IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Sustainable Development and Planning
Vol. 18, No. 1, January, 2023, pp. 255-263
Journal homepage: http://iieta.org/journals/ijsdp

Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University)

Kennedy Okokpujie[1,2] *, Chinyere G. Kennedy[3], Kamsiyochukwu Nnodu[1], Etinose Noma-Osaghae[1]

[1] Department of Electrical and Information Engineering, Covenant University, Ogun State, Ota 112101, Nigeria
[2] Africa Centre of Excellence for Innovative & Transformative STEM Education, Lagos State University, Lagos State, Ojo 102101, Nigeria
[3] Department of Computer Science and Engineering, Kyungdong University, Goseong-si 219-705, Korea

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

https://doi.org/10.18280/ijsdp.180127

Received: 11 July 2022
Accepted: 1 November 2022

Keywords:
academic environment, cybersecurity awareness, detection, email attack, investigation, phishing, social engineering

ABSTRACT

With the advancement in information communication technology (ICT), cyber-attacks have become a global phenomenon, with email phishing at the topmost. Academic institutions' ICT infrastructures are one of many targets, thus the need to facilitate cybersecurity awareness among students. This research is aimed at investigating students' susceptibility to phishing attacks for sustainable safe electronic mail (email) usage in the academic environment. Two email phishing tests were carried out during this research work to discover how students reacted to phish emails and understand how students respond to phish emails where all group members are recipients. Finally, questionnaires are administered to participants after completing the exercise to ascertain the students' awareness of phishing attacks based on received emails. The results show that 70.6% of college students surveyed are susceptible to this form of attack due to unawareness. In conclusion, recommendations are outlined on securing the academic community and ICT infrastructures to achieve a sustainable and Safe email usage environment.

1. INTRODUCTION

The latest advances in online and mobile technologies have drawn most institutions to make their services available to their customers via online platforms. As an increased number of people maximize the benefits of the availability of Internet services to carry out transactions online, Internet fraud becomes a significant threat to the privacy and safety of people [1]. As per Internet world figures, the total number of Internet users worldwide in 2014 amounted to 2.97 billion; that is, over 38 per cent of the world's population is using the Internet [2]. While a total of 5.16 billion people around the world use the internet at the start of 2023, which is equivalent to 64.4 percent of the world's total population. Generally, internet fraud may be described as an act of deceiving individuals into revealing their personal information, ultimately for financial or personal benefit. Phishing attack has been considered one of the topmost internet frauds.

Phishing is a cyber-attack in the form of socially engineered messages propagated via electronic channels of communication such as social networking sites, VoIP, phone calls, SMS, email, and instant messengers. The most popular propagation channel of phishing attacks is by email communication as 65% of the total attacks result from visiting hyperlinks attached to emails. Phishing attacks implement professionally crafted email messages and web pages that look close to organizations' legitimate emails and websites to compel users to reveal data or financial details. The intruder then uses the obtained confidential user information for their profit. There are various types of phishing attacks, of which spear phishing is the most commonly launched against higher academic institutions of learning via students' official emails.

Spear phishing" is a sort of phishing effort that targets a particular individual or group in this case the academic institutions in a view to incorporating data known to hold any importance for malicious reasons. Business Email Compromise (BEC) is a significant threat in which the intruder uses spear-phishing techniques to trick organizations and individuals on the Internet. More complex cases of spear-phishing attacks directly exploited specific groups or individuals within organizations. The phishing email launched directly against academic institutions in the hope of extracting information from students for fraud purposes is an example of spear-phishing and BEC [3-5].

Figure 1 shows the phishing cycle. According to a new Google study, 45 per cent of phishing websites tricked their intended victims into revealing their passwords, and the attacker changed their password within 30 minutes after infiltration. The attackers also use the avenue to trick people on the victims' contact list by communicating with the hijacked account and posing as the victim [6].

There is a need to create cybersecurity awareness among the students in the academic environment knowing that the fraudsters could gain access via their email to the critical ICT infrastructures with the view of tempering results, illegal insurance of certificates and transcripts etc. Thus, the need to investigate students’ susceptibility to phishing attacks for sustainable safe email usage in the academic environment in which this research is aim at.

2. LITERATURE REVIEW

2.1 Phishing attack statistics

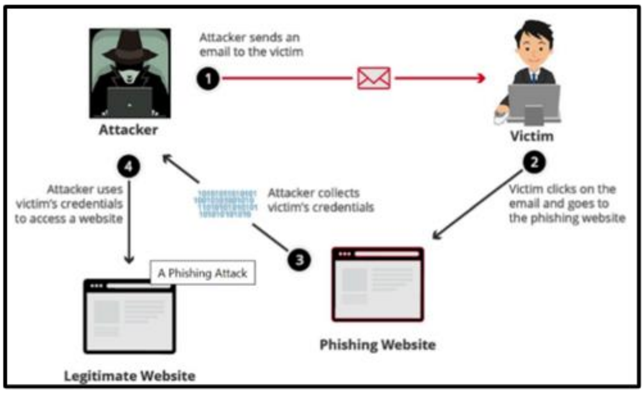
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
A Phishing Attack
Phishing Website
Legitimate Website

Figure 1. Phishing attack cycle [6]

In 2022, six billion attacks are anticipated to happen. In 2021, 83% of institutions announced encountering phishing attacks. In 2020, the unique phishing sites were identified as about 214,345, and the number of recent phishing attacks has doubled since early 2020. The Anti-Phishing Working Party (APWG) report of 2020 acknowledged that the number of phishing websites detected increased from the Q4 of 2019 to Q1 of 2020 [7-10].

In 2012, the phishing attack total went up by one hundred and sixty per cent compared to 2011, indicating a record year in phishing volumes. The total phishing attacks discovered in 2013 were placed at about 450000 and unavoidably led to financial losses that cost more than $5.9 billion. The whole attack went up by 1% in 2013 compared with 2012. The total number of phishing attacks observed in Q1 of 2014 was 125,215, representing a 10.7 per cent increase over the Q4 of 2013. Over 55% of phishing websites consist of the name of the target site in a certain way intended to trick users, and 99.4% of phishing websites use port 80. Also, in Q1 of 2014, the second-highest number of phishing attacks ever recorded occurred during January and March 2014 and payment facilities were the most significant targeted area. Likewise, in the second half of 2014, the phishing attacks unraveled were 123,972. In 2011, the financial losses accrued to 1.2 billion, which escalated to about $5.9 billion in 2013 [11, 12].

According to the Federal Bureau of Investigation's Internet Crime Report (IC3) in 2018 [13], a total of 46,752 complaints of BEC/EAC, phishing, vishing, and pharming attacks in the U.S. alone. The combined total adjusted losses stood at $1,346,045,237, with BEC/EAC contributing more than 90% to this figure.

2.2 Phishing attack stages

Phishing attacks consist of three major stages, which include:

Stage 1: The likely victim of the attack receives a phish.

Stage 2: The victim goes ahead to perform the suggested action contained in the message, usually to visit a fake website but can also be in the form of replying with confidential information or installing malware.

Stage 3: This is the point at which the attacker monetizes or gains other benefits from the obtained information.

Most phishing attacks convince users to visit a fake site where confidential information is collected. Scammers utilize free web space and a corrupted computer to host a phony website or register a new domain [14]. In this step, an attacker defines the target as a reputable organization. The attacker visits the organization's website and captures detailed information about them. The attacker then uses the data to set up the fake website.

a) URL sending/ fake phishing email: phishing email messages often use conventional techniques to trick users rather than technical strategies. An attacker puts together a deceptive email and sends it to thousands of users in this step. Attackers attach the fake website's URL to the email. Selected users get the emails in the case of a spear-phishing attack.

b) Stealing of user credentials: Consequently, the created fake website opens when a user clicks on the URL attached to the email sent by an attacker. The phony website usually includes a login form to collect the user's credentials. The attacker can also access other information given by the user on the website.

Identity theft: An attacker can go ahead and make use of the stolen credentials to carry out malicious actions.

2.3 Related works

Foremost researchers Andrić et al. [15] carried out an online survey using an online questionnaire containing 23 questions. Recipients determined if each sample question was malicious, legit or indeterminable. Based on the survey results analyzed by the data with the help of correlations and analysis of variance, the Pearson correlation coefficient was used, which is sensitive only to the linear relationship between the variables. The correlation showed the link between education and phishing attacks and the prevention of these same attacks.

Jagatic et al. [16] involved an actual (but harmless) phishing attack aimed at university students aged between 18–24 years of age. The targets represented typical phishing victims. The study sought to discover how reliable social context would increase the success of a phishing attack while still trying to be ethical. An attack was 'successful' when the target clicked the link and authenticated it using valid credentials in the phishing site created for the survey. From a t-test, the difference is very significant ($p < 10-25$).

Toolan and Carthy [17] applied a two-phase classification model of emails. In the first phase, a set of classification algorithms (C5.0, Naive Bayes, SVM, Linear Regression and K-Nearest Neighbors) classified legitimate and phishing emails. Standard evaluation metrics evaluated each algorithm including accuracy, precision, recall and F-score. The algorithm with the best classification results was C5.0 with an average accuracy rate of 97.15%, average precision of 98.56%, average recall of 95.64% and average F-score of 97.08%. The legitimate emails in the first phase were input to an ensemble classifier in the second phase.

Senthilkumar and Easwaramoorthy [18] surveyed students' responses to various cyber themes, including viruses, fake publications, pop-up advertisements, and other attacks that flood the internet space. Only 10 out of the 379 students who participated in the survey stated that they would report malicious activities to their cybercrime office.

Similarly, Kim [19] studied many undergraduate students who majored in Business Studies on their perceived knowledge of cyber-related topics. The survey revealed that understanding most issues covered in NIST Standard 800-50 suggested training programs for all students helped increase student awareness, as proved in an unannounced phishing test on the United States Military Academy students. This test evaluated their cyber training programs and concluded that the more educated a student was in a school year, the less possible it was to be attacked using phishing scams.

Tak and Ojha [20] proposed a browser knowledge-based compound approach for detecting phishing attacks. The proposed model analyses web URLs using parsing and a set of maintained knowledge bases that store the previously visited URLs and previously detected phishing URLs. The experimental results indicated 96.94% accuracy in detecting phishing URLs with a little compromise in degrading the browser speed.

Abbasi et al. [21] quizzed the assumption that those who feel unsafe are bound to be careful and use protective methods, as this did not mean that they are now immune to attacks. The research was fed with samples of 509 college students, staff, and public members from two cities in the United States. The study categorized individuals into groups based on similar online experiences and scrutinized their interactions with various fake phishing sites. Indeed, it was discovered that the users who were most successful in detecting the phish were those who were previously aware of the act of phishing. They were quite familiar with blacklisted websites; they also had excellent opinions about the efficacy of anti-phishing tools. It was further discovered that they had once experienced financial losses attributable to phishing.

Nonetheless, some of these same qualities also adversely affect an individual's ability to detect phishing attempts successfully. This was due to the overconfidence syndrome past encounters on users that accentuated their ability to detect malicious websites. Also, the acquaintance with frequented websites made the user develop over-reliance and trust for the sites. The study, however, did not explore how these traits form perceptions of safety. However, the results indicate that more robust notions of Internet risk and vulnerability may assist in phishing avoidance.

From the related works reviewed, it was discovered that there are correlations between phishing attack and education institution. Thus there is need to investigate students' susceptibility to phishing attacks for sustainable safe email usage in academic environment in view of creating awareness.

3. RESEARCH METHODOLOGY

3.1 Introduction

Two email phishing tests were carried out in the course of this research work. In the first test, we sought to discover how students reacted to phish emails addressed to select recipients in a group. In the second test, we aimed to understand how students respond to phishing emails where all group members are recipients. The first test ran for thirty-three hours, while the second ran for twenty-six hours. We also broadcast a questionnaire after the test to the selected students after completing the test. The survey included a description of the tests, questions about their response to the email and their knowledge of phish and phish reporting tools. The details of the methodology are shown in Figure 2.

3.2 Requirement analysis

3.2.1 Functional requirements

The software was required to create phish emails, distribute them, record interactions between selected students and these emails, and host the landing pages of the respective tests. The software must store and generate a report of all interactions between students and the phish emails. Such interactions include:

i. Email Opened: the student opens the email but has not clicked the link.

ii. Clicked link: the student has clicked the link but has not submitted any data.

iii. Submitted Data: the student has attempted to log in with their school credentials.

3.2.2 Non-functional requirements

The software to be used was also required to operate in real-time to catch interaction events and store them in a database. The system was needed to host the landing page using HTTP format with port 80 to prevent certificate issues posed by students' browsers and mask the port number attached to the URL seeing as port 80 is a standard.

An admin panel was required to monitor the perform all the tasks needed for the test. The admin panel needs to be secure and only accessible through the specific internet protocol (IP) addresses of the collaborators.

We needed to host the software on a server to achieve the functional requirements. A static IP is also a requirement for the server, as only one link containing a specific IP address is sent in each email. It is required for the software to run as a service that boots the server to recover from unprecedented downtimes quickly.

The software must identify each student and monitor their interactions uniquely. Hence the software must generate, store, and define individual students using a unique identifier (ID). The system is required to record the platform and device used by the student in interacting with the email. This requirement is essential to gain insight into students' preferred email viewers and the respective platforms they run on.

The software was required to accept bulk email from CSV files to speed up the email input process and generate a CSV file in return containing all relevant information needed for this study.

3.2.3 Software implementation

An open-source phishing software called GoPhish was procured. The software delivered the majority of the functional and non-functional requirements. GoPhish is a framework that affords individuals and organizations all the professional tools required to conduct phishing tests all in one package [17]. The software provides a user interface with which users can create emails templates and landing pages, input and store emails of participants in different categories, connect to SMTP mail servers for sending emails and a neat display of the activities occurring in real-time.

It is possible to run GoPhish can on several platforms such as Mac, Linux, Windows, and Unix. The application also specifies two port numbers with which it listens for admin instructions and participants' interactions separately.

3.2.4 Server setup

The chosen server for this project is Amazon's virtual Elastic Compute Cloud (EC2) server. The selected operating system for this project is Ubuntu 18.04 LTS for its ease in deploying applications and its stability. The server system resources were too minimal to avoid the high cost of the instance. We set up the server with four access ports, each serving different purposes. Port 80 and 443 provided standard HTTP and HTTPS access, respectively. Port 22 provided SSH access for the remote configuration of the server. Port 8080 provided web access for admins to interact with the GoPhish software. We set up port 8080 and port 22 to receive requests solely from the admin's IP address while the other HTTP and HTTPS ports were open for connection from any IP address.

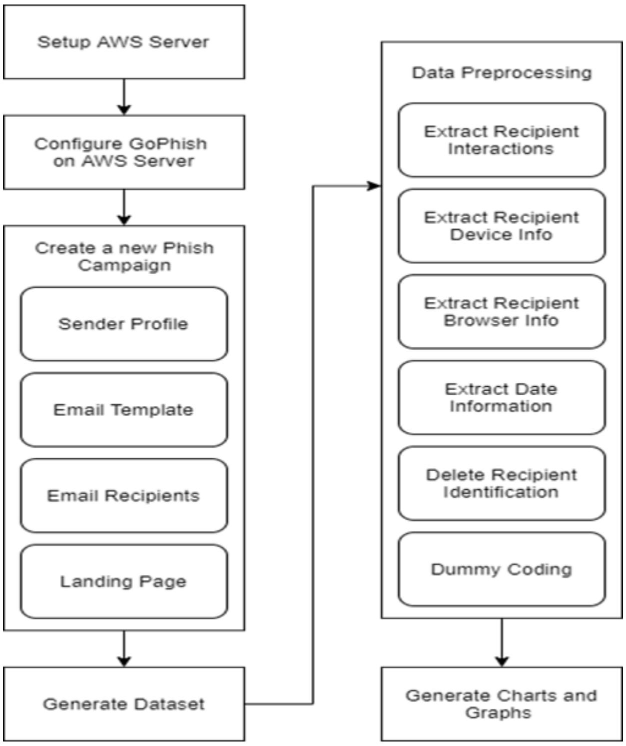
Setup AWS Server
Configure GoPhish on AWS Server
Create a new Phish Campaign
Sender Profile
Email Template
Email Recipients
Landing Page
Generate Dataset
Data Preprocessing
Extract Recipient Interactions
Extract Recipient Device Info
Extract Recipient Browser Info
Extract Date Information
Delete Recipient Identification
Dummy Coding
Generate Charts and Graphs

Figure 2. The research methodology flowchart

a. GoPhish SETUP

We performed remote server configuration through Bitvise SSH Client installation on the Windows platform. A new profile was set up on Bitvise to handle the store settings of this instance. The AWS service created the public and private key pairs for authenticating SSH connections stored locally in a folder designated entirely to the project. We set the user policy only to authorize the system admin. We used a terminal window provided by Bitvise to run remote configurations. Initial setup of the Ubuntu instance, including password authentication and user policies. We used a new directory to store all GoPhish files downloaded from its GitHub repo. A snippet of the configuration file for GoPhish [22].

After unzipping, modifications were made to the program's configuration file to allow it to listen to requests from all IP addresses directed to the specific port numbers 80 and 8080. Port 8080 listens for requests from an IP address specified in the virtual server's security group. The admin port is also set up with TLS through SSL, allowing for a secure connection between the admin's browser and the virtual server. This setup contains a certificate and public key signed by a Certificate Authentication (CA). The CA is the use of an electronic Certificate to identify a user, machine, or device before giving permission to access a network, resource, or application. The software was configured to listen to HTTP port 80 for incoming requests from all internet protocol addresses and preset it in the virtual server security group. Extra configuration was required to bind the application to port 80. Service was created on the server to run the software and bind port 80 to it at startup.

After launch, the software sets up the admin webpages on port 8080 and a default username and password. A new password was set to ensure extra security on the admin server. At this point, the software setup is complete and ready for deployment.

3.2.5 Data cleaning

We performed some cleaning operations to extract practical information from the datasets properly. The following sections detail each data cleaning process performed on the dataset and the cleaning contact details are as follows.

All identifiable user information was removed from the dataset, including name, email address, internet protocol address and GPS coordinates of the internet protocol Only recipients' colleges and levels were required for this study and hence would be extracted from the dataset along with other fields. In this use case, the University consist of four (4) different colleges which are: College of Engineering (COE), College of Science and Technology (CST), College of Business and Social Sciences (CBSS) and College of Leadership Development Studies (CLDS).

3.2.6 Extracting unique ID

Regular expressions were used extensively to determine patterns in the payload of the request sent by recipients' devices. A regular expression is a sequence of characters used to identify specific characters in an arrangement of characters such as strings and texts [23].

The unique I.D. was not readily available in the raw events file and was required to be extracted from the interaction details field in the request's payload sent to the virtual server.

3.2.7 Extracting recipient interactions

A formula was created to record each recipient's first interaction using their unique I.D as a search criterion from the new raw events sheets named 'Result on Email Interaction'.

The formula for email opened required extra care, given that some emails are opened periodically by the mail service provider. A general pattern was discovered with these server events. These requests seemed to originate from a Microsoft Edge user agent. They would run for several mails unevenly distributed across a timeframe, usually between the time the email was sent and an hour afterwards. To reduce its effect on the dataset, open email events that ran in quick successions with Edge browsers were separated from the database. Due to this email service, open events are represented in this study with some uncertainty.

A second formula was used to record the time of the first interaction performed by the recipient.

A third formula was run to find the total number of interactions and the total number of opens, clicks and data submissions.

3.2.8 Device and browser information

We extracted device and browser information from the user agent's details field of the raw events file and placed it in another sheet. A user agent is a string of text that describes information about the browser and device used to access a particular resource.

3.2.9 Extracting date information

To operate effectively on the DateTime data we afforded, we had to convert the ISO-8601 string format generated by GoPhish into a regular DateTime format.

We also extracted the time taken to each interaction to get a holistic view of the entire test. It involved subtracting the time at the start of the campaign from the interaction time in question.

3.2.10 Dummy coding

We dummy coded occurrences of the interactions. It is necessary to perform numerical calculations on the type of interaction. A sample of the code used to transform the types of interaction into a dummy code.

3.2.11 Datasets

Several datasets were created to store information about the recipients and their various interactions. These datasets produced the many charts and graphs seen in the result sections.

3.2.12 Dataset on individual recipients

Separate sheets were used to store data on individual students and data on their various interactions. Some fields in the student dataset include their UID, test number, level, college, email status, first interaction of each type, their own time, the total number of interactions, and several dummy coded variables.

3.2.13 Dataset on recipient interaction

As mentioned in the previous section, the second sheet contained interactions made by the recipients of the various emails. Interactions stored here included opening an email, clicking the link, and submitting data in an attempted login. Some fields in this dataset have a UID, a test number, interaction time, and its duration from the starting point. Information about the type of interaction, the device type, category (mobile or desktop) and its operation system (OS) are also present in the dataset. Applications used to interact with the email and dummy coded variables of the type of interaction inhabit the dataset.

Determining the status of the emails was relatively simple. Gmail sends an additional message whenever an email is not delivered successfully. The admin accessed all emails that were not returned quickly within a particular timeframe. The opening of these emails is recorded as an interaction in the GoPhish database. We appended a 'bounced' key phrase to emails opened with the specific timeframe, internet protocol address and user agent in the database. Manual crosschecking was also performed to minimize the risk of misclassification.

3.2.14 Survey dataset

Recipients were surveyed to understand the context in which they interacted with the phishing email. The questionnaire was arranged in the form of a test with which recipients could measure how well they performed during the test. Results from the questionnaire were stored in the same database. Some fields in the dataset include a timestamp, score, questions about their email correspondence, actions taken and their knowledge of Gmail's phish protection feature, suspicion level, and thoughts in the test overall.

4. RESULTS AND DISCUSSION

A few emails bounced out of the selected students due to invalid mail composition, while others were sent successfully. The distribution of bounced and delivered emails are shown in Figure 3. These emails bounced could be because their addresses were invalid. These could be for many reasons due to a misspelling of names, an improper arrangement of email strings or inadequate documentation of students' names on the part of the school's technical team.

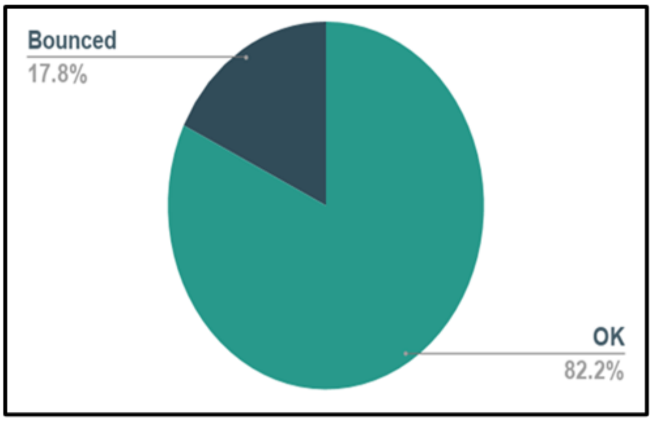

Figure 3. Percentage of bounced emails

The overall number of bounced emails were relatively low, and subsequent tests with larger samples and more effective screening can mitigate the effects of bounced emails.

Interactions per college and level

The student dataset provided several ways of looking at the dataset. Figures 4 to 8 show the relationships between the students' colleges and level with their nature and interactions.

From these Figures the percentages of interactions made by individual students are derived. Only the first interactions are included in these percentages. Comparing single interaction charts and total interactions per college, we see that multiple students repeatedly interacted with the emails. Therefore, it is necessary to separate the first interaction made by students to prevent skewing of the results. From Figures 4 to 8 we can notice a general trend in the interaction with phish emails. A more significant percentage of students opened their respective emails than clicking the link and submitting data.

The survey representing 50% of the sample shows that the recipients were more likely to involve their peers before further interacting with information from the school, as seen in Figure 9.

Recipients clicked the link more times than they performed other interactions. The email link directs the user to a cloned page on the dedicated server. After an attempted login, the software redirects the user to the original school login page, as if the recipient inputted the wrong credentials. From the survey result in Figure 10, 25% of the respondents attempted to log in via the link.

The survey also questioned respondents on their awareness of phish protection tools on the school email platform provided by Gmail. From Figure 11, 80.6% of the respondents were unaware of these features. None of the emails was reported as phish during the test, attesting to this data visualized.

Email Opened	Clicked Link	Submitted Data
🟦	🟥	🟨

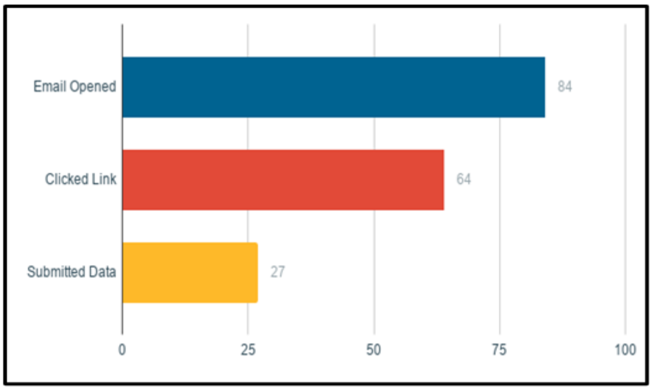

Figure 4. Total interaction of student with the phishing email

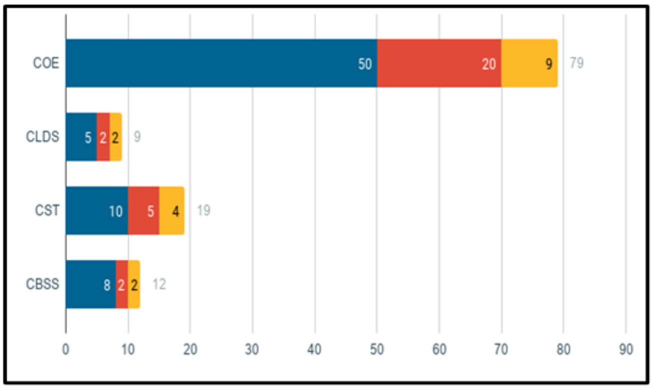

Figure 5. Single interactions per college

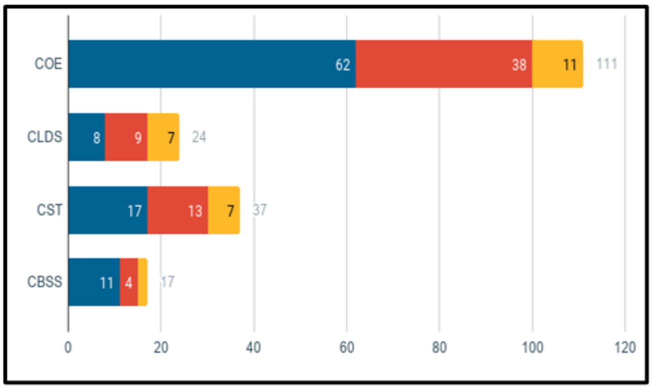

Figure 6. Total interactions per college

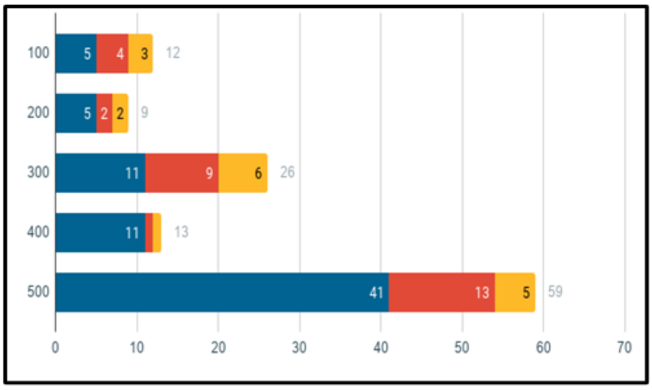

Figure 7. Single interactions per level

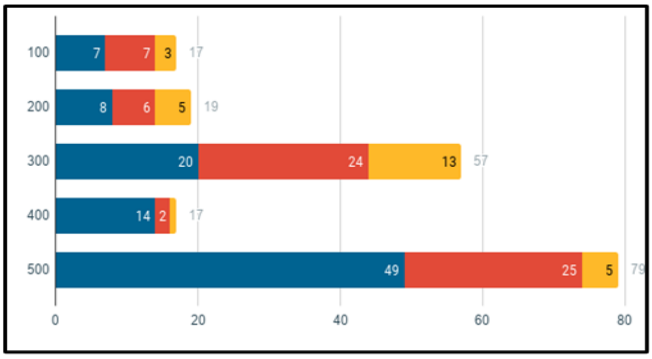

Figure 8. Total interactions per level

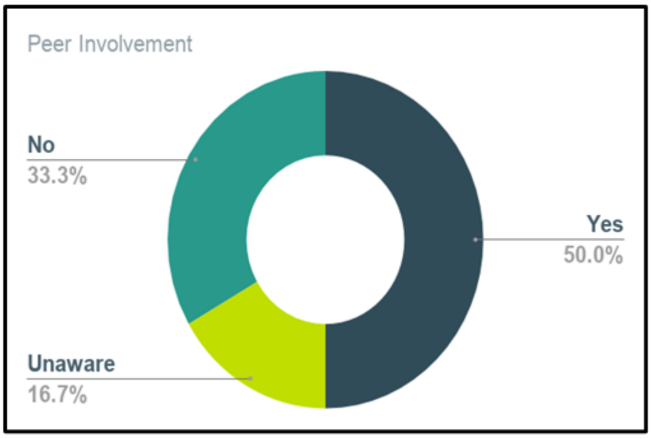

Figure 9. Peer involvement rate

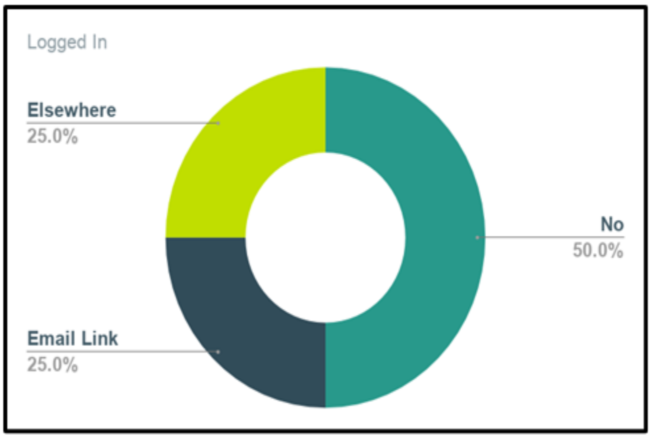

Figure 10. Login attempt

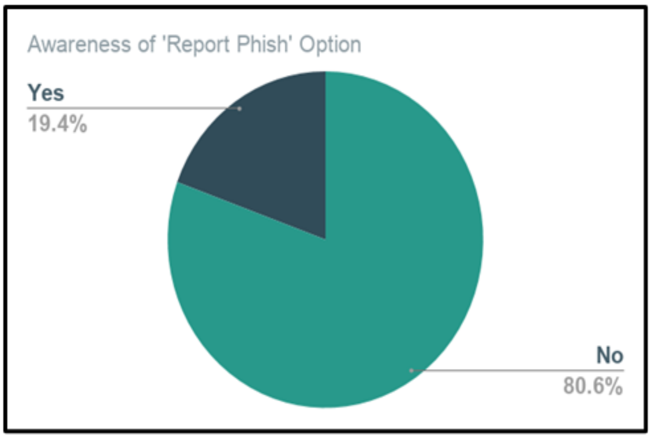

Figure 11. Awareness of security tools

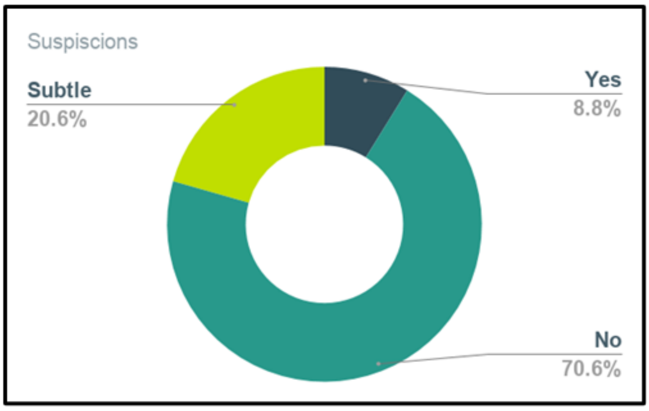

Figure 12. Phish suspicion

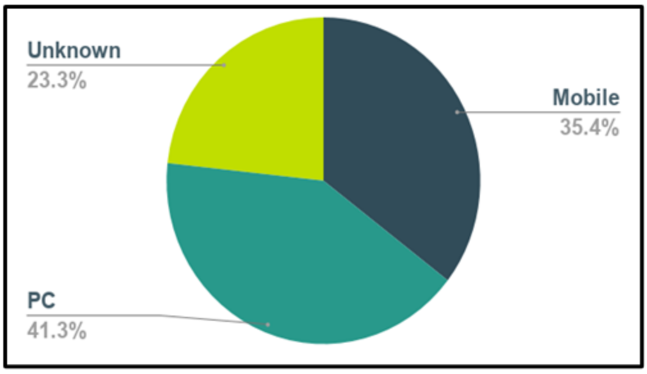

Figure 13. Distribution of device category

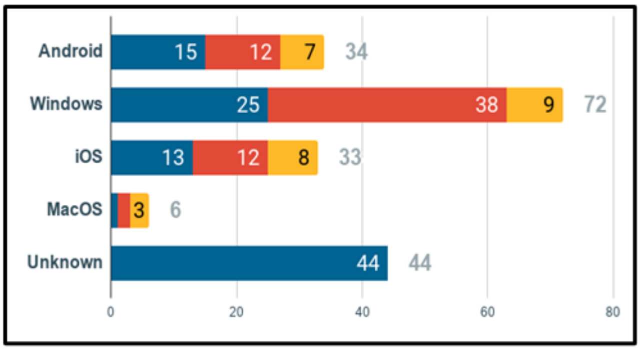

Figure 14. Distribution of operation system

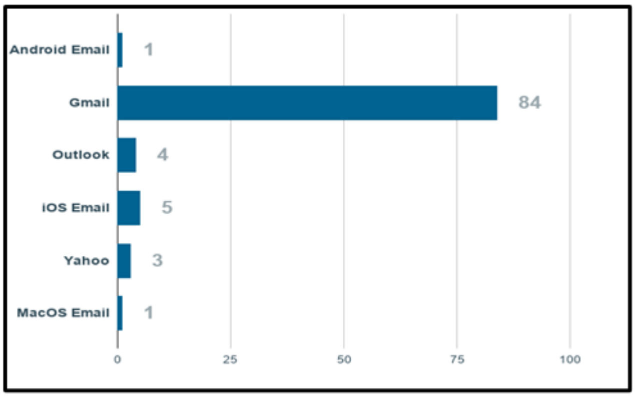

Figure 15. Distribution of email viewers

In Figure 12, we examine the suspicion rate of the survey respondents. 70.6% of the respondents did not suspect the nature of the email. Many factors could account for this response, including the lingering uncertainty in this period and the scarcity of information available to students. Relatively fewer respondents (8.8%) claimed to be utterly suspicious of the emails than those who were only marginally questionable.

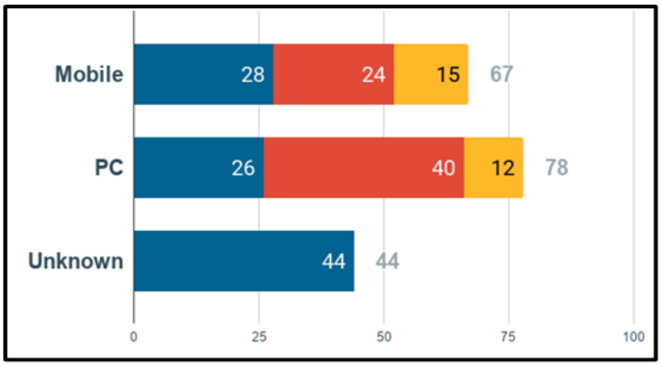

Figure 16. Distribution of device category based on interaction

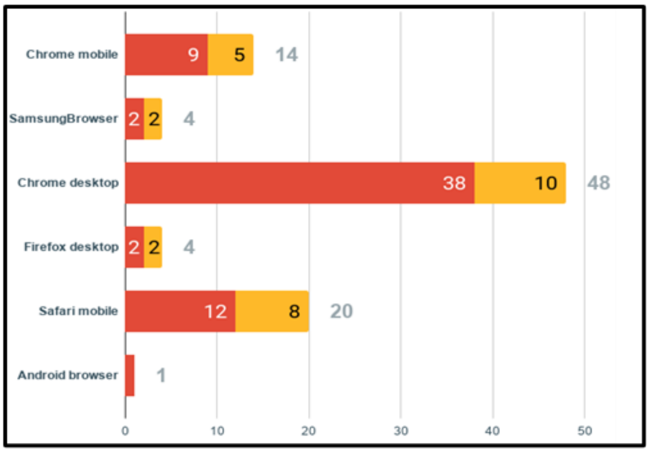

Figure 17. Distribution of browsers interactions with the emails

The system also recorded each interaction, device details making the request and the time the interaction was performed. In this section, the nature of email interactions is discussed.

User-agents are assigned to the specific browser used to request a server. Some critical information contained in the user-agent includes the operating system and its version, the type of device in some cases, and some data that uniquely identifies the client's browser.

Each interaction comes with a user-agent field. Browser and device information was extracted. Figures 13 to 17 show the distribution of devices, operation systems, browsers and mail service providers the participants used to interact with the emails.

Figures 13 and 16 show the distribution of devices based on their categories. The categories of devices are not limited to mobile and personal computers but are suitable classifications for this particular use case. The 'Unknown' in Figure 16 represents unknown device types that interacted with the emails via an email viewer such as Gmail, Yahoo and Outlook. In Figure 15, most open email interactions were performed on Gmail. This behaviour is expected as Gmail is the school's email provider. However, Gmail and Yahoo do not give information about their host device; hence, there are many unknowns in Figure 16. This policy has a profound impact on the data obtained in this study. One can only infer that PCs have the most interactions if Gmail interactions were shared between the two device categories based on their total number of subsequent interactions. The Gmail application on mobile devices have an in-built Chrome Browser that parses webpages from URLs in emails. It accounts for Chrome mobile having more interactions than most other mobile applications, as seen in Figure 17. However, Safari mobile has the largest share of mobile interactions. Safari mobile browser is only present on iOS devices and is popularly used by iPhone, iPod and iPad owners. Also, these Apple devices had more email open interactions outside of Gmail than their counterpart Android devices, as depicted in Figure 17. It indicates that more people use the inbuilt email app on iOS than on Android. On the desktop side, Chrome holds the most interactions. With Microsoft Edge recently employing Chrome as its main engine and many other browsers following suit, it is easily understood why Chrome desktop has the most interactions among its peers.

5. CONCLUSION AND RECOMMENDATIONS

This paper investigated the students' susceptibility to phishing attacks for sustainable safe email usage in an academic environment and discovered that most students are susceptible due to unawareness of this form of a cybersecurity attack. Therefore, it is necessary to educate stakeholders on the dangers of phishing attacks and prepare them to respond in those times appropriately. However, there is much debate about the ethics and accuracy of phish tests. Opting for more precision in phish tests brings up several ethical concerns, which, when strictly adhered to, may reduce the accuracy of the test [24-27]. In this study, we consulted with a leading cybersecurity expert in the school who oversaw the extent to which the test was carried out and ensured best practices were followed.

The relative success of these tests uncovers some vulnerabilities in the school's resources. One of them is the ability of hackers to clone pages of the school's websites successfully. Some websites these days include some technologies to prevent their web pages from being successfully cloned elsewhere. Some educational website such as Coursera, for one, immediately displays an error if a page is not hosted on a verified server. Implementation of these technologies across educational institution websites would frustrate the efforts of phishing attacks.

The use of mobile devices was relatively high during the tests. It shows that many students employ their mobile for school-related tasks. Therefore, optimizing the various school platforms for a better mobile experience is a worthwhile investment.

ACKNOWLEDGEMENT

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

REFERENCES

[1] Yasin, A., Abuhasan, A. (2016). An intelligent classification model for phishing email detection. arXiv preprint arXiv:1608.02196. https://doi.org/10.48550/arXiv.1608.02196

[2] Jain, A.K., Gupta, B.B. (2017). Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017: 5421046. https://doi.org/10.1155/2017/5421046

[3] Eftimie, S., Moinescu, R., Răcuciu, C. (2022). Spear-phishing susceptibility stemming from personality traits. IEEE Access, 10: 73548-73561. 10.1109/ACCESS.2022.3190009

[4] Das, S., Nippert-Eng, C., Camp, L.J. (2022). Evaluating user susceptibility to phishing attacks. Information and Computer Security, 30(1): 1-18. https://doi.org/10.1108/ICS-12-2020-0204

[5] Jain, A.K., Gupta, B.B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, 16(4): 527-565. https://doi.org/10.1080/17517575.2021.1896786

[6] 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, 27(4): 4729-4752. https://doi.org/10.1007/s10639-021-10806-7

[7] Wang, S., Liu, J. (2011). Biometrics on mobile phone. Recent Application in Biometrics, 3-22.

[8] Shahbaznezhad, H., Kolini, F., Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? Journal of Computer Information Systems, 61(6): 539-550. https://doi.org/10.1080/08874417.2020.1812134

[9] Azeez, N.A., Misra, S., Margaret, I.A., Fernandez-Sanz, L. (2021). Adopting automated whitelist approach for detecting phishing attacks. Computers & Security, 108: 102328. https://doi.org/10.1016/j.cose.2021.102328

[10] Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. Computers & Electrical Engineering, 96: 107546. https://doi.org/10.1016/j.compeleceng.2021.107546

[11] Priya, S., Selvakumar, S., Velusamy, R.L. (2021). Evidential theoretic deep radial and probabilistic neural ensemble approach for detecting phishing attacks. Journal of Ambient Intelligence and Humanized Computing, 1-25. https://doi.org/10.1007/s12652-021-03405-4

[12] Jain, A.K., Gupta, B.B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems, 16(4): 527-565. https://doi.org/10.1080/17517575.2021.1896786

[13] Internet Crime Report (IC3). Report 2018. https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219, accessed on 16. Sep., 2020.

[14] John, S.N., Noma-Osaghae, E., Oajide, F., Okokpujie, K. (2020). Cybersecurity education: The skills gap, hurdle! In: Daimi, K., Francia III, G. (eds.), Innovations in Cybersecurity Education. Springer, Cham. https://doi.org/10.1007/978-3-030-50244-7_18

[15] Andrić, J., Oreški, D., Kišasondi, T. (2016). Analysis of phishing attacks against students. 2016 39th International

Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1423-1429. https://doi.org/10.1109/MIPRO.2016.7522363

[16] Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10): 94-100. https://doi.org/10.1145/1290958.1290968

[17] Toolan, F., Carthy, J. (2009). Phishing detection using classifier ensembles. 2009 eCrime Researchers Summit, pp. 1-9. https://doi.org/10.1109/ECRIME.2009.5342607

[18] Senthilkumar, K., Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. IOP Conference Series Materials Science and Engineering, 263: 042043. https://doi.org/10.1088/1757-899X/263/4/042043

[19] Kim, E.B. (2013). Information security awareness status business college: Undergraduate students. Information Security Journal: A Global Perspective, 22(4): 171-179. https://doi.org/10.1080/19393555.2013.828803

[20] Tak, G.K., Ojha, G. (2013). Multi-level parsing based approach against phishing attacks with the help of knowledge bases. International Journal of Network Security & Its Applications, 5(6): 15-30. https://doi.org/10.5121/ijnsa.2013.5602

[21] Abbasi, A., Zahedi, F.M., Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), pp. 169-174. https://doi.org/10.1109/ISI.2016.7745462

[22] Wright, J. (2019). GophishOpen-Source Phishing Framework. https://getgophish.com/.

[23] Goyvaerts, J., Levithan, S. (2012). Regular Expressions Cookbook. O'Reilly.

[24] Jakobsson, M., Ratkiewicz, J. (2006). Designing ethical phishing experiments: A study of (ROT13) rOnl query features. Proceedings of the 15th international conference on World Wide Web, pp. 513-522. https://doi.org/10.1145/1135777.1135853

[25] Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76(1): 139-154. https://doi.org/10.1007/s11235-020-00733-2

[26] Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3: 563060. https://doi.org/10.3389/fcomp.2021.563060

[27] Sadiq, A., Anwar, M., Butt, R.A., Masud, F., Shahzad, M.K., Naseem, S., Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5): 854-864. https://doi.org/10.1002/hbe2.301