Dutse Journal of Pure and Applied Sciences (DUJOPAS) Vol. 4 No. 1 June 2018

PHISHING AWARENESS STRATEGIES: A CLEAR CASE OF USER AND INDUSTRIES RESPONSIBILITIES

I.R. Saidu
Computer Science Department
Nigerian Defence Academy, Kaduna

Saadu Zakariya
Computer Science Department
Nigerian Defence Academy, Kaduna

Bello Aliyu Anka
Computer Science Department
Nigerian Defence Academy, Kaduna

Muazu Ibrahim Muhammad
Computer Science Department
Nigerian Defence Academy, Kaduna

Abstract

Phishing is a cybercrime fraudulent activity that cause harm to both users and industries especially in online business transactions. The aim of this study was to gain a better understanding of how phishing occurs and how good anti-phishing awareness strategies can be used to combat the threat caused by the phishing attacks. Although, some of the users that performs online transactions appeared to fundamentally lack the understanding about phishing and how to combat it. This study looks at the users' and industry ability in providing better educational and technical responses to phishing. It was achieved by looking at how users react to phishing and exploring the existing anti-phishing methods and examining questions of responsibility. The approach taken was quantitative using data gathered from users and industry experts that are engaged in various online transactions. The findings from each approach were analysed. The results have shown that differences between user views and industries experience was far apart. In particular there was confusion about how phishing differed from other types of security threats. Contrary to expectations, users displayed higher levels of concern about damages and losses caused by phishing frauds.

Keywords: Phishing, Phishing Attack, Anti-Phishing, Education Awareness, Users, Industries.

Introduction

Phishing is a major problem nowadays causing losses of finance, particularly in online transactions (Financial Fraud Action UK & Credit clearing Company, 2012). Phishing definition varies from literature to literature. Jagatic *et al* (2007) defined phishing as an act to fraudulently acquire user's sensitive information (personal identity number, passcode, password, credit/debit card number) through illegitimate website that looks exactly like the target website.

Phishing is a criminal activity employing both social engineering and technical subterfuge to steal consumers' personal and financial data. Social engineering schemes use spoofed emails purporting to be from legitimate businesses and agencies to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as usernames and passwords. Technical subterfuge schemes install crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account usernames and passwords and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes (Anti Phishing Working Group, 2011).

However, anti-phishing awareness is seen as one of the prominent ways of combating phishing attacks, where users are educated in an attempt to enhance their classification accuracy to correctly identify phishing messages. Also apply proper actions on the correctly classified phishing messages, such as reporting attacks to system administrators or avoid any action that will affect them negatively. Furthermore, (Sheng *et.al*, 2010) revealed that, anti-phishing software is designed to better classify phishing messages on behalf of the users or industries, or provide information in a more obvious way so that the user would have less chance to ignore it.

Most of the users are of the view that combating phishing attacks is not their responsibility especially when they are dealing with organisation or industries websites. This is not a legal requirement in the way that the industries or organisation are obliged for that (Consumer Direct, 2012). While some experts felt simultaneously that users were completely liable for their own safety online but could not be trusted with the agency to create that safety.

Related Work

Most of the related works reviewed on phishing do not take many responsibilities on awareness and strategies into considerations. Some authors reviewed discussed how to recognise phishing emails rather than websites and individual messages. According to a study by (Alpar et.al, 2011) which focused much on phishing attacks consequences pointed out that phishing attacks may in the future extend from aiming to obtain credentials from individual service providers (such as banks) to targeting identity provider credentials, compromising users over a wider part of their Internet activities.

There are various works about why users still fall prey to phishers, even though phishing has been a recognised phenomenon for many years. According to a study by (Yu, et.al, 2008), lack of technical expertise, fear of, and panic about losing money brought about by wording of phishing emails and failure to read anti-phishing education (Yu et.al, 2008). but Yu, did not state any workable strategy. Also study by (Anandpara et.al, 2007) argues that people only react to threats they are aware of. It was discovered in the work of (Roessler & Saldhana, 2010), that users may also not be able to decide how to handle security interactions, they may believe that existing protection is stronger, they dislike having task based activity interrupted, they may become fatigued by warning messages, messages are presented in a way that is confusing and user education is too complex to understand.

According to another study by (Kumaraguru et.al, 2007) argued that user training is not effective because, user education about security does not work. Instead, Nielsen (2004) stated that technological changes were necessary to protect users because user education was unrealistic in its demands, ineffectual, wrongly supposed that humans were easier to change than technology, and hindered full use of the Internet. Another researcher has discovered that attempting to educate users is largely futile and would be better replaced by improving technology (Schneier, 2006). While, (Ranum, 2006) argued implicitly for a behavioural approach, saying that only "pain and humiliation" work as learning tools and that people should be left to learn from their mistakes.

Research Questions

This paper seeks to discover and understand phishing threats that affect computer end-users and to explore anti-phishing education awareness and strategies that will help users to combat it. In order to achieve this, the following questions need to be answered:

Q1: Why do users fall for phishing? Some major factors that caused users fall for phishing will be investigated

Q2: What are the medium for effect phishing awareness?

Q3: How do users react to existing anti-phishing methods?

Q4: How can we improve on existed anti-phishing methods?

Q5: Whose responsibility is it to protect users against phishing?

Methodology

This study was designed to ascertain different level of phishing awareness and strategies that occurred to users and industries especially in online business transaction. The descriptive survey research designed was used, the survey designed was chosen because it employs the applications of scientific method by critically analyse and examined the fact and view of peoples in particular issues that concerned them.

The original impetus for this paper was the desire to investigate why, despite the amount of effort that appears to have gone into educating users about phishing, people still fall victim to phishing attacks and whether this is due to limited awareness and strategies or lack of fundamental misunderstanding of how users understand themselves and their online identity. The study would be conducted using two possible means of population. Expert opinion and user's observation. The population sample comprised of 120 respondents randomly selected. Random sampling technique was employed in selecting the sample, the research adopted questionnaire as an instrument for the study. A structured self-administered questionnaire was used to collect data from expert opinion. The research adapted questionnaire as this will enable each participant to respond to the same set of question in predetermined pattern. The questionnaire was structure using Likert type five point rating scale (5, 4, 3, 2, 1) as of strongly agree, agree, neutral, disagree, disagree strongly respectively.

Experimental Environment

Before the commencement of this work, we obtained a formal permission from each candidate before passing the questionnaire to respondents in the field. In the process of gathering expert opinion from Banks in Kaduna metropolis were used. Because they participated very much in an online business transactions. Each expert was passed the research questionnaire and answers where obtained from the expert based on their experiences. Prior to administrating of the questionnaires, an interactive orientation briefing was organised with the participant to educate them for the purpose of the study and the need to answer all the questions bluntly. The data was collected by administering the scale in the group of participants. The respondents were instructed to complete the scale by giving response to every item in the scale.

Data Analysis

Data analysis is done immediately after the requested data have been generated. The questionnaire was serially numbered for easy identification and was finally scored. Item on the five point Likert scale was scored 1,2,3,4 and 5 for items with the response disagree strongly (SD), disagree (D), neutral (U), agree (A), and strongly agree (SA) respectively.

Descriptive and inferential tools were used to analyse the collected data with aid of Microsoft Excel statistical package. The level of significant (LOS) was used as criteria for decision making, which is set at 0.05%. If the calculated max is less than 5% of the LOS, the respondents is rejected otherwise, it is accepted.

Result and Discussion

The research work was conducted using primary source of data collection and the gathered data were analysed using effective instruments. The result of this dissertation will be from the implementation analysis below:

Demographic Information of Respondents

The demographic characteristic illustrates the distribution of respondents' categories in relative to Age, Gender, and Status of the participant as described in Table 4.1. The finding in Table 4.1 showed that 50% of the respondents were male and 50% female. 50% of the participants were experts in the field while 50% were general end users. About 37.5% fall between the range of 16-25 years, 50% are between 26-30 year, and 10% are within 41-50 while the remaining 0.8% are within 31-41 years.

Table 1. Demographic Information of Respondent

Variable		Frequency	Percent	Valid Percent	Cumulative Percent
Gender	Male	60	50.0	50.0	100.0
	Female	60	50.0	50.0	100.0
	Total	120	100.0	100.0	
Status	Expert	60	50.0	50.0	100.0
	User	60	50.0	50.0	100.0
	Total	120	100.0	100.0	
Age	16-25	35	27.5	38.1	65.6
	26-30	45	40.0	40.8	80.8
	31-40	32	10.0	10.2	20.2
	41-50	16	6.0	6.0	12.0
	Total	118	98.3	100	

Source: Field Survey, 2018

Respondent's Opinion on Causes for Phishing Attacks

The finding Table 2 revealed in that most of the phishing attacks is caused by both the users and industries due to lack of knowledge from the users, lack of proper and regular awareness by organisation and industries. The result also confirmed that a lot of people fall victims due to their carelessness attitude where users clicked links without properly reading the contents

.

Table 2. Respondents' Opinion on Causes for Phishing attacks

Variables	N	SA	A	U	D	SD	MAX	LOS	REMARK
Have you found yourself a victim of phishing attack?	119	44	9	35	31	0	44	2.2	Accepted
Could it be lack of knowledge?	133	40	21	35	13	24	40	2.0	Accepted
Or lack of proper/regular awareness?	114	48	9	31	0	28	48	2.4	Accepted
Or clicking links without reading the contenst?	116	2	2	14	62	36	36	1.8	Accepted

Note: SA= Strongly Agree, A= Agree, U= Neutral, D= Disagree, SD= Disagree Strongly, N= Number of Respondents

Source: Field Survey, 2018

Respondents' Opinion on Efficient Medium for Phishing Awareness

An item in the questionnaire was presented concerning phishing awareness to the respondents to rate findings are shown in Table 3.

The findings in Table 3 have shown that online awareness on regular bases should be the most efficient.

Table 3. Respondents' Opinion on Efficient Medium for Phishing Awareness

Variables	N	SA	A	U	D	SD	MAX	LOS	REMARK
Is education awareness and precaution strategies would be the best?	116	39	40	25	12	10	48	2.4	Accepted

Source: Field Survey, 2018

Respondents' Opinion on How Users React to Existing Anti-Phishing Methods

Two item in the questionnaire were presented to the respondents to rate the interest on how users reacts to existing anti-phishing methods and strategies.

The findings revealed that some users believed that the methods are good while others viewed that much more strategies are needed to combat phishing attacks, as displayed in table 4.

Table 4. Respondents' Opinion on How Users React to Existing Anti-phishing Methods

Variables	N	SA	A	U	D	SD	MAX	LOS	REMARK
Is Anti-spyware software tools performed the best?	93	12	28	23	20	10	28	1.4	Rejected
Or combination of education awareness and anti-phishing tools strategy should be the best?	115	1	3	63	21	27	63	3.15	Accepted

Source: Field Survey, 2018

Respondents' Opinion on Whose Responsibility to Protect Users against Phishing

Two items in the questionnaire were presented to the respondents to rate the interest on whose responsibility is to guard against phishing attacks.

The findings indicated that industries and organisations are the once with much responsibilities than the users, as in table 5.

Table 5. Respondents' Opinion on Whose Responsibility to Protect Users against Phishing

Variables	N	SA	A	U	D	SD	MAX	LOS	REMARK
Users are responsible for their safety and security of their credentials?	120	31	26	0	43	20	43	2.15	Accepted
Industries and organisations are responsible?	118	54	39	12	7	6	54	2.7	Accepted

Source: Field Survey, 2018

Cumulative Results Analysis

The study revealed that various phishing awareness and strategies are everlasting task that seems to be regularly updated. The study established why users fall victims of phishing attacks and about (60.8%) cumulative of the respondents agreed that lack of knowledge, proper awareness and clicking links by the users without reading contents are among the factors that caused users fall into phishing attacks.

The second research question of this study is regarding the efficient medium for phishing awareness. The study revealed that about (28.8%) of the cumulative respondents indicates that industries awareness seems to be the most appropriate not the users because users are always clients to industries.

The study further revealed that anti-phishing software tools are always most appropriate in most circumstance as the cumulative respondents of (37.8%), have chosen strongly that education awareness is the best.

Last question of this study deducted that whose responsibility is to protect users against phishing attacks. The study revealed about (32.4%), respondent strongly agreed that industries and organisation have most of the responsibilities than users who happens to be their client most of the time.

Conclusion

The main contribution of this paper was the educational awareness and initiatives together with good technical strategies which are more relevant to both users and industries worldwide. The study produced some interesting answers to the research questions posed in questionnaire of this dissertation and throughout the work about user attitudes, behaviours, and reactions to phishing and anti-phishing awareness strategies. Some of the findings revealed that phishing awareness education and strategists is an everlasting task for both the user and industries. Therefore, joint effort should be made by both users and industries in other to combat phishing threat because its damages can be catastrophic not only to users or industries but to the entire society or nations who happen to be an ICT connected.

Future Work

In the future research plan would be made to demonstrate the users plan in the adoption of different strategies that will help them in combating Phishing. The industries perspectives toward the need of securing their clients who happens to be engaged in online business transaction and how both users and industries will join hands by providing security frameworks and policies that will help them mitigate phishing attacks and its damages.

REFERENCES

Alpar, G., Hoepman, J.-H., and Siljee, J. (2011). *The Identity Crisis. Security, Privacy and Usability Issues in Identity Management.* Retrieved January 19, 2012, from Cornell University Library: http://arxiv.org/abs/1101.0427.

Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., and Roinestad, H. (2007). Phishing IQ Tests Measure Fear, Not Ability. *Lecture Notes in Computer Science. pp.* 362-366.

Anti-Phishing Working Group (APWG), "Phishing activity trends report - first half 2011," available [Online]: http://apwg.org/reports/apwg trends report h1 2011.pdf.

Anti-Phishing Working Group (APWG), "Phishing activity trends report - second half 2011," http://apwg.org/reports/apwg trends report h2 2011.pdf, 2011, accessed July 2012.

Consumer Direct (2012). *Fraudulent Websites: Police Operation.* Retrieved April 22, 2012, from FindLaw: http://findlaw.co.uk/law/consumer/consumer_protection/22284.html.

Dhamija, R., and Dusseault, L. (2008). The Seven Flaws of Identity Management. *IEEE Security and Privacy. Vol 6, issue 2.* pp. 24-29.

Downs, J., Holbrook, M., and Cranor, L. F. (2007). *Behavioural Response to Phishing Risk.* Pittsburgh: Institute for Software Research, Carnegie Mellon University. pp. 123-211.

Financial Fraud Action UK. (2012). *2011 Fraud Losses Continue Downward Trend.* Retrieved March 25, 2012, from UK Payments Administration: http://www.financialfraudaction.org.uk/cms/assets/1/end%20of%20year%20fraud%20figures%20final.pdf

Jagatic, T., Johnson, N., Jakobsson, M., and Menczer, F. (2007). Social Phishing. Communications of the ACM. pp.23-34.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., et al. (2007). Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer. *APWG eCrime Researchers Summit.* Pittsburgh: Institute for Software Research, Carnegie Mellon University.

Nielsen, J. (2004). *User Education is Not the Answer to Security Problems.* Retrieved February 23, 2012, from Alertbox: http://www.useit.com/alertbox/20041025.html.

Ranum, M. (2006). *User Education.* Retrieved March 2, 2012, from Ranum.com: http://www.ranum.com/security/computer_security/editorials/point-counterpoint/users.html.

Sample, I. (2012). *MPs call for media campaign to raise awareness of cybercrime.* Retrieved February 2, 2012, from The Guardian Online: http://www.guardian.co.uk/technology/2012/feb/02/mps-media-campaign-awareness-cybercrime.

Schneier, B. (2006, August 22). *Educating Users.* Retrieved March 2, 2012, from Schneier on Security: http://www.schneier.com/blog/archives/2006/08/educating_users.html.

Sheng, S., Kumaraguru, P., Acquisti, A., Cranor, L., and Hong, J. (2009). Improving Phishing Countermeasures: An Analysis of Expert Interviews. *eCRIME '09* (pp. 1-15).

Sheng S., 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 28th international conference on Human factors in computing systems*, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 373–382.

Wilson, C., and Argles, D. (2011). The Fight against Phishing: Technology, the End User and Legislation. *i-Society 2011* (pp. 501-504). London: IEEE.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology,* pp. 662-674.

Yu, W., Nargundkar, S., and Tiruthani, N. (2008). A Phishing Vulnerability Analysis of Web Based Systems. *Symposium on Computers and Communications* (pp. 326-331). Marrakech: IEEE.