# Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria

**Rume Elizabeth Yoro[1], Fidelis Obukohwo Aghware[2], Bridget Ogheneovo Malasowe[2], Obinna Nwankwo[3], Arnold Adimabua Ojugo[4]**
[1]Department of Computer Science, Dennis Osadebey University Asaba, Asaba, Nigeria
[2]Department of Computer Science, University of Delta, Agbor, Nigeria
[4]Department of Computer Science, Novena University Ogume, Delta State, Nigeria
[5]Department of Computer Science, Federal University of Petroleum Resources Effurun, Effurun, Nigeria

**Article Info**

***Article history:***

Received Jul 13, 2021
Revised Oct 7, 2022
Accepted Nov 1, 2022

***Keywords:***

Federal University of Petroleum Resources Effurun's
Online presence
Personality traits
Phishing vulnerability
Social media contents
Socially-engineered attacks

**ABSTRACT**

In this observational quasi-experimental study, we recruited 200 participants during the Federal University of Petroleum Resources Effurun's (FUPRE) orientation, who were exposed to socially engineered (phishing) attacks over nine months. Attacks sought to extract participants' data and/or entice them to click (compromised) links. The study aims to determine phishing exposure and risks among undergraduates in FUPRE (Nigeria) by observing their responses to socially-engineered attacks and exploring their attitudes to cybercrime risks before and after phishing attacks. The study primed all students in place of cybercrime awareness to remain vigilant to scams and explored the various scam types with their influence on gender, age, status, and their perceived safety on susceptibility to scams. Results show that contrary to public beliefs, these factors have all been found to be associated with scam susceptibility and vulnerability of the participants.

***Corresponding Author:***

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

## 1. INTRODUCTION

The internet's birth also witnessed the ever-increasing need for its users to stay connected via enabling support devices. However, such a need to stay connected and share data with other users within and outside of the user's locality has continued to open up many such users on a larger scale, to avenues of exploitation that can be harnessed by adversaries via threats and cyber attacks [1], [2]. This consequently has birthed the social media websites that have today, continued to gain great and significant popularity over the years, with over a 3.484 billion users worldwide reported in 2019 [3]. As users connect and perform many other feats over such media, they become more prone to threats and attacks of various forms. These attacks (many of which, socially-engineered today) reveal how vulnerable and susceptible a connected user is over the network-as the attacks are designed to exploit system errors and behavioral traits resulting from relations and operations between users. An adversary seeks to exploit an unsuspecting user as its victim and weakest link within the network. These amongst others are the reason(s) for which socially engineered attacks will continue to rise [4], [5].

Adversaries seek to compromise a potential victim and often succeed based on the target's (potential victim's) judgment rather than considering the security measure in place on the victim's network [4], [6]. The first quarter of 2018 witnessed a launch of fake Facebook pages with 60% of phishing attacks on social media networks and later on, in 2019, phishing on both Instagram and Facebook among others saw a 74.7%

increase [7]. These statistics highlight that the threat of phishing shows no sign of retreating. The gain therein a system to be exploited provides an adversary with an attractive entry point to a potentially compromised network as well as provides a pilot/pivot point for attack propagation [8].

The traditional platform for conducting attacks via spam has evolved to include network messages, e-mails, and short messages (SMS). These attacks have experienced now over 30% increase as they have now migrated and ported on social media platforms. Spams often involve harmless advertising and are laced with malware designed to exploit its recipients [9], [10]. Spams are deployed as attacks to target high-volume, low-value victims because they are relatively easy to distribute and do not require advanced expertise [11]. Spams are misunderstood as insignificant-even when they have shown an estimated daily volume of over 422 billion in January 2018 [12] and about 612 billion in January 2021 [8]. This constitutes over 85% of daily global data traffic a distribution eased by spammers who are capable of sending tons of messages via botnets in seconds to recipient's databank that are potentially vulnerable due to ineffective anti-virus and other countermeasures [11].

## 2. MATERIALS/METHODS

### 2.1. Phishing susceptibility: a review of related literature

Life's daily activities are rippled with risks and challenges and result in choices made from decisions cum conclusions reached as we traverse it. These risks are often associated with decisions and choices that we assumed are purely logical implying them to be rationale based on objective features. However, Kahneman and Tversky [13] note that many decisions are biased due to certain explicable factors. And as thus, a scam is a disguise, used by an adversary in an attempt to extract valuable data for monetary gain from an unsuspecting victim. Thus, a response to a scam becomes a decision error, if a user does not correctly estimate the risks due to certain biases. These and other reasons are why scams will continue to flourish as people tend to fall for them. Scams provide an attacker with the requisite chance to steal a victim's data or get money directly from the scam victims [14]. All scams are socially-engineered to appeal to different human vulnerabilities. They include (and are not limited to) desire for immediate gain, to help people, and to be liked by scam initiators. It suggests certain persons have 'victim traits' that make them more vulnerable/susceptible to scams [15], [16]. A victim may fall repeatedly into a scam. A factor that makes a person more likely to become a victim is the lack of emotional control. A University of Exeter study [17] reported that victims are incapable to resist response to persuasion and offers they responded to. Thus, the study concludes that often about 10-20% of a population are vulnerable to scams. Some people become serial scam victims and experience scams repeatedly.

Phishing is an identity theft targeted at compromising sensitive unsuspecting victim's data often for personal gains [18]. Phishing can involve the creation of compromised websites, the acquisition of email lists and botnets, and spoofing of mails, SMS designed to deceive an unsuspecting victim into downloading the malicious contents therein as originating from a legitimate and trustworthy source(s) [5], [8]. A phishing attack has three (3) elements: a lure, hook and catch. A lure message is received by a potential victim as originating from a legitimate source and its reliability is strengthened via exploiting the potential victim's desire for: i) curiosity as the message consists of compromised links; ii) fear as the message urges the potential victim to validate their data as a result of an account breach; and iii) empathy as the message seeks to impersonate a close associate in need of financial aid or personal data [19], [20].

De Kimpe *et al.* [18] known feats of phishing attacks include spelling errors, and monetary offers. If a user is convinced the message is genuine-the vulnerable victim is then convinced to divulge sensitive data. Phishers employ several social manipulators such as a trusted email source, implicating reciprocity (i.e., return of favors), social proof that allows others to participate in the scheme, creating a sense of scarcity via authorized source all of which aids the success of the deception. Phishers often employ a 3 parts scheme called the hook, catch and lure. A hook message includes a compromised attached link. While catch obtains and uses extracted data. This technique may appear simple but, it constantly evolves to reflect new trends [12] or use new methods of bypassing security measures to evade detection [11]. These attacks vary in frequency and diversity increasing their chances and likelihood of success [21].

Phishing has become more effective via social engineering techniques, to persuade potential victims to act [22]. The techniques are poised to appeal to a victim's emotions creating trust between a phisher and the unsuspecting victim via personalized emails. To ensure a high success rate, an attack is enacted in 2-stages namely: i) firstly, the phisher initiates contact with a potential victim and is able to assess the victim's friends and personal details and ii) next, the phisher contacts the victim requesting personal data via social media platform [23]. Request for personal data can also be via the provided data on a victim's page such as photos, a news feed, and other likely posts. Often, the messages include links/attachments that are laced with malware to impact the potential victim's device. With success now attained, the data retrieved is often used for further attacks on potential victims connected to the first victim as they now view the phisher as a mutual friend and believe him/her to genuine and/or legitimate [24].

### 2.2. Phishing and the Nigerian University Frontiers

Nigerian undergraduates have become phishing targets as well as perpetrators of phishing attacks. Crave for quick means to wealth has bedeviled Nigeria with myriads of fraudulent acts that robs her youth of the needed opportunities and progress [25], [26]. With ICT potentials and growth for users worldwide, a sine-qua-non effect is its plethora of attacks that seeks to exploit various associated compromises of the techs and mislead unsuspecting victims under guise of benefits; But, aimed at defrauding potential victims [27], [28].

Chanvarasuth [29] studied and compared the effectiveness of phishing versus vishing techniques for smartphone users-sampling 772 Thai undergraduates between the ages of 18-23 years. Result noted that phishing had a higher rate of success in comparison to vishing-as many of these factors such as age, gender, online habits, and personality traits had their varied impact on the rate of success for each of the technique.

Ojugo and Yoro [30] implemented a smartphone model to provide a dependable, e-banking app that ensure transaction authenticity, and message authorization to detect threats to account holders. They examined threats, focusing on the effectiveness of phishing-sampling 600 participants in Southern Nigeria. Their result indicates and supports Chanvarasuth [29] phishing yields more risk with higher rate of success, than vishing.

### 2.3. Study objectives

Previous studies observe that some users have an almost addictive habit to remain online with great time over social media sites. This allows them to participate in repeated behaviors, forming habit patterns that may involve page likes, message posts and comment on images. To address the inability to adequately process info contents, we posit a framework using the heuristic systematic model. It notes that participants can engage 2-modes to assess received messages [31], [32]. This is because Enos *et al.* [33] note that users with high score on neuroticism can barely detect lies as they become more upset when lied to and will rather believe people are truthful so as to avoid emotional drama/pain. Also, Parsons *et al.* [34] and Mayhorn *et al.* [35] stressed that premeditation allows users to highly detect lies. On personality traits thus, some studies believe that agreeable people are better equipped to detect lies [33]; while, other studies disagree with the case [34]–[36]. Thus, the objective of the study is to help identify and ascertain why some people are more susceptible and vulnerable to phishing over social media, and also therein identify factors that contribute greatly to such victim susceptibility and increased vulnerability to user trust-level and attacks.

### 2.4. Survey research

Research has begun to investigate how various aspects of psychology vis-à-vis personality traits seek to compromise potential victims as they traverse the internet via social media networking websites. One such concern is that the internet may soon replace normal social activities as individuals now preoccupy themselves with social media as they seek to compensate for loneliness and social seclusion. Previous studies successfully tagged the contributor features of phishing attacks as thus:

#### 2.4.1. Personality traits/framework

Personality is a consistent pattern of how people respond to stimuli in their environment and their attitude towards different events. McCrea and John [37] used a 5 factor model to measure personality. And as extended by Helavi *et al.* [38] it leverages a theoretical conceptualization using the following: i) neuroticism is the tendency to experience negative feelings such as guilt, anger, fear, and sadness. Studies showed that high neuroticism yields increased susceptibility to irrational thoughts, is less able to control impulses, and may not handle stress well; ii) conscientiousness is the tendency to show high self-control and strong-willed; iii) openness indicates the willingness to try new experiences, become more imaginative and intellectually curious; iv) agreeable is a person’s willingness to help others and believe in reciprocity; v) extroverted persons are more friendly and interact more. It samples 60 questions to capture the most common elements of personality traits with a precise structure description. It is considered superior and robust for understanding the relations between personality and various academic behaviors. This study seeks to examine if this relation extends to network security, traits, and privacy behavior [38] as shown in Figure 1.

#### 2.4.2. Demographics

It has been observed that another feature that influences susceptibility to phish attacks is gender, age as well as online presence pattern. Users between the ages of 18 and 29 were identified as being the most susceptible to phishing attacks on both email and social media platforms [8], [39]; while females between the ages of 24 to 42 were identified as being the most vulnerable to phishing attacks. This can be attributed to the fact that these young adults and females are constantly engaged to boycott social seclusion-leading to addiction [40]. Excessive social media use and dependence create opportunities for such potential victims to targets of phishers, which will in turn expose their close associates [41]. Other studies have also linked age to risky behavior that increases their chances of being phished and younger adults have less education and caution for financial risk; And thus, less exposure to phishing training [25]. Also, women have been identified as most susceptible to phishing and social engineering [4], [39], and has been 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 [2]. The complete demography of the participants is as in Table 1.

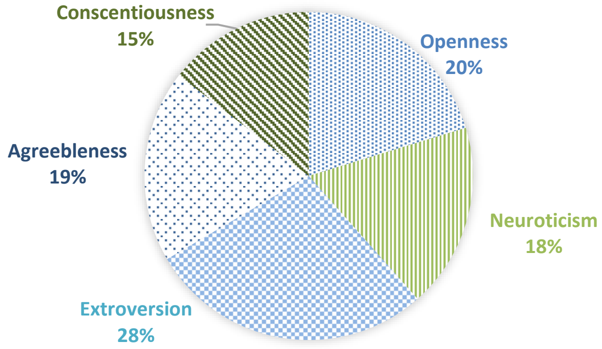


Figure 1. Personality traits factors that influence phishing susceptibility

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 |
| | | 21-25 | 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 |

### 2.4.3. Online presence

The presence of a potential victim as he/she surfs the internet can evolve into habits, which have also been found to influence phishing susceptibility. Highly active users on social media are more susceptible to social engineering attacks than those who participate less often [3]. Thus, a person's online habits influence the way they process misleading attack techniques on these sites [22]. Poor online habits increase susceptibility as these persons automatically click on links and respond to messages without engaging sufficient cognitive resources or paying enough attention to their online behavior [22], [23]. These can further cause a potential victim to be lured, hooked, and captured with little cognitive engagement using such social sites. This increases the probability that these users will thoughtlessly click on malicious links and/or accept a friend request from a fake profile without thinking about the impact of such actions [42]. Behaviors such as click on links, and share-like-scroll through posts regularly result in the user not paying attention to suspicious information on social media [43]. These in turn further impact negatively the user's trust and risk perception [44]. This is as shown in Figure 2, which details survey of online presence by users.

### 2.4.4. Media data content processing

Data processing involves two (2) modes namely: i) heuristic processing, and ii) systematic model [23], [45] allows an individual perceives if the available data is sufficient for him or her to determine the choice to be undertaken. Thus, the individual utilizes both heuristic processing (by taking cues that impact the limited cognitive resources to make judgments and decisions) and systematic processing (which involves the careful examination of the data to reach a decision [24]. The risk of info overload on social media sites and technology affordances encourages individuals to process content heuristically; and thus, leads to quick and effortless judgments [46]. Though heuristic processing is far more efficient, it significantly increases an individual's susceptibility to phishing attacks [47]. The reason is that with heuristic processing, individuals often overlook data cues that suggest the message is malicious and might pose a threat. Heuristic processing relies on judging the credibility of superficial cues-leading users to trust phishing messages [22].

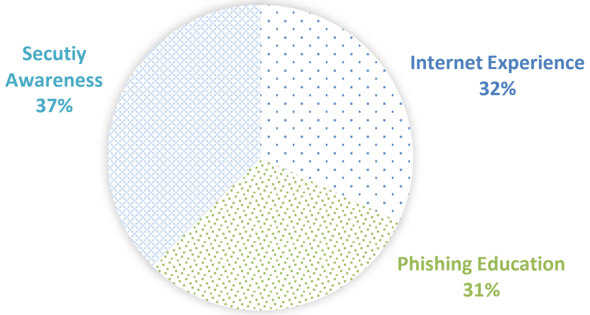
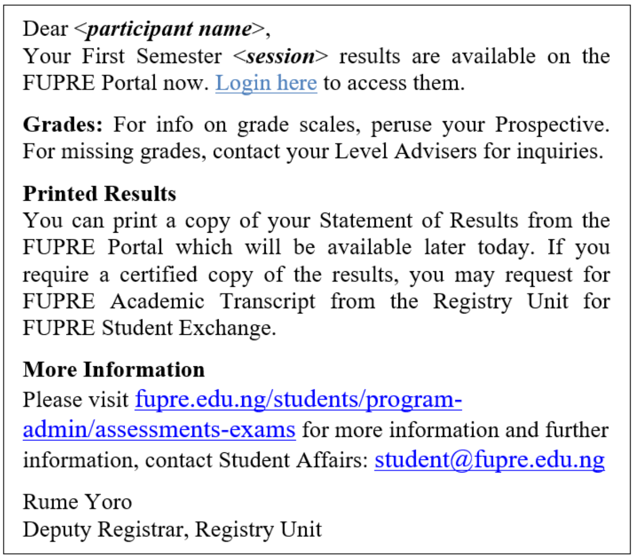


Figure 2. Online presence factors that influence phishing susceptibility

### 2.5. Technical details for phishing

Each participant's personal data extracted from their profiles was used to create content for the tailored emails, containing compromised links that required immediate response cum action. Thus, students (participant) who clicked the links and/or login here to enter their details, were phished. We tracked all phished participants. Sample emails for the tailored and spear-phished mails as in [48]. Mail sought to lure potential victims namely: i) mail seem sent from a trusted source, ii) requested immediate response to reduce the need for a thorough check, iii) likely increased their impulsive response, and iv) triggered visual processing to ensure they were expectant of their results in next screen. Sample email created for this (and other) participant(s) as in Figure 3. 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 the lack of social media presence, and restrictive privacy settings, personal data for all participants could not be acquired.



Dear <***participant name***>,
Your First Semester <***session***> results are available on the FUPRE Portal now. Login here to access them.

**Grades:** For info on grade scales, peruse your Prospective. For missing grades, 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 3. Sample tailored email

## 3. RESULTS AND DISCUSSION

### 3.1. Experiment's procedure

The study is divided into parts with link(s) to an online questionnaire to be filled out by students. The questionnaire consists of 3-parts: i) demographics part that included student's age, academics, and background data, ii) online activity part where students were assessed via a 5 point Likert scale of their online activity, and iii) privacy settings. To correlate the SN activity with the personality traits, the test participants were asked what kind of data they put on Facebook and Instagram, the frequency of postings, the number of images they post, and their privacy settings. The survey uses self-reported data and is back-checked for the accuracy of the values. We extracted personal data from participants. Value '1' is assigned to each element posted and all the variables were added together to create one 'social-network data'. Log-value for both the number of weekly posts and the overall number of images participants were collated with their Facebook/Instagram page as separate values (accounts). We compute updated variables via (1).

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

The same calculation was computed for the total number of photos. To evaluate privacy settings, participants were asked questions on 6 different privacy settings options namely: posting to SN wall, profile lookup, friends request, messaging, navigating their wall and that of others, and sharing and/or importing personal information into friends' page. Each entry therein was assigned a value between '0' (for nobody) and '3' (to make the item visible to everybody) to each privacy setting element. These values were then added to create a combined value for the Facebook privacy settings.

### 3.2. Findings

We selected a total of four hundred and eighty (480) participants from the Federal University of Petroleum Resources Effurun as in Table 1 and Figures 4 and 5. We observed that an overall 47% of the participants were phished; while an approximately 53% of the participants were not phished. Of 480 students that were sent the phishing email, about 72% (346 students) opened it. We observed actions of these participants that just opened it and noticed that of the 72% of students, that about 80% were in arts, humanities, and social sciences; while, about 20% are in engineering, natural and physical sciences. Furthermore, of the 346 participants that opened it, we observed that about 47% phished participants (i.e., students that proceeded to further click the compromised links as provided in the emails sent to these students) were found to be in the arts, humanities, and social sciences.

Of the 480 students that received the phishing email, approximately 72% (346 students) opened the mail. We further observed the actions of these participants that just simply opened the mail, we noticed that of the 72% of students who opened the email we observed that 80% of them were in the arts, humanities, and social sciences majors; while 20% were found to be in engineering, natural and physical sciences. In furtherance to the 346 participants that opened the email, the study observed that a majority of the 47% phished participants (i.e., students that proceeded to further click the compromised links as provided in the emails sent to these students) were found to be in the arts, humanities, and social sciences.

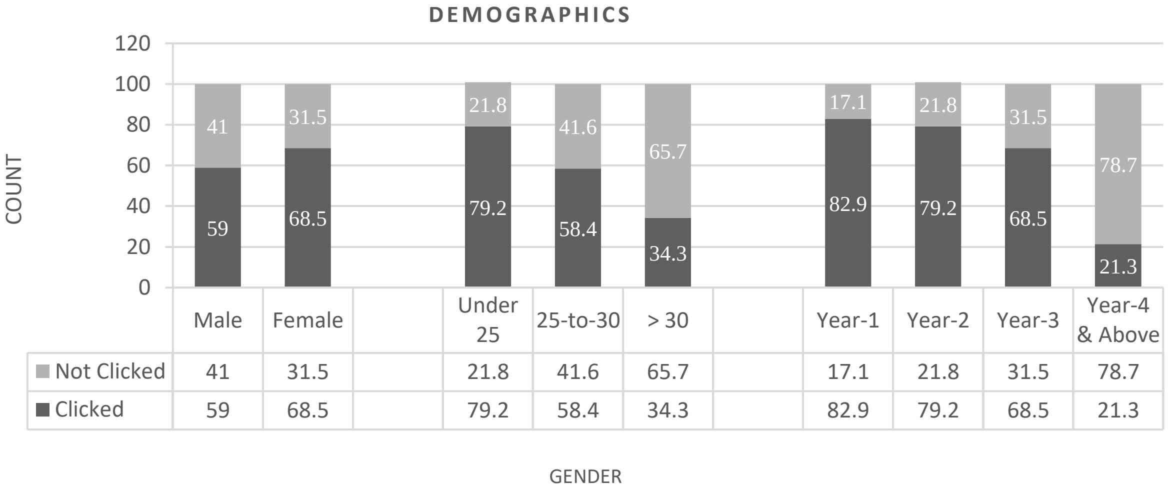


Figure 4. Demographics factor impacts on phishing susceptibility by percentage

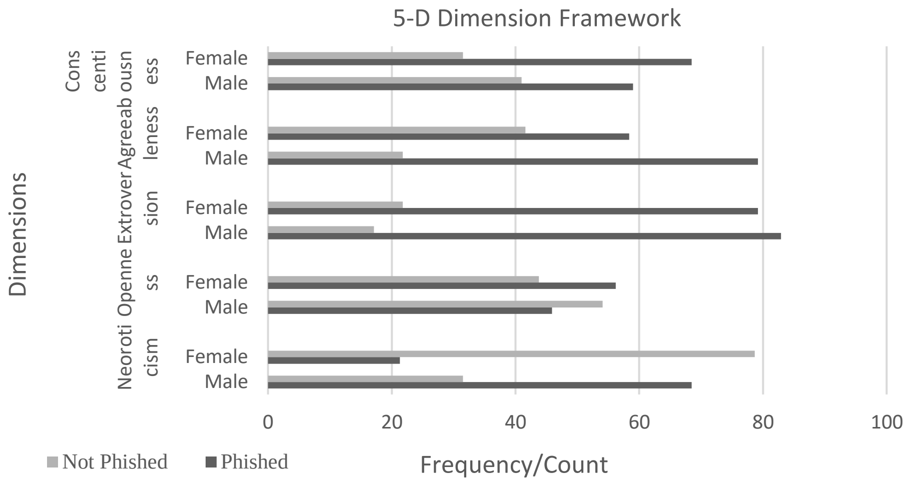


Figure 5. The big-5 framework for phished/not phished participants

### 3.3. Discussion of findings

Results have shown that phishing campaigns and awareness among students on campus, hours spent on the internet-enabled devices such as smartphones and computer systems, cyber training, academic year, age, gender, and affiliation are all significant variables and factors that impact participants' susceptibility. The aggregated college affiliation on demographics data for students in science, technology, engineering, and mathematics (STEM) with info and communication technology majors in particular were seen to have lower phishing susceptibility rates (i.e., opened emails received as well as clicking on the compromised links). The increasing academic year progression also saw a decrease in phished participants and click rates to open the email. We observed that increased time on the computer and cyber-awareness correlated with lower click rates. Contrary to our expectations, students who were unaware of phishing attacks performed better than students who were primed and aware of phishing attacks, or students who understood what phishing attacks agreed with [49]–[55].

## 4. CONCLUSION

As a conclusion, we believe that the success rate of a fake scam (phishing scheme) is richly attributed to a combination of personal relevance (featuring as traits), emotional gaps/strength, and the fear factor. It is thus, important to educate users on the need to provide control measures over their social media pages so as to prevent socially-engineered attacks. As an example, Facebook has launched phish@fb.com, a dedicated email address to support users wishing to report scam/phishing attempts so that Facebook can investigate, blacklist, and hold phishers accountable. They also provide info equipping users of the steps to follow (if and when phished) and/or attacked by malware. This 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. Together both the user and the social media platform are responsible for preventing, reporting, dissolving, and remaining aware of phishing attacks. The social media platform is responsible for educating users and providing controls to reduce phishing attacks. On the other hand, users bear the responsibility of staying informed regarding prevention techniques and using the controls put in place to reduce these incidents. Thus, 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. 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. Kemp, “Digital trends 2019: every single stat you need to know about the internet,” *thenextweb*. 2019, Accessed: Sep. 16, 2019. [Online]. Available: https://thenextweb.com/news/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet.

[4] 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.

[5] 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.

[6] 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, 2018.

[7] I. Barker, “Social media phishing attacks up more than 70 percent,” *betanews*. 2019, [Online]. Available: https://betanews.com/2019/05/02/social-media-phishing/.

[8] 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.

[9] 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.

[10] 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.

[11] M. Alazab and R. Broadhurst, “Spam and criminal activity,” *Trends and issues in crime and criminal justice*, no. 526, pp. 1–20, 2016.

[12] D. Gudkova, M. Vergelis, T. Shcherbakova, and N. Demidova, “Spam and phishing in Q3 2017,” *Securelist*. 2017, Accessed: Jan. 25, 2018. [Online]. Available: https://securelist.com/spam-and-phishing-in-q3-2017/82901/.

[13] D. Kahneman and A. Tversky, “Prospect theory: an analysis of decision under risk,” in *Handbook of the fundamentals of financial decision making: Part I*, World Scientific, 2013, pp. 99–127.

[14] 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.

[15] 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.

[16] D. Modic and S. E. Lea, “How neurotic are scam victims, really? The big five and Internet scams,” *The Big Five and Internet Scams (September 10, 2012)*, 2012.

[17] S. E. G. Lea, P. Fischer, and K. M. Evans, “The psychology of scams: provoking and committing errors of judgement.” Office of Fair Trading, 2009.

[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] 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.

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

[21] W. Rocha 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.

[22] E. D. Frauenstein and S. V Flowerday, “Social network phishing: becoming habituated to clicks and ignorant to threats?,” in *2016 Information Security for South Africa (ISSA)*, Aug. 2016, pp. 98–105, doi: 10.1109/ISSA.2016.7802935.

[23] 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, Jan. 2015, doi: 10.1111/jcc4.12100.

[24] A. Vishwanath, B. Harrison, and Y. J. Ng, “Suspicion, cognition, and automaticity model of phishing susceptibility,” *Communication Research*, vol. 45, no. 8, pp. 1146–1166, Dec. 2018, doi: 10.1177/0093650215627483.

[25] 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 *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010, pp. 373–382.

[26] J. Wang, R. Chen, T. Herath, and H. R. Rao, “An empirical exploration of the design pattern of phishing attacks,” *Annals of emerging research in information assurance, security and privacy services. Bingley, England: Emerald Publishers*, 2009.

[27] E. O. Yeboah-Boateng and P. M. Amanor, “Phishing, SMiShing and 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.

[28] A. A. Ojugo, C. O. Obruche, and A. O. Eboka, “Quest for convergence solution using hybrid genetic algorithm trained neural network model for metamorphic malware detection,” *ARRUS Journal of Engineering and Technology*, vol. 2, no. 1, pp. 12–23, Nov. 2021, doi: 10.35877/jetech613.

[29] 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.

[30] A. Adimabua Ojugo and R. Elizabeth Yoro, “Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 21, no. 3, pp. 1673–1682, Mar. 2021, doi: 10.11591/ijeecs.v21.i3.pp1673-1682.

[31] 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, 2012.

[32] 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.

[33] 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,” Sep. 2006, doi: 10.21437/Interspeech.2006-278.

[34] 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.

[35] C. B. Mayhorn, A. K. Welk, O. A. Zielinska, and E. Murphy-Hill, “Assessing individual differences in a phishing detection task,” 2015.

[36] 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.

[37] 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.

[38] 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.

[39] A. A. Algarni, Y. Xu, and T. Chan, “Susceptibility to social engineering in social networking sites: The case of Facebook,” 2015.

[40] M. N. Banu and S. M. Banu, “A comprehensive study of phishing attacks,” *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 768–783, 2013.

[41] D. Brecht, “Phishing attacks targeting young adults,” *Infosec*. 2017, Accessed: Mar. 10, 2020. [Online]. Available: https://resources.infosecinstitute.com/topic/phishing-attacks-targeting-young-adults/#gref.

[42] A. A. Ojugo and A. O. Eboka, “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, Dec. 2020, doi: 10.5815/ijmecs.2020.06.03.

[43] 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.

[44] S. M. Albladi and G. R. S. Weir, “User characteristics that influence judgment of social engineering attacks in social networks,” *Human-centric Computing and Information Sciences*, vol. 8, no. 1, Dec. 2018, doi: 10.1186/s13673-018-0128-7.

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

[46] X. Lin, P. R. Spence, and K. A. Lachlan, “Social media and credibility indicators: The effect of influence cues,” *Computers in Human Behavior*, vol. 63, pp. 264–271, Oct. 2016, doi: 10.1016/j.chb.2016.05.002.

[47] D. Liu and W. K. Campbell, “The Big Five personality traits, Big Two metatraits and social media: A meta-analysis,” *Journal of Research in Personality*, vol. 70, pp. 229–240, Oct. 2017, doi: 10.1016/j.jrp.2017.08.004.

[48] Y. Zhang, S. Egelman, L. Cranor, and J. Hong, “Phinding phish: evaluating anti-phishing tools,” *Carnegie Mellon University*, 2007.

[49] 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.

[50] 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, Apr. 2020, doi: 10.11591/ijict.v9i1.pp9-18.

[51] R. Broadhurst, K. Skinner, N. Sifniotis, and B. Matamoros-Macias, “Cybercrime risks in a University Student Community,” *SSRN Electronic Journal*, 2018, doi: 10.2139/ssrn.3176319.

[52] 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.

[53] 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.

[54] A. A. Ojugo and O. Otakore, “Mitigating social engineering menace in Nigerian Universities,” *Journal of Computer Sciences and Applications*, vol. 6, no. 2, pp. 64–68, Aug. 2018, doi: 10.12691/jcsa-6-2-2.

[55] “What can I do about malicious software on Facebook?,” *Facebook*. 2020, Accessed: Mar. 11, 2020. [Online]. Available: https://www.facebook.com/help/389666567759871.

## BIOGRAPHIES OF AUTHORS

**Rume Elizabeth Yoro** received B.Sc in Computer Science from the University of Benin Edo State in 2000, M.Sc 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 Cyber Security, Faculty of Information Technology at the Dennis Osadebey University Asaba. Her research interests include: Network Management, Cyber Security 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 email: rumerisky5@gmail.com.

**Fidelis Obukohwo Aghware** received his B.Sc in Computer Science from The University of Benin, Benin City in 1998; M.Sc 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 Cyber Security, 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: email: fidelis.aghware@unidel.edu.ng.

**Bridget Ogheneovo Malasowe** received her B.Sc in Computer Science from The University of Benin, Benin City in 1998. She obtained her M.Sc 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 are 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 email: 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 is a member of: The Nigerian Computer Society. He is married to Jennifer Nwankwo, and they both have two daughters. He can be contacted at email: tuk2obinna@gmail.com.

**Arnold Adimabua Ojugo** received his B.Sc, M.Sc 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, Cyber Security, 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 email: ojugo.arnold@fupre.edu.ng.