International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 2, April 2023, pp. 1943~1953
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i2.pp1943-1953

Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian

Rume Elizabeth Yoro[1], Fidelis Obukohwo Aghware[2], Maureen Ifeanyi Akazue[3], Ayei Egu Ibor[4], Arnold Adimabua Ojugo[5]
[1]Department of Computer Science, Dennis Osadebey University Asaba, Asaba, Nigeria
[2]Department of Computer Science, University of Delta, Agbor, Nigeria
[3]Department of Computer Science, Delta State University, Abraka, Nigeria
[4]Department of Computer Science, University of Calabar, Calabar, Nigeria
[5]Department of Computer Science, Federal University of Petroleum Resources Effurun, Effurun, Nigeria

Article Info

Article history:

Received Sep 5, 2020
Revised Oct 7, 2022
Accepted Oct 18, 2022

Keywords:

Cyber security
Fraud
Personality traits
Phishing
Spam
Transactions

ABSTRACT

Access ease, mobility, portability, and improved speed have continued to ease the adoption of computing devices; while, consequently proliferating phishing attacks. These, in turn, have created mixed feelings in increased adoption and nosedived users' trust level of devices. The study recruited 480-students, who were exposed to socially-engineered attack directives. Attacks were designed to retrieve personal data and entice participants to access compromised links. We sought to determine the risks of cybercrimes among the undergraduates in selected Nigerian universities, observe students' responses and explore their attitudes before/after each attack. Participants were primed to remain vigilant to all forms of scams as we sought to investigate attacks' influence on gender, students' status, and age to perceived safety on susceptibility to phishing. Results show that contrary to public beliefs, age, status, and gender were not among the factors associated with scam susceptibility and vulnerability rates of the participants. However, the study reports decreased user trust levels in the adoption of these new, mobile computing devices.

Corresponding Author:

Arnold Adimabua Ojugo
Department of Computer Science, Federal University of Petroleum Resources Effurun
Effurun, Nigeria
Email: ojugo.arnold@fupre.edu.ng

1. INTRODUCTION

As more individuals become connected to the Internet via enabling devices/supports-it consequently, also opens up many of such persons on a larger scale, to avenues of exploitation that can be harnessed by adversaries via threats and cyber-attacks [1], [2]. The attacks reveal how vulnerable a device connected over the network is, with such attacks continually advanced via socially engineered. 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 [3], [4]. An adversary attempts to hack, distribute malware and steal victims' data via socially-engineered attacks (which include and are not limited to) phishing, vishing, and spam methods-their assertion of success rate is based on the target's judgment rather than the security measure in place over/on the victim's network [3], [5]. Thus, providing attackers with attractive entry point to the victims' compromised system and providing a pilot cum pivot point for attack spread cum propagation [4], [6].

Socially-engineered attacks (e.g., spam) often involve harmless advertising via unsolicited emails/short message service (SMS) as network messages. They may contain viruses designed to retrieve a user’s personal data [7], [8]. The nature of spam is such that they are structured as a target mechanism for high-value victims and sent out to target high-volume unsuspecting victims besides distribution ease [9]. Spams are often seen as insignificant. Even with an estimated daily distribution of over 422 Billion and 612Billion spam in 2021 [4], [10]. Spams consists over 85-percent of daily global data traffic, and is made possible via botnets that target potentially, vulnerable recipients due to ineffective anti-virus amongst other countermeasures [6], [9]–[12].

2. LITERATURE REVIEW

2.1. Phishing attacks explained to users

Phishing can include the development of hacked websites, the purchase of email lists and botnets, and the spoofing of emails and SMS to trick an unwary victim into downloading dangerous content that appears to come from a legitimate and trustworthy source. A typical phishing attack consists of 3-elements: lure, hook, and catch. For example, a potential victim receives a lure message, which appears as originating from a genuine or legitimate source. Its dependability is improved by utilizing: i) the curiosity message contains compromised links to videos of recent news/events; ii) the fear message urges a user to validate their data due to an account breach; and iii) the empathy message impersonates a close associate in need of favor [13]–[17]. Kimpe *et al.* [18] lists spelling and design/format problems, monetary offers, and other as hallmarks of phishing attacks/attempt. They note that if a victim believes a message to be real, they are then persuaded to divulge personal data. Spammers use social manipulators like trusting of email source, implicating reciprocity (e.g., returning favors), or 'social proof' (i.e., others are participating), establishing a sense of scarcity, and invoking an authoritative source as means to ensure the success of the deception. The hook is the message's compromised link and/or attachment; while, the catch is the attacker's acquisition of the victim’s personal data alongside its usage. This may appear simple; but, the technique or procedure involved is constantly evolving to reflect new social trends occurring in the world [19], or methods for bypassing security protocols to evade detection [9]. The continued proliferation of the Internet has continued to allow these attacks to vary in their frequency and diversity, and so-enhancing the greater likelihood for these spammers to succeed [20].

2.2. Literature review: personality traits versus scams

Kahneman and Tversky [21] notes that in extenuating circumstances, decisions are often prejudiced and not purely logical. Thus, a scam is a masquerade used by an adversary to acquire important information or money from an unsuspecting victim. If the user does not accurately assess the risks due to specific biases, the response to the fraud becomes a judgment error. Scams will continue to thrive for these and other reasons since a certain percentage of individuals fall for them. As a result, scams give an attacker the opportunity to take a victim's data and/or obtain money directly from scam victims [22].

Scams are socially engineered to target certain human weaknesses. These include (but are not limited to) the drive for rapid gratification, the desire to help others, and the desire to be loved by scammers, implying that certain people have 'victim personality features' that make them more vulnerable to scams [23], [24]. Thus, a victim may be duped several times, and the lack of emotional control is a critical feat that makes one more susceptible cum prone to becoming a victim. In [25], scam victims reported the inability to resist persuasion, and the offers, they accepted. The study concludes that scams affect between 10 to 20% of the population. Some people become serial scam victims, falling for frauds over and over again.

2.3. Factors influencing scam susceptibility and vulnerability

Various researches today into cyber-security have begun to now investigate how the various aspects of psychology seek to compromise data over measures of Internet security. One such concern is that the internet may soon replace normal social activities as individuals now preoccupy themselves with social media as well as other Internet-enabled modes-as they seek to compensate for loneliness and social seclusion. McCrea and John [26] as extended by Halevi *et al.* [27] employed the big five (5) personality traits to include: neuroticism, extroversion, openness, agreeableness, and consciousness as in section II.

Studies have examined the relations between personality traits, susceptibility, and scam- seeking the underlying feats of interest that aid to victim’s scam vulnerability. Enos *et al.* [28] note that victims with high scores on neuroticism had a worse probability of detecting lies-as they become more upset when/if lied to. Thus, they will rather believe people are truthful always (to avoid emotional pain). Parsons *et al.* [29] and Mayhorn *et al.* [30] advanced that premeditation was also linked to the ability to detect lies/fraud (for many users who sought to actively detect such offers). Their result, however-was divided on the feats that greatly contributed to the personality traits responsible for scam susceptibility. While some studies agree that some persons can better detect lies/fraud [28], some other studies disagree with this fact [30], [31].

2.4. The university frontiers and experience

Undergraduates in Nigeria have become both phishing victims and perpetrators of socially engineered attacks. Nigeria has been plagued by a desire for quick money, which has resulted in a rash of fraudulent and unethical practices that have robbed the country's youth of necessary changes and advancement. Fraud is a criminal crime that involves embezzlement and theft in which a criminal takes advantage of an unwitting victim (usually aimed at a financial transaction). Exchange of goods and services for gains or money delivery is known as a transaction [32]–[35]. With improvements in information and communication technology (ICT) demonstrating their potential to people all over the world, the multitude of attacks that exploit vulnerabilities of linked technologies has become a sine-qua-non impact. These take different shapes like deceptive things that appear to benefit the naïve victim but are actually intended to scam them [36]–[38].

Chanvarasuth [39] investigated the dangers that people face by comparing the efficiency of phishing and vishing approaches, utilizing a sample of 772-Thai undergrad students aged 18 to 23 years old. According to their findings, the phishing problem has a higher success rate than vishing. Other characteristics, such as gender, can influence the success rate of each approach. On the Android smartphone, Akazue *et al.* [33] introduced a client-trusted detection framework for e-banking that aimed to create a secure mobile banking platform and handle threats through transaction authenticity and message authorization. They focused on comparing the effectiveness of phishing and vishing in order to investigate threats faced by smartphone users. They surveyed 600 people in Nigeria's South-South and South-East zones. Their findings suggest that phishing is more dangerous and has a greater success rate than vishing.

3. MATERIALS AND METHODS

3.1. Campus demographics/sample population

We selected total of four hundred and eighty (480) students as in Table 1. Students from the Southern region (i.e., South-East, South-West, and South-South geo-political zones) in Nigeria-who were recruited for this study. Students were not selected from the Northern region due to the state of the insecurity, and kidnapping.

Table 1. Demographic characteristics of samples

S/N	Characteristics	Dependent variables	All participants
1	Gender	Male	50.9
		Female	49.1
2	Age	Under 21	21.5
		21 to 25	34.5
		26 and above	44.0
3	Student status	Domestic	89.1
		International	11.9
4	Faculty	Science-Technology	40.1
		Environmental	15.2
		Medicine	12.0
		Others	32.7
5	Year of study	1-Year	36.0
		2-Years	19.8
		3-Years	19.5
		4-Years and above	25.7

3.2. Grouping the participants/data collection

For scam susceptibility, we adapt Broadhurst *et al.* [40] grouping participants into three (3) namely:

a. Generic

Here, the content of fake scams was not personally relevant to participants. It replicated mass real-world scams, which are typically sent to a large number of users with the expectation that a small number will fall victim. Its contents are broad and impersonal; and, applied to a large audience. Scams in this group were thus characterized by impersonal content with no personal relevance to participants [41].

b. Tailored

Contents of a scam related to a particular institution the target participant(s) is recruited from – since real-world scammers impersonate well-known institutions. Thus, we exploit known trustworthiness and legitimacy of known institutions (e.g. FUPRE) by scammers who wish to target persons associated with such places. Such tailored scams are intended to replicate scammer impersonations. Participants' connections to FUPRE (among other varsities) enabled this – so we can present contents that appeared to be originating from their varsity. Though, the mails were not specific to a user but tailored to the institution and provided a mid-point of specificity between generic and spear-phishing emails.

c. Spear-phishing

Here, scam content was personally relevant to the individual because spear phishers take a great deal of time and effort to understand their targets to maximize the perceived legitimacy of their mails. Such emails may thus be relevant and relate both to institutions as well as the individual's personal and social lives. Thus, we adopt highly targeted data relating directly to each individual as assessed from their registration records. To assess overall scam susceptibility, the total number of scams that deceived participants (also referred to as scam count) was counted. Additionally, to assess the participants’ susceptibility to a particular scam type, the number of scams fallen for at each specificity level was counted. It was assumed that falling for fake scams at a particular level reflected susceptibility to real-world scams at the same level. For example, a participant that falls only to a fake spear-phishing attack is presumed to be susceptible primarily to spear-phishing attacks in the real world. Similarly, participants who fell for both mass generic and spear-phishing attacks in the experiment were thought to be susceptible to both kinds of attacks in the real world. Higher scam counts indicated greater scam susceptibility [42]–[44].

3.3. Susceptibility threshold and framework

On social networks, participants create ties and patterns that bind them to such sites and other persons over the network. Thus, no matter how loosely bound, this provides an adversary with the requisite structure upon which they now introduce these attacks. This reflects how participants' interactions are influenced to click/open malicious content over the social site or otherwise [45]. Participants often vary in their willingness to risk opening emails from unknown sources-and thus, they will rather wait until close associates and confidants have done the same with such mails or social network sites. The measure of this willingness to adopt is termed threshold value for an actor [46], and is measured via Toivonen *et al.* [47], Haythornthwaite [48], and Gilbert and Karahalios [49] using the linear combiner in (1):

$$FA_d = \frac{|\Phi(0) \cap P_i(\mathrm{G})|}{|P_i(\mathrm{G})|} \geq \ \phi_i \Rightarrow i \in \Phi([0,1] \tag{1}$$

Set $\Phi([0,1])$ are participants exposed to the mail and who will consider clicking with little social manipulation like trusting the source of the mail. Thus, the threshold is collective behavior where a participant (in this study) for example, considers opening (or clicking) the mail sent to him or received from a source. A participant easily does so based on behavior of close friends (associates) or other participants in his/her immediate neighborhood. A participant with a low threshold is susceptible and will click to open any mail received from known associates with the blink of an eye before many other participants. Conversely, participants with a high threshold only click to open emails (even from known sources) after genuine inquiries and consciousness [45].

3.4. Procedure

The experiment last for nine (9) months and participants signed consent forms. Each participant's data was extracted from social media pages to create content for spear-phishing emails-providing data such as age, political leanings, social relations, religion, and club affiliations. From here, a tailored, personally relevant fake attack was created for each participant. For example, we retrieved a participant's data that he was a part of the FUPRE team that competed in the 2019/2020 industrial games. Many students wish to join the competition and it allowed us to impersonate the industrial-games organizers via spear-phishing. Sample email created for this (and other) participants as in Figures 1 to 3 respectively.

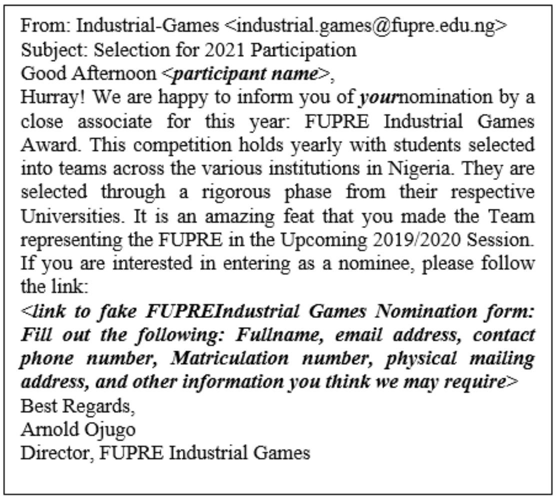
This email attempts to entice the participant to click on the link, which is a real scam situation-have been compromised. The content of all other spear-phishing emails was similar and varied based on the type of personal information available on the Internet. Due to i) the lack of social media presence and ii) restrictive privacy settings, personal data for all participants could not be acquired. Thus, we have specialized emails created only for participants with adequate amounts of online personal information (N=25).

3.5. The big-5 framework

Personality is a recurring pattern of how people react to stimuli in their surroundings and how they react to various events. A 5-D assessment that evaluates personality was developed by McCrea and John [26]. Halevi *et al.* [27] expanded it-stating that its purpose is to encapsulate personality into five unique components that allow for the theoretical conception of people's personalities. Thus, we use these dimensions namely:

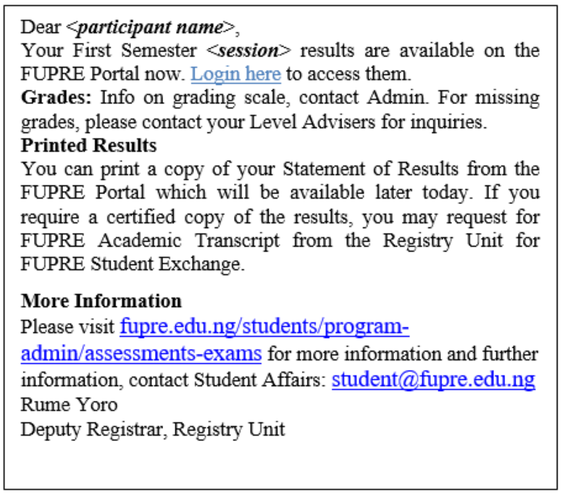
a. Neuroticism is the tendency to experience negative feelings that include guilt, disgust, anger, fear, and sadness. A previous study indicates that a high neuroticism score indicates that a person is susceptible to irrational thoughts, is less able to control impulses, and does not handle stress well.
b. Conscientiousness: Persons with such quality display high self-control. They are more organized, strong-minded, purposeful, dependable, and hardworking. They also possess a high level of conscientiousness that may also manifest via over-working and compulsiveness about cleanliness.
c. Openness refers to a desire to explore new things. Openness scores indicate that people are more inventive and intellectually curious. They are more receptive to fresh and unusual ideas and views.
d. Agreeability: People who are agreeable are helpful, ready to assist others, and believe in reciprocity. Egocentric and competitive people have low agreeableness scores.
e. Extroverted persons are more friendly, and outgoing and interact more; while introverts are more reserved.

The most widely used measure is NEO-PI FFM test, which provides a quick, reliable, and accurate measure of a participants personality across 5-D. It captures common personality traits with a precise description. Its merits have been made for its integration into education [50], and employment [51]. It is considered superior and robust for understanding the relations between personality and various academic behaviors. This study sets to examine if this relation extends to network security, traits, and privacy behavior [27].



From: Industrial-Games <industrial.games@fupre.edu.ng>
Subject: Selection for 2021 Participation
Good Afternoon <***participant name***>,
Hurray! We are happy to inform you of ***your***nomination by a close associate for this year: FUPRE Industrial Games Award. This competition holds yearly with students selected into teams across the various institutions in Nigeria. They are selected through a rigorous phase from their respective Universities. It is an amazing feat that you made the Team representing the FUPRE in the Upcoming 2019/2020 Session. If you are interested in entering as a nominee, please follow the link:
<link to fake FUPREIndustrial Games Nomination form: Fill out the following: Fullname, email address, contact phone number, Matriculation number, physical mailing address, and other information you think we may require>
Best Regards,
Arnold Ojugo
Director, FUPRE Industrial Games

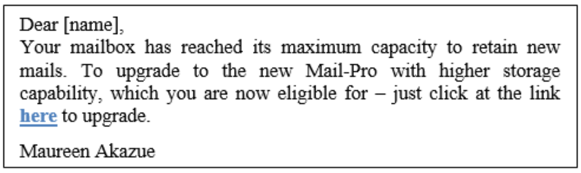
Figure 1. Sample spear-phished email-1



Dear <***participant name***>,
Your First Semester <***session***> results are available on the FUPRE Portal now. Login here to access them.
Grades: Info on grading scale, contact Admin. For missing grades, please contact your Level Advisers for inquiries.
Printed Results
You can print a copy of your Statement of Results from the FUPRE Portal which will be available later today. If you require a certified copy of the results, you may request for FUPRE Academic Transcript from the Registry Unit for FUPRE Student Exchange.

More Information
Please visit fupre.edu.ng/students/program-admin/assessments-exams for more information and further information, contact Student Affairs: student@fupre.edu.ng
Rume Yoro
Deputy Registrar, Registry Unit

Figure 2. Sample tailored email-1



Dear [name],
Your mailbox has reached its maximum capacity to retain new mails. To upgrade to the new Mail-Pro with higher storage capability, which you are now eligible for – just click at the link **here** to upgrade.

Maureen Akazue

Figure 3. Generic email-1-mailbox full, upgrade now

3.6. Social networking activities

The test participants were asked what kind of data they put on Facebook and Instagram, the frequency of postings, the amount of photographs they upload, and their privacy settings in order to correlate SN activity with personality factors. The poll relies on self-reported data, which is double-checked for correctness. Participants' personal information was gathered. Each element was given a value of one, and the variables were put together to form one 'social-network data'. Participants' log-values for several weekly posts and the aggregate quantity of photographs were collected as distinct values/accounts on their Facebook/Instagram pages. We compute updated variables via (2) [27]:

$$SN_{posts} = log_{10}(TotalEntry + 0.001) \quad (2)$$

The total number of photographs was calculated using the same formula. Participants were asked questions about six different privacy settings options, including; i) posting to SN wall, ii) profile lookup, iii) friends request, iv) messaging, v) navigating their own and others' walls, and vi) sharing and/or importing personal information into friends' pages, in order to evaluate privacy settings. Each privacy setting element was given a value between '0' (for nobody) and '3' (to make an item available to all) for each entry inside. These numbers were then joined together to generate a total value for Facebook's privacy settings. Overall participant’s data statistics are found in Table 2. 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. *Dyads* are all pairs of interactions to measure relations of n participants with m ties that result in an $m \times n$ binary matrix for a social connection. Thus, our participants’ page(s) are linked to persons who may or may not be a part of the experiment; and is thus, measured and denoted by $+D_i$ (for each participant)-which evaluates the value in the strength of the ties between all connections on such a participant's page [45]. Conversely, EL_i refers to minor shocks as well as influences that tip such participants to trust the mails as originating from a trusted source.

Table 2. 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			

From Table 2, 4 to 22 percent of the participants do not post any data nor did they reply to or shared the 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.

3.7. Hypotheses

H_1: *Some traits lead to high susceptibility and vulnerability rates, and allow participants to share private data-online*

H_2: *Participant complacency with privacy settings on social media platforms-leaves them vulnerable as scam victims.*

4. RESULTS AND DISCUSSION

4.1. Data preparation and cleaning

Screening, cleaning, and subsequent analyses were done using the Statistical Package for Social Sciences (SPSS v24). The dataset was examined for out-of-range and missing values as well as for adherence to the assumption of Chi-Square and analysis of variance. All data were within range-though, some of the missing values were found in the questions about students and residential status; But they did not impact the result of the study. Also, visual inspection of charts revealed approximately normal distribution for all relevant variables, and skewness and kurtosis statistics revealed no significant violations of normality for any relevant demographic variable.

4.2. Resultant hypothesis

Study seeks to find the probability distribution, and resultant correlation for the stated hypothesis.

H_1: *Some traits lead to higher susceptibility and allow such participants to share more private data-online.*

Evaluating H_1 whether some personality traits lead to a higher susceptibility with increasingly tailored and spear-phishing mails to participants, we use Wilcoxon signed-rank test as in Figures 4 to 6 respectively. The results therein, revealed no significant differences in scam susceptibility between generic and tailored scams (Z=-0.546, p =0.585), tailored and spear phish scams (Z=0.000, p=1.00), or generic and spear phish scams (Z=-0.646, p=0.518). Thus, the hypothesis was not supported. Going further, we sought to assess whether the rate of these participants’ susceptibility to scams, was associated with gender, age, and students' status-we employ fisher’s exact test as shown in Figures 4 to 6 respectively, with p=0.57. Result shows there are no significant differences in gender and other traits, as being reason for their susceptibility and vulnerability to scams.

H_2: *Participants’ complacency with privacy settings over social media platforms–leaving them vulnerable as victims of the scam.*

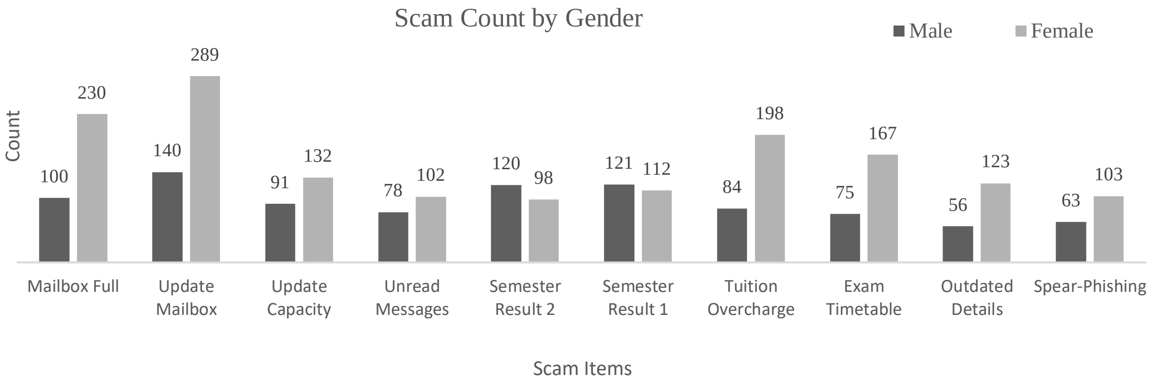
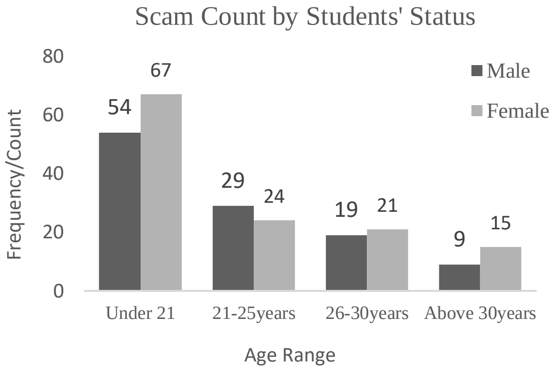


Figure 4. Scam count by gender



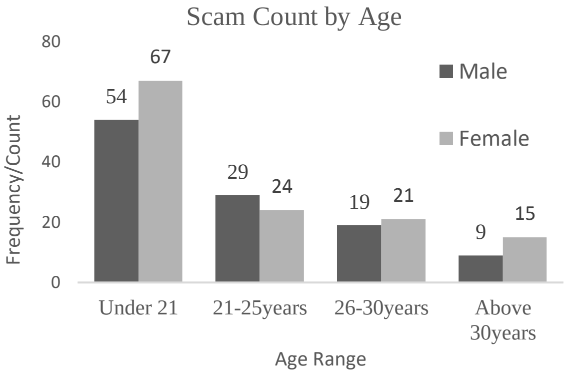
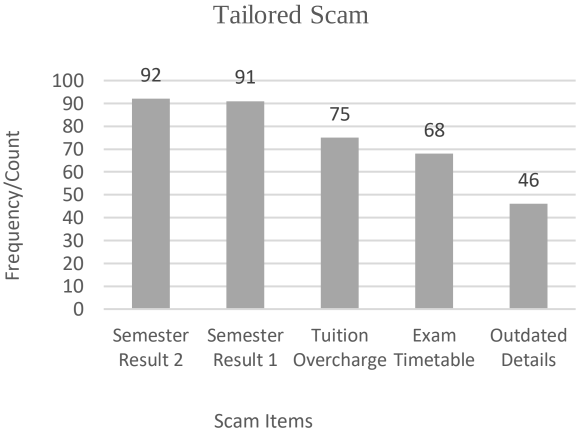


Figure 5. Scam count: students' status/year of study

Figure 6. Scam count by students' age

The overall result shows that there appeared to be no trend in the relation between the scam-type employed (i.e., generic, tailored, and spear-phishing) and participant cum victim susceptibility or vulnerability. Participants were most susceptible to a scam with the heading "Mailbox Full", "Update Mailbox" and "Update Mailbox Capacity" which are generic scams. We also notice that many participants were also susceptible to the "Semester Result", which were scams tailored to participants' institution of study as seen in Figures 7 and 8 respectively. The pie chart in Figure 9 shows the percentage of the participants who fell for each scam.



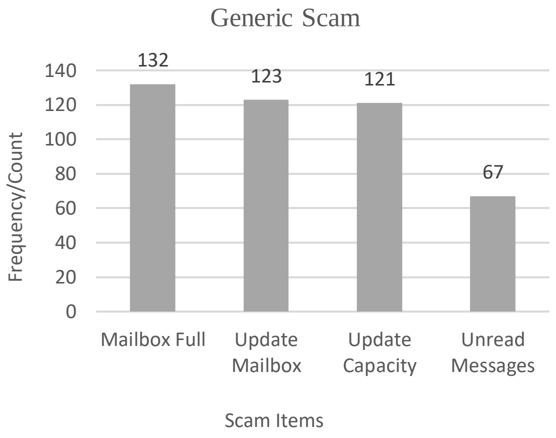


Figure 7. Participants who fell for generic scam

Figure 8. Participants who fell for tailor-scam

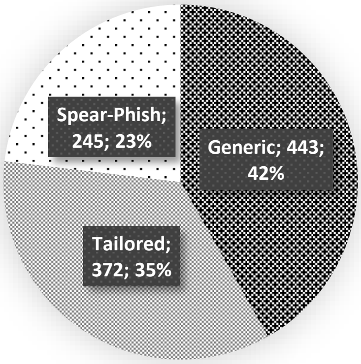


Figure 9. Percentage of participants who fell for each scam

4.3. 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 and vulnerability rates among students. Though, relevant literature(s) suggests that scam susceptibility may be influenced by the level of specificity in a scam. That is, individuals may be more likely to be deceived by scams, tailored to their circumstances (spear-phishing) compared to those with generic content (phishing). Also, other variables have been flagged as potential contributors to scam susceptibility (including and not limited to) gender, age, and status. Broadhurst *et al.* [40] 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.

Results revealed no relations between scam type(s) and participants' susceptibility cum vulnerability to these scam types as participants were not found to be more susceptible to spear-phishing attacks when compared to generic and tailored attacks. However, email content that deceived most participants also provides insight into the types of scams that may succeed. The most successful attack related to these participants' updated mailbox. This email was urgent and was sent during the FUPRE First and Second Semester Examinations for the 2019/2020 Academic Session. With these, we can proffer three (3) likely explanations for its success namely: i) that due to the upcoming exams, portal information as regularly sent to the students' mailbox gave this mail high relevance to participants' circumstances at the time, ii) Exams are of critical matter and nature to all participants and thus, became a panacea for the increased susceptibility, and iii) Exams generally instill fear in students (cum participants)-and this mail detailed an 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. Broadly, 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 (IJ-AI)*, vol. 10, no. 3, pp. 623–635, Sep. 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. 1, 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, Apr. 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 & Security*, vol. 73, pp. 345–358, Mar. 2018, doi: 10.1016/j.cose.2017.11.015.

[6] A. A. Ojugo, A. O. Eboka, R. E. Yoro, M. O. Yerokun, and F. N. Efozia, “Hybrid model for early diabetes diagnosis,” in *2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, Aug. 2015, pp. 55–65, doi: 10.1109/MCSI.2015.35.

[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 (IJ-AI)*, vol. 10, no. 3, pp. 519–527, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp519-527.

[8] 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, Jul. 2019, doi: 10.5815/ijmsc.2019.03.05.

[9] M. Alazab and R. Broadhurst, “Spam and criminal activity,” *SSRN Electronic Journal*, no. 526, pp. 1–20, 2014, doi: 10.2139/ssrn.2467423.

[10] A. Lee and D. Harley, “Phish phodder: is user education helping or hindering?,” in *Virus Bulletin Conference*, 2007, pp. 1–7.

[11] D. Irani, S. Webb, J. Giffin, and C. Pu, “Evolutionary study of phishing,” in *2008 eCrime Researchers Summit*, Oct. 2008, pp. 1–10, doi: 10.1109/ECRIME.2008.4696967.

[12] R. Manning, “Phishing activity trends report: 2nd Quarter/2010,” APWG, 2010.

[13] A. Eboka and A. A. Ojugo, “A social engineering detection model for the mobile smartphone clients,” *African Journal of Computing & ICT*, vol. 7, no. 3, pp. 91–100, 2014.

[14] A. A. Ojugo and A. O. Eboka, “Empirical evidence of socially-engineered attack menace among undergraduate smartphone users in selected Universities in Nigeria,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 3, pp. 2103–2108, Jun. 2021, doi: 10.30534/ijatcse/2021/861032021.

[15] 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.

[16] A. Abbasi, F. M. Zahedi, and Y. Chen, “Phishing susceptibility: The good, the bad, and the ugly,” in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Sep. 2016, pp. 169–174, doi: 10.1109/ISI.2016.7745462.

[17] 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.

[18] 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.

[19] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, “Spam and phishing in Q3 2017,” Securelist.com, 2017. https://securelist.com/spam-and-phishing-in-q3-2017/82901 (accessed Jan. 25, 2018).

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

[21] D. Kahneman and A. Tversky, “Prospect theory: An analysis of decision under risk,” *Econometrica*, vol. 47, no. 2, pp. 263–292, Mar. 1979, doi: 10.2307/1914185.

[22] H. Kornor and H. Nordvik, “Five-factor model personality traits in opioid dependence,” Biomedcentral.com, 2007. http://www.biomedcentral.com/1471-244X/7/37 (accessed Mar. 01, 2020).

[23] 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.

[24] D. Modic and S. E. G. Lea, “How neurotic are scam victims, really? The big five and internet scams,” *Security and Human Behaviour*, 2012.

[25] “The psychology of scams: Provoking and committing errors of judgement,” *Office of Fair Trading*, 2009. Accessed: Mar. 01, 2020. [Online]. Available: https://ore.exeter.ac.uk/repository/bitstream/handle/10871/20958/OfficeOfFairTrading2009.pdf;sequence=1

[26] R. R. McCrae and O. P. John, “An introduction to the five-factor model and its applications,” *Journal of Personality*, vol. 60, no. 2, pp. 175–215, Jun. 1992, doi: 10.1111/j.1467-6494.1992.tb00970.x.

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

[28] 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,” in *INTERSPEECH 2006 - ICSLP, Ninth International Conference on Spoken Language Processing*, 2006, pp. 813–816.

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

[30] C. B. Mayhorn, A. K. Welk, O. A. Zielinska, and E. Murphy-Hill, “Assessing individual differences in a phishing detection task,” *Proceedings of 19th Triennial Congress of the IEA*, Melbourne: IEA, 2015.

[31] 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.

[32] A. A. Ojugo and A. O. Eboka, “Comparative evaluation for high intelligent performance adaptive model for spam phishing detection,” *Digital Technologies*, vol. 3, no. 1, pp. 9–15, 2018, doi: 10.12691/dt-3-1-2.

[33] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, “Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

[34] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?,” in *Proceedings of the 28th international conference on Human factors in computing systems - CHI ’10*, 2010, pp. 373–382, doi: 10.1145/1753326.1753383.

[35] J. R. C. Wang, T. Herath, and H. R. Rao, *An empirical exploration of the design pattern of phishing attacks*. Emerald Publishers, 2009.

[36] E. O. Yeboah-Boateng and P. M. Amanor, “Phishing, SMiShing & vishing: An assessment of threats against mobile devices,” *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 4, pp. 297–307, 2014.

[37] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, “Phinding phish: Evaluating anti-phishing tools,” in *Proceedings of the Network & Distributed System Security Symposium (NDSS 2007)*, 2007, pp. 1–16.

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

[39] P. Chanvarasuth, “Knowledge on phishing and vishing: An empirical study on thai students,” *International Journal of Humanities and Applied Sciences*, vol. 2, no. 3, pp. 58–62, 2013.

[40] R. G. Broadhurst, K. Skinner, N. Sifniotis, and B. Matamoros-Macias, “Cybercrime risks in a university student community,” *Australian National University Cybercrime Observatory*, Canberra, 2018.

[41] 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, pp. 9–18, Apr. 2020, doi: 10.11591/ijict.v9i1.pp9-18.

[42] 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, Jun. 2021, doi: 10.30534/ijatcse/2021/851032021.

[43] A. Jayatilaka, N. A. G. Arachchilage, and M. A. Babar, “Falling for phishing: An empirical investigation into people’s email response behaviors,” *arXiv2108.04766*, Aug. 2021.

[44] M. L. Hale, R. F. Gamble, and P. Gamble, “CyberPhishing: A game-based platform for Phishing awareness testing,” in *2015 48th Hawaii International Conference on System Sciences*, Jan. 2015, pp. 5260–5269, doi: 10.1109/HICSS.2015.670.

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

[46] T. W. Valente, “Social network thresholds in the diffusion of innovations,” *Social Networks*, vol. 18, no. 1, pp. 69–89, Jan. 1996, doi: 10.1016/0378-8733(95)00256-1.

[47] 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.

[48] C. Haythornthwaite, “Strong, weak, and latent ties and the impact of new media,” *The Information Society*, vol. 18, no. 5, pp. 385–401, Oct. 2002, doi: 10.1080/01972240290108195.

[49] E. Gilbert and K. Karahalios, “Predicting tie strengths with social media,” *Journal of computer and Human Interface*, vol. 15, pp. 76–97, 2009.

[50] 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.

[51] S. Rothmann and E. P. Coetzer, “The big five personality dimensions and job performance,” *SA Journal of Industrial Psychology*, vol. 29, no. 1, pp. 68–74, Oct. 2003, doi: 10.4102/sajip.v29i1.88.

BIOGRAPHIES OF AUTHORS

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 a Senior Lecturer with the Department of Cybersecurity, Faculty of Information Technology at the Dennis Osadebey University Asaba. Her research interests include: network management, cybersecurity 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 Technology the International Association of Engineers. She is married to Fred Yoro with five children. She can be contacted at rumerisky5@gmail.com.

Fidelis Obukohwo Aghware received his BSc in Computer Science from The University of Benin, Benin-City in 1998; MSc in Computer Science in 2005 from the Nnamdi Azikiwe University Awka, and received his Ph.D. Computer Science in 2015 from The Ebonyi State University, Abakiliki. He is a Senior Lecturer with the Department of Computer Science, Uniiversity of Delta, Agbor in Delta State of Nigeria. His research interest are in cybersecurity, data science and information technology. He is a member of Nigerian Computer Society of Nigeria and the Council for Registration of Computer Professionals of Nigeria, and the International Association of Engineers. He can be contacted at fidelis.aghware@unidel.edu.ng.

Maureen Ifeanyi Akazue received her MSc Information Science in 2001 from the University of Ibadan, Nigeria, M.Sc. Computer Science in 2008 and Ph.D. Computer Science in 2014, both from the University of Benin, 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 akazuem@gmail.com.

Ayei Egu Ibor is a Lecturer and Cyber Security Researcher at the Department of Computer Science, University of Calabar, Nigeria. His research interests are cyber security, cyber resilience, cyber threat intelligence, deep learning and digital forensics. His scholarly footprints include. He can be contacted at ayei.ibor@unical.edu.ng.

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 intelligent systems, data science, cybersecurity, and graph applications. He has a great many scholarly publications and with footprints of Author IDs. 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, Council Registration of Computer Professionals of Nigeria, and International Association of Engineers. He can be contacted at ojugo.arnold@fupre.edu.ng.