' FEATURE

■ Yes ■ No

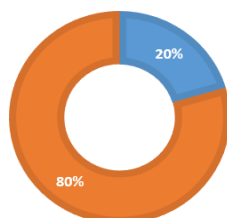


Figure 12. Awareness of 'Report Phish' feature

5. CONCLUSION AND RECOMMENDATIONS

The assessment of susceptibility to phishing attacks among engineering students at the 500 level has underscored the pressing necessity for enhanced awareness and education

regarding cyber security at Covenant University. Based on a comprehensive analysis of the phishing campaign, it is evident that technological, psychological, and educational factors contribute to students' susceptibility to phishing attacks.

In key findings include that the students exhibited impulsive behaviour, coupled with their limited knowledge of phishing techniques and cyber security best practices, significantly heightening their susceptibility to becoming targets of phishing attacks.

To effectively address this matter, educational institutions must prioritise including cyber security education as a fundamental element within their curriculum. Equipping students with essential knowledge and skills to identify and respond to phishing attacks or other types of cyber-attacks enables them to cultivate a proactive mindset and enhance their resilience against these threats. Furthermore, fostering collaboration among academic institutions, cyber security experts, and industries can facilitate the development of tailored strategies and solutions to address the evolving landscape of phishing attacks effectively.

Additionally, it is imperative to foster a culture of cyber security knowledge and awareness among students. Students can develop an understanding of the potential repercussions associated with falling victim to phishing attacks through the implementation of various strategies. These include fostering an environment of open dialogue, organising informative seminars, and conducting simulated phishing campaigns. Implementing this proactive strategy will empower students to navigate the digital environment effectively by equipping them with the necessary knowledge and skills to safeguard their personal information efficiently.

During the experiment, a vulnerability in the school's system was discovered, specifically pertaining to the possibility of a school homepage being replicated and exploited for a phishing attack. Technological advancements play a crucial role in mitigating phishing attempts in various domains. The effectiveness of such attacks can be significantly reduced by implementing robust security measures, employing multi-factor authentication. In order to stay ahead of evolving phishing strategies, it is imperative to implement consistent monitoring, prompt incident response, and regular updates to security policies.

There is a potential to enhance Universities cyberspaces overall security posture and protect students from phishing attacks and other cyber security threats. This can be achieved by cultivating a cyber security-aware environment, providing comprehensive education to students, and implementing advanced technological solutions.

ACKNOWLEDGEMENT

The authors acknowledge the sponsorship of the Covenant University Centre for Research, Innovation, and Discovery (CUCRID), Ota, Ogun State, Nigeria.

REFERENCES

- [1] Butcher, D.S., Brigham, C.J., Berhalter, J., Centers, A.L., Hunkapiller, W.M., Murphy, T.P., Palm, E.C., Smith, J.H. (2023). Cybersecurity in a large-scale research facility-One institution's approach. Journal of

- Cybersecurity and Privacy, 3(2): 191-208. <https://doi.org/10.3390/jcp3020011>
- [2] Abdullah, N.Z.I., Sedi, N.A.A.M., Muhamad, N.M., Alias, N.R. (2023). A review of cybersecurity awareness focusing on software and email security. In Proceedings of 1st Glocal Symposium on Information and Social Sciences (GSISS) 2023, p. 10. <https://doi.org/10.5281/zenodo.8180686>
 - [3] Haque, M.A., Ahmad, S., John, A., Mishra, K., Mishra, B.K., Kumar, K., Nazeer, J. (2023). Cybersecurity in universities: An evaluation model. SN Computer Science, 4(5): 569. <https://doi.org/10.1007/s42979-023-01984-x>
 - [4] Burvall, F. (2023). Development of a guideline for cybersecurity awareness-Raising in large Swedish public organizations: A design science project. Digitala Vetenskapliga Arkivet.
 - [5] Sharma, P., Dash, B., Ansari, M.F. (2022). Anti-phishing techniques-A review of cyber defense mechanisms. International Journal of Advanced Research in Computer and Communication Engineering ISO, 3297: 2007.
 - [6] Baig, M.S., Ahmed, F., Memon, A.M. (2021). Spear-phishing campaigns: Link vulnerability leads to phishing attacks, Spear-phishing electronic/UAV communication-Scam targeted. In 2021 4th International Conference on Computing & Information Sciences (ICIS), Karachi, Pakistan, pp. 1-6. <https://doi.org/10.1109/ICIS54243.2021.9676394>
 - [7] Chandarman, R., Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication, 20: 133-155. <https://doi.org/10.23962/10539/23572>
 - [8] Okokpujie, K., Kennedy, C.G., Nnodu, K., Noma-Osaghae, E. (2023). Cybersecurity awareness: Investigating students' susceptibility to phishing attacks for sustainable safe email usage in academic environment (a case study of a Nigerian leading university). International Journal of Sustainable Development and Planning, 18(1): 255-263. <https://doi.org/10.18280/ijstdp.180127>
 - [9] Garba, A.A., Siraj, M.M., Othman, S.H., Musa, M.A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. International Journal on Emerging Technologies, 11(5): 41-49.
 - [10] Alharbi, T., Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2): 23. <https://doi.org/10.3390/bdcc5020023>
 - [11] Aljeaid, D., Alzhrani, A., Alrougi, M., Almalki, O. (2020). Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks. Information, 11(12): 547. <https://doi.org/10.3390/info11120547>
 - [12] Daengsi, T., Pornpongtechavanich, P., Wuttidittachotti, P. (2022). Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 1-24. <https://doi.org/10.1007/s10639-021-10806-7>
 - [13] Gordon, W.J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R.J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., Landman, A.B. (2019). Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Network Open, 2(3): e190393. <https://doi.org/10.1001/jamanetworkopen.2019.0393>
 - [14] Althobaiti, M.M. (2021). Assessing user's susceptibility and awareness of cybersecurity threats. Intelligent Automation & Soft Computing, 28(1). <https://doi.org/10.32604/iasc.2021.016660>
 - [15] Diaz, A., Sherman, A.T., Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1): 53-67. <https://doi.org/10.1080/01611194.2019.1623343>
 - [16] Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O.D., Anderson, P. (2020). Investigating teenagers' ability to detect phishing messages. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, pp. 140-149. <https://doi.org/10.1109/EuroSPW51379.2020.00027>
 - [17] Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1): 4-23.
 - [18] Alwanain, M.I. (2019). Effects of user-awareness on the detection of phishing emails: A case study. International Journal of Innovative Technology and Exploring Engineering, 8(4): 480-484.
 - [19] Abroshan, H., Devos, J., Poels, G., Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. IEEE Access, 9: 44928-44949. <https://doi.org/10.1109/ACCESS.2021.3066383>
 - [20] John, S.N., Noma-Osaghae, E., Oajide, F., Okokpujie, K. (2020). Cybersecurity education: The skills gap, hurdle!. Innovations in Cybersecurity Education, Springer, Cham, 361-376. https://doi.org/10.1007/978-3-030-50244-7_18
 - [21] Okokpujie, K., Kennedy, G.C., Oluwaleye, S., John, S.N., Okokpujie, I.P. (2023). An overview of self-organizing network (SON) as network management system in mobile telecommunication system. Information Systems for Intelligent Systems: Proceedings of ISBM 2022, Springer, Singapore, 324: 309-318. https://doi.org/10.1007/978-981-19-7447-2_28
 - [22] Okokpujie, K., Okokpujie, I.P., Ayomikun, O.I., Orimogunje, A.M., Ogundipe, A.T. (2023). Development of a web and mobile applications-based cassava disease classification interface using convolutional neural network. Mathematical Modelling of Engineering Problems, 10(1): 119-128. <https://doi.org/10.18280/mmep.100113>
 - [23] Okokpujie, K., Okokpujie, I.P., Ogundipe, A.T., Anike, C.D., Asaboro, O.B., Vincent, A.A. (2023). Development of a sustainable internet of things-based system for monitoring cattle health and location with web and mobile application feedback. Mathematical Modelling of Engineering Problems, 10(3): 740-748. <https://doi.org/10.18280/mmep.100302>