Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Assessment of Information Security Awareness among Online Banking Costumers in Nigeria

Morufu Olalere[1], Victor O. Waziri[2], Idris Ismaila[3], Olawale S. Adebayo[4], Ololade O.[5]
[1, 3, 4] Department of **Cyber Security Science**, Federal University of Technology, Minna Nigeria.
[2]Head, Department of **Cyber Security Science**, Federal University of Technology, Minna Nigeria.
[5]Final Year Student, Department of **Cyber Security Science**, Federal University of Technology, Minna Nigeria.

Abstract— Internet banking system has classically supplanted traditional banking system in both developed and developing nations due to rapidly growing Information Technology (IT) in today world. Internet banking which is also refer to as online banking has not only increase the productivity of banks but also give room for easy transactions by the customers. Since the introduction of internet banking into the country (Nigeria), the banking sector has experienced a tremedious change in its mode of operations. Meanwhile, Internet banking system has some challenges including information security. Information security challenge mostly affects online banking customers who supply their details during online transaction. For costumer not to be a victim of this information security challenge, there must be proper information security awareness. This information security awareness will serve as guide for online banking customers. Many costumers enter into banking hall to apply for internet banking and start using such immediately on the approval of their banks. The question is, do the customers aware of information security implication of the online banking? If yes, what is the level of their awareness? To address these questions, we carried out a survey that uses questionnaires to assess the level of awareness of online banking costumers on information security. The analysis of our survey revealed that online banking customers are not fully aware of the threats and risks associated with online banking which means that the level of information security awareness is low. This suggests that the existing methods of creating information security awareness are weak. We therefore proposed methods for the improvement of information security awareness program.

Keywords— Information security, Information security awareness, online banking, threat, Attack

I. INTRODUCTION

Internet banking system has classically supplanted traditional banking system in both developed and developing nations due to rapidly growing IT in today world. Internet banking system which is the same thing as online banking system has not only increase the productivity of banks but also gives room for easy transactions by the customers. Internet banking uses the Internet as the delivery channel by which a customers conduct banking activities such as transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing financial instruments and certificates of deposit. As a result of this delivery channel, internet banking provides customers a big advantage of not having to go to the banking hall before carry out their transactions. An Internet banking customers access accounts from a browser and software that runs Internet banking programs resident on the bank's World Wide Web server, not on the customer Personal Computer (PC) or mobile device(such as smart phone, palm top, lap top and so on) which are just tools for accessing internet. This means that, customer confidential information move from their device through network to their Banks' server when performing online banking.

Meanwhile, customers confidential information has always be the target of attackers. Attacker uses different means to get information from online customers. For instance, attackers use malware to steal online banking customers' confidential information. This malware may get to the internet user device as a result of download from the internet. Any time user performs transaction on the device, the confidential information of the user get to the attacker. Phishing is also one of the methods attacker used to get confidential information from online banking customers. Phishing is a form of internet fraud that aims at stealing confidential information (such as credit cards, social security numbers, user Identity and password) from internet users. The attacker carries out phishing by simply creating a fake web site similar to the bank of the target customers and asks (through e-mail or text message) the customers to log in into the web site to supply their confidential information. When the customers are through with the submission of their confidential information, they are redirected to the bank original website from the fake web site in order not to give room for detection. General user education is considered one of the most important and widely-use approaches in fighting phishing attacks **[1]**. For online banking customers not to fall victim of all these attacks, there is need for different banks to create information security awareness for their customers. This information security awareness will serve as informal education for the customers and will provide them with necessary information including different form of attacks, how to detect attack,

what to do when attack is detected, how to prevent such attack for future occurrence and so on. This is not to say, the awareness should be technical.

It is in line with this need that our survey aims at assessing the level of information security awareness among online banking customers in Nigeria. Our survey provides answers to various questions about information security awareness among online banking customers in Nigeria. The remaining part of this study is structured as follows: The next section briefly discusses various form of online banking threats follow by brief discussion on Information security awareness; we then reviewed the existing literature and this is followed by research methodology; we present data analysis and results; finally, we present result discussion and conclusion.

II. DIFFERENT FORMS OF ATTACKS ON ONLINE BANKING SYSTEM AND THEIR PREVENTIVE MEASURES

In traditional banking system attack on costumer is committed physically in most case but in an online banking system attack is carry out on cyber space. This type of attack on online banking customers is called cyber-attack and the perpetrator is referred to as cyber-criminal (attacker or hacker). Cyber criminals are developing increasingly sophisticated tools to steal financial information of customers either through the banks or the customers themselves. The use of online banking has led to increased risks as attackers use various forms of strategies and can now carry out attacks from a separate place without having to see or be in contact with the victim, most of the attack strategies that are used by attackers are usually to steal or to modify costumers' financial information (Johnson, 2008). A recent report on Internet security highlighted high levels of malicious activity across the Internet with increases in phishing, spam, 'bot' networks, Trojans, and zero-day threats.

In the past, these threats were usually distinct and could be addressed separately but attackers are now refining their methods by carrying out multiple attack vectors. Attack vectors used in internet banking can also be categorized into two groups; Local attacks which is carried out during online banking session which is usually against end users who think the SSL connection is safe such as the Man-in-the-middle attack and use of key loggers and Remote attacks which is carried out by redirecting victims to a remote site such as the phishing attack, also both forms of attack could be combined and used by the attacker which can lead to serious damage to unsuspecting users [2]**.** Reference [3**]** categorizes threats to online banking into various forms which includes; Threat to using Personal computers (PCs) which is usually targeted at end user systems which is vulnerable as a result of consumers usage of their PC to constantly web surf and download all sorts of applications, Threat to personal data input describes the use of key loggers as a form of attack, Threat to web browser which uses Man-in-the –browser attack to intercept users information and Threat to SSL communications which occurs as a result of users conducting transactions using public Wi-Fi network. Similarly [4] categorized online banking security threats as either internal/external, human/non-human, accidental/intentional. Below are the common threats to online banking.

A. *Malware*

Malwares are malicious softwares that are designed to cause damage on stand alone or networked computers. Attacker uses different types of malware for different purposes. There are malwares that can cause damage to device being used for online banking (such as desktop, laptop, PDA, palm top and smartphone) and there are some malwares that are meant for stealing confidential information of internet users. Most of these malwares cause damage by obstructing or slowing down the security structure of personal device. Malware threats in online banking can come in form of Ransomware Trojan, which causes damage by obstructing or slowing down the security structure of a personal computer. When malware comes in form of rootkit, it hides registry edit and file folder. Online banking customers can prevent malware by: having antivirus software installed on personal device; avoiding unnecessary/untrusted link for downloading; scanning a personal device before engage in an online transaction; avoiding using someone else's personal device for online transaction.

B. *Keylogger*

A keylogger which is sometimes called a keystroke logger or system monitor is a hardware or software that monitors each keystroke a user types on a specific computer's keyboard. When hardware fashion is plug into the victim computer by attacker, all information that the victim typed in during online transaction will be available on the keylogger. Attacker can make use of this information later to perform illegal transaction on the victim bank account. Also, software fashion performs the same function as hardware fashion. Unlike the hardware that is just plug and remove, software need to be installed on the victim computer. Some of the keylogger softwares fashion forward keystrokes to a remote location where attacker can retrieve information about the victim. This means that after installation, attacker does not need to be available to get the stored keystrokes when transaction is being performed. Keyloggers can be detected by antivirus software [5]. Online banking customers can prevent this type of attack by: avoiding using public computer (such as café computer) to carry out online transaction.

C. *Identity theft*

Identity theft is a form of attack in which attack assumes someone else's identity in order to gain access to the person's resources and other benefits in the person's name. Attacker may have little information about the victim and use these information to perform illegal transaction on the victim account presenting himself as legal owner of the victim account. This attack normally occurs when attacker has gotten information like password, PIN number and so on. Identity theft can be avoided by jealously guiding financial information such as password and PIN.

D. *Social engineering*

Social engineering is usually used to describe a non technical aspect of cybercrime, such that attack gets an unsuspecting persons information by manipulating on their trusting ability. There are offline and online social engineering techniques. Online social engineering techniques are: Phishing, website spoofing, Pharming while offline includes; shoulder surfing, dumpster diving and so on. Social engineering can be avoided by: avoiding sharing username and password with anyone; avoiding fraudulent sites; mindful of surrounding when performing online transaction.

E. *Phishing*

is an act of attempting to obtain user's information such as passwords,PINs, credit card information through an electronic communication by disguising to be a trusted entity. Phishing attack starts from unsolicited e-mail with a link asking the victims to click the link and supply their information for a reason that maybe sound reasonable. The link normally look like original web site of the victim bank. Personal Information such as account number, PIN number, Password, account name and so on are normally requested for by the attacker. The best way to protect one's self from phishing is to recognise a phish. Phished email comes in a way that tells victim to respond urgently or something bad (properly to your money in the bank) will happen if urgent response to the email is not made. They usually require a sense of urgency. Reference [6] gives detail on how to prevent phishing.

F. *Man-in-the-Middle Attack(MitM)*

Man-in-the-middle attack is a form of active eavesdropping (secret interception) in which an attacker makes independent connection between two victims, making them believe they are communicating with each other over a private network while the attacker is relaying messages between them and controlling the whole conversation. When this occurs, attack get access to the message on transmission. Attacker can modify the message and retransmit without the knowledge of the sender or receiver. Reference [7] gives details on how Man-in-the- middle attack is perpetrated by attacker and how it can be prevented in an online banking system environment.

G. *Shoulder surfing*

Shoulder surfing refers to using direct observation tecniques such as looking over one's shoulder to get information, it is usually used to obtain password and PINs.One can protect himself from this attack by: guarding one's private information conciously when typing in during online transaction; looking around before typing in financial information and basically just being careful of one's surrounding.

III. INFORMATION SECURITY AWARENESS

From organizational perspective, Information security awareness is about guaranteeing that all employees are aware of the rules and regulations regarding securing the information within organization [8**]**. Also, Information Security Forum [9] defines information security awareness as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual responsibilities, and acts accordingly. From these definitions, organisations focus their information security awareness program on their employees with the intension of protecting confidentiality, integrity and availability of information. Meanwhile, organisations like banks that carry out online transactions need information security awareness for their customers. There is need for them (customers) to know way and manners in which online transaction works in term of information security threats. Each day that passes without educating your commercial customers and financial institution staff provides cyber-thieves another opportunity to compromise accounts and commit fraud [10**]**.

For the purpose of this study, we therefore define information security awareness for online banking costumer as informal training and knowledge acquire to expose them to adequate information on how to handle information security threats surrounding online transaction in order not to fall victim of attackers. Trainings and awareness campaigns are capable of preventing sophisticated attacks simply by making both staff and customers of banks aware of the signs to look for when it comes to fraudulent schemes.

IV. LITERATURE REVIEW

Since the introduction of online banking in the banking sector in the late 90's, researchers had shown interest in addressing various challenging confronting online banking. The challenges range from employee and bank customers' attitude towards the adoption, to the information security challenges. Various researches conducted on online banking from different countries can be found in [11]. On the adoption of online banking by customers, [12]-[13**]** concluded that time and cost savings and freedom from place have been found as the main reasons underlying online banking acceptance. Reference [14**]** examined the impact of perceived usefulness, perceived ease of use, consumer awareness on internet banking and perceived risk on the acceptance of Internet banking by the consumers. Their study shows that perceived usefulness, perceived ease of use, consumer awareness and perceived risk are the important determinants of online banking adoption.

In an empirical investigation carried out by [15] on the adoption of internet banking, it was concluded that secuirty concerns and lack of awareness about internet banking and its benefits stands out as being the obstacles to the adoption of internet banking. Reference [16] study established the importance of adequate security in order to raise the confidence of customer to use internet banking. On the information security awareness in Nigeria, [17] investigation examined

information security awareness among Small and Medium Scale (SME) Enterprises within the business hubs of south-western Nigeria. According to the authors, the aim of the study is to provide data that would be useful to the management of SME's in designing and developing training program to attain appropriate information security awareness levels. The investigation shows that there are varying degree of significant difference between the information security awareness of IT professionals, their educational level, gender, orientation on access control in (SMEs) and years of experience. Their work examine information security awareness among SMEs in the south-western Nigeria while our work assesses the level of information security awareness among online banking customers in Nigeria.

V. RESEARCH METHODOLOGY

In order to accomplish the aim of the research, questionnaires were distributed to people who use online banking in some selected states in the country. The questionnaire begins by probing users on their general information and then goes on to their knowledge on internet banking and basic awareness on internet banking security. The questionnaires were distributed to the people that use Internet banking of one bank or the other. We used cluster sampling techniques. The cluster technique ensures that all the segment of the population is included in the sample and also makes it possible to produce unbiased estimates of population totals and because the sample is quite large and had to be grouped and narrowed down. Questionnaires were distributed in four (4) states including Lagos state, Kwara state, Niger state and FCT. The population selected was to obtain adequate and diverse views pertaining to the level of knowledge users of internet banking have on the security of their information in carrying out their transactions online. A total of 200 questionnaires were distributed to internet banking users in the four states. At the end of the exercise, 150 questionnaires were properly filled while the remaining 50 questionnaires were either not fill correctly or not fill at all. Our analysis was based on the properly filled 150 questionnaires.

Data were collated and we employed both descriptive and inferential statistics as a method in analysing collated data in which analysis was made on each responses gotten from the questionnaires. Analysis is presented in frequencies and percentages, hypothesis were also formulated which led to making required deductions which were drawn based on a decision rule of 0.05 significant level. The data was also further analysed by using cross tabulations and chi-square tests.

A. *Test of Hypothesis and Inference*

The Chi-square test was used in this research to test the significance of responses gotten from online banking users in Nigeria. The chi square test is performed by defining the numbers categories and observing the number of case that falls into each category and knowing the expected number of cases fully in each category.

The formulae for the Chi square is $X^2 = \Sigma (Oi - Ei)^2 / Ei$

Where X^2 = Chi Square

Oi= Number of Observed Cases which were calculated from the number of respondents. Ei = Number of Expected Cases which was calculated by multiplying the total of the rows and total of the columns and dividing it by the total number of respondents.

VI. HYPOTHESIS OF THE STUDY

Our study is guided by the following hypothesis:

1. **Ho:** The education level of respondents does not influence their level of awareness on phishing attacks.
   Hμ: The education level of respondents does influence their level of awareness on phishing attacks.
2. **Ho:** The rate at which respondents information has been breached while banking online does not influence their level of awareness on virus/malware attacks.
   Hμ: The rate at which respondents information has been breached while banking online does influence their level of awareness on virus/malware attacks.

VII. RESEARCH QUESTIONS

1. Are online banking users in Nigerians fully aware of the threats that comprises online banking and if they are, what is the level of their awarenes?
2. Can possession of tertiary education by online banking customers provide has effect on their level of information security awareness?
3. Has standard ways or methods of educating or raising awareness being made available to Nigerians about online banking and its risks?
4. Has there been an high rate of infro mation security breaches among users of online banking while banking online and how have they reacted to it?

VIII. DATA ANALYSIS AND RESULT

TABLE I: GENDER ANALYSIS OF RESPONDENTS

		Frequency	percentage	Valid percentage	Cumulative percentage
Valid	MALE	76	50.7	50.7	50.7
	FEMALE	74	49.3	49.3	100.0
	TOTAL	150	100.0	100.0	

Table 1 shows the gender difference between the respondents, the data collected indicates that 76 or 50.7% of Respondents are male and 74 or 49.3% of them are female. Therefore, it can be concluded that there's a 1.4% difference which is not so much between the respondents gender wise.

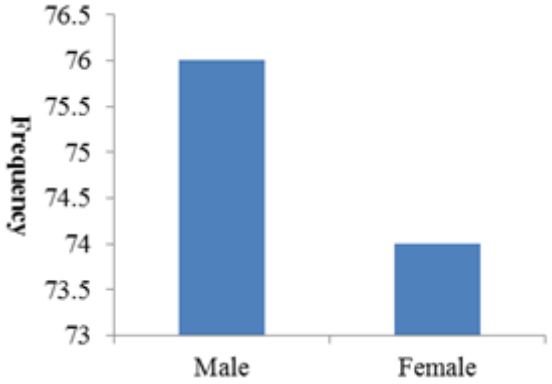

Fig. 1 Genda of respondents

TABLE II
AGE CATEGORY OF RESPONDENTS

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	<20	1	.7	.7	.7
	21-25	22	14.7	14.7	15.3
	26-30	37	24.7	24.7	40.0
	31-35	39	26.0	26.0	66.0
	36-40	27	18.0	18.0	84.0
	>40	24	16.0	16.0	100.0
	Total	150	100.0	100.0	

Table 2 shows the age category of respondents, 1 or 0.7% of them is below 20 years old, 22 or 14.7% of them are 21-25 years old, 37 or 24.7% of them are 26-30 years old, 39 or 26% of them are 31-35 years old, 27 or 18% of them are 36-40 years old, 24 or 16% of them are 40 years old and above. In view of this fact, it can be deduced that the highest number of people using internet banking in Nigeria are between the ages 31-35 years followed closely by the ages 26-30 with a 1.3% difference, the lowest age category is the age 21-25 years.

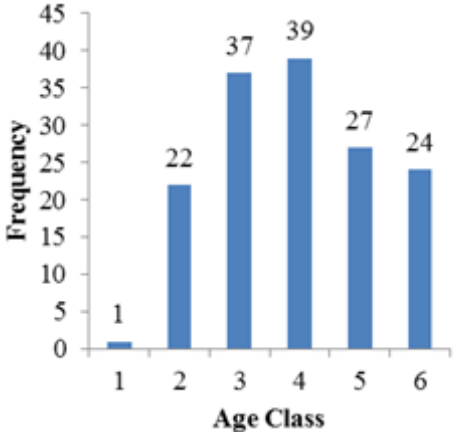

Fig. 2 Statistics of frequency of age of respondents

TABLE III
EDUCATION LEVEL OF RESPONDENTS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	PRIMARY	0	0.0	0.0	0.0
	SECONDARY	6	6.0	6.0	6.0
	TERTIARY	144	94.0	94.0	100.0
	Total	150	100.0	100.0	

As shown in table 3 above respondents with the primary educational level are 0%, respondents with the secondary educational level are 6 or 6% while respondents with tartiary educational level is seen to be the one with the highest number of respondents with 144 or 94% of them which proves that majority of the people who use online banking have tertiary educational level.

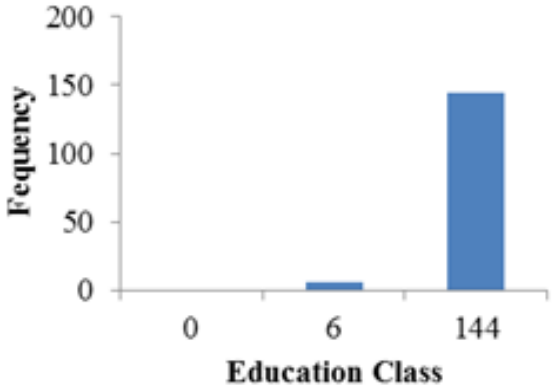

Fig. 3 Frequency of education level of respondents with tertiary education having highest

TABLE IV
OCCUPATION OF RESPONDENTS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	STUDENT	0	0.0	0.0	0.0
	EMPLOYED	135	90.0	90.0	90.0
	UNEMPLOYED	15	16.3	10.0	100.0
	Total	150	100.0	100.0	
Missing	System				
Total		150	100.0		

As shown in the table above 0% of respondents are students, 135 or 90.0% of them are employed and 15 or 16.3% of them are unemployed, Based on this analysis its safe to conclude that majority of online banking users are employed with a huge difference in the percentage of students and the unemployed.

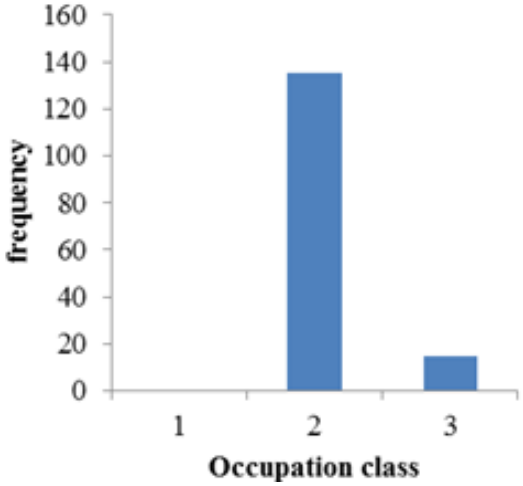

Fig. 4 Occupation of respondents with higher number of employed respondents

TABLE V
HOW LONG RESPONDENTS HAVE BEEN USING ONLINE BANKING?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	UNDER 1 YEAR	54	36.0	36.0	36.0
	1-3 YEARS	68	45.3	45.3	81.3
	OVER 3 YEARS	28	18.7	18.7	100.0
	Total	150	100.0	100.0	

The table above shows that 54 or 36% of respondents have been using internet banking not up to a year, 68 or 45.3% of them have been using internet banking for 1-3 years and 28 or 18.7% of them have been using internet banking for over 3 years, from this analysis it can be deduced that only a few people have been using internet banking for over 3 years even though its been around since, however more people have adopted it in the past 3 years as the category has the highest percentage of respondents and also the second higher percentage being the adoption under 1 year. Therefore, it can be concluded of this analysis is that internet banking is spreading fast and gaining more awareness among users across the country.

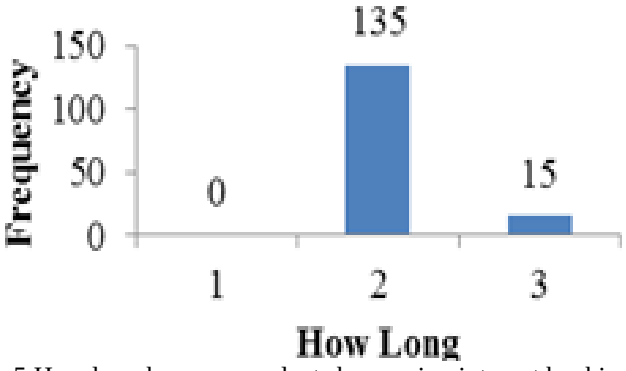

Fig. 5 How long have respondents been using internet banking

TABLE VI
HOW KNOWLEDGEABLE RESPONDENTS ARE ABOUT INTERNET BANKING

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	FAIR	18	12.0	12.0	12.0
	AVERAGE	56	37.3	37.3	49.3
	V.KNOWLEDGEABLE	76	50.7	50.7	100.0
	Total	150	100.0	100.0	

As shown in the table above 18 or 12% of respondents said they are knowlegeable fairly, 56 or 37.3% of them said they are averagely knowledgeable while 76 or 50.7% of them said they are very knowlegdeable about internet banking which concludes that majority of the respondents agree that they are very knowleageable about internet banking.

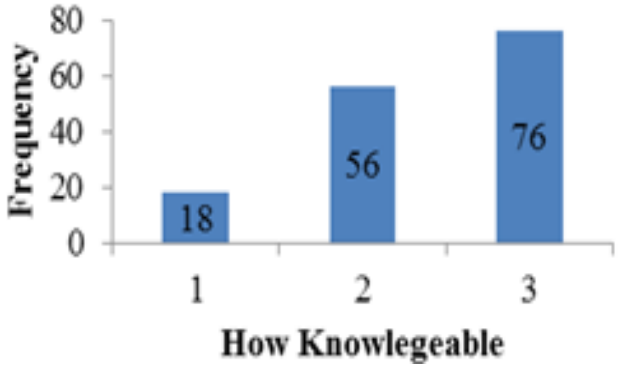

Fig. 6 How knowledgeable are the respondents about internet banking

TABLE VII
BREACH OF RESPONDENTS INFORMATION WHILE BANKING ONLINE

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	YES	12	8.1	8.1	8.1
	NO	114	76.0	77.0	85.1
	I DO NOT KNOW	24	14.9	14.9	100.0
	Total	150	100.0	100.0	
Total		150	100.0		

As shown in the table above, 12 or 8% of the respondents claimed to have had their financial information compromised, 114 or 76% of them claimed to have not and 24 or 16% of them have no idea if their information have ever been compromised or not, From this analysis it can therefore be concluded that information security breaches of online banking customers in Nigeria is still low as a higher percentage of people claims to not have had any information breached since they have been banking online.

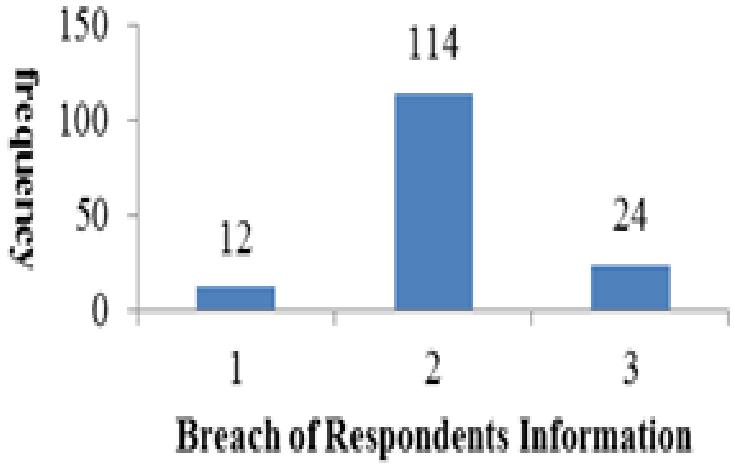

Fig. 7 Breaching of respondents' information during online transaction

TABLE VIII
RESPONDENTS AWARENESS ON THREATS OF ONLINE BANKING

Variables	Respondents									
	TD	P	PD	P	NAD	P	PA	P	TA	P
Trusts internet banking is private and safe	70	46.7%	54	36.3%	18	12.3%	6	3.7%	2	1.0%
Sharing of passowrd and PINs	38	25.6%	40	27.0%	33	21.7%	26	17.0%	13	8.7%
use passwords relating to information	8	5.3%	24	16.0%	29	19.3%	56	37.3%	33	22.1%
I Respond to all e-mails because I always believe the mails are from my bank.	10	6.7%	20	13.3%	39	26.0%	37	24.7%	44	28.7%
Download all sorts of applications to the PC/mobile phone for banking online, I always trust it's very secure.	11	7.3%	23	15.0%	63	42.5%	32	21.2%	21	14.0%
I don't have to look over my shoulders or when typing information	11	7.3%	10	6.7%	15	10.0%	36	24.0%	78	52.0%

TD- Totally Disagree
PD- Partially Disagree
NAD- Neither Agree nor Disagree
PA- Partially Agree
TA- Totally Agree
P- Percentage

IX. TEST FOR HYPOTHESIS

HYPOTHESIS 1*(Ho):* The education level of respondents does not influence their level of awareness on phishing attacks.

TABLE IX
CROSS TABULATION OF EDUCATION LEVEL AND I I RESPOND TO E-MAILS WITH REGARDS TO MY BANKING INFORMATION, I TRUST THEY ARE FROM MY BANK.

Educational Level	I RESPOND TO E-MAILS WITH REGARDS TO MY BANKING INFROMATION.					
	TOTALLY DISAGREE	PARTIALLY DISAGREE	NEITHER AGREE OR DISAGREE	PARTIALLY AGREE	TOTALLY AGREE	TOTAL
Primary	0	0	0	0	0	0
Secondary	1	1	0	3	1	6
Tertiary	9	19	39	34	43	144
Total	10	20	39	37	44	150

TABLE X
CHI-SQUARE TEST

O*i*	E*i*	O*i*-E*i*	(O*i*-E*i*)²	(O*i*-E*i*)²/E*i*
0	0	0	0	0
1	0.4	0.6	0.36	0.9
9	9.6	-0.6	0.36	0.04
0	0	0	0	0
1	0.8	0.2	0.04	0.05
19	19.2	-0.2	0.04	0.002
0	0	0	0	0
0	1.56	-1.56	2.43	1.56
39	37.44	1.56	2.43	0.06
0	0	0	0	0
3	1.48	1.52	2.31	1.56
34	35.52	-1.52	2.31	0.06
0	0	0	0	0
1	1.76	-0.76	0.58	0.33
43	42.24	0.76	0.58	0.01

Level of significance = 0.05
Decision Rule: Reject the null hypothesis if $X^2 > 9.488$, where $X^2 = \Sigma (Oi\text{-}Ei)^2/Ei$ and 9.488 is the value of X^2.
Therefore X^2 Calculated = 4.57
X^2 Tabulated = 9.488
Conclusion: Since the X^2 calculated is lesser than X^2 tabulated (4.57 < 9.488), the null hypothesis is accepted which means the educational level of respondents does not affect the level of awareness respondents have on phishing attacks which means their educational level does not influence their level of awareness on phishing attack. Simply mean that formal education does not solve the problem of information security awareness.

.

HYPOTHESIS 2(*Ho*): The rate at which respondents information has been breached while banking online does not influence their level of awareness on virus/malware attacks.

TABLE XI

CROSS TABULATION OF HAS YOUR INFORMATION EVER BEEN BREACHED OR COMPROMISED WHILE BANKING ONLINE AND DOWNLOADING ALL SORT OF APPLICATIONS TO PC/MOBILE PHONE

Information Breached	DOWNLOD VARIOUS APPLICATIONS TO PC/MOBILE PHONE, TRUSTS IT VERY SECURE					
	TOTALLY DISAGREE	PARTIALLY DISAGREE	NEITHER AGREE OR DISAGREE	PARTIALLY AGREE	TOTALLY AGREE	TOTAL
Yes	1	1	7	3	0	12
No	10	17	46	25	16	114
I don't know	0	5	10	4	5	24
Total	11	23	63	32	21	150

TABLE XII

CHI-SQUARE TEST

O*i*	E*i*	O*i*-E*i*	(O*i*-E*i*)²	(O*i*-E*i*)²/E*i*
1	0.88	0.12	0.01	0.01
10	8.36	1.64	2.69	0.32
0	1.76	-1.76	3.09	1.76
1	5.04	-4.04	16.32	3.23
17	47.88	-30.88	953.57	19.91
5	10.08	-5.08	25.81	2.56
7	1.84	5.16	26.63	14.47
46	17.48	28.52	813.40	46.53
10	3.68	6.32	39.94	10.85
3	2.56	0.44	0.19	0.07
25	24.32	0.68	0.46	0.02
4	5.12	-1.12	1.25	0.24
0	1.68	-1.68	2.82	1.68
16	15.96	0.04	0.002	0.0001
5	3.36	1.64	2.69	0.80

Level of significance = 0.05

Decision Rule: Reject the null hypothesis if $X^2 > 9.488$, where $X^2 = \Sigma (Oi\text{-}Ei)^2/Ei$ and 9.488 is the value of X^2.

Therefore X^2 Calculated = 102.45

X^2 Tabulated = 9.488

Conclusion: Since the X^2 calculated is greater than X^2 tabulated (102.45 > 9.488) the null hypothesis is rejected which means that the level of information security awareness on malware and phishing attacks does influence the level of infromation security breaches customers have had while banking online does. which means users are influenced by the amount of times their information has being compromised online to their knowledge or awareness on malware and phishing attack.

X. EXISTING METHODS OF CREATING INFORMATION SECURITY AWARENESS AND THEIR WEAKNESSES

Below are some of the methods that have been adopted by most banks to spread information security awareness on threats and attacks associated with online banking and the weakness of the methods:

1. Through Short Service Messages(SMS): Highlighted weaknesses include

a) Users might not read these messages.

b) Users might not get the messages as a result of poor network connection.

c) Users might not pay attention to the messsage as they might consider it a random bulk text message.

d) Message that would be sent might be limited and incomprehensible therefore not all aspects of information on online banking security awareness is passed across to user.

2. Through Electronic Mails(E-mails): Some of the rules for the sms method also applies in the email method which includes:

a) Users may not pay attention to the mail or not even read them believing it might be a spam mail or even a phished mail.

b) Users might not get the email as a result of poor network connectivity.

c) Some users don't check their emails very often thereby not getting the message.

d) Some users might might change thier email address and forget to notify banks on the change.

3. Through Newspapers: Weaknesses include:
a) Most people don't read newspapers anymore.
b) Can only pass limited information across to users.
c) People are more likely to focus on serious news in the paper thereby causing less attention to be paid to information security awareness.
4. Through Bank Websites: Banks usually paste information on online banking threats and forms of attacks and also ways in which users can prevent from these attacks on their websites, the weaknesses in this method include:
a) Users tend to forget these information.
b) Users might be more focused on carrying out their transactions thereby neglecting the information security awareness on bank websites.

XI. PROPOSED METHODS THROUGH WHICH AWARENESS CAN BE IMPROVED

In addition to the existing methods of creating information security awareness, we propose the following methods for an improvement in information security awareness program.

A. *Television and radio advertisement*

Banks in Nigeria have not been using Television and Radio media to pass the message of information security relating to online banking to their customers. The banks can use different jingles for awareness creation with different local languages. These two media can be used to spread possible threats and attack that customers can experience vis-à-vis what need to be done when fraudulent attempt is been made by attacker. Apart from allowing existing customers to get familiar with security challenges, this will further encourage new customers (whose security issues has been the hindrance for adoption of online banking system) to adopt online banking knowing fully well that there are ways to address the issue of security challenges confronting the system.

B. *Quarterly seminars*

Since the in introduction of online banking system into Nigeria, there has never been a single seminar organized purposely for information security awareness creation for online banking customers. Perhaps, most banks believe that information security awareness is only meant for their employees. Whereas, both the staff and costumer need the information security awareness. It will be good if banks can make it as part of their policy to organize quarterly information security awareness program for both new customers and the old once to inform them about possible security challenges relating to online banking. As attackers are getting new sophisticated methods every day to carry out their attacks, there is need for costumers to be aware of latest possible threats. To give room for good attendance by customers, the seminar should be made compulsory for all customers of online banking system and properly should be a branch affair so that there will be proper coordination. Also, there should be away for costumers' motivation.

C. *Use of application technology*

Applications being developed in recent times do just about anything. Based on our survey, many online banking costumers carry out their transaction on their mobile devices (such as Smartphone, palm top, laptop and so on). Banks can come up with an application that will be installed on costumers' mobile devices, with an interface that show costumers latest threats, possible attacker, step to take when attempt is made by attacker and what should be done if attacked. Maybe customer can be asked to download the application during activation of online banking by customer. Which means that, bank can make the download of the application by customer a compulsory step before activation. People access their mobile devices frequently.

XII. RESULT DISCUSSION AND CONCLUSION

Majority of the respondents are male though the different is not so much from the female gender. Also majority of the respondents who use online banking are within ages 31-35 years, majority of them also have a tertiary educational. Most of the users of online banking are employed, a higher number of people have been using internet banking between 1-3 years now, most of the internet banking users also claim to be very knowledgeable about internet banking, however majority of the people said they have not had their information breached or compromised while banking online as very few people said they have had theirs compromised.We have based our survey on five common threats of online banking system. Our analysis shows that many respondents believe that banking online is safe and secure. Those that believe that there are risk associated with internet banking system are those that have in one time or the other have their information compromised. This means that great number of respondents are not even aware of security risk associated to online banking. Although, in the case of PIN/password sharing threat the result shows that a good number of the respondents believe that by sharing their password they put their information at risk which shows they are well aware this particular threat but in the area of using guessable passwords as a form of threat the result shows that many respondent are not aware. Also, in the cases of phishing attack, virus/malware attack and shoulder surfing attack, the results show that many respondents are not aware. hypothesis one shows that the level of education of costumers does not fill the gap of information security awareness need for online banking. This means that customer with tertiary education need information security awareness. Also, hypothesis two shows that the rate of information security breaches some respondents have had while banking online has an influence on their level of awareness on virus and malware attacks.

Finally, the result of our survey presented above shows that existing methods of creating information security awareness is not yielding good results. Therefore there is need for our banks to intensify effort on information security awareness creation for their customers so that their existing customers will not be discouraged by attack from attackers and the new customers who are yet to adopt online banking will be encouraged too. It is in line with the need for the banks to intensify their effort that we have proposed new methods in which information security awareness creation can be improved.

ACKNOWLEDGMENT

Our sincere appreciation goes to those who participated in our survey exercise. Without respondents, this survey would not have been possible.

REFERENCES

[1] F. A. Aloul, "The Need for Effective Information Security Awareness." *International Journal of Intelligent Computing Research*, vol. 1, pp. 130-137, June 2010.
[2] W. Candid, "Threats to Online Banking," Symantec, Symantec security response, white paper, 2005.
[3] (2012) Online Security: Online Banking, the Threats and Countermeasures. [Online]. Available: https://sqnetworks.com/downloads/AhnLab_AOS_WhitePaper.pdf
[4] A. M. French, "A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information," *Journal of Internet Banking and Commerce*, vol. 17, No.2, pp. 3-13, August 2012.
[5] (2013) What are the dangers of online banking? [Online]. Available: http://blogs.norman.com/2013/for-consumption/what-are-the-dangers-of-online-banking
[6] (2013) 10 Tips to Prevent Phishing Attacks. [Online]. http://support.pandasecurity.com/blog/security/10-tips-prevent-phishing-attacks/
[7] L. Anthony, K. Stephen and K. Micheal, "Identify threaths associated with Man-in-the-middle attack during communication between a mobile devices and the back end user in mobile banking application," IOSR Journal of Computer Engineering, vol. 16, pp. 35-42, April 2014.
[8] Essays, UK. (November 2013). Effectiveness of information security awareness information technology essay. [Online]. http://www.ukessays.com/essays/information-technology/effectiveness-of-information-security-awareness-information-technology-essay.php?cref=1
[9] H. A. Kruger, W. D. Kearney, "Aprototype for assessing information security awareness," Computer & Security, vol. 25, pp. 289-296, Feb. 2006.
[10] K. Crumbley. (2012). Postponing Decisions for Online Banking Security Awareness Training = Risky Business. [Online]. Available: http://discover.profitstars.com/strategicallyspeaking/bid/60825/Postponing-Decisions-for-Online-Banking-Security-Awareness-Training-Risky-Business
[11] C. prema. (2009) Factors Influencing Consumer Adoption of Internet Banking in India. [Online]. Available: http://www.presidencybusinessschool.org/download/Factors_influencing_consumer_adoptionof_internet_banking%20_in_India.pdf
[12] N. j. Black, A. Lockett, C. Ennew, H.Winklhofer, and S. McKechnie, " Modeling consumer choice of distribution channels : an illustration from financial services," International Journal of Bank Marketing , vol. 20 , pp. 161-173, 2002.
[13] B. Howcroft, R. Hamilton and P. Hewer, "Consumer attitude and the usage and adoption of home-based banking in the United Kingdom," The International Journal of Bank Marketing, vol. 20, pp. 111-121, 2002.
[14] R. Safeena, Abdullah and H. Date, "Customer Perspectives on E-business Value:Case Study on Internet Banking," Journal of Internet Banking and Commerce, vol. 15, pp. 1-13, April 2010.
[15] S. Milind , "Adoption of Internet banking by Australian consumers: an empirical investigation," International Journal of Bank Marketing, Vol. 17, pp. 324 - 334, 1999.
[16] N. O. Ndubisi, R. Supinah, and P. Guriting, "The extended technology acceptance model and internet banking usage intention," in proc. ILCP'04,2004, Turkey pp. 973-988
[17] A. Okunoye, L.A. Adebimpe, A. Omilabu, I.O. Olapeju and O. B. Longe, "Information Security Awareness among SMEs in the South Western Nigeria – Significance of Factors," African Journal of Computing and ICT, Vol 5, pp. 3-10, September. 2012.

