AN EMPIRICAL SURVEY TO SUBSTANTIATE THE NEED FOR IMPROVEMENT IN USER SECURITY AWARENESS IN MOBILEBANKING IN NIGERIA

Emmanuel Eturpa SALAMI[1], Osaremwinda OMOROGIUWA[2], Luck J. OGBOGBO[3]

[1] Igbinedion University Okada, Edo State Nigeria - Department of Computer Science and Information Technology

[2] Igbinedion University Okada, Edo State Nigeria - Department of Computer Science and Information Technology

Salami.emmanuel@iuokada.edu.ng; ask4osas@iuokada.edu.ng; ogbogbo.lucky@iuokada.edu.ng

ABSTRACT:

Mobile banking application solutions are now the most preferable means of performing financial transactions and almost all banks in Nigeria have developed and deployed at least one mobile application to service their Client (Customers). However, the security of users of these solutions is a critical issue that cannot be overlooked and understand the concerns of users (Customers) when it comes to their privacy, data, and their perceptions on the issues of access delegation, an empirical survey was conducted to identify what user opinion and concerns are. This study seeks to investigate if users of mobile banking applications have sufficient security awareness and if it has translated into better security protection measures. Also, the knowledge level on the security features available on mobile banking apps and the best way users can be educated to understand their role in securing their privacy. The research work investigates the security risk in access delegation by the account holders to third parties. The findings from the survey identified a low level of security awareness among users in terms of security safety measures as only 14.4% of respondents admitted that they will consider security as a factor which further that there is a lack of security awareness among users and this has heightened the concerns of users with 58.2% expressing serious concern over their privacy and the problem of Access delegation as a risky behavior most users indulge in. The study also reveals that most users believe that the current security measures in mobile banking are at a low level. An Empirical Survey using quantitative descriptive analysis was used for analyzing the data collected and the tool used for data collection was a structured questionnaire and Statistical Package for Social Science (SPSS) to code the data for analysis.

KEYWORDS: Cybersecurity, Hacking, Awareness, Mobile baking, *Users'*

INTRODUCTION

The internet has made a significant impact on banking and financial institutions, giving customers access to several banking services around the day. at an equivalent time, it made an enormous cut on banks' costs. Previous research shows that mobile banking provides the cheapest delivery service for several banks. Mobile banking is a facet of electronic banking and is considered a crucial distribution and channel for retail banking [1 and an extension of internet banking with its unique characteristics that make it one of the foremost promising tools in banking services (Laukkanen, 2007). The first development of the mobile banking app was within the simple form quite two decades ago. Typically, mobile banking services enable users to receive information on their account balances via SMS (Short Messaging Service). With the introduction of the GPRS (General Packet Radio Services) network and the development of more technologies, the services expanded to fund transfers between accounts, stock trading, and confirmation of direct payments via the phone's browser (Mallat, 2004). With mobile phones and smartphones becoming very fashionable and other people spending more average time on mobile devices than they do with a personal computer since 2014, it simply means more people are becoming used to their mobile devices to perform the services which were in time past available only on their computers. A report from the Association of Mobile Network Operators worldwide (GSMA, 2019) shows there are 747 million SIM (Subscriber Identity Module) connections in Sub-Saharan Africa, which is 75 percent of the population. These indeed may be a viable marketplace for financial institutions to develop and deploy mobile banking Apps in other to succeed in getting more clients but this is often not without an attending security issue arising. The steady rise in mobile usage in Nigeria has opened new opportunities for financial institutions in Nigeria to adopt mobile banking in place of the on-banking method. The report by geopoll.com (2019) shows that the present mobile penetration in Nigeria stands at 84 percent out of which 64 percent are account owners with at least one of the 22 commercial banks in Nigeria but only 6 percent of the account owners use their device to perform any mobile banking transaction. Even though most commercial banks in Nigeria have successfully developed and deployed mobile banking applications, the acceptance and usage of this banking option have suffered some setbacks in Nigeria due to security concerns by the users. Most users are skeptical and are not very confident in the safety of the solution, especially with growing issues of cybercrimes in the financial sector. Smartphones running on the Android Operating System (OS) have become more fashionable phones among users today due to their user-friendliness and as open-source software, developers can record and publish their android application thereon but this is not without some attendant security issues such as malicious codes being easily deployed, which will affect applications built for android OS (Kouraogo, 2017). Also, attacks that occur through Android OS leave room for a takeover of the complete control of a phone and supply access to victims' private data, elevating privileges and access to cryptographic keys stored on the Android mobile platform. Applications developed to run on Android are easily decompiled due to their structural characteristics (Misra and Smita, 2015) which makes it possible to even perform a more sophisticated attack than those cited

previously. Using a mobile platform in performing any form of financial transaction will usually face two limitations: the security of the payment system and the users of the system. When considering the security of mobile applications, the security of the server-side and the security of the client-side must be carefully factored into the planning, design, and implementation of any mobile banking solution.

Most commercial banks in Nigeria provide mobile banking services simply because it has become a necessity as it provides a convenient means of transaction and helps them remain relevant in the business of financial service provision. However, some banks have not done very much in terms of securing their applications. Security updates and patches are not provided by some of these applications and where such patches are provided, it comes only after a breach has occurred. A study of most mobile banking applications developed for use by customers shows that most bank customers are not aware of how-to safeguard their privacy and account when using this mobile banking solution and as a result, so many customers have experienced one form of attack or the other by the way of social engineering. Also, the problem of access delegation by a user to a third party who then exploit such means to steal from their account has become a reoccurring problem. The absence of any means of creating awareness in the existing mobile banking application has further affected the trust and confidence customers have in these banking solutions. Bank customers have expressed concerns and reservations on the integrity of this application because they feel it is not secured enough and that can be attributed to the level of awareness in terms of security risk and safety measures available for them. This paper is aimed at carrying out an empirical survey to substantiate the need for improvement in user security awareness with an emphasis on mobile banking users in Nigeria. The objectives of this work are;

i. To ascertain the current security awareness level among users of mobile banking applications.
ii. To determine users' privacy concerns in the usage of mobile banking applications.
iii. To determine the need for an improved data protection mechanism in mobile banking applications.
iv. The determine the challenges and risks associated with access delegation by mobile banking application users.

REVIEW OF RELATED LITERATURES

Several studies have been conducted to understand the awareness level of users of mobile applications both locally and internationally and the result of these studies identified some of the challenges that creating awareness among users faces and the reason why users don't seem to be aware of safety measures available to adopt in preventing their privacy. Though previous works were focused more on the study of the awareness of users on the security of smartphones and information systems, this study is primarily focused on awareness of security issues and safety measures in mobile banking applications. A study conducted by Abayomi, (2021) proposed that more enlightenment (awareness) should be done to encourage students of tertiary institutions to

learn how to use other means for storing their information outside their mobile phones and the use of periodic text and seminars to create enlightenment. (Kearney, 2006) using three factors: behavior, cognition and affect to develop a prototype for information security awareness identify that user's knowledge and behavior have an effect on their security awareness but the behavior of users alone cannot be relied on completely to develop an information security awareness model. Susanto, (2021) carried out a survey study with a focus on the hardware and software of users' mobile devices, the study looked at the behavioral and influence factors, and the findings revealed users' application of mobile phones in performing several duties does not mean that they were satisfied with the security awareness also it showed the most users do not adopt basic security measure therefore, they are exposed to threats and vulnerabilities through their mobile devices. The study recommended the need to create security awareness on implications of users' behavior and its impact on their mobile devices as this will help increase the security awareness level among users. Kurlyk et al, (2020) reported from their work after studying the various participants from three different countries (Germany, Romania, and Spain) they discover that participants from Germany gave more attention to security and privacy compared to those from Romania and Spain which further reveals that enforcement of Implementation Security Policy regulations by regulators differs for various countries and this is as a result of awareness among users. Esmaeili (2014) using his model for assessing factors that affected information security behavior in smartphone networks identified attitude, intention, computing experience, breaching experience, and facilitation condition as the main and direct factors that influence information security behavior of users of smartphones. Peer, (2015) developed and examined the validity of the Security Base Information System, using a security questionnaire to measure the attitude of users towards security-related topics in the study three distinct variables were used for the experiment which is; requesting the subjects to suggest a strong password and identify phishing URLs, examining the operating system version of the subjects personal computer two weeks after a release of an update, and checking for the existence of a secure lock screen on the subject's personal smartphone. Wijesekera et al., (2015), studied the perception of smartphone users regarding permission. In their experiment, the authors collected contextual information about the state of the device when permissions are requested. At the end of the experiment, in a concluding survey, they asked the subjects about the permissions granted and denied as well as their decision making in accordance with specific contexts and arrived at the conclusion that the perception of users impacts the subject of permission. Pawel and Mazurczyk, (2018) in their study of User Perspective and Security of a New mobile authentication method observed that a new authentication scheme that is based on the Open ID Connect standard and Subscriber Identity Module card (SIM) yielded better results in providing an authentication than the existing methods. Their proposed method was compared with existing ones such as biometrics. Their proposed solution enables users to access websites, services, and applications without the need to remember passwords, responses, or support of any equipment.

METHODOLOGY

An Empirical Analysis is used in this study as its obtainable in other Computer Science research (Omorogiuwa and Chiemeke, 2008). It entails the use of quantitative descriptive analysis in analyzing the data collated from users of mobile banking applications of some selected banks. Empirical analysis is an evidence-based approach for the study and interpretation of information. The sample size chosen for this study is 261 mobile banking application users irrespective of their gender, educational qualification, computer skill set, or occupation. The questionnaire was designed using google form and self-administered both physically and online.

Tools used for the study are questionnaires and SPSS (Statistical Product and Service Solutions) for the collection and analysis of data. Descriptive statistical tools such as frequency count, mean, and standard deviation was used. The data collected through the administered questionnaire was collected and subjected to descriptive and inferential analysis. Both Frequency distribution and Percentage were used to determine the number of respondents in every section. Pearson value (P. Value) was set at 0.05 alpha level of significance, and this test was used to determine the significant relationship in the response between the group categorization of the questions. Data reliability test was carried out to justify the final data collected using Fleiss multi-rater Kappa reliability test measurement and agreement. To get a conclusive result we use the following formula Fleiss Kappa formula

$$\kappa = \frac{\bar{P} - \bar{P}_e}{1 - \bar{P}_e} \qquad (1)$$

Where the values in the formula are represented as follows;

K= number of evaluation categories

P_e= observed percentage of chances of agreement

P= observed percentage of agreement

The factor $(P - P_e)$ gives the degree of agreement that is attainable above chance and, $(1 - P_e)$ gives the degree of the agreement actually achieved above chance. Where the raters are in complete agreement (K = 1) and if there is no agreement among the raters (other than what would be expected by chance) then ($K \leq 1$).

Overall Agreement[a,b]

		Asymptotic			Asymptotic 95% Confidence Interval	
	Kappa	Standard Error	z	Sig.	Lower Bound	Upper Bound
Overall Agreement	.001	.000	1.243	.214	.000	.001

a. Sample data contains 201 effective subjects and 36 raters.

b. Rating category values are case sensitive.

The P.value (significance value) is (p=0.214) which makes the data reliable.

The questionnaire was structured into five thematic areas with a total of thirty questions using a five-point scale of measurement for each question. The questionnaires were grouped into User Awareness (to ascertain the current awareness level of users), User Privacy (to ascertain the privacy concerns of users), User Data protection (to assert the perception of users on their data) User Access delegation (to evaluate user opinion on the subject of access delegation) and Users Device/Application security. (to understand user behavior towards their device security).

FINDINGS AND DISCUSSION

261 questionnaires in total were distributed out of which 210 were handed out physically to participants and 201 questionnaires were returned. 150 questionnaires were complete and usable, and 51 responses were received from the online participants, with an overall response rate of 85%. Only 201 of the answered questionnaires were useful after performing data cleaning and filtration. 150 of the returned questionnaires were complete and usable, and 51 responses were received from the online participants, with an overall response rate of 85%. Only 201 of the answered questionnaires were useful after performing data cleaning and filtration.

Table 2.1 Respondents' Demography

Items	Variables	Frequency	Percent
Please indicate your gender:		3	1.5
	Female	98	48.8
	Male	100	49.8
	Total	**201**	**100.0**
Please indicate your age group	Less than 18	49	24.4
	18 to24	81	40.3
	25 to 39	34	16.9
	40 to 60	33	16.4
	Greater than 60	4	2.0
	Total	**200**	**100.0**
Please indicate your current occupation:	Student	149	74.1
	Self Employed	8	4.0
	Employed	40	19.9
	Unemployed	1	0.5
	Others	3	1.5
	Total	**201**	**100.0**
Please indicate your highest educational level:	Primary	1	0.5
	Secondary	102	50.7
	Graduate	37	18.4
	Post Graduate	39	19.4
	Others	22	11.0
	Total	**201**	**100.0**
How would you grade your Computer Skills:	Basic	63	31.3
	Intermediate	64	31.8
	Advanced	50	24.9
	Expert	11	5.5
	Others	13	6.5
	Total	201	100.0

As seen in Table 2.1 Users of mobile phones today are relatively young people within the age group of 18-24 and this can be attributed to the growing penetration of internet connectivity within Nigeria. As at December 2020, the teledensity of Nigeria was put at 107.18% from the report by Nigeria Communication Commission (NCC). 40.3% of the respondents aged between 18 and 24 years are fast adopting either mobile banking or other related solution as compared to 16.9% and 16.4% aged between 25years to 60years. With 74.1% of respondents being students, this indeed shows the need to give attention to the security behind mobile banking solutions since the majority of these categories of users are still naïve when it comes to how best to protect themselves from attacks through social engineering, Phishing or any other types of security threats that they can become exposed to while using these mobile solutions. The sample survey also presents a worrisome picture of computer literacy levels with only 31.3% having Basic computer skills and 31.8% having at least an intermediate knowledge level. This shows that the level of computer literacy is still at a very low level in Nigeria. And to effectively use mobile banking solutions in a safe and secured way will quire users to have at least basic knowledge of IT (Information Technology) which will help the user know the fundamental data privacy and protection steps.

Table 2.2: Awareness and usage

Items	Variables	Frequency	Percent
Do you use Mobile Application in General?	Yes	178	88.6
	No	4	2.0
	Not often	10	5.0
	I don't Know how to use it	2	1.0
	Only when the need arises	7	3.5
	Total	**201**	**100.0**
Does your bank have a mobile banking application and do they offer mobile banking services?	Yes	190	94.4
	No	1	0.5
	Maybe	4	2.0
	I don't know	1	0.5
	Am not sure	4	2.0
	Total	**201**	**100.0**
Do you carry out banking transactions on your mobile device (either via mobile browser or mobile banking app)	Yes, only through mobile application	89	44.3
	Yes, through both ways	82	40.8
	No, I don't know how to use it	7	3.5
	I don't know how to use it at all	7	3.5
	Not often	16	8.0
	Total	**201**	**100.0**
To what extent are you satisfied with your Banks' Mobile banking services?	Highly Satisfied	35	17.4
	Satisfied	104	51.7
	Highly dissatisfied	3	1.5
	Dissatisfied	2	1.0
	Neutral	57	28.4
	Total	**201**	**100.0**
Which of the following factors influence you the	All time Accessibility	48	23.9
	Direct Access	27	13.4

most to use Mobile banking services?	Ease of use	83	41.3
	Friends/Relatives	6	3.0
	Security	37	14.4
	Total	**201**	**100.0**
Why would you consider using Mobile banking services.	Easy of fund transfer	43	21.4
	Easy processing	27	13.4
	Inexpensive	8	4.0
	Privacy	25	12.5
	Time Saving	98	48.8
	Total	**201**	**100.0**

Though there is a significant growth in the percentage of mobile phone usage as seen in Table 2.2, when compared with the level of security consciousness of most users, there is a significant difference. Most mobile phone users are not really aware of the extent to which their behavior in handling their devices affect their privacy and how this exposes their online credentials security-wise. While the sample survey shows 88.6% of respondents use phones generally. Table 2.2 shows that 94.4% of the respondent are aware their banks provide mobile banking services but this awareness among users' does not necessarily mean that they are aware of how to use this mobile solution in a secure way. As observed by the European Network and Information Security Agency (ENISA) 2010, the issue of security awareness is not training but is an attempt to change the behavior and patterns of how people use technology and the internet. The kind of awareness that users need to have then is such that their behavioral patterns are changed in such a way that they know what to do and not do. Puhakainen (2006) theory on security awareness among users identified three key steps that can help increase awareness which include; (i) increase training on Information Security Awareness. (ii) Rewards and Punishment to Increase Information Security awareness (iii) Campaigning to Increase Information Security Awareness. 41.3% say they are influenced to use mobile because they consider it as easy to use while 48.8% state that they would consider using mobile banking app because it is time-saving and "time-saving" simply means that users are not constraint by location except their connectivity, however, only 14.4% respondent see security as a factor that will influence their usage of the mobile banking app. This goes to show that while security today is an issue on any mobile platform, users seem not to see it as something they should give more priority to above other considerations and this can be because they don't have the right understanding of the significant impact it can create to their privacy. Table 2.2 shows 51.7% of respondents are satisfied with their bank's mobile app solution and services while 28.4% are neutral however, 17.4% of users are highly satisfied with the services provided to them through mobile banking. This shows that users' satisfaction is tied to some factors such as their confidence in the bank protecting their privacy and data captured when performing any transaction using the mobile application.

Table 2.3: User Privacy

Items	Variables	Frequency	Percent
How concerned are you about security in mobile banking applications?	Very Concerned	117	58.2
	A little Concerned	46	23.4
	Somewhat Concerned	17	8.6
	Not at all Concerned	16	8.0
	I know that I should be concerned but I am not	4	2.0
	Total	**201**	**100.0**
Would you report a security break-in of your personal data to your bank	Yes	172	85.6
	No	9	4.5
	Not Likely	2	1.0
	Maybe	17	8.5
	I don't care	1	0.5
	Total	**201**	**100.0**
Indicate which of the following statement(s) you are in agreement with.	Bank should do more to improve the privacy of their mobile banking services	89	44.3
	Banks should be held responsible when customers privacy is compromised	32	15.9
	The privacy protection put in place by banks are insufficient.	10	5.0
	There should be penalty for banks when customer privacy is compromised	34	16.9
	There should be stricter laws to protect privacy online	36	17.9
	Total	**201**	**100.0**
Which is more important to you: CONVENIENCE or PRIVACY	Both	92	45.8
	Convince	29	14.4
	Privacy	74	36.8
	None	2	1.0
	Others	4	2.0
	Total	**201**	**100.0**
Kindly rate the following reasons enlisted for not using Mobile banking services	Hidden Cost	28	13.9
	Insecurity	74	36.8
	lack of knowledge on how to use it	37	18.4
	No access to Internet	48	23.9
	No need, I am satisfied with traditional banking	14	7.0
	Total	**201**	**100.0**
What privacy issue are you concerned about with mobile banking	Exposure of my credit card account details	32	15.9
	Hacking of personal data by cyber criminals	89	44.3
	None	19	9.5
	Sharing of my personal data with third parties without my consent	21	10.4
	Unauthorized access to personal information	40	19.9
	Total	**201**	**100**

Table 2.3 presents respondents' concern over the security of their mobile banking app as 58.2% (117) of the users state that they are very concerned with the security of the application. It is therefore certain that banks need to do more to build up the confidence of users. Privacy security is a key issue when it comes to the adoption of mobile banking solutions as security bridges have been observed to be on the increase in recent times, especially in mobile phones. 44.3% of the respondents are of the opinion that banks

should do more to improve the issue of privacy on the mobile banking application solution. This concern by respondents is built from the fact that most mobile banking applications have sections that app Poorly coded or have incorrect design security during development. 36.8 % of respondents identify insecurity while 23.9% state that internet access is one of the reasons, they will not use mobile banking solutions and can be to the fact that most rural areas and few urban cities in Nigeria are still not connected to the internet and the perception of some of the respondents on the security of the cyberspace is yet another reason. 44.3% feel that the privacy protection on these applications is not reliable enough and so the concern over their personal data being hacked by cybercriminals online will make them not consider using mobile banking applications.

Table 2.4: User Data Protection

Items	Variables	Frequency	Percent
Are you concerned with data security when using mobile banking	No, I trust in my bank services	30	14.9
	No, it is unlikely for a security breach to happen	10	5.0
	No, not at all	4	2.0
	Yes, but I use it anyway	124	61.7
	Yes, that is the main reason that I don't use it	33	16.4
	Total	**201**	**100.0**
Are you concerned about your data that is being captured when performing a transaction via mobile banking app	Certainly	6	3.0
	Most Likely	8	4.0
	No	37	18.4
	Not at all	5	2.5
	Sometimes	22	10.9
	Yes	123	61.2
	Total	**201**	**100.0**
Have you ever had your banking credentials stolen (such as PIN, Password & BVN)	I can't recall anytime	5	2.5
	No	164	81.6
	Once	2	1.0
	Yes	26	12.9
	Others	4	2.0
	Total	**201**	**100.0**
In your opinion, does sharing your mobile banking credentials with close friends a security risk	I don't think so	6	3.0
	May be	23	11.5
	Never thought of it as a risk	1	0.5
	Not at all	3	1.5
	Yes, it is a risk	167	83.1
	Total	**201**	**100.0**

In your opinion, what information ought to be collected when using your mobile banking application to transact a payment.	All your banking credentials	17	8.5
	I can't say	29	14.5
	Your Account Number and Biometrics (Finger print/Iris)	59	29.4
	Your BVN and E-mail only	24	11.9
	Your Password and Account Number only	72	35.8
	Total	**201**	**100.0**
How confident are you in your bank in protecting your data during and after any mobile banking transaction?	A little confident	65	32.3
	Am not sure	16	8.0
	Highly confident	8	4.0
	Not too confident	42	20.9
	Very confident	70	34.8
	Total	**201**	**100.0**

Though 61.7% of respondents are concerned with data security and 61.2% of respondents agreed to be worried about the captured data by these mobile banking applications at the point of transaction, this growing concern has not stopped the user from using the services as this can be attributed to the user-friendliness of some of the application and the ease of use and all-time availability. To most users this enough reason for them to keep using the mobile services even if there is risk involved. 83.1% agreed that sharing their banking credentials with others is a security risk and while the cases of stolen banking credentials may not be high among the respondent, this dose does not translate to users having high confidence on the mobile banking services as captured from the sample survey table 2.4 where only 34.8% (70) of the respondents say they are very confident with the protection provided by their banks in safeguarding their data (credentials). 35.8% of respondents are of the opinion that their password and account number should be the only credentials that their bank mobile application should request and be able to store when performing a transaction even though this is already an option in some of the existing banks, but the period of time these credentials are held in the cache on the mobile phones might be long enough for hackers to crawl them before they are been erased.

Table 2.5: Delegation of Access Right

Items	Variables	Frequency	Percent
Do you do think there is danger with delegating access right to anyone to carry out a mobile banking transaction on your behalf	I have never thought about it	5	2.5
	Maybe	32	15.9
	No, i don't	23	11.4
	Not really	9	4.5
	Yes, it has great danger	132	65.7
	Total	**201**	**100.0**
To whom would you most likely delegate your access right, to perform a transaction on your behalf	A Spouse	75	37.3
	Close friend	9	4.5
	Family member	105	52.2
	Others	4	2.0

	Relation	8	4.0
	Total	201	100.0
Have you ever experienced any breach of trust from someone you provided with your banking credentials to help perform a mobile banking transaction	Never	27	13.4
	No, not at all	108	53.7
	None, I can remember	18	9.0
	Yes, more than once	23	11.4
	Yes, once	25	12.4
	Total	201	100.0
What criteria would you consider before delegating access right to someone? (e.g handing over ATM card, banking credentials, etc.).	Familiarity	9	4.5
	Others	2	1.0
	Past Experience	7	3.5
	Relationship	44	21.9
	Trust	139	69.2
Do you consider delegation of access right to a third party as a serious security issue	Maybe	39	19.4
	Most likely	17	8.5
	Never thought of it	9	4.5
	No	34	16.9
	Yes	102	50.7
	Total	201	100.0
Which of these would you most likely share with your close associate or trusted friends?	Account Number and Password	49	24.4
	Both Account Password and Bank Verification Number (BVN)	3	1.5
	None	97	48.3
	Phone Password/Personal Identification Number (PIN)	45	22.4
	Your Bank Verification Number (BVN)	7	3.5
	Total	201	100.0

The perception of users towards delegation of access right to a third party is relatively high as 65.7% view delegation of access to be highly risky and 52.2% affirm their family member will be the most likely people they will delegate their access right to and their decision is based on trust which they believe their family members would not breach as seen in Table 2.5. However, trust as a determinant for delegation of access right has been observed to be risky because over time it has been reported that most cases of security breach recorded has been traced to those who the users once trusted with their account credentials.

Table 2.6: Application/Device Security

Items	Variables	Frequency	Percent
Which Type of Operating System does your mobile phone use	Android	168	83.6
	I don't know	8	4.0
	iOS	20	10.0
	Others	3	1.5
	Windows	2	1.0
	Total	**201**	**100.0**
How often do you update your mobile banking apps	I don't know how to use it	4	2.0
	No at all	19	9.5
	Not often	47	23.4
	Rarely	56	27.9
	Very often	75	37.3
	Total	**201**	**100.0**
Which of the following actions should be taken in order to increase mobile banking security?	I can't tell	48	23.9
	Use Antivirus	15	7.5
	Use Trusted application	64	31.9
	Use Trusted Networks	44	21.9
	Use Trusted website	30	14.9
	Total	**201**	**100.0**
For mobile banking application usage, please indicate how safe you think they are in terms of security:	High-level Security	42	20.9
	Low-level Security	24	11.9
	Medium-level Security	111	55.2
	None	2	1.0
	Not sure	22	10.9
	Total	**201**	**100.0**
What is the top most reason you are dissatisfied with in mobile banking experience	Am concerned about my personal information being disclosed as a result of mobile banking	85	42.3
	Applications for mobile banking are too complicated to use	18	9.0
	Banking on my mobile phone takes too long	9	4.5
	I am actually satisfied with mobile banking	64	31.8
	I have had problems getting the applications to work properly	25	12.4
	Total	**201**	**100.0**
What measure do you take to protect your device(s) and the data stored in them	Add extra security features such as device location and deactivation app	16	8.0
	Maintain the default security settings on my device	5	2.5
	Use a very strong password and PIN	92	45.8
	Use an easy to remember password/PIN and backup my data in an external location	10	5.0
	Use biometric (fingerprint/Iris) to secure my device and pattern recognition	78	38.8
	Total	**201**	**100.0**

Form Table 2.6 Mobile phone running on the Android Operating system is the most popular among mobile phone users in Nigeria that is because of their user-friendly interface, ease of use, and low cost. 83.6% of respondents use mobile phones run on android OS (Operating System). Mobile devices running on Android have been observed to be prone to attacks, especially those running on a lower version of the Android OS. Unlike mobile devices running the Apple Operating System (iOS) that has more security

features, Android OS has been identified with the following security issues; it has a greater potential risk for application-level security due to the extensive and open nature of the SDK while Apple's iOS model provides out of the box security because Apple has total control over their device. Another problem the survey identified is the percentage of those who do a regular update of their mobile phone OS. Both Android and Apple do regularly provide updates and newer versions for their devices with the aim of addressing issues of security but only 37.3% of respondents perform a regular update of their OS. When the version of OS on the mobile phone is too low it makes it easier for hackers to override the security of that mobile device. 31.9% believe that the use of the trusted application is another form of security measure and banks need to use the right channel to authenticate the credibility of the application that is released to users. Because there are a lot of fake mobile banking apps out there that are designed for the purpose of impersonating the official banking mobile apps. Banks need to add features that will make their application to make it difficult for a hacker to replicate and also feature that will make their official apps easier for customers to identify. 55.2% of respondents believe that the security level of mobile banking apps at it best is at a medium level which means there still see gaps in the area of safety of mobile devices in general and specifically in mobile banking applications.

Key Findings:

The following are the key findings made from the research;

i. There is an appreciable level of awareness among users of mobile banking application service solutions provided by their banks (94.4%) are aware that their banks provide these services but only 14.4% of users view security as a factor that will influence their choice of using mobile banking service and this is because most of the users are not properly aware or informed on why they should be more concerned with security more than ease of use and convenience.

ii. The findings from the empirical study show more users are likely to delegate their access rights to their family member or spouse on the bases of TRUST even though they admitted to the fact that it is a risk. Delegation of access rights will continue to be an issue that users need to be educated on. The finding showed that though 50.7% admitted that delegation of access is a risky thing, 65.7% said they will delegate their access right to at least a family member based on trust.

iii. The result shows that 58.2% of the respondents admitted that they are very concerned when it comes to the issue of security of their mobile banking app and while 61.2% are concerned about their data. Therefore, 44.3% will want their banks to do more to improve on the privacy issues. Most users (55.2%) believe that the safety level of the mobile banking application is at a medium level.

iv. Users believe the current authentication and authorization process put in place should be further hardened to help keep their banking credentials safe which in turn will increase their confidence. 45.8% of respondents believe that stronger passwords and PINs should be enforced to further strengthen the authentication process by the banks.

v. When it comes to the security measures to adopt in protecting their devices, users' awareness of the best practice is at a low level.

CONCLUSION AND RECOMMENDATION

Judging from the evidence provided by the study, it is clear that users' security awareness which is only about 14.4% needs to be heightened and where possible integrated into the mobile banking application as this will increase the confidentiality and integrity of the mobile banking application solutions and their usage. It is apparent that the existing security measures in most mobile banking applications are not clearly understood by customers and this has led to a growing concern among mobile bank application users as 44.3% admitted that they would prefer their banks do more to improve the privacy issues. Creating proper awareness of security issues that affect the privacy, Data, and device of bank customers through the same mobile application will help to change their attitude towards their safety. Banks need to consider integrating new features that will mitigate the issues that arise from Access delegation. Even though almost all the banking application has provided the options for users to reset their passwords, most customers might be reluctant in doing so except if they experience a bridge. Therefore, these banking applications should be designed to mandate users to change their password after a specified period which will be a good way of helping users take responsibility for protecting their banking credentials.

References

Abayomi, G. O. (2021, November). Assessment of Security Awareness Level of Mobile Device Users in Tertiary Institutions in Plateau State of Nigeria. Journal of Advanced Computing Technology and Application (JACTA), 3, 1-8. Retrieved April 25, 2022

Ahonen, P. a. (2006). A Design theory for Information Security. Oulu, Finland: Faculty of Science, Department of Information Processing Science, University of Oulu, P.O.Box 3000, FI-90014 University of Oulu, Finland .

GSMA. (2019). Mobile Phone Penetration in Sub-Saharan Africa.

Kearney, H. K. (2006, February 6). A Prototype for Assessing Information Security Awareness. Science Direct. Retrieved April 25, 2022, from www.sciencedirect.com

Laukkanen, T. (2007, November). Internet vs mobile banking: Comparing customer value perceptions. Business Process Management Journal (13), 78-79. doi:DOI: 10.1108/14637150710834550

Kurlyk, B. R. (2020). Security and Privacy Awareness in Smart Environments: A cross country investigation. Springer International Journal, 84-101.

Mazurczyk, P. L. (2018). User Perspective and Security of a New mobile authentication method. Journal of Telecommunication System, 365-379. doi:https://doi.org/10.1007/s11235-018-0437-1

Muhammad. (2015). CBN warns against scammers as BVN registration ends today. Retrieved 11 2, 2020, from http://www.dailytrust.com.ng/news/general/cbn-warns-against-scammers-as-bvn-registration-ends-today/117236.html: http://www.dailytrust.com.ng/news/general/cbn-warns-against-scammers-as-bvn-registration-ends-today/117236.html

Peer, S. E. (2015). Predicting privacy and security attitudes. ACM SIGCAS Computers and Society, 45. doi:10.1145/2738210.2738215

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. Communication Research, 40(2), 215–236. https://doi.org/10.1177/0093650211418338

Schurig, P. a. (2004). Assessment of Today's Mobile Banking Applications from the View of Customer Requirements. Published in the Proceedings of the Hawai'i International Conference on System Sciences. Big Island, Hawaii.

Susanto, H. (2021). Awareness, Revealing Cyber Threat of Smart mobile device withing digital Ecosystem: User information security. InTechOpen, 1-26.

Voudouris, K. (2010). The European Networks and Information Security Agency – ENISA.

O. Omorogiuwa and S.C. Chiemeke , (2008). Critical Factors Affecting the Usability of Igbinedion University Online Portal System. Asian Journal of Information Technology, 7: 109-116.