Acta Informatica Pragensia, 2018, 7(2), 138–151
DOI: 10.18267/j.aip.119
Original Article

A Users' Awareness Study and Influence of Socio-Demography Perception of Anti-Phishing Security Tips

Abdul Orunsolu [1], Omorinola Afolabi [2], Simon Sodiya [3], Adio Akinwale [3]

Abstract

Security tips are now used as a method of priming online users from falling prey for fraudulent scams. These security tips usually come as email, SMS or online posts where they can be easily accessed by the users. In this work, phishing attacks are simulated with varying cues that are available in such fraudulent email messages, SMS and web pages were used to investigate the effectiveness of the security tips used by Nigerian banks to prime their customers of online threats. A total of 427 respondents, purposively selected from three tertiary institutions in Ogun State, participated in the study. Each respondent was asked to identify five messages with varying phishing cues to evaluate their understanding of the security tips messages. The results which were computed at 95% Confidence Interval, indicated that 58.91% failed on the first attribute, 58.59% failed on the second attribute while 58.73% failed on the third attribute. 74.24% of the participant could not correctly identify a fake email message (fourth attribute) while 76.71% could not correctly identify a phished bank verification number update message (fifth attribute). Using the Mann Whitney Test, the result further showed that overall, those who failed the test are significantly more than those who passed. Moreover, a regression model is proposed to evaluate the influence of the socio-demographic factors used in the study. This result indicated that gender, academic qualification and user's computer knowledge significantly influences their ability to recognize phished messages.

Keywords: Anti-phishing, Electronic commerce, Phishing cues, Security tips, User awareness.

1 Introduction

The widespread use of computers, mobile devices and network systems has increased the online market penetration of most businesses. Every day, the sales channels of various businesses are gradually shifted to the Internet. This transformation offered numerous potentials in terms of global presence, automated availability of products/services etc. However, these opportunities are being continuously challenged by increasing rate of cybercrimes (Konradt et al., 2016; Li et al., 2016; PandaLabs Report, 2012). These

[1] Department of Computer Science, Moshood Abiola Polytechnic, Ojere, P.M.B. 2210, Abeokuta, Nigeria
✉ orunsolu.abdul@mapoly.edu.ng

[2] Department of General Studies, Moshood Abiola Polytechnic, Ojere, P.M.B. 2210, Abeokuta, Nigeria

[3] Department of Computer Science, Federal University of Agriculture, Alabata, P.M.B 2240, Abeokuta, Nigeria

cybercrimes range from malware attacks, botnets attacks, drive-by download, spam-advertised commerce etc.

One of the most widely reported cybercrimes is the phishing attack. Phishing is a social engineering attack which attempts to fraudulently obtain users' personal and financially sensitive information through electronic communication (Parsons et al., 2015). In a typical phishing attack, both service providers, online companies and users suffer from brand damages, enormous financial losses, breach of confidence and unhealthy exposure of users' credentials, which provide negative incentives for e-commerce. According to the Central Bank of Nigeria White paper, it was estimated that about $250 million was lost to cybercrime in 2013 (Longe, 2014). In addition, in one FBI report, the damage from Nigerian phisher activity from October 2013 to May 2016 was estimated to exceed US$ 3 billion in a number of attacks that and affected 22,143 companies scattered across 79 countries of the world. Figure 1 provides the scary report on the incident of phishing websites in the First Half of 2017 from Anti-Phishing Working Group (APWG, 2017).

Faced with this negative reality, online security providers, as well as the academic community, responded with a number of countermeasures to arrest the ugly incidences of phishing attacks. These solutions range from software enhancement methods to anti-phishing education. In the software enhancement method, detection tools called anti-phishing systems are designed and implemented to identify a typical phishing attack in an online transaction. However, research indicated that it does not matter the number of firewalls, encryption system, security certificate or authentication mechanisms employed by an organization if the user using the system fails to understand phishing attacks (Hong, 2012).

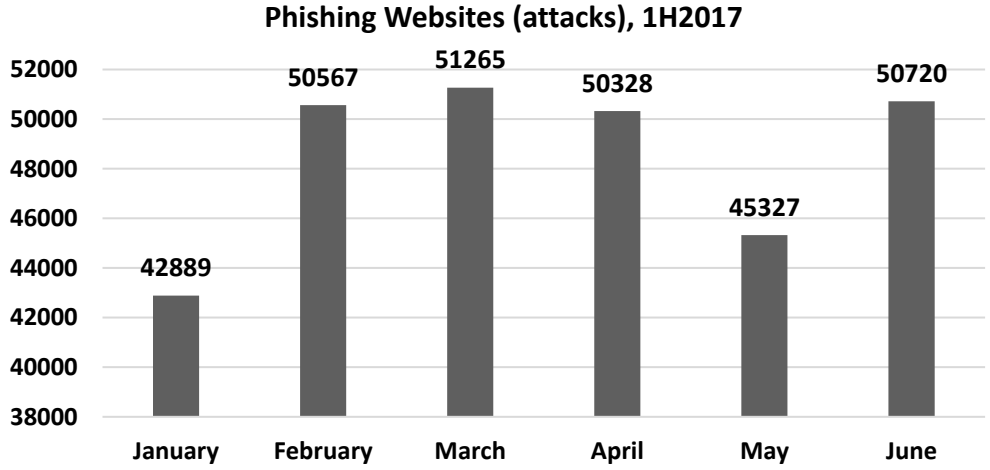

Fig. 1. *Number of Unique Phishing Websites in 1H 2017. Source: (APWG, 2017)*

Today, most financial institutions provide security tips to their customers to enable them to identify online scams. For instance, Nigerian Banks send security tips via SMS, email and online security centres to provide anti-phishing education to their customers. How effective is this anti-phishing security tip to these customers in an online transaction? To this end, we report a simulated study to evaluate the effectiveness of this method by using phishing messages with varying phishing cues (Orunsolu et al., 2016). In addition, a regression model is developed to evaluate the socio-demographic factors that affect respondents' ability to identify such fraudulent messages.

The rest of the paper is organized as follows: Section 2 presents the research methods used to investigate the research question. related work. The results analysis of the research

experiments is discussed in Section 3. In Section 4, the regression analysis and design variables are discussed. Section 5contains the general discussion and conclusions.

1.1 Literature review

Phishing education is meant to protect individual users against phishing threats. Anti-phishing security awareness education offers online training materials, testing, and situated learning to enhance users' avoidance capability in detecting phishing attacks. Online security training materials have been provided by anti-virus companies, government organizations, non-profits security institutions (e.g. Anti-Phishing Working Group) and businesses (e.g. eBay, Microsoft, Google). This security awareness describes how phishing works and provide solutions to escape phishing attacks. For instance, Nigerian Banks send security tips to their customers and equally posted such tips on the security centre of their home page (Figure 2). These tips inform users on how well they can identify which messages are legitimate and which are not. Besides, a number of research works have investigated the role of education in phishing as well as why people fall for Phish.

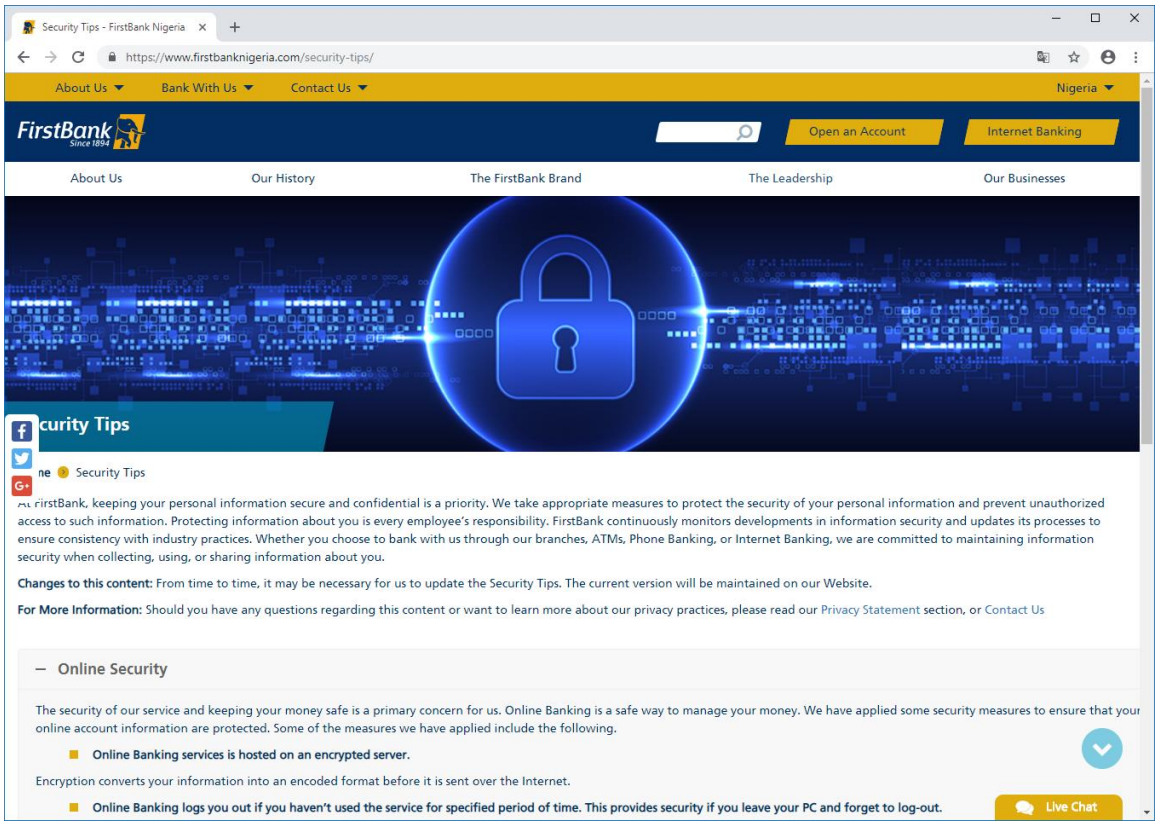

Fig. 2. *Example of Security Tips from First Bank Nigeria. Source Authors.*

Jagatic et al. (2006) researched into spear-phishing attacks in which the attackers employed specific knowledge of users and their companies to conduct an attack. Their investigation showed that individuals were more likely to fall for phishing attacks originated from existing-known contacts over standard phishing attacks. This is why social networking sites like Facebook are now more patronized by phishers. In another development, Sheng et al. (2010) and Jakobsson et al. (2007) provided useful insights on why phishing works using demographic data. While Sheng et al. 2010 revealed that women-folk are more vulnerable than their male counterpart due to their less exposure to computer technical knowledge;

Jakobsson et al. (2007) revealed users' sensitivity to numbers of common trust/security symbols such as favicon, brand logos, padlock icons etc. when navigating web pages.

Kumaraguru et al. (2007) presented a study which focuses on educating people about phishing attacks and assisting such users to make a positive decision when faced with the real-life situation. The authors showed that a number of challenges affected end-user security awareness education in general. In the end, the authors designed an automated email based anti-phishing system known as PhishGuru and an online game called "Anti-Phishing Phil". These automated anti-phishing systems educated users on how to understand cues in domain names to detect phishing attacks. The empirical results suggested that, while technical systems should be served as the first line of defence against phishing attacks, user security awareness education offers a complementary approach to assist users better identify fraudulent emails messages and websites. Similarly, Sheng et al. (2010) presented a usability study in which a role-play survey of 1,001 online participants was used to demonstrate the relationship among demographics, phishing susceptibility and the effectiveness of a number of anti-phishing security educational materials. The finding of this work indicated that security awareness materials reduced participants' tendency to input sensitive information into fake URLs by 40%. On the contrary, there was decreased participants' tendency to click on benign links with some other security awareness materials.

Arachchilage and Love, (2013) proposed and developed a framework using a game approach which enhanced participant avoidance behaviour through motivation by protecting users from phishing attacks. A theoretical model derived from Technology Threat Avoidance Theory (TTAT) was used in the game design framework. The TTAT identified the issues that the game design framework needed to address by developing threat perceptions that motivated individuals to avoid phishing attacks and use safeguarding measures. The study emphasized that avoidance motivation for phishing attack was majorly influenced by combined factors of perceived threat and safeguard effectiveness. In addition, the study bridged the gap in the software-based anti-phishing approaches through user awareness model using a game design approach. However, the work did not provide empirical evidence to explain the interaction of perceived threat and safeguard effectiveness.

Alsharnouby et al. (2015) presented a user study where the use of eye tracker was employed to obtain quantitative data on user judgment of phishing sites. The results of their work showed that 53% of the participants detect phishing pages when primed to identify such pages with little attention to security cues. Similarly, Parsons et al. (2015) conducted a role-play usability study to experiment people's ability to distinguish between phishing and genuine emails. The authors had previously informed half of the participant about the purpose of the study as a control group. The evaluation results indicated that the control group performed remarkably better at discriminating between phishing and genuine emails than the non-informed group.

Our contributions: Our work is hinged on the fact that the effectiveness of security tips in the fight against phishing attacks is yet to be subjected to empirical research. We are reporting on a first tripartite study of participants' response to SMS, email and web pages with varying phishing cues. Our study provides the following major contributions to anti-phishing security education research:

1. We pursue a novel methodology that develops an automated Anti-Phishing Questionnaire which elicits users' judgments on phishing messages based on their knowledge of security tips.

2. We evaluate the effectiveness of the security tips based on data collected from three different institutions located in three different places within Ogun State, South West, Nigeria. However, most previous studies based their evaluation on data collected within a single geographical environment (e.g. Dhamija et al., 2005; Vishwanath, 2016; Parsons et al., 2015; Neupane et al., 2015; Downs et al., 2006).
3. Our work extends and supports prior studies by independently re-affirming the findings of the previous study on anti-phishing education within the Nigeria perspective.
4. Our work develops a regression model to investigate factors that actually influence the users' identification of fraudulent messages even after being primed with previous security tip messages.

2 Research methodology

The objective of the study is to determine the effectiveness of security tips sent by Nigerian Banks to their customers, in the fight against phishing attacks. In order to achieve this objective, we design a Computer-based Anti-Phishing Questionnaire (CAPQ) to test user's ability to detect fake SMS, email and web pages. The CAPQ consists of the Data Collection phase, Site Selection phase and Test phase. In the Data Collection phase, personal details of respondents are captured. Such details include gender, educational qualification, computer literacy and occupation. Based on the user's responses, the CAPQ categorizes users as informed or non-informed. To determine the user's level of being informed, the application assigned a value 1 or 0 to each data supplied by the user. The value 1 indicates that the data has a significant influence on the user's knowledge of computer/Internet and its services. For instance, Figure 3 presents the interface of CAPQ with a data value of 1 on its leftmost part. On the other hand, the value 0 indicates that the data does not significantly influence the users' knowledge. For example, age, gender and Local Government of Residence do not indicate ones' knowledge of computer and its associated services. For a user to be classified as informed, the user must score 5 points on all the significant data values. A simple pseudocode for this is as follows:

```
If informed.Text < 5 Then
                set.status.Text = "non-informed"
                     Else
        set.status.Text = "Informed"
End If
```

Thus, an informed user is a person that has appreciable knowledge of how computers/Internet works and a non-informed user is one without adequate knowledge of computer/Internet.

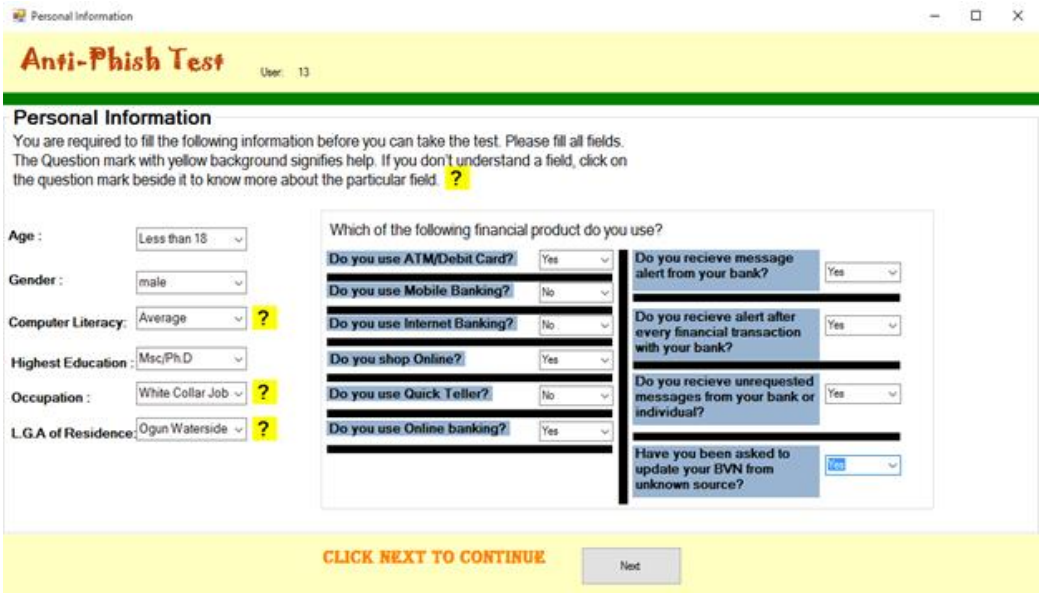

Fig. 3. *A CAPQ Interface with a data value of 1 at the leftmost part. Source Authors.*

After the status of the respondent has been determined, the user is allowed to select a number of online services or webpages they are accustomed to. In this way, the application is able to customize the user's text messages in the Test phase to the web pages that are known to them. For example, if a user selects First Bank Nigeria PLC and OLX as brands that are known to him, then the application will ask such user to identify the Home page of such online brands.

The final phase of the application is the Test phase where the users are asked to judge the status of 5 random messages consisting of email, SMS and Web pages with varying phishing cues. In each of the five tests, certain phishing cues are embedded in the message to assess the users' understanding of the security tips. Each message provides a Yes or No answer displayed at the upper part of the page for users to judge. The following parameters are tested in each of the messages:

a. In Link (Inlink)

b. URL with more than three dots (three dots)

c. URL using IP Numbers (IPadd)

d. Fake Bank Verification Number (BVN) message (BVN message)

e. Fake Customer Care email message (email)

The first three parameters are common phishing cues which are mostly used by phishers to deceive online users. For instance, In Link is used when a URL within a webpage is directed to another domain. Cybercriminals use this method to divert user's content to their fake page without the user being aware. In addition, fake websites with IP based address and URL with more than three dots were created by using the logo and layout of the corresponding real bank sites or online shopping stores. The remaining parameters are mostly used as SMS or email ploy to deceive bank users. This SMS or email message contains a private number and uses a sense of urgency to deceive users. In addition, bad grammars are common in this message. In order to protect the respondents from real-world phishing messages, we downloaded these sites and messages for offline use and hosted them on our local machine.

Our experiment is designed so that users are asked to identify fake messages and our focus is then to determine users' performance based on their understanding of the security tips send by their Banks. Based on the foregoing, the study seeks to test the following hypothesis:

H_0: *Security tips are well understood by bank customers.*

H_1: *Security tips are not well understood by bank customers.*

2.1 Participants Recruitment and Experimentation

Previous empirical study on phishing attacks usually selects respondents from only one geographic location (Vishwanath, 2016; Parsons et al., 2015; Neupane et al. 2015). Downs et al. (2006). To improve on this, this study selects participants from three different tertiary institutions in Ogun State. The target population for this study is staff and students in tertiary institutions because young people and middle-aged adults, who are predominantly found in the tertiary institution environment, are the most relevant demographic strata for a technological driven-research such security of e-commerce transaction. In addition, it is believed that while this demographic group could be found in other areas of the workforce like banking, those in the tertiary institution environment are more likely to be able to spare the time to participate in the study considering that the data collection phase would require participants to come to the data collection site for participation. The actual institutions used for the research were selected based on the ease of accessibility of the researcher and participants were selected using judgment sampling technique – a non-probability sampling method where the investigator chooses stratum to be surveyed based on their knowledge and professional judgment. Informed consent of selected participants was obtained prior to their participation and participants were assured that participation is voluntary, and they can withdraw from the study at will without any negative consequence.

A total of 427 participants were involved in the study. These participants were purposively selected from the staff and student population in three tertiary institutions in Ogun State – Tai Solarin College of Education, Omu-Ijebu; Gateway ICT Itori and Moshood Abiola Polytechnic, Abeokuta.

Fig. 4*. Process Flow Diagram for CAPQ. Source Authors.*

There were 245 males and 182 females. There were 55% NCE/OND holders, 30% HND/BSC holders and 9% SSCE/WASCE holders in the population (see also Section 4). Also, the frequency of the type of financial services used by our participants is as follows: 91% used ATM card, 51% used Mobile Banking, 36% used Internet Banking, 22% used Quick Teller and 41% used Online Banking and Online Shopping services. Moreover, about 91% of the respondents claimed to have received security message from their banks. In terms of age distribution, 80% of the participants were under 25 years, 14% between 26 and 35, 6% between 36 and 50 and less than 1% above 50. The composition of the participants could limit the generalization in our findings. On the contrary, Lin and Lu (2000) posited that the results drawn from the analysis of this type of sample can still show the real phenomena and provide major outcomes. This is due to the fact that the young and the middle-aged population are the

most significant groups for a technological based-research such security of electronic commerce transaction. In fact, notification sounds and indicator lights which frequently heralds social feeds, emails, SMS etc. through which the malicious messages under investigation are spread are very common within this age bracket (Vishwanath, 2016).

In our experiments, participants commenced a session by going through a welcome page. The welcome page contains the instruction on the experiment. Then, the participant is asked to fill in personal data and the number of online services/web pages they patronized. In the final stage, participants are asked to judge 5 randomized messages with varying phishing cues. These messages consisting of one (1) fake BVN message, one (1) fake email messages and three (3) web pages of the banks/online shopping sites used by the participants. The fake BVN message contains bad grammars and private number call centre as portrayed in most of such unsolicited fake messages. The fake email message asked the user to update their details. On the other hand, the three fake web pages used the logo and visual similarity of a known financial brand and online shopping sites. The first fake webpage used In Link attributes as a phishing cue. The second webpage used an IP-based URL with a look and feel of the known financial institution and the third fake webpage used the three dots attributes. Each trial consisted of a message (e.g. webpage or BVN or email) shown for as long as the participant responded. The response consists of a panel with a question," Is this a legitimate website" or "Is this a legitimate BVN message" or "Is this a legitimate email" and a "Yes" or "No". This panel is displayed at the header part of each investigative page. Each participant took about 9 minutes to complete the study. The process flow diagram of the experiment with an average time duration is presented in Figure 4. The participants' responses are recorded into our database and exported in a spreadsheet format for easy statistical analysis.

3 Results

The results in this research work are reported at the significance level (α) of 0.05 using two-tailed Test. Table 1 shows the Test statistics used in computing the results. The Mann-Whitney U test was used to test if there is a significant difference between participants who passed and those participants who failed on each of the test attributes. Furthermore, the Wilcoxon W Test was chosen to examine the difference in each of the attribute. About 58.91% failed on the three dots attributes, 58.59% failed on the use of IP attribute while 58.73% failed on the In Link. In addition, 76.71% could not correctly identify a phished BVN Update message while 74.24% could not correctly identify a fake email message. This suggests that in spite of the security messages they had received from their banks; they are still unable to correctly identify a phished message.

	Three Dots	**IP-based URL**	**In Link**	**BVN Message**	**Fake email**
Mann-Whitney U	12539.500	11384.000	11233.000	14920.500	15073.000
Wilcoxon W	40034.500	38879.000	38494.000	42415.500	42568.000
Z	-6.735	-7.919	-7.619	-4.618	-4.479
Asymp. Sig. (2-tailed)	.000	.000	.000	.000	.000

Tab. 1. *Test Statistics. Source Authors.*

To test the Hypothesis, the Mann Whitney U test was carried out to ascertain if there is a significant difference between those who passed and those who failed on each of the test

attributes. The result in Table 1 shows that those who failed the test are significantly more than those who passed. This suggests that Bank customers do not really understand the security messages they receive from their banks. Hence, we reject the null hypothesis that security tips are well – understood by bank customers.

4 Regression Analysis and Design Variables

Dependent Variable

The aggregate score of respondents in the pretest phase (Pretest Score abbreviated as PTSC) was used as a measure of their ability to detect phished messages and it served as the dependent variable for the regression analysis.

Independent Variables

All independent variables are categorical variables on either the ordinal or nominal scale of measurement. Four variables (Gender, Occupation, Highest Academic Qualification and computer Literacy) are self-reported while User type is computer generated. All 427 respondents provided information on all variables, hence, there was no missing value.

i. Gender

This is a categorical variable on the nominal scale of measurement where 1 represented the male and 2 represented females. 245 (57.51%) of the respondents reported being male and 181 (42.49%) reported being female.

ii. Occupation

Respondents' occupation is also on the nominal scale of measurement. Since the study was carried out in tertiary institutions, we defined only three categories of occupation viz – White Collar, Blue Collar and Students. It is believed that these three mutually exclusive categories sufficiently cover all occupation types present within a tertiary institution environment. 53 (12.41%) reported being in white-collar occupation, 13 (3.04%) reported engagement in blue-collar occupation while 361 (84.54%) reported that they are students.

iii. Highest Academic Qualification

This is a categorical variable on the ordinal scale of measurement. This variable is also presented as four categories – Senior School Certificate Examination (SSCE) or West African School Certificate (WASC); National Certificate of Education (NCE) or Ordinary National Diploma (OND); Higher National Diploma (HND) or Bachelor of Science (BSC); Master of Science (MSC) or Doctor of Philosophy (PHD). 38 (8.94%) had only SSCE/WASC qualification, 235 (55.29%) had NCE/OND qualification, 129 (30.35%) had HND/BSC qualification and 23 (5.41%) had MSC/PHD qualification.

iv. Computer literacy

This variable is a self-reported evaluation of respondents perceived computer literacy level. It was captured on the ordinal measurement scale, in four categories namely – not literate, represented as 1, low literacy represented as 2, average literacy represented as 3 and high literacy represented as 4. Two (0.47%) reported no literacy, 31 respondents (7.28%) reported low literacy, 269 respondents (63.15%) reported average literacy while 124 respondents (29.11%) reported high literacy.

v. User Type

This is a binary variable. It is a computer-generated assessment of respondents' computer literacy level. Based on the user's responses, the APQ categorizes users as informed or non-informed. To determine this, the application assigned a value 1 or 0 to each data supplied by the user. The value 1 indicates that the data has a significant influence on the user's knowledge of computer/Internet and its services. On the other hand, the value 0 indicates that the data does not significantly influence the users' knowledge. For a user to be classified as informed, the user must score 5 points on all the significant data values. Thus, an informed user is a person that considered having appreciable knowledge of how computers/Internet works while a non-informed user is one who is considered not having adequate knowledge of the computer/Internet. Of the 427 participants, 324 (75.88%) were categorized as informed users while 103 (24.12%) were categorized as non-informed users.

Model Specification

The proposed model for the regression analysis is given as:

$$Y = b_0 + b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 + b_5X_5$$

Where:

X_1 = Gender

X_2 = Occupation

X_3 = Highest Academic Qualification (HAQ)

X_4 = Computer Literacy

X_5 = User Type

Regression Analysis Diagnostic Checks

i. Normality check

This was carried out with the Shapiro-Wilk's test, which is recommended for data with less than 2000 items. The test confirmed that the data on the four variables – are normally distributed as evidenced by the test statistics; 0.946 ($p \leq 0.316$), 713 ($p \leq 0.200$), 0.827 ($p \leq 0.215$), 0.913 ($p \leq 0.297$), 0.841 ($p \leq 0.255$) for Gender, Occupation, Highest Academic Qualification, Computer Literacy and User Type respectively.

Variable	R^2	B	T (Sig)	F (Sig)	DW
Gender	0.014	0.079	2.429 (0.016)	5.902 (0.016)	2.346
Occupation	0.000	0.002	0.76 (0.940)	0.006 (0.940)	2.608
HAQ	0.025	0.072	3.321(0.001)	11.029 (0.001)	2.683
Computer Literacy	0.003	0.27	1.038 (0.300)	1.077 (0.300)	2.614
User Type	0.029	0.23	0.598 (0.550)	0.358 (0.550)	2.606

Tab. 2: *Summary of simple univariate linear regression of independent variables.*

ii. Collinearity Check

The Variance Inflation Factor (VIF) was employed to assess the collinearity of the independent variables. The result shows that the VIF for the four independent variables is 1.042, 1.220, 1.120, 1.112 and 1.065 for Gender, Occupation, Computer Literacy, HAQ and User Type respectively.

iii. Autocorrelation Check

The Durbin Watson statistic was used to check if the assumption of no autocorrelation was satisfied. The Durbin-Watson's tests the null hypothesis that the residuals are not linearly auto-correlated. The Durbin Watson Statistics was 2.05, this confirmed that there is no auto-correlation in the multiple linear regression data.

Model Construction and Analysis

A preliminary multiple regression analysis was carried out to determine the suitability of each of the independent variables for inclusion in the final regression model. This was done in two stages. In the first stage, each of the independent variables was regressed with the dependent variable as simple linear univariate regressions. The second stage seeks to identify the best combinations of the independent variables to include in the model. Here, all the independent variables were regressed with the dependent variable simultaneously. Table 2 and 3 shows a summary of stage 1 and stage 2 model building. The result in Table 2 and Table 3 shows that occupation and computer literacy did not have a significant R2 value in the univariate model and neither did they contribute significantly to either the univariate model or the multivariate model. Therefore, both variables are excluded from the final multiple regression model.

Variable	Coefficient (B)	SE	T Value	P Value
Intercept	0.612	0.109	3.924	0.00
Gender	0.076	0.013	2.481	0.016
Occupation	0.000	0.000	0.039	0.940
HAQ	0.053	0.013	2.716	0.001
Computer Literacy	0.007	0.012	0.096	0.630
User Type	0.042	0.019	2. 914	-.015

Tab. 3. *Summary of simultaneous regression of independent variables. Source Authors.*

Variable	Coefficient (B)	SE	T -value	P Value
Intercept	0.500	0.112	4.481	0.000
Gender	0.080	0.034	2.331	0.020
HAQ	0.069	0.024	2.855	0.005
User Type	0.054	0.027	2.672	0.010

Tab. 4. *Summary of final analysis. Source Authors.*

Finally, gender, HAQ and User Type are used as the independent variables for the model. The result of the analysis is presented in Table 4. For the final regression model, the DW statistic was 1.996, while the VIF remained 1.042, 1.120 and 1.065 for Gender, HAQ and User Type respectively. The three variables together explain about 36.1% variation in the pretest score of the respondents. And the overall regression model has F Statistic 4.109, which is significant at $p \leq 0.03$. The model obtained is given as:

$$PTSC = 0.5 + 0.08X_1 + 0.069X_2 + 0.054X_3$$

The result suggests that gender, academic qualification and user type significantly influences respondents' ability to recognize a phished message purportedly sent by their banks.

5 Discussion and Conclusion

This study examined how effective the security tips messages are through hypothesis formulation and experimental method. The study offers further insights that individuals are poor at discriminating phishing messages despite the availability of the security tips provided by their banks. This is because most people lack a basic understanding of internet technology. Phishing and online scams exploit this lack of knowledge by using forged email header, fraudulent URLs (e.g. many participants think *www.firstbank.com* and www.firstbank@intergold.com belong to the same category), the absence of https or closed padlock etc. For instance, most respondents incorrectly labelled phishing pages as genuine despite the presence of conspicuous incorrect URL. This is consistent with the works of Dhamija et al. (2005) and Alsharnouby et al. (2015)

In addition, most participants (about 59%) failed to recognize fake web pages in our study because of the visual similarity cue. From our observation, most participants focused on the logo and images of familiar brands as evidence of benignity of a webpage. The implication of this is that most banking customers in Nigeria may still fall for deceptive online scams where logos and images of known brands are employed. This observation is more disturbing as our study consist about 84.54% of students and 89 % of the literate population (OND/NCE and HND/BSC). This group represents individuals who are more likely to be consulted by others people when such a situation arises. For instance, a retired pensioner may ask his daughter in a polytechnic to help him confirm whether a message he received was actually from a genuine pension administrator or not. Although Dhamija et al. 2006 showed that people were easily deceived through visually similar images, logos, texts and homographic attacks (i.e. replacement of similar texts in URL e.g ***w*** written as ***vv*** – double ***v***), the reality is still the same in Nigeria. The success rate of Dhamija et al. (2006) was 58% whereas in our study the failure rate of the participants on these visually looking sites was averagely 58.74%. However, Alsharnouby et al. (2015) showed that participants that are primed to understand phishing attacks scored 64% success rate in their own study.

Our findings with regards to email and BVN message have important implications for e-commerce and research community. The performance of the participants in our study was very poor on these two metrics. On email, about 74.24% of the participant could not correctly classify the message as fake in spite of the presence of bad grammars and other irrelevant indicators that show that such message could not possibly originate from a trustworthy entity like their banks. Similarly, on the BVN message, the failure rate was 76.71%. This is the highest failure rate in our study. This finding may not be unconnected with the fact that most people now received such message on their BVN message update from their banks. However, since such message has grave implication on users' personal credentials (e.g. account number) one expects participants to be more careful now that online scams are now very common. Unfortunately, this is not the case even despite the use of poor grammar in the BVN message

as common with such message from con artists (Ramanathan et al., 2013; Maurer & Hofer, 2012). Not even the presence of private phone number in these messages give most participants a hint that the message is faked. The implication of this is alarming as most people now receive these unsolicited messages more than before. In addition, the proliferation of mobile-internet enabled smartphones now make more people susceptible to these fake messages. This is consistent with the work of Vishwanath (2016) which demonstrated that smartphones are likely to increase the likelihood of online deception. In addition, Parsons et al. (2015) in their study classified participants as informed and non-informed based on the priming the participants with the purpose of the study. Interestingly, most primed participants significantly identified phishing emails than the unprimed participants. This is inconsistent with our study because we assumed that the participants are well primed with the availability of the security tips send to them. In the light of this, we can comfortably conclude that the security tips message is not effective at assisting the users to recognize online scams and phishing attacks.

The implication of this is that most customers in the Nigerian financial sector do not understand the security tip and by extension the antics of the online criminals. In addition, a number of test statistics were used to explain the influences of the demographic factors in the sample population. In this way, a regression model was built which explain that the influence of gender, academic Qualification and user type played a significant role in their identification of fraudulent messages. This implies that consideration should be made to these factors by the banking authorities when sending these messages to their customers. Unless these factors are well-considered in the design of a new security tip messages, the financial losses through these online criminals' activities are likely to continue on increase over the coming years as more institutions adopt the culture of e-commerce.

Acknowledgement

The research reported in the paper is fully supported by TETFUND research projects intervention 2013 and 2014 (merged). We are grateful to the management of *Moshood Abiola Polytechnic, Abeokuta* for approving this research for TETFUND sponsorship.

References

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, 82, 70-82. doi: 10.1016/j.ijhcs.2015.05.005

APWG. (2017). APWG Phishing Attack Trends Reports. *Anti-Phishing Working Group*. Retrieved August 27, 2018, from: https://www.antiphishing.org/resources/apwg-reports/

Arachchilage N., & Love S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3), 706-714. doi: 10.1016/j.chb.2012.12.018

Dhamija, R., Tygar, J.D. & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). New York: ACM. doi: 10.1145/1124772.1124861

Downs, J.S., Holbrook, M.B. & Cranor, L.F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). New York: ACM. doi: 10.1145/1143120.1143131

Hong, J. (2012). The state of phishing attacks. *Communication of the ACM*, 55(1), 74-81. doi: 10.1145/2063176.2063197

Jagatic, T., Johnson, N., Jakobsson, M. & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 50(10), 94-100. doi: 10.1145/1290958.1290968

Jakobsson, M. & Myers, S. A. (2007). *Phishing and Countermeasures: Understanding the increasing problem of identity theft*. New York: John Wiley & Sons.

Konradt, C., Schilling, A., & Werners, B. (2016). Phishing: An economic analysis of cybercrime perpetrators. *Computers & Security*, 58, 39-46. doi: 10.1016/j.cose.2015.12.001

Kumaraguru, P., Rhee, Y.W., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905-914). New York: ACM. doi: 10.1145/1240624.1240760

Li, Y., Yang, L. & Ding, J. (2016). A minimum enclosing ball-based support vector machine approach for detection of phishing websites. *Optik - International Journal for Light and Electron Optics*, 127(1), 345-351. doi: 10.1016/j.ijleo.2015.10.078

Lin, J., & Lu T. (2000). Towards an understanding of the behavioral intention to use a website. *International Journal of Information Management*, 20(3), 197-208. doi: 10.1016/S0268-4012(00)00005-0

Longe, T. (2014). Ensuring Information Security Assurance through Policy Framework. In *Proceedings of the First National Cyber Security Forum*. Nigeria: Punch News.

Maurer, M., & Hofer, L. (2012). Sophisticated Phishers Make More Spelling Mistakes: Using URL Similarity Against Phishing. In *Cyberspace Safety and Security* (pp. 414-426). Berlin: Springer. doi: 10.1007/978-3-642-35362-8_31

Neupane, A., Rahman, L., Saxena, N., & Hirshfield, L. (2015). A Multi-Modal Neuro-Physiological Study of Phishing Detection and Malware Warning. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 479-491). New York: ACM. doi: 10.1145/2810103.2813660

Orunsolu, A.A, Alaran, M.A, Bamgboye, O.O, Sodiya, A.S., & Omorinola, A.O. (2016). A User's Awareness Study of Anti-Phishing Security Tips. In *Proceedings of the 2nd International Conference on Intelligent Computing and Emerging Technologies* (pp. 46-55). Ilisan-Remo: Babcock University.

PandaLabs Report. (2012). PandaLabs Annual Report – 2012. Retrieved September 30, 2018, from: https://www.pandasecurity.com/mediacenter/social-media/pandalabs-annual-report-2012/

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, 52, 194-206. doi: 10.1016/j.cose.2015.02.008

Ramanathan V., & Wechsler H. (2013). Phishing detection and impersonated entity discovery using Conditional Random Field and Latent Dirichlet Allocation. *Computers & Security*, 34, 123-139. doi: 10.1016/j.cose.2012.12.002

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and the effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). New York: ACM. doi: 10.1145/1753326.1753383

Vishwanath, A. (2016). Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Computers in Human Behavior*, 63, 198-207. doi: 10.1016/j.chb.2016.05.035

The article has been reviewed. | **Received:** 7 August 2018 | **Accepted:** 4 November 2018

Academic Editor: Zdenek Smutny