Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria

Maureen Ifeanyi Akazue[1], Arnold Adimabua Ojugo[2], Rume Elizabeth Yoro[3], Bridget Ogheneovo Malasowe[4], Obinna Nwankwo[5]
[1]Department of Computer Science, College of Science, Delta State University, Abraka, Nigeria
[2]Department of Computer Science, College of Science, Federal University of Petroleum Resources, Effurun, Nigeria
[3]Department of Computer Science, Faculty of Information Technology, Dennis Osadebey University, Asaba, Nigeria
[4]Department of Computer Science, Faculty of Computing, University of Delta, Agbor, Nigeria
[5]Department of Computer Science, College of Computing & Telecommunications, Novena University, Ogume, Nigeria

Article Info

Article history:

Received Jul 19, 2021
Revised Aug 24, 2022
Accepted Sep 19, 2022

Keywords:

Cybercrime
FUPRE undergraduates
Malicious contents
Phishing susceptibility
Socially-engineered attacks

ABSTRACT

In our exploratory quasi-experimental study, 480-student were recruited and exposed to social engineering directives during a university orientation week. The directives phishing attacks were performed for 10 months in 2021. The contents attempted to elicit personal user-data from participants, enticing them to click compromised links. The study aimed to determine cybercrime risks among undergraduates in selected universities in Nigeria, observe responses to socially-engineered attacks, and explore their attitudes to cybercrime risks before/after such attacks. The study generalized that all participants have great deal awareness of cybercrime, and also primed all throughout study to remain vigilant to scams. The study explores various types of scam and its influence on students' gender and age on perceived safety on susceptibility to phishing scams. Results show that contrary to public beliefs, none of these factors were associated with scam susceptibility and vulnerability rates of the participants.

Corresponding Author:

Arnold Adimabua Ojugo
Department of Computer Science, College of Science, Federal University of Petroleum Resources
Effurun, P.M.B. 1221, Delta State, Nigeria
Email: ojugo.arnold@fupre.edu.ng

1. INTRODUCTION

The daily rise in the adoption of information and communication technology (ICT) devices vis-à-vis their usage over the Internet due to its ease of use, speed, accuracy, and portability among other features have also, in turn, birthed and continued to advance socially-engineered attacks, designed to evade detection, and poised to help attackers have access to user data. Thus, user trust-level over the adoption and adaptation of ICT devices in today's digital transformation era, has become a global issue [1]. Digital transformation seeks to integrate technology into various facets of life-endeavors and to fundamentally change how we operate/deliver value-chain to clients. It proposes a culture change for businesses to constantly challenge, experiment, and get comfortable with failure. And as more users become connected to internet-based supports, it also opens them up to avenues of exploitation harnessed by adversaries via socially-engineered threats and attacks [2].

Socially-engineered attacks are an old paradigm that continues to steadily grow, with no end in sight. Its continued growth hinges on the human nature of trust instincts and insatiable wants that attacker ultimately exploits to steal user data. These attacks reveal how vulnerable a connected device is [3], as they are designed to exploit human errors and insatiable traits resulting from relationships and operations between connected users. Thus, adversaries will continue to exploit its weakest links such as relations and human errors. A reason why socially-engineered attacks will continue to rise [4]. Common methods adopted by such attackers include (but are not limited to) phishing and spamming. These provide an attacker with an attractive entry point of contact to the victims' compromised system and provide a pilot cum pivot point for attack spread cum propagation [5]. With such attacks targeted at Internet-connected user devices as well as with over 200-percent adoption of smartphones, many users have become susceptible, vulnerable targets as well as victims alongside the range of complications to work-related and business issues on the exposure of sensitive user-data to these attackers or adversaries [6].

2. LITERATURE REVIEW

2.1. An overview of phishing

Socially-engineered attacks use technical subterfuge to defraud a victim of their data by posing as a trusted identity. The messages (also called spam) involve harmless advertising via unsolicited emails, SMS, or network messages, and contain mechanisms to exploit recipient data [7], [8]. The adoption of spam is due to its low-volume-and-high-value target successes, and distribution ease [9]. Spams today, has an estimated daily volume of over 612-billion [4], which makes up over 85% of the daily global traffic used by spammers on potentially, vulnerable recipients' databank with ineffective countermeasures to defend themselves against such evolving attacks [10]–[12].

Phishing uses multiple means such as spoofed emails, weblink forgeries, phone calls, man-in-middle chat, and covert redirect, to convince a user to divulge confidential data or indulge in fraudulent transactions. An effective and favored variant of phishing is spear phishing. It uses targeted mail with access links to cleverly persuade potential victims, and redirect them to spoofed websites containing malware that aim to compromise user data. Another variant is SMS-phishing (or Smishing), which tricks a user into downloading malware onto his cellular phone or other mobile devices [13]. Most phishing redirects user traffic to a fake site, by either changing the host's file on a victim's device or by exploiting the vulnerability in the domain name service server software. Thus, it allows an adversary to install malware onto a user's device and redirects the user to a fraudulent site without their consent and/or knowledge [14]–[18].

Phishing involves an attacker redirecting a user's access to malicious content shared from spoofed websites from a viewpoint that such sites are legitimate and trustworthy sources [19]. A typical phishing attack consists of 3-elements: lure, hook, and catch, and explained as thus [20]–[23]: i) lure message is received by the potential victim as originating from a legitimate source. Its reliability is strengthened via exploiting user curiosity, fear, and empathy, ii) a hook is the compromised link/attachment included in the message, and iii) the catch involves an attacker obtaining user private data.

This may appear simple; But, the techniques and procedures constantly evolve, to reflect new social trends [24], that use new methods to bypass security, and evade detection [9]. Its continued spread over the internet has allowed attacks to vary in frequency and diversity, enhancing their likelihood of success [20]. Thus, phishing is often positioned as trusted entities seeking to defraud a victim (via mail, SMS, or instant network messages). Its characteristics include: i) message often makes unrealistic threats/demands via various forms of intimidation targeted at a user's psych, ii) there is always a catch, iii) there are often missing data with spelling errors and poor grammar, iv) there is often a mismatch in URL (uniform resource locator) to redirect users to a faked website, and v) messages often demands sensitive, confidential user data [5].

2.2. Malicious web-contents

With the internet advancing as an efficient and effective means of data sharing and dissemination, many adversaries have since begun to use the medium as a tool for the propagation of malicious content. Thus, access to malicious content over the Internet has also since become a multi-billion dollar challenge that continues to impact a variety of users daily [25], [26]. Despite the plethora of continued studies that sought to improve detection techniques using filtering and classification frameworks, more users continue to fall prey to such deceptive scams. This is attributed to the fact that websites are rippled with malware that presents themselves as unsolicited unsecured adverts and/or hides in third-party legitimate software [4], [27].

Hale *et al.* [27] further notes that many of these attacks today are targeted at mobile platform and users with over a million malicious files sent daily. Thus, malicious contents are so pervasive and barraged that some percentage eventually makes it to a user's screen. However, they further posited that once on screen for a certain user, prevention and mitigation is no longer a question of technical measures; Rather, control is now ceded to the user. However, their level of suspicion, control of emotions, and awareness of these attack menaces become the critical components required to ascertain the success or failure of such attacks. Understanding the human emotions, personality traits, and behavior as factors and cues that drive success or failure includes the desire for immediate gain, the desire to help people, and the desire to be liked.

All of these suggest that certain individuals have 'victim personality traits' that make them more vulnerable as well as susceptible to scams [13], [28]; And such victims, may fall repeatedly to a scam.

2.3. Classifying malicious contents

Various research has begun to investigate how various aspects of psychology seek to compromise data, even with a plethora of cyber-security measures in place. One such concern is how the Internet is gradually replacing normal social activities as users now engage themselves with web content as tools to compensate for loneliness and social seclusion. Halevi *et al*. [29] used the 5-D traits to include: neuroticism, extroversion, [30], [31], and consciousness. It has been successfully used to model and observed students' responses to socially-engineered attacks vis-à-vis exploring their attitude before/after a phishing attack [6].

Hale *et al*. [32] used CyberTrust (a game-based simulated learning tool) with web content that sought to investigate how users perceived and trusted different types of content. They investigated the trustworthiness of contents by characterizing malicious content using a set of design factors grouped into sophistications (a feat that ensures difficulty in identifying malicious contents), and degradations (another feat that makes it easier to identify malicious contents). Thus, with such web contents there exists relevant lures and cues to persuade user trust with the set of design factors, which are linked to taxonomy elements, posied to ask users questions that sought to retrieve the existence of relevant lures and/or cues within the malicious content to aid grouping of these contents into structural classes.

In furtherance, Hale *et al*. [27] used victimization parameters to characterize how such design factors impact both the structure of the content and the probability of how much content will victimize the user. The study sought to understand malicious web contents vis-à-vis its victimization potentials. Thus, with adequate training drafted to identify/remove gaps as well as improve user awareness/recognition of such malicious web content. They used 2-parameters namely: i) believability which identifies how sophistication increases the possibility that users will believe a message, and ii) insidiousness to measure the subtle, malicious potency of degradations, and how much they increase attack impact while remaining undetectable to users.

3. MATERIAL AND METHOD

3.1. Sample demographics

A common feat that influences phishing/scam susceptibility is demographics (gender, age). Previous studies have identified users between the ages of 18-29 as the most susceptible vis-à-vis web content [33]–[35]; while female users between the ages of 24 to 42 were identified as being the most vulnerable [36], [37]. It has been suggested that young female adults are constantly engaged to boycott social seclusion which leads to addiction whereas, excessive online presence and dependence on social media content used are often relevant lures and cues for potential victimization by phishers [31], [38] and lead to the exposure of associates. Ojugo and Eboka [37] posit that age is linked to risky behavior, which increases the chances of these young (female) adults being phished as they have less education and caution for financial risk [1], [39]. Goel *et al*. [3] postulated that women are easier to entice to open phishing emails, but are equally as capable and proficient as men in detecting a deceptive message. We selected a total of four hundred and eighty (480) students from the southern region in Nigeria, who were recruited.

3.2. Technical procedures for web-content classification

The sophistication and degradation in [32] were coined as pointers for various lures/cues present in malicious content. Afterwards, the design factors were refined and mapped to taxonomy elements, categorized into user-perceivable feats commonly found in a phishing attack to include these 3-classes: the web content, its context, and its contract which is explained as: i) a web content seeks to classify elements of both textual and visual nature in a web content such as the appearance of a padlock icon on a html link to shows and indicate a secure site, and also describe features that describes also how the domain is structured, the use of URLs, e-mail attachment(s), greetings for an email, and signatures, ii) content context helps us classify taxonomy elements that includes structural use of a language and its tone, the nature of the grammar and spelling(s), and origin/intended recipient of a message, and iii) the contract groups and focus on the value proposition of a trust decision. Each element in each class includes whether a message asks for personally identifiable information or offers some benefit in return. We adapt Hale *et al*. [27] to classify web contents into sophistication and degradation as in Tables 1 and 2. Experiment lasted for 10-months, and all participants signed consent forms.

Table 1. Website malicious contents sophistication lures and cues

ID	Sophistication lures/cues
S01	Use of legitimate logos on website
S02	Duplicates the look and feel of legitimate website
S03	Provides contextual or personal information
S04	Legitimate links where malicious contents can be hidden
S05	Provides a sense of previous trust
S06	Mimics intercepted communication
S07	Formal grammar and style in writing without typos
S08	Uses official account usernames
S09	Identifies a known group of recipients
S10	Recognizes file types as downloads/attachments

Table 1 identifies sophistication contents that are hard; Thus, complicate user trust decisions. It makes mapping of taxonomy in [17] (given the length constraints) to yield the sample list as thus:
S07: free grammar and style in writing: uses generic greetings instead of receiver names

- *Context-Language-Tone-Professional*

S10: unrecognize file types as downloads/attachments: file extension is unknown

- *Content-URL Links-Obfuscated*

Table 2. Malicious content sophistication lures and cues for malicious websites

ID	Degradation lures and cues
D01	Suspicious URL identifying the sender or site
D02	Contains suspicious links and/or Pop-ups
D03	Poor spelling and/or grammar issues
D04	Uses odd greetings and/or catchy phrases
D05	Contains unnecessary warning messages
D06	Involves people posing as friends or acquaintances
D07	Uses generic greetings instead of receiver names
D08	References obscure products
D09	Information or item prices too good to be true
D10	Missing security designators, e.g. https padlock
D11	Directly requests the input of personal data
D12	Uses of iframes or overlays on legitimate sites
D13	Contains survey requests with links
D14	Appeals to an emotion, e.g., urgency and greed
D15	Includes suspicious attachments in email
D16	Missing links or buttons that should be present
D17	Offers ambiguous access to a product
D18	Continuous messages/posts of similar content from the same person
D19	Unrecognized file types as download/attachments

Table 2 are degradation samples that may be well-known to a user. Users, often associate these contents as potentially malicious. Leading examples to the degradation taxonomy are as:
D05: contains unnecessary warning

- *Context-Language-Tone-Unnecessary*

D14: content appeals to user emotions such as greed, and time urgency

- *Context-Language-Tone-Professional*

D09: item price is too good to be true

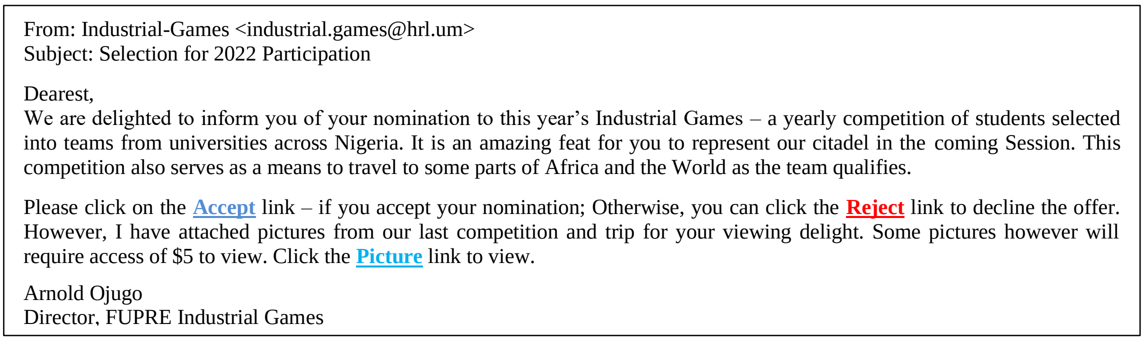
- *Contract-Offer-Monetary-Products*

3.3. Retrieving malicious contents/data gathering

When conducting such an experiment, it is important to ensure that contents retrieved are relevant to what might be seen in real scenarios. Thus, to gather crucial/relavant user e-mails, Gudkova *et al*. [6], Kornor and Nordvik [8] provides us with sample tailored, generic and spear-phishing emails collected from various participants' account(s) as contents undetected by spam-filters. We retrieved contents phishing contents from phishtank site, a repository via which we extracted 25-newest phishing websites. We also collected posts from Facebook and Instagram accounts of participants using terms like "free cash", "You have won", "you were recommended" amongst other contents. Once gathered, degradation and sophistication were designed on each content.

The degradation and sophistication of content attempts to lure participant to click on the link(s), which is a real scam situation have been compromised. All other spear phishing emails were created, and varied from students to student based on personal user-data as available online. Some user-data could not be collected due to either the absence of social media presence for such users, and/or user restriction with their social media privacy settings. Also, accordingly, highly tailored emails were created only for students with adequate amounts of user data, and online presence cum information (N=25).

The aim of the experiment is to understand how users make trust decisions, identify their deficiencies, and adapt training or awareness so as to prevent user victimization which may further leave their associates compromised (in this case, friends, and relatives). The experiment is presented as a mixture of normal and malicious content to simulate real-time interactions with an email client, web browser, and social network. The experiment follows a scene where a participant must respond to phishing and malicious insider tactics to keep them quite interested and engaged online (increased online presence). Simulation provides the participant with rich interaction capabilities that allow them to hover over links and attachments and see natural browser-like behavior. Figure 1 shows emails with links to social media posts and website content samples. Underlying each user interface (as seen in this sample mail) is a *trust decision box* that allows users to either trust (*blue for accept*ing) or not trust (*red for reject*) using content-specific decisions.



From: Industrial-Games <industrial.games@hrl.um>
Subject: Selection for 2022 Participation

Dearest,
We are delighted to inform you of your nomination to this year's Industrial Games – a yearly competition of students selected into teams from universities across Nigeria. It is an amazing feat for you to represent our citadel in the coming Session. This competition also serves as a means to travel to some parts of Africa and the World as the team qualifies.

Please click on the **Accept** link – if you accept your nomination; Otherwise, you can click the **Reject** link to decline the offer. However, I have attached pictures from our last competition and trip for your viewing delight. Some pictures however will require access of $5 to view. Click the **Picture** link to view.

Arnold Ojugo
Director, FUPRE Industrial Games

Figure 1. Sample malicious game email-1 content

3.4. Web-content activity and correlation

To correlate activity, students were asked what messages they uploaded online, the frequency of their uploading, the number of images posted, and their privacy settings. The survey uses self-reported data, and is back-checked for accuracy. We extracted personal data from participants. Value '1' is assigned to all elements posted that falls under the various taxonomy. These variables were all added together, so as to create the study's web-content data. The log-value showing both the participant's number of weekly online presence as well as the access to malicious web content, were collated. We compute updated variables via (1) [38], [40].

$$SN_{posts} = log_{10}(TotalEntry + 0.001) \quad (1)$$

The same calculation was computed for the total number of access to sophistication and degradation classes content. Overall participant(s) data statistics are found in Table 3 describing the mean, standard deviation, and dyads (i.e. strength in the relationship between any two users for each participants).

Table 3. Overall participant statistics

N	Dependent variables	Mean	Std	$+D_i$	EL_i	No activity
1	Data/Messages	12.7	0.94	0.89	0.21	14%
2	Photos	441	0.87	0.89	0.10	18%
3	Posts	15.9	0.42	0.43	0.19	22%
4	Privacy settings	10.3	9.34			

We have that each participant's page builds up with a friend and possible acquaintances connection leading up to the personal network of such a participant, which in turn allows data such as photos, messages, and posts to be shared over such social networking sites. From Table 2, 14-to-22-percent of the participants do not post any data nor do they reply to or share messages, posts, and photos that appear on their social network pages. The study also observed that the privacy settings average was in the middle range of 10.3 out-of-40, where 0 is the most conservative [41], [42].

3.5. Study hypothesis

Previous studies have successfully shown that some factors are responsible for phishing susceptibility of users as well as vulnerability of client devices. These have been attributed to personality traits, malicious media contents, online presence, and demographics. In furtherance to these, we wish to investigate other critical factors and features as thus:

- H_1: age factor results in lesser awareness of sophistication and degradation as well as training of malicious content classification higher vulnerability, and allow students to share private data online
- H_2: students' complacency with privacy settings in accessing sophistication and degradation content over social media leaves them vulnerable as scam victims.

4. RESULTS AND DISCUSSIONS

4.1. Resultant hypothesis

Our study seeks to find the probability distribution and correlation for the hypothesis therein stated. H_1: age factor results in lesser awareness of sophistication and degradation as well as training of malicious content classification higher vulnerability, and allow students to share private data onlinen. Evaluating the first hypothesis as to the increase in scam vulnerability as the mails became increasingly tailored to the participants and spear-phishing, we used Wilcoxon signed-rank test. The results therein, revealed no significant differences in scam susceptibility between generic and tailored scams (Z=-.546, p=.585), tailored and spear phish scams (Z=.000, p=1.00), or generic and spear phish scams (Z=-.646, p=.518), as thus, the hypothesis was not supported. Going further, we sought to assess if the rate of these participants' susceptibility to scams was associated with gender as well as age/status using Fisher's Exact Test (see Figure 2 and 3 respectively) with p=.57. Result showed that there is no significant differences in gender and other traits, as being the reason for their susceptibility and vulnerable rates to scams.

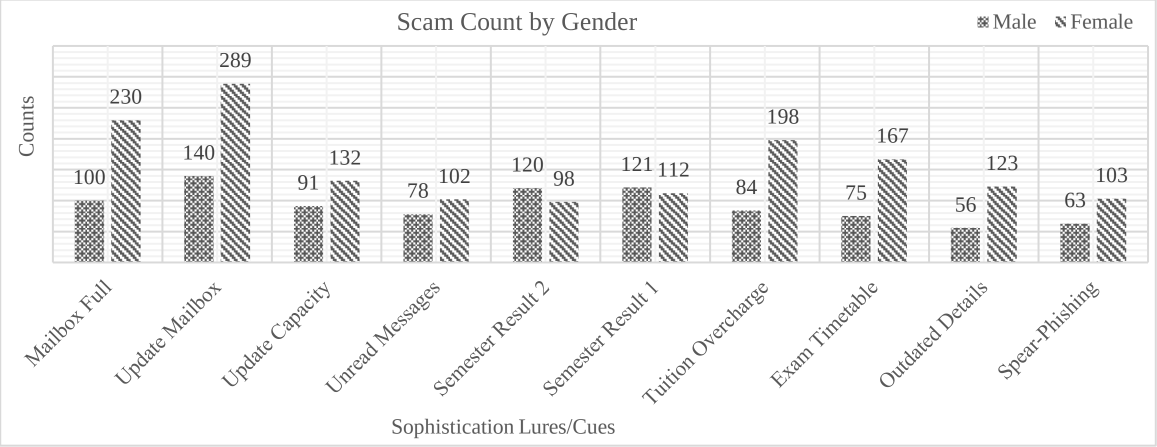


Figure 2. Cues for students scammed by gender

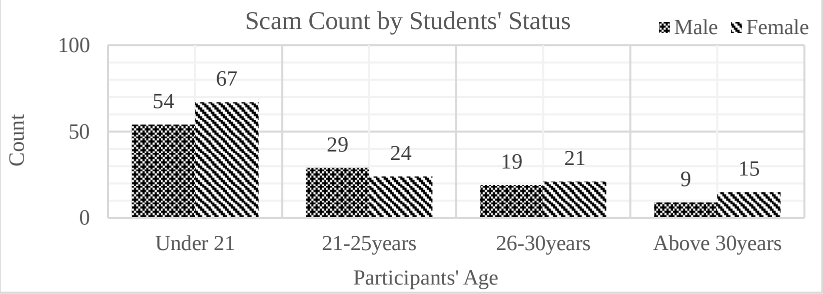


Figure 3. Cues for students scam by Age/Status

H_2: participants' complacency with privacy settings in accessing sophistication and degradation content over social media leaves them vulnerable as scam victims. Figure 4 shows that overall result appears to have no trend in the relation between the type of phishing or scam used and the susceptibility of the victims. In furtherance, results shows that many of the participants were most susceptible to the phishing email (scam) with the heading "Mailbox Full", "Update Mailbox" and "Update Mailbox Capacity" (i.e. generic scams). Figure 5 shows that participants trusted the phishing mail (and were also found to be) susceptible to the mail with the tag "Semester Result". These, were phishing attacks tailored to specific participants' via their institution mail. This is in agreement with [43], [44].

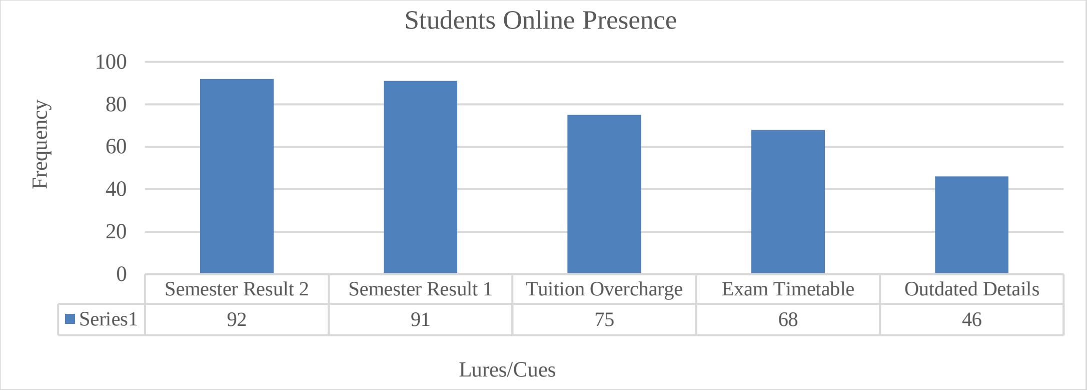


Figure 4. Students who clicked *Trust* on social network

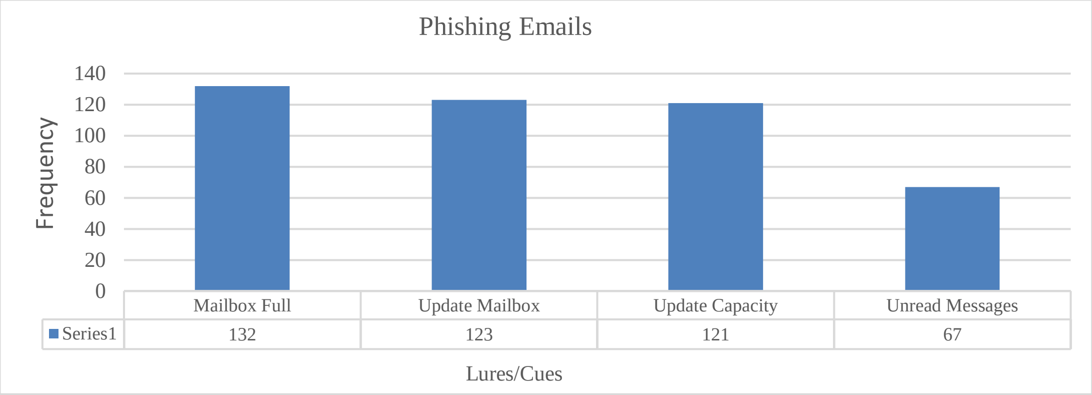


Figure 5. Students who click *Trust* on email

4.2. Discussion of findings

This study was designed to assess the rate of susceptibility and vulnerability among undergraduates in selected universities in Nigeria. At the heart of this study, was the interest in how to scam type and campus demographics influenced susceptibility rates among students. Though, relevant literature(s) suggests that scam susceptibility may be influenced by the level of specificity in a scam. That is, users are more likely deceived by scams, tailored to their circumstances (spear-phishing) compared to those with generic-content. Also, other variables have been flagged as potential contributors to scam susceptibility (includes but not limited to) gender, age, and status. Broadhurst *et al.* [45] agree with these and state that besides these, other variables including the level of cybercrime awareness, IT competence, and gender are also flagged as potential contributors therein.

To explore these possibilities, participants were exposed to social engineering directives in the form of fake email attacks that attempted to either elicit personal data from participants or compel them to click links that could contain malware in the real world. In addition, to determine these participants' rate of susceptibility to tailored and spear phishing attacks rather than generic attacks, email content was engineered to replicate these three (3) scams types (generic, tailored, and spear phishing) with the concept of lure, hook and capture. These scam types differed in their level of personal relevance (specificity) to each of the participants [14].

Results showed no relations between participants' susceptibility and scam types as participants were not found to be more susceptible to any particular phishing attack. However, email content that deceived most participants, provided insight into scam types that may succeed. And, the most successful attack were students' updated mailbox. This email's success was due to its being sent during the first/second semester exams for 2019/2020 session. With these, we proffer 3-likely explanations namely: i) that due to the upcoming exams, portal info as regularly sent to the student's mailbox gave this mail high relevance, ii) exams are critical matter, and thus, became a panacea for the increased susceptibility, and iii) exams generally instill fear in students and this mail's urgent requirement for participants to take action and ensure that with the receipt of the mails therein, they are aware of the when and where their exams were to take place. These among others, we posit are reasons that may have compelled participants to click on the link.

5. CONCLUSION

We believe in general that the success of a fake scam can be richly attributed to a combination of personal relevance and fear. This indicates that individuals in the real world may be more susceptible to scams that tap into salient life circumstances and instill a sense of fear and urgency. The ever-increasing magnitude and impact of phishing have necessitated studies on minimizing attacks among students and the broader public. Also, understanding factors that influence susceptibility will help users to protect themselves against phishing and other forms of cybercrime. Also, tackling the many complex events linked to 'cybercrime' requires effective training and campaign among undergraduates and the general public as well as require methods of attaining knowledge via processes that sought to explore ways to observe victimization in a real-world setting.

REFERENCES

[1] A. A. Ojugo and A. O. Eboka, "Empirical bayesian network to improve service delivery and performance dependability on a campus network," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 3, pp. 623–635, 2021, doi: 10.11591/ijai.v10.i3.pp623-635.

[2] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: factors impacting susceptibility to phishing attacks," *Human-centric Computing and Information Sciences*, vol. 6, no. 8, Dec. 2016, doi: 10.1186/s13673-016-0065-2.

[3] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems*, vol. 18, no. 1, pp. 22–44, Jan. 2017, doi: 10.17705/1jais.00447.

[4] A. A. Ojugo and R. E. Yoro, "Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1498–1509, 2021, doi: 10.11591/ijece.v11i2.pp1498-1509.

[5] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers and Security*, vol. 73, pp. 345–358, Mar. 2018, doi: 10.1016/j.cose.2017.11.015.

[6] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, "Spam and Phishing in Q3 2017," Securelist, 2017, viewed 25 Jan. 2018, [Online] Available: securelist.com/spam-and-phishing-in-q3-2017/82901/

[7] A. A. Ojugo and D. A. Oyemade, "Boyer moore string-match framework for a hybrid short message service spam filtering technique," *IAES International Journal of Artificial Intelligence (IJAI)*, vol. 10, no. 3, pp. 519–527, 2021, doi: 10.11591/ijai.v10.i3.pp519-527.

[8] H. Kornor and H. Nordvik. "Five-factor model personality traits in opioid dependence," Biomedcentral, 2007, [Online] Available: http://www.biomedcentral.com/1471-244X/7/37.

[9] A. Ojugo and A. O. Eboka, "Signature-based malware detection using approximate Boyer Moore string matching algorithm," *International Journal of Mathematical Sciences and Computing*, vol. 5, no. 3, pp. 49–62, 2019, doi: 10.5815/ijmsc.2019.03.05.

[10] M. Alazab and R. Broadhurst, "Spam and criminal activity," *Trends and Issues in Crime and Criminal Justice*, vol. 526, no. 526, pp. 12–34, 2016, doi: 10.2139/ssrn.2467423.

[11] D. Harley and A. Lee, "Phish Phodder: is user education helping or hindering?," *Virus Bulletin Conference*, 2007, pp. 1–7.

[12] D. Irani, S. Webb, J. Giffin, and C. Pu, "Evolutionary study of phishing," *eCrime Researchers Summit*, 2008, doi: 10.1109/ECRIME.2008.4696967.

[13] C. L. Udeze, I. E. Eteng, and A. E. Ibor, "Application of machine learning and resampling techniques to credit card fraud detection," *Journal of the Nigerian Society of Physical Sciences*, p. 769, Aug. 2022, doi: 10.46481/jnsps.2022.769.

[14] J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao, "Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email," *IEEE Transactions on Professional Communication*, vol. 55, no. 4, pp. 345–362, Dec. 2012, doi: 10.1109/TPC.2012.2208392.

[15] A. Abbasi, F. Mariam Zahedi, and Y. Chen, "Phishing susceptibility: The good, the bad, and the ugly," in *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data*, ISI 2016, Sep. 2016, pp. 169–174, doi: 10.1109/ISI.2016.7745462.

[16] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, "Phishing attacks and defenses," *International Journal of Security and its Applications*, vol. 10, no. 1, pp. 247–256, Jan. 2016, doi: 10.14257/ijsia.2016.10.1.23.

[17] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a phishing target," *Telematics and Informatics*, vol. 35, no. 5, pp. 1277–1287, Aug. 2018, doi: 10.1016/j.tele.2018.02.009.

[18] W. R. Flores, H. Holm, M. Nohlberg, and M. Ekstedt, "Investigating personal determinants of phishing and the effect of national culture," *Information and Computer Security*, vol. 23, no. 2, pp. 178–199, Jun. 2015, doi: 10.1108/ICS-05-2014-0029.

[19] H. Kornør and H. Nordvik, "Five-factor model personality traits in opioid dependence," *BMC Psychiatry*, vol. 7, no. 1, Dec. 2007, doi: 10.1186/1471-244X-7-37.

[20] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 1–31, May 2010, doi: 10.1145/1754393.1754396.

[21] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *International Journal of Modern Education and Computer Science*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.

[22] D. Modic and S. E. G. Lea, "How neurotic are scam victims, really? the big five and internet scams," *SSRN Electronic Journal*, no. 2011, pp. 1–32, 2014, doi: 10.2139/ssrn.2448130.

[23] A. A. Ojugo, A. O. Eboka, R. E. Yoro, M. O. Yerokun, and F. N. Efozia, "Hybrid model for early diabetes diagnosis," *Proceedings - 2015 2nd International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2015*, vol. 50, no. 3–5, pp. 55–65, 2016, doi: 10.1109/MCSI.2015.35.

[24] D. Huang, Y. Lin, Z. Weng, and J. Xiong, "Decision analysis and prediction based on credit card fraud data," in *ACM International Conference Proceeding Series*, Apr. 2021, pp. 20–26, doi: 10.1145/3478301.3478305.

[25] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The design of phishing studies: Challenges for researchers," *Computers and Security*, vol. 52, pp. 194–206, Jul. 2015, doi: 10.1016/j.cose.2015.02.008.

[26] C. B. Mayhorn, A. K. Welk, O. A. Zielinska, and E. Murphy-Hill, "Assessing individual differences in a phishing detection task," *Proceedings 19th Triennial Congress of the IEA*, 2015, p. 1-5.

[27] M. L. Hale, R. Gamble, J. Hale, M. Haney, J. Lin, and C. Walter, "Measuring the Potential for victimization in malicious content," in *Proceedings - 2015 IEEE International Conference on Web Services, ICWS 2015*, Jun. 2015, pp. 305–312, doi: 10.1109/ICWS.2015.49.

[28] R. Manning and G. Aaron, "Phishing activity trends report," *Anti Phishing Work Group, Tech. Rep. 2nd Quarter*, 2010

[29] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web*, May 2013, pp. 737–744, doi: 10.1145/2487788.2488034.

[30] A. A. Ojugo and E. Ekurume, "Deep learning network anomaly-based intrusion detection ensemble for predictive intelligence to curb malicious connections: an empirical evidence," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 3, pp. 2090–2102, 2021, doi: 10.30534/ijatcse/2021/851032021.

[31] J. Staggs, R. Beyer, M. Mol, M. Fisher, B. Brummel, and J. Hale, "A perceptual taxonomy of contextual cues for cyber trust.," *Proceeding of the Colloquium for Information System Security Education CISSE*, 2014, vol. 2, pp. 152–169.

[32] M. L. Hale, R. F. Gamble, and P. Gamble, "CyberPhishing: a game-based platform for phishing awareness testing," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, Jan. 2015, vol. 2015-March, pp. 5260–5269, doi: 10.1109/HICSS.2015.670.

[33] J. C. Y. Sun, S. J. Yu, S. S. J. Lin, and S. S. Tseng, "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference," *Computers in Human Behavior*, vol. 59, pp. 249–257, Jun. 2016, doi: 10.1016/j.chb.2016.02.004.

[34] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Conference on Human Factors in Computing Systems - Proceedings*, 2010, vol. 1, pp. 373–382, doi: 10.1145/1753326.1753383.

[35] A. Jayatilaka, N. A. G. Arachchilage, and M. A. Babar, "Falling for phishing: an empirical investigation into people's email response behaviors," *arXiv preprint*, no. Fbi 2020, pp. 1–17, 2021, [Online]. Available: https://arxiv.org/abs/2108.04766.

[36] P. Chanvarasuth, "Knowledge on phishing and vishing: an empirical study on Thai students," *Psrcentre.Org*, vol. 2, no. 3, 2013, [Online]. Available: http://psrcentre.org/images/extraimages/IJHAS023044.pdf.

[37] A. A. Ojugo and A. O. Eboka, "Memetic algorithm for short messaging service spam filter using text normalization and semantic approach," *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 9, no. 1, p. 9, 2020, doi: 10.11591/ijict.v9i1.pp9-18.

[38] R. Toivonen, L. Kovanen, M. Kivelä, J. P. Onnela, J. Saramäki, and K. Kaski, "A comparative study of social network models: Network evolution models and nodal attribute models," *Social Networks*, vol. 31, no. 4, pp. 240–254, Oct. 2009, doi: 10.1016/j.socnet.2009.06.004.

[39] V. V. Busato, F. J. Prins, J. J. Elshout, and C. Hamaker, "The relation between learning styles, the big five personality traits and achievement motivation in higher education," *Personality and Individual Differences*, vol. 26, no. 1, pp. 129–140, Jan. 1998, doi: 10.1016/S0191-8869(98)00112-3.

[40] A. A. Ojugo and D. O. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES International Journal of Artificial Intelligence (IJAI)*, vol. 9, no. 3, pp. 497–506, 2020, doi: 10.11591/ijai.v9.i3.pp497-506.

[41] S. Rothmann and E. P. Coetzer, "The big five personality dimensions and job performance," *SA Journal of Industrial Psychology*, vol. 29, no. 1, Oct. 2003, doi: 10.4102/sajip.v29i1.88.

[42] A. Vishwanath, "Habitual Facebook use and its impact on getting deceived on social media", *Journal of Computer-Mediated Communication*, vol. 20, no. 1, pp. 83–98, Sept. 2015, doi: 10.1111/jcc4.12100

[43] F. Enos, S. Benus, R. L. Cautin, M. Graciarena, J. Hirschberg, and E. Shriberg, "Personality factors in human deception detection: Comparing human to machine performance," *Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH*, 2006, vol. 2, pp. 813–816, doi: 10.21437/interspeech.2006-278.

[44] Y. Zhang, S. Egelman, L. F. Cranor, and J. Hong, "Phinding phish: evaluating anti-phishing tools," In *Proceedings of the Network & Distributed System Security Symposium (NDSS 2007)*, no. March, 2007, pp. 1–16.

[45] R. Broadhurst, K. Skinner, N. Sifniotis, and B. Matamoros-Macias, "Cybercrime Risks in a University Student Community," *SSRN Electronic Journal*, no. May, 2018, doi: 10.2139/ssrn.3176319.

BIOGRAPHIES OF AUTHORS

Dr. Maureen Ifeanyi Akazue is a Lecturer in the Department of Computer Science at the Delta State University, Abraka, Delta State, Nigeria. She received a Master of Information Science degree in 2001 from the University of Ibadan, Oyo State, Nigeria, M.Sc. Computer Science in 2008 and Ph.D. Computer Science in 2014, both from the University of Benin, Edo State, Nigeria. She currently lectures with the Department of Computer Science at the Delta State University, Abraka, Delta State, Nigeria. Her research interests are HCI, online fraud prevention modeling, IoT, trust model, cyber security, and E-commerce. She is a member of The Nigerian Computer Society and Computer Professionals of Nigeria. She can be contacted at email: akazuem@gmail.com.

Prof. Arnold Adimabua Ojugo received his BSc, MSc and Ph.D. in Computer Science from Imo State University Owerri, Nnamdi Azikiwe University Awka, and Ebonyi State University Abakiliki in 2000, 2005 and 2013 respectively. He is a Professor with the Department of Computer Science at Federal University of Petroleum Resources Effurun – with research interest(s) in: Machine Intelligent Systems, Data Science, CyberSecurity, and Graph Applications. He has a great many scholalrly publications and with footprints of Author IDs as thus: (a) Scopus ID 57189005682, (b) Publons 2978638, (d) ORCID: 000-0003-4150-5163, (e) Loop ID 1747264, and (e) Semantic 6663691. He is a member of various Editorial Boards and Reviewer (to include and not limited to): The International Journal of Modern Education in Computer Science IJMECS, Frontiers in Big Data, and Progress for Intelligent Computation and Application, and many others. He is a member of the Nigerian Computer Society, the Council Registration of Computer Professionals of Nigeria, and International Association of Engineers (IAENG). He can be contacted at email: ojugo.arnold@fupre.edu.ng.

Dr. Rume Elizabeth Yoro received her BSc in Computer Science from the University of Benin Edo State in 2000, MSc in Computer Science from both Benson Idahosa University and the University of Benin respectively in 2009 and 2013. She currently lectures as a Senior Lecturer with the Department of CyberSecurity in the Faculty of Information Technology at the Dennis Osadebey University Asaba. Her research interests: network management, computer forensics and machine learning. She is a member of: Computer Professionals of Nigeria, Nigerian Computer Society, Computer Forensics Institute of Nigeria and Nigeria Women in Information Technolgy the International Association of Engineers. She is married to Fred Yoro with five children. She can be contacted at rumerisky5@gmail.com.

Dr. Bridget Ogheneovo Malasowe received her BSc in Computer Science from The University of Benin, Benin-City in 1998. She obtained her MSc and Ph.D. in 2012 and 2017 respectively – both in Computer Science from The Babcock University, Ilisan-Remo in Ogun State. She is currently, a Senior Lecturer with the Department of Computer Science, Uniiversity of Delta, Agbor in Delta State of Nigeria. Her research interest is in green information technology, data science with machine learning approaches, cyber-security, and bioinformatics. She is a member of Nigerian Computer Society of Nigeria and Computer Professionals of Nigeria. She can be contacted at: bridget.malasowe@unidel.edu.ng.

Obinna Nwankwo received his B.Sc in Computer Science from The Cross River University of Technology Calabar (CRUTECH) in Cross River State in 2008, M.Sc also in Computer Science from The University of Lagos, Akoka in 2011 – and currently, undergoing his Doctoral Studies at the University of Benin. He currently lectures with the Department of Computer Science at the Novena University Ogume, Delta State. His research interests: software engineering, artificial intelligence, genetic algorithms and machine learning. He has a good scholalrly publications and with footprints of Author IDs as thus: (a) Publons 5013320, (b) ORCID: 0000-0001-8744-2554. He is a member of: The Nigerian Computer Society. He is married to Jennifer Nwankwo, and they both have two daughter. He can be contacted at tuk2obinna@gmail.com.