Journal of Computer Sciences and Applications, 2018, Vol. 6, No. 2, 64-68
Available online at http://pubs.sciepub.com/jcsa/6/2/2

DOI:10.12691/jcsa-6-2-2

Mitigating Social Engineering Menace in Nigerian Universities

A.A. Ojugo[*], O. Otakore[*]

Department of Mathematics/Computer Science, Federal University of Petroleum Resources Effurun, Nigeria
*Corresponding author: ojugo.arnold@fupre.edu.ng, kekeje.debby@fupre.edu.ng

Abstract Advances in technology continues to facilitate data processing activities; and plays a critical role to serve users' social needs. The advent of smartphones has further eased the adoption and caused a spike in the usage of these technologies as well as the deployment of Internet-based applications. Our study examines known social engineering attack techniques on users by focusing on comparison as used by intruders. Data is collected from some selected Nigerian undergraduates. Result of the conducted survey suggests that phishing method hits a higher success rate than other techniques; while other factors such as gender, also had an impact on the success rate of each technique used.

Keywords: *phishing, cybersecurity, fraud, mitigate, Nigeria, university*

Cite This Article: A.A. Ojugo, and O. Otakore, "Mitigating Social Engineering Menace in Nigerian Universities." *Journal of Computer Sciences and Applications*, vol. 6, no. 2 (2018): 64-68. doi: 10.12691/jcsa-6-2-2.

1. Introduction

The crave for quick wealth and survival of the fittest, has consequently bedazzled the economy Nigeria with sprees of fraudulent and corrupt practices that continues to rob the nation of opportunities and progress in the right direction. Fraud is a criminal act, perpetrated via embezzlement, larceny and theft in which a criminal uses falsehood to benefit from an unassuming victim of great returns (if it is aimed at a financial transaction) such that the victim relies on such falsehood; And transaction is the exchange of goods and services for gains or money deliverables [1]. Advancement in the field of information and communication technology continues to beam its many benefits on users, which is today permeated into our lives via its use in personal, biz and recreational feats. A sine-qua-non effect of such advancements, are also a myriad of threats that exploit the inherent vulnerabilities of Internet and its associated technologies. These challenges and threats manifests in various forms and/or ways – presenting itself as misleading items of benefits to unsuspecting users, aimed at defrauding a user [2].

Criminals often task themselves with exploiting of potential victims than exploiting network connection or web application in their quest. Yet, businesses that heavily invest towards a highly sophisticated security technology – also consequently often fail to adequately address their biggest vulnerability threat, which is the deception of their employees. Increasingly, criminals use deceptive techniques to exploit corporate biz and coy practices so as to circumvent control measures in place with the goal of tricking unsuspecting victims into sending money or diverting payments to imposters. Many studies have been reported to examine the increasingly, sophisticated tactic of deception fraud – so as to proffer actionable suggestions for effective risk mitigation.

Social engineering threats is not a new paradigm; But, it has steadily grown with no-end-in-sight. Its continued growth borders on human nature of trust instincts, on which intruders manipulate human emotion and ultimately, exploit this trust to steal user data. Common methods used by social engineers are phishing, vishing, smishing, pharming etc [3]. These attacks are mostly targeted at Internet-based connected devices. This has tripled with adoption of mobile smartphone, resulting in the increased growth of user access to these technologies from 42.5% in January 2013 to 78.9% by December 2013. The advent and adopted choice of Android smartphones over personal computers due to its portability, functionality, design, speed and ease of Internet access has further spiked up significantly these threats. Consequently, these have its range of implication to work-related functions and business issues as it often exposes sensitive data to adversaries [1,3].

1.1. Evolving Method of Attack

Ojugo and Eboka [3] Social engineering threat simply use technical subterfuge to defraud an online account holder of their financial data by posing as a trusted identity. ***Phishing*** employs mass mail to defraud victims. Today, phishing uses multiple means like spoofed emails, web link manipulation and forgeries, man-in-middle chat, phone calls, covert redirect etc – aimed at convincing an unsuspecting user to divulge confidential data or indulge in fraudulent transactions. A more effective favored variant of phishing is ***spear*** phishing, which involves highly targeted email messages sent to a victim persuaded via clever tactics to access links that redirect them to spoofed websites containing malware that aim to siphoned

and compromise a users' credentials/data. Another variant of phishing includes ***Smishing*** (SMS phishing) which is a security attack in which a user is tricked into downloading a malware unto his cellular phone or other mobile device.

Ojugo et al [1] ***Vishing*** (voice phishing) is a method of social engineering, designed to steals payment card data and credentials over the phone or via SMS text messages. Here the fraudsters pose as banks or other institutions in order to convince victims into divulging their card information, and data is used for card-not-present transactions (e.g. shopping online or via phone) or is encoded onto new cards to purchase goods or withdraw cash from automated teller machines; while ***pharming*** is an attack intended to redirect a website's traffic to another fake site and is conducted by either changing the hosts file on the victim's computer or mobile device, or by exploiting of vulnerability in the domain name service server software. It is a scamming approach that allows an intruder to install malware unto a user device or server, which redirects unsuspecting users to a fraudulent site without their consent and/or knowledge. It is also known as phishing without a lure.

1.2. Related Literature

Chanvarasuth [4] examined threats people experience by focusing on the comparison between the effectiveness of phishing and vishing methods, sampling 772-Thai undergrad students with age ranges between 18-to-23 years old. Their result suggests that phishing problem tends to get higher success rate than vishing. Some other factors, such as gender also has an impact on the success rate of each technique.

Ojugo and Eboka [1] proposed and deployed a client-trusted detection framework employed in e-banking over the android (smartphone) platform as it sought for a dependable, mobile banking to address threats via transaction authenticity and message authorization. The framework notably increased clients' trust level against social engineering threats targeted at smartphones with about 72percent for mobile online-banking applications (and also ported on a community-cloud). They attempted to examine threats experienced by smartphone users by focusing on the comparison between the effectiveness of phishing and vishing techniques. He sampled 600respondents in the South-South and South-East Geo-Zone of Nigeria. Results indicated that phishing poses more of a problem with higher success rate than vishing.

2. Materials and Methodology

2.1. Dataset Used

The study adopts a survey design were samples are chosen at random (with bias of knowledge of social engineering attacks) to help analyze selected data. The study covers South-South, South-West and South-East Zones in Nigeria through stratified sampling across the randomly selected targets. 2-Universities were selected at random with 10-students from each university from computer science, electrical/electronic, library science and computer engineering departments. Study design allows effective representation of results with 600-questionnaires administered. The achieved co-efficient r = 0.73, which accounts for the reliability of instrument (i.e. questionnaire) used for study.

Table 1. Target List of Attempts

No	*Threat Attempts On*	*Percent*
1	Phishing	52.1
2	Vishing	21.3
3	Pharming	11.2
4	Whalling and Others	15.4

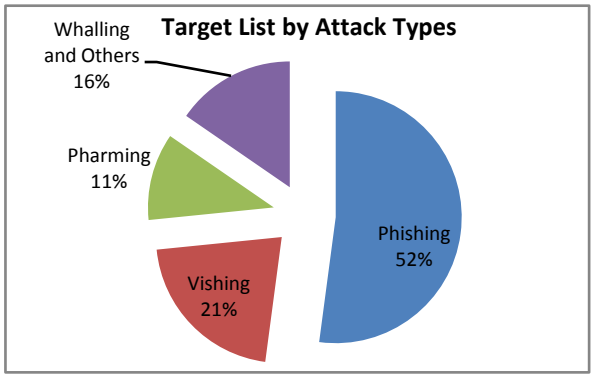

Figure 1. Target List by Attacks Types

Table 2. Attacks on Types of Businesses

No	*Types of Organisations*	*Percent*
1	Government Officials in MDAs	8.3
2	Financial and Banking Services	34.4
3	Portals	19.7
4	Social Sites	15.2
5	Military	9.8
6	Others	12.6

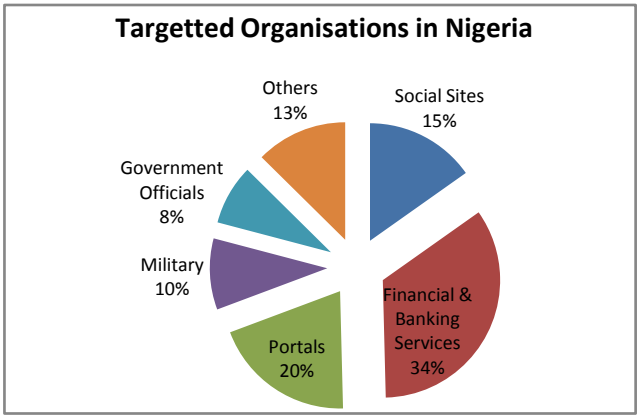

Figure 2. Targeted Businesses by Social Engineering Attacks

Table 3. Targeted Users for Social Engineering Attacks

No	*Types of Mobile Smartphone*	*Percentage*
1	iOS	12.9
2	BlackBerry	10.6
3	Android	34.2
4	Symbian	9.1
5	Windows	21.8
6	Others	11.4

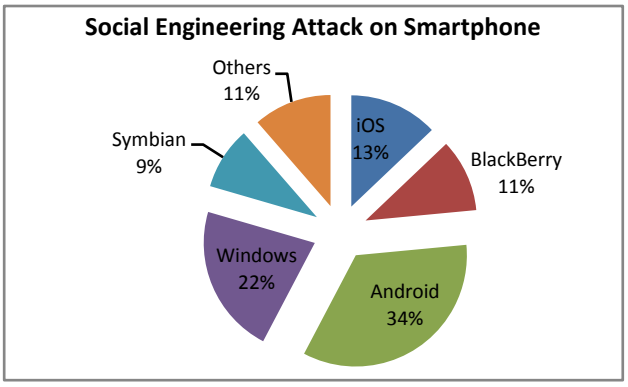

Figure 3. Social Engineering Attacks over Smartphone Platforms

2.2. Hypothesis

The hypotheses developed for the study includes:

a. H_o1: Phishing is more effective than vishing technique.
b. H_o2: Response rate of phishing is higher than vishing.
c. H_o3: Success rate of phishing is higher than vishing.

The ***objective*** of this study is to: (a) compare the effectiveness between phishing, vishing, pharming and whaling techniques of social engineering threats on Nigeria Undergraduates in relation to exploring how human traits affect these threats and the use of specific techniques.

2.3. Data Collection and Analysis

In a phishing experiment, it is important to make interaction look like phishing, without actually compromising credentials. A conductive study such as carrying out phishing attacks, in the academic environ is especially difficult for reasons that include attaining the University's approval and for her ICT personnel(s) to carry out such attacks. In our experiments, we illustrated methods to avoid having to handle credentials, but still being able to verify whether they were correctly entered. This was achieved by obtaining feedback from a server log files we had access to. Undergraduates in both the Colleges of Science and Technology (as stated above) in the selected Nigerian Universities were invited via email to participate in a short-web survey about student e-mail usage and information on their future plan for pursuing graduate studies. Webpage was used to collect the data. We provided a link to webpage with misspelt URL (Uniform Resource Locator) to the targets. Web pages were designed similar to the official webpage of their institution. Web pages that replicated from the official institution website were designed. All menus and functions are similar to the official institution website. We used the *dot.com* domain as it is cheaper than other host; And, it seems to be the most effective for phishing as adopted from Chanvarasuth [4] and Pibulyarojana and Jirawannakool [5].

Step of phishing technique appears when the targets receive phishing e-mail that contains the link to the phisher website. First the targets will see the login page on this page, the targets are asked to login by using their own student ID and password on the registration page. The website also asks each student to fill their information such as name, last name, age, e-mail, and others. Our questionnaire is adapted from Wang et al [6], which divided their survey into 3 parts; demographic, scale of awareness, and riskiness caused by phishers. After acquiring the data from social engineering techniques, we use victim's data to analyze/compare the effectiveness of these techniques. This study seeks to compare effectiveness between phishing and vishing techniques among other techniques. Then, use a paired sample *t*-test to compare means of same for comparison between 2-sample groups; And, One-Way ANOVA to analyze the data which has more than two groups of sample results.

3. Result Findings and Discussion

The study obtained responses from total of 458-participants in phishing, 532 in vishing and 400 in pharming and other social engineering attack techniques.

Table 4. Number of Respondents Attacked

No	*Social Engineering Attacks*	*Count*	*Percent*
1	Phishing	458	77
2	Vishing	532	89
3	Pharming and Others	198	33

Data was divided into 3-groups: phishing, vishing and others as in Table 4. For *phishing*, email was sent to all 600-persons and 458-respondents were attained to represent 77% of sample population. For *vishing*, phone calls were made to 600-persons and received 532-respondents to represent 89% success rate of sample population. For *pharming* and others, 198 respondents representing 33% had other techniques used on them.

Table 5. Number of Respondents by Gender

Attacks	*Sex*	*Percent*	*Count*	*Total*
Phishing	Male	71	327	458
	Female	29	131	
Vishing	Male	72	331	532
	Female	38	201	
Pharming etc	Male	67	132	198
	Female	33	66	

In Table 5, 327-respondents (71%) of the 458-respondents as obtained for phishing data were male; while 131 (29%) of the sample population for phished clients are female. Conversely, 331 representing 72% of vished respondents are male; while, 201 representing 38% of the vished clients were female of entire vished sample population. Lastly, 132 respondents of the entire pharmed sample population are male; while, 66 of the sample respondents are female.

Table 6. Media Respondents Learned of Social Engineering

Activity	*Percent*
Internet / Social Media	69
Newspaper	3.2
Televised News	2.1
Movies / Films	11.4
Friends / Others	14.3

Table 6 shows all types of media that make respondents aware of social engineering attacks included internet (69%), movies (11.4%), newspaper (3.2%), televised news (2.1%) and friends cum others such as billboard, radio, word of mouth (14.3%). Our finding implies that in order to make people more aware of phishing, they should use internet as a major channel since most of the respondents currently follow the news via internet, radio, billboard, and word of mouth.

Table 7. Comparison on Effectiveness of Attacks

No	*Hypothesis*	*F-critical*	*F-Statistics*	*Significance*
$H_0$3	Home	1.732	1.360	0.688
	Private	1.437	1.360	0.647
	Mobile	2.716	1.360	0.070

*p<0.05.

On hypothesis: whether students are more aware of phishing than any other technique, we use an awareness factor to determine the result. Our result notes that respondents who are undergraduate students are more familiar with phishing than vishing technique. Response rate of phishing is higher than vishing response rate. The result of phishing is obtained by the victim response to e-mail and sign up on our website. On the other hand, the result of vishing technique is acquired by the number of times undergraduate students respond to the call. From our finding, it can be concluded that undergraduate students are more vulnerable to phishing than vishing. Thus, we note that success rate of phishing is higher than vishing. On phishing, we obtained students' name, last name, and the mobile phone number to count as success; while, for vishing, the needed information is name, last name, and student ID. On this hypothesis, the researcher found out that undergraduate students are more vulnerable to phishing technique than vishing and others.

4. Recommendations and Conclusion

Some recommendations and actionable suggestions to help mitigate risks of deception and fraud losses:

1. Training: (a) keep employees informed on type of scams being perpetrated, (b) provide anti-fraud training on how to recognize attacks and report suspicious activities that violate coy policies and procedures, (c) train employees on what information is confidential and what should never be released unless approved by management, (d) train employees to slow down if the message conveys a sense of urgency, intimidation, or high pressure sales tactics, (e) train employees not to forward, respond to, or access attachments or links within unsolicited emails, (f) hold employees accountable but also create a culture where they are rewarded for verifying suspicious activity.
2. Provide Internal Controls by: (a) authenticating changes to users' contact and internal bank data, (b) require supervisor sign-off on any changes to vendor and client information, (c) validate requests from users, (d) validate all internal requests to transfer data, (e) limit transfer permissions to specific employees, (f) guard against unauthorized physical access (theft of keys, access cards, ID badges etc.), (g) keep physical documents locked and secured and shred documents not in use, (h) monitor the use of social media, (i) develop reporting and tracking programs that document incidences of deception fraud or attempts of deception fraud, (j) keep cyber security software up to date, (k) implement mobile device security procedures, (l) use 2-factor authentications on your organizations computer platform(s).
3. Organizations should continually monitor effectiveness of their education, training, and internal controls by conducting third party penetration testing. These fake hacks provide valuable information on how to focus training and educational efforts.
4. Ojugo and Eboka [1] provides a client-trusted security model for smartphones in mobile banking, to help account for a more dependable framework to help with transaction authenticity and message authorization. Result of study shows framework is capable of increasing client's trust level in relation to social engineering attacks with 72% as implemented over their firewall by the banks (ported on a community-cloud) for user access.
5. Exchange of fraud detection data is a prerequisite for curbing the menace and though, these data if often limited and sometimes, experts deem it unwise to describe as well as share such data over public domain (since an extensive knowledge of fraud detection techniques in great detail) will consequently arm intruders on evasive techniques to curb detection. Thus, as a dual effect, it will further equip users and hackers with adequate data required to combat as well as evade significant detection (for hackers).

There has been an increasing in the degree of sophistication in the methods that phishers use to attack consumers. Since phishers are continually designing new ways to execute their attacks on online users, phishing research must stay abreast and ahead of the scammers in terms of the sophistication and type of phishing strategy, otherwise the knowledge cannot come up with up-to-date approaches to defend against these attacks and protect both users and providers [4,7,8].

The study examines the differences on phishing technique which are spoofing website, and vishing. It found that no matter how different of method in each phishing technique, the results of both techniques are still the same which the target always loses sensitivity information and some of their property. Therefore, user prior education or user awareness appears to be the best weapon to combat against phishing [9,10]. The result also reveals that phishing technique is more effective than vishing technique. In general, phishing technique provides higher response rate and success rate. Women are easily to get phished more than men. In addition, an academic major is not a factor affecting the effectiveness of phishing technique. However, we also found that the type of incoming telephone call seems to have an impact on phishing's success rate. Our finding agrees with [11] on the issue that women are phished easier than men, but disagree with the statement of [12] mentioned that gender does not have any effect on phishing. Moreover, our

findings also agree with the study by [13] that academic majors do not have any effect on phishing at all.

References

[1] Ojugo, A.A., Oyemade, D.A., Allenotor, D., Longe, O.B and Anujeonye, C.N., "Comparative Stochastic Study for Credit-Card Fraud Detection Models", African Journal of Computing & ICT, 2015, Vol 8, No. 1, Issue 2. Pp 15-24.

[2] Yeboah-Boateng, E.O and Amanor, P.M., Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices, Journal of Emerging Trends in Computing and Information Sciences, 2014, Vol. 5, No. 4, pp297-307.

[3] Ojugo, A.A and Eboka, A.O., "A Social Engineering Detection Model for Mobile Smartphone Clients", African Journal of Computing & ICT, 2014, Vol 7, No. 3, Issue 1. Pp 52-64.

[4] Chanvarasuth, P., "Knowledge on Phishing and Vishing: An Empirical Study on Thai Students", International Journal of Humanities and Applied Sciences, 2013, Vol. 2, No. 3, pp 58-62, ISSN 2277-4386.

[5] Pibulyarojana, K. and Jirawannakool, K., "ThaiCERT Annual Report of 2007,": http://www.ieee.th.org/IEEEConference2008/Proceedings2008 /papers/IEEE_Full_Paper_Komain.doc_Paper_5.pdf.

[6] Wang, J.R.C., Herath, T., Rao, H. R., "An Empirical Exploration of the Design Pattern of Phishing Attacks", in: S.J. Upadhyaya, H.R. Rao (Eds.), Annals of Emerging Research in Information Assurance, Security and Privacy Services, Emerald Publishers, 2009.

[7] Stamm, S., Ramzan, Z., and Jakobsson, M., "Drive-by Pharming," Technical Report TR641, Indiana University, December 2006.

[8] Kay, R., "Quick Study: Phishing, Computerworld," 2004, http://www.computerworld.com/s/article/89096/Phishing.

[9] Baker, E.M., Baker, W.H., and Tedesco, J.C., "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box", Communication Research Reports, 2007, vol. 24, no. 4, pp. 327-339. International Journal of Humanities and Applied Sciences (IJHAS) Vol. 2, No. 3, 2013 ISSN 2277- 4386.

[10] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J., "Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", In the Proceedings of CHI '10, SIGCHI Conference on Human Factors in Computing Systems, 2010, pp. 373-382.

[11] Colley, A. and Maltby, J., "Impact of the Internet on our lives: Male and Female Personal Perspectives", Computers in Human Behavior, 2008, vol. 24, no. 5, pp. 2005-2013.

[12] Jagatic, T., Johnson, N.A., Jakobsson, M., and Menczer, F., "Social Phishing", Communications of ACM, Vol. 50, No. 10, 2005, pp. 94-100.

[13] Case, C.J. and King, D.L., "Phishing for Undergraduate Students", Research in Higher Education Journal, 2006, pp. 100-106.