Usability and Security Factors in Mobile Financial Services and Their Impact on End-User Trust

Stephen Ambore[1], Edward Apeh[1], Huseyin Dogan[1]

[1] Department of Computing and Informatics
Faculty of Science and Technology
Bournemouth University, Talbot Campus
Fern Barrow, Poole BH12 5BB, UK
{sambore, eapeh, hdogan}@bournemouth.ac.uk

Abstract. Delivering financial services on mobile phones has gained traction in recent years due to the pervasiveness of mobile phones and the cost-effectiveness of Mobile Financial Services (MFS). However, the dark side of this development is that incidents of cybercrime perpetuated via MFS are growing and has affected end-user trust in the use of MFS. Usable security in MFS is a major concern leading to this lack of trust. While previous research has advocated focusing on a trade-off between usability and security as a means of improving usable security, others have focused on factors central to both usability and security as a means of addressing the trade-off. To understand the factors affecting usability and security in the use of MFS and their impact on end-user trust, 698 MFS users were surveyed. We then ran a Principal Component Analysis (PCA) on the data and identified six observable and four latent variables that are central to both usability and security in MFS. Furthermore, a Confirmatory Factor Analysis (CFA) was conducted to determine the model fit. Finally, a Structural Equation Model (SEM) was developed to show the impact of these variables on trust. The outcome of this extended paper proposes practical elements that would strengthen usable security in MFS.

Keywords. Trust, Usable Security, Usability, Cognition, Security, Mobile Financial Services, Socio-Technical Systems, Human Factors, Cybersecurity.

Paper Highlights

- The mobile phone is the new frontier for financial services, but lack of trust due to cybersecurity concerns chief of which is usable security is slowing down adoption.
- Understanding how customers use the product can provide relevant insights that would facilitate the development of MFS systems that are highly secure and usable.
- This study revealed that observable and latent variables exist that impact usability and security and that these factors have an impact on the trustworthiness of the system.

1 Introduction

The number of unique mobile phone subscribers globally grew to 5 billion in 2017 and is estimated to reach 5.9 billion by 2025, which is about 71% of the world's population. Over 57% of connected mobile phones are smartphones. It is estimated that by 2025, that 77% of connected mobile phones will be smartphones (GSMA, 2018). The increasing availability of better cellular capability like the 4th Generation (4G) and 5th Generation (5G) technology (GSMA, 2018) and the sizeable unique subscriber base of mobile phones have made the mobile phone a crucial tool in providing the end-user solution on a massive scale.

In the recently published World Bank Global Findex 2017, Asli et al. (2018) estimated the number of adults without access to formal financial services, that is, the unbanked, at 1.7 billion globally. Mobile Financial Services (MFS) is being used as a tool to reach the unbanked with relevant financial services. Also, smartphone capabilities now enable the development of a robust mobile application for financial services making banks to increasingly use the mobile phone as an alternative banking channel allowing them to reach a new market segment in a cost-effective manner.

In spite of the exciting prospects of the mobile phone as the new frontier for financial services delivery, cybersecurity concerns in MFS have increased over the years, raising trust concerns that are slowing down the adoption of MFS. Only recently, Indian banks warned its customers of a malware that affected over 200 mobile banking applications (Shetty, 2018). Similarly, researchers in the UK discovered vulnerabilities in MFS offered by some banks in the UK (Stone et al., 2017). In the same vein, researchers in the US found that 47 MFS solution in 28 countries had weak security controls (Reaves et al., 2015). Improving usable security in an end-user solution like MFS will facilitate good end-user security practices and minimise the impact of the cybersecurity concerns in the use of MFS.

The papers by Stone et al. (2017) and Reaves et al., (2015) exposed the magnitude and spread of vulnerabilities in MFS and the weakness of existing technical security controls in addressing these vulnerabilities. These studies did not explore the impact of the usability of MFS on the identified gaps. However, other researchers have conducted research that identified usability related attributes and their effect on MFS adoption. For instance, Lee et al., (2012) identified perceived usefulness and perceived ease of use as factors that affect the intention to use MFS. Furthermore, Chemingui and Ben lallouna, (2013), surveyed 300 non-users of MFS to identify amongst other things, the impact of trust on the intention to use MFS. The research determined that system quality has a high positive impact on trust.

These papers though valuable in understanding the threat landscape and providing an understanding of some factors that drive end-user adoption of MFS, focused more on usability attributes of MFS like the ease of use and usefulness. In other to have a more circumspect view of the impact of usability on adoption of MFS, it is imperative to understand the end-user perspective of usability and security in MFS, as these factors affect each other.

This paper will contribute to existing literature on MFS by examining the factors that affect usability and security from the end-user perspective and their impact on trust in the use of MFS. It will provide MFS designers and decision makers with information on factors to consider when considering a trade-off between usability and security during MFS solution design. This will further improve MFS security and mitigate the risk of cyber-attacks that might lead to financial loss to end-users, most of whom were unwittingly exposed to the risk of the cyberspace via MFS. Section 2 of this study examines the related literature on the subject matter, while section 3 describes the methodology adopted for the study. Section 4 presents the findings from the study. The paper concludes in section 6 after discussing the results of the study in section 5.

2 Related Work

The end-user has been described as the "weakest link" in the security value chain because of their propensity to make errors or poor security decisions in the use of a system (Sasse et al., 2001). Irrespective of the security controls put in place, the action or inaction of end-users can make a system susceptible to cyber-attacks. Analysing the psychological perceptions on why users make unsafe security decisions, West et al., (2009) posited that errors by end-users in the use of a system, and not sufficiently addressing human factor considerations during design are major contributors to cybersecurity risks. While investment in technical controls would help mitigate the risk of cybercrime, mitigating the vulnerability associated with the "weakest link" is imperative to build security controls that do not discourage good use practice and further jeopardise security objectives.

To address the usability gap, various usability models have also been developed. For instance, Harrison et al., (2013) proposed a usability model that considered the unique characteristics of mobile devices. Moreover, how usability is designed in relation to security is also essential. While both usability and security are crucial, the way they are built into a system determines whether the implemented controls would meet the intended objective. To buttress to this argument, using the analogy of user authentication, Ferreira et al., (2009) posited that without a password, a system is more usable, and conversely, an authentication mechanism that frequently requests revalidation while highly secure might be less usable.

Furthermore, various approaches have been proposed on how to design systems that are both highly secure and usable. In a study by Bai et al., (2017) on balancing usability and security in the use of encrypted emails explained that encryption was challenging to use because of poor interface design and difficulty in key management. Furthermore, the paper reported the finding of a study that gauged participants understanding and how they valued usability and security trade-off in email encryption. Factors like privacy, ease of use and trust were observed to influence usability and security trade-off decisions. Also, Cranor and Buchler (2014) advocated considering usability and security together during the design. They opined that the end-user decision-making process does affect the balance between usability and security. They placed the onus

on system designers to actively consider which decision requirements are assigned to end-users.

In a bid to improve usability while minimising threat scenarios, a study to analyse factors affecting both security and usability together was conducted (Kainda et al., 2010). The study introduced the concept of usability scenario to examine factors that might improve usage and threat scenarios to investigate factors that might minimize risky security behaviour, the study developed a model that also considered system motivators and external motivators that might cause user to perform a threat scenario and de-motivators that might hinder users from performing a usability scenario. The usability and security research reviewed so far focus on traditional system settings and have no consideration for the mobile phone and MFS context. Hoehle and Venkatesh (2015), recognised the need for an instrument for mobile application usability. To address the gap, they conducted a study that conceptualised, developed, and validated a comprehensive construct for mobile application usability. However, the instrument developed by Hoehle and Venkatesh (2015) focused only on the usability of mobile application and not security. More so, MFS adoption literature focuses more on intention to use and perceived usefulness and does not adequately address usable security (Lee et al., 2012, Chemingui and Ben lallouna, 2013). These identified gaps in the literature and the need to ensure MFS is highly secure yet usable necessitates the need for an instrument for MFS usability and security that will be applied to understand factors that affect both usability and security in MFS.

Drawing from these studies, 698 MFS users were surveyed intending to understanding factors that affect usability and security in the use of MFS, and how these factors affect end-user trust in MFS.

3 Methodology

To achieve the objective of the research, appropriate survey tools and methodologies were applied as described in this section.

.

3.1 Survey Design and Administration

We developed a survey questionnaire based on literature review and distributed the questionnaires through electronic means and paper-based. Survey questions were designed based on variables identified from the literature review in section II, including usability security constructs from Kainda et al., 2010 and usability and security constructs from Hoehle and Venkatesh (2015), and a review of MFS threat landscape. A pilot was conducted through two focus groups for both the electronic and paper-based version to test the survey logic and average completion time. The electronic questionnaire was designed using Bristol Online Survey (BOS), and the survey link was sent to the target audience via email, and social media platform, predominantly Facebook and WhatsApp, while the paper-based questionnaires were distributed to a wide range of participants by hand. The survey was segmented into nine sections for ease of administration (see Appendix). The investigation targeted MFS users.

Using the number of unique bank accounts in Nigeria, the total survey population was 31 million. Based on Cochran's formulas, a population sample size of 385 was required to achieve a confidence level of 95% and an error margin of 5%. However, a total of 698 were completed/submitted. The survey ran for two months, during which 328 electronic studies were submitted, and 370 paper-based surveys were also completed. The survey was designed in such a way that non-MFS users were asked two questions before permitted them to exit the study. They were asked why they do not currently use MFS and what change would be necessary for them to consider using MFS in the future. Feedback from 29 non-users was obtained. Furthermore, 53 paper-based returned questionnaires had a large number of question unanswered. However, since only 385 was required, the outstanding 616 survey feedback was sufficient for the analysis. This number is the total number of completed surveys (698) less feedback from non-users (29) and less (58) returned paper-based surveys with a significant number of questions unanswered.

3.2 Survey Analysis

The paper-based survey feedback was inputted to BOS where the electronic version was saved. The entire data was then exported to SPSS 22 for further analysis. Data cleansing was conducted before the commencement of data analysis.

To answer the research question, it was imperative to use methodologies that would identify the observable and latent construct from the data. To that end, Principal Component Analysis (PCA) an exploratory multivariate analysis technique which seeks to describe the underlying structure in a data matrix, according to Abdi and Williams (2010), was used as it can provide the insight from the data that will address the research question. The Factor Analysis module in SPSS was used to conduct the PCA on a set of transformed variables obtained from the survey data. SPSS was used to transform the data. In the transformation, variables that sought to analyse the same factors were re-coded into a new compound variable. The re-coding of variables were both based on ideas from the literature and inductive reasoning. PCA was then conducted on the recoded variable. The re-coded variables are as described in table 1.0.

Table 1. Re-coded variables

#	Code	Description	Code Abbreviation
1	Complexity of System	Measures user perception of complexity of MFS and its security mechanism	CS
2	Awareness of privacy	Measures awareness of privacy in use behaviour of MFS.	AP
3	End-user patching	Measures user behaviour in maintaining critical updates for MFS, mobile phone antivirus and underlying mobile phone Operating System	EP
4	Usability	Measures user perception of usability of MFS	U

#	Code	Description	Code Abbreviation
5	Security	Measures user perception of security of MFS	S
6	Environmental Impact	Measures impact of sounding factors e.g. distraction from incoming calls, strength of network signal on usable security of MFS	EI

The code name in the 4th column was done for the convenience of analysis. These codes will be used to refer to these variables in the rest of this paper.

To test the model fit and to analyse the impact of the variables on Trust we ran a Confirmatory Factor Analysis (CFA) and a Structural Equation Model (SEM) using AMOS 24. AMOS was chosen above SPSS in conducting CFA and SEM as it provides graphic description and details not available in SPSS which only includes regression analysis details. To develop the SEM, 4 Likert scale questions were transformed using SPSS and re-coded as a new variable trust. The new variable included in the questionnaire to determine the level of user trust on MFS.

Descriptive statistics tools in SPSS was used to provide insight into other aspects of the survey data.

4 Results

Majority of the respondents were between the ages of 18 to 44 years. While 20.1% of the respondents were between the ages of 18 to 24 years, 35.6% were between 25 to 34 years of age. The largest group of responded (36.7%) were between 35 to 44 years of age. The rest of the respondents were between 45 to 60 years, and over 60 years. The population sample included only adult population; 18 years of age and above. Figure 1.0 below shows the pie chart of the age distribution.

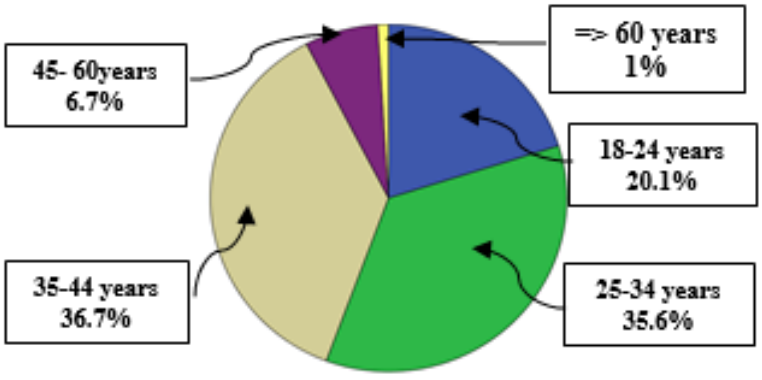

Fig. 1. Participants age distribution

42.7% of the participant have an undergraduate level degree, 32.5% have a postgraduate degree, 12.3% have a diploma. About 8.4% of the respondents possess a secondary school qualification while the rest have either primary school or had no formal education. Student, IT-related jobs, and Accountants were the occupations with the highest respondents amongst the 31 occupations that participated in the survey. The government sector had the largest respondents out of the 20 sectors. This tallies with the reality on the ground where the government is the highest employer of labour in the environment where the study was conducted.

Most of the participants use an Android-based phone. 17 participants use 2 or 3 phones to access their MFS. Mobile Banking (78.2%) is the MFS product most accessed by participants, with just about 5% using Mobile Money. 65% of the respondents have used MFS for over 12 months, 21.8% between 7 to 12 months while the others have used MFS for six months or less.

4.1 User Experience

Only about 13% of the respondents believe MFS was challenging to use, 20.8% of the respondents perform a single task several times due to the complexity of the MFS. 12.6% of the respondents believe the reason they need to complete the task more than once was lack of sufficient knowledge of how to use the system. 44.2% think MFS meets their needs and 18.3% believe MFS was secure. 26.6% of MFS users often experience errors in their transactions.

Older respondents (60 years and above) tend to recall their authentication credential more than younger respondents. 26.6% of respondents tend to forget their login credentials easily. A similar number of respondents (27%) write down their login credential on their phones to enhance easy recall.

Only 78 of the respondents (about 12%) have experienced unauthorised access to their MFS accounts. Out of these group of respondents, 69% share their phones with their acquittances and out of the 88% that have not experienced unauthorised access to their MFS 62% also share their phones with their acquittances. The group of respondents that have experienced unauthorised access to their MFS were overwhelmingly (86%) satisfied with the control put in place to mitigate unauthorised access to their MFS solutions.

4.2 Principal Component Analysis

A PCA correlation matrix between component shows the relationship of these factors against each other. The complexity of the system (CS) loads inversely on Awareness of Privacy (AP) at -.376. This implies the perception of the user on the complexity of MFS and its security control correlates inversely with user awareness of privacy in the use of MFS. CS also loads inversely on all factors except End-User Patching (EP). CS

also loads inversely on Usability (U), Security(E) and Environment Impact (EI), while it loads positively on EP.

User attitude towards privacy (AP) in the use of MFS loads inversely on CS and EP with a correlation coefficient of -.376 and -.1 respectively. Finally, all factors except CS correlates to both U and S. None of the elements loaded inversely on U.

4.3 Latent Constructs

To determine the number of latent constructs, a scree plot was developed. The plot shows that the first three slopes were steep and the last two slopes did not show sufficient variation between the eigenvalue and number of components, and it implies the latent components that explain the difference lies within the first three slopes. The total number of points within the three slopes are 4. Consequently, we focus our analysis on these four latent components and the observable factors analysed in section 4.2. To further investigate the relationship between the observable and latent construct we generated a Pattern matrix. The first latent component of the matrix loads heavily on U(0.869) and S(0.841) but loads negatively on CS (-.388). The second component loads positively on EP and CS while the third component loads only on EI, while the last component loads heavily on AP and inversely on CS. While not all latent components load directly on usability and security, the correlation matrix has already shown that all the observable constructs load against each other, as such all latent component that has an impact on the observable constructs might have an indirect correlation with both usability and security.

4.4 Confirmatory Factor Analysis Model

The PCA Pattern matrix discussed in section 4.3 shows that four latent components load on at least one of the observable components. Three of these observable components (U, CS and EI) relate more to Usability while the other three (S, EP, AP) relates more to Security. Assuming Usability to be the latent component that loads on U, CS and EI and Security the latent component that loads on S, EP, and AP we ran a

CFA to test the fit of the model. Figure 2.0 shows the model obtained from the CFA.

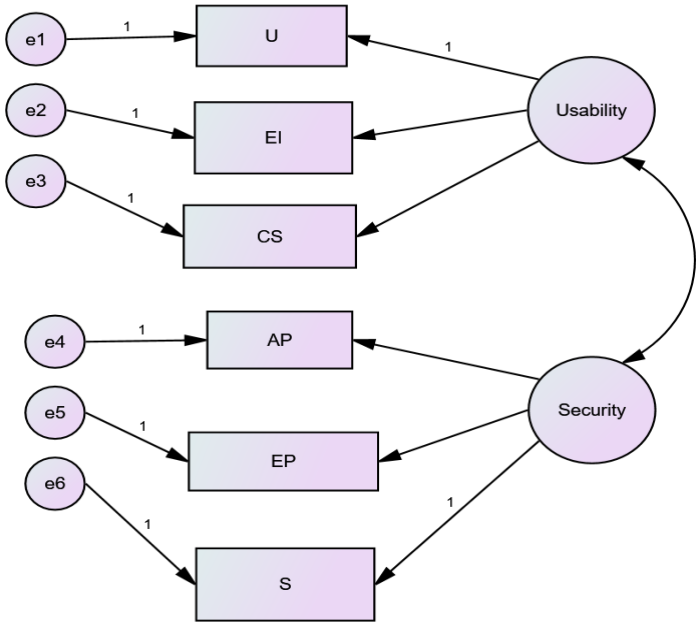

Fig. 2. CFA Model

The Maximum Likelihood Estimate (MLE) in table 2.0 shows that the influence of Usability is significant on Complexity of System (CS) with an estimate of -1.124 and on Environmental Impact (EI) with an estimate of 0.176. Furthermore, MLE shows that the influence of Security is significant on End-User Patching behaviour (EP) with an estimate of 1.234 and Awareness of Privacy (AP) with an estimate of 0.423.

Table 2. Maximum Likelihood Estimates for CFA

Factor	Reletionship	Latent Component	Estimate	S.E.	C.R.	P
CS	<---	Usability	-1.124	.173	-6.511	***
EI	<---	Usability	.176	.040	4.362	***
U	<---	Usability	1.000			
S	<---	Security	1.000			
EP	<---	Security	1.234	.203	6.085	***
AP	<---	Security	.423	.089	4.732	***

***Indicate a highly significance at < 0.001 S.E. = Standard Error and C.R. = Critical Ratio

The model fit indices are all within specifications, the values generally indicate a good fit as follows:

I. CMIN/DF (Relative chi-square) = 14.669 [dropped too many paths if >3]
II. GFI (Goodness of Fit Index) = 0.937 [Normal GFI range =< 1. A value of 1 indicates a perfect fit, ideal should exceed 0.9 for a good model]
III. NFI (Normal Fit Index) = 0.945 [above .95 are good]
IV. RFI (Relative Fit Index) = 0.895 [close to 1 indicate a very good fit]
V. IFI (incremental fit index) = 0.945 [close to 1 indicate a very good fit]
VI. TLI (Tucker-Lewis coefficient) = 0.903 [close to 1 indicate a very good fit]
VII. CFI (Comparative Fit Index) = 0.945 [close to 1 indicate a very good fit]
VIII. RMSEA (Root Mean Square Error Approximation) = 0.149 [ideal should be <0.5 for good fit]

4.5 Structural Equation Modeling

To analyse the impact of the variables in section 4.4 on trust, we developed a SEM linking the constructs with the cluster variable *trust*. The model shows the correlation of all observable factors to Usability and Security and their relationship to the trust construct in figure 3.0.

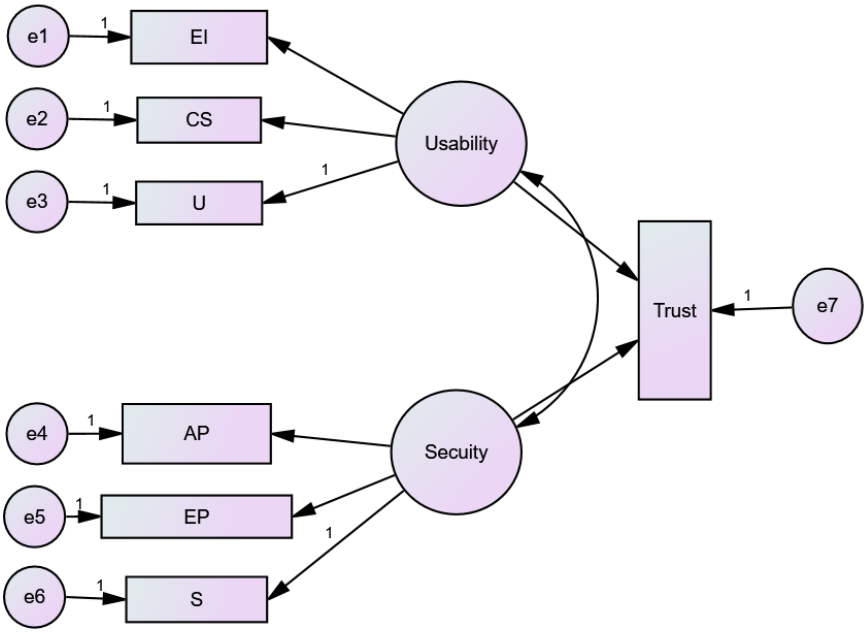

Fig. 3. SEM Model

MLE for the SEM model shows that though Usability and Security have a significant influence on trust, Security (0.263) has a much higher impact on trust when compared to Usability (0.055). The model also shows that Security load more on End-user Patching (0.785), the highest of any of the component. On the other hand, there is a significant inverse relationship between Usability and Complexity of System (-0.735). Table 3.0 shows the SEM MLE.

Table 3. Maximum Likelihood Estimates for SEM

Factor	Reletionship	Latent Component	Estimate	S.E.	C.R.	P
U	<---	Usability	1.000			
CS	<---	Usability	-.735	.121	-6.080	***
EI	<---	Usability	.112	.028	4.050	***
S	<---	Security	1.000			
EP	<---	Security	.785	.118	6.642	***
AP	<---	Security	.224	.054	4.114	***
Trust	<---	Usability	.055	.009	6.299	***
Trust	<---	Security	.263	.014	19.328	***

The SEM result shows that a good fit was achieved for the model, as follows:

I. CMIN/DF (Relative chi-square) = 11.763 [dropped too many paths if >3]
II. GFI (Goodness of Fit Index) = 0.938 [ideal should exceed 0.9 for a good model]
III. NFI = 0.940 [above .95 are good]
IV. RFI = 0.895 [close to 1 indicate a very good fit]
V. IFI = 0.945 [close to 1 indicate a very good fit]
VI. TLI = 0.903 [close to 1 indicate a very good fit]
VII. CFI = 0.945 [close to 1 indicate a very good fit]
VIII. RMSEA (Root Mean Square Error Approximation) = 0.132 [ideal should be <0.5 for good fit]
IX. RMR = 1.565 [For comparison smaller is better]

5 Discussion

Though various work has been undertaken on ensuring the right balance between usability and security, none of the existing studies was conducted in the context of MFS. Because the mobile phone is now the new frontier for MFS that will unwittingly add new users to the cyberspace, it is imperative to ensure that the product is highly secure yet usable. Drawing from usable security, MFS threat landscape and mobile phone usability literature, this study developed a questionnaire that was used to obtain usage data from 698 users. To identify the observable and latent factor, a PCA was conducted. The investigation revealed that six components; Usability(U), Security(S), Complexity of system and security mechanism (CS), Environmental Impact (EI), End-User Patching behaviour (EP) and Awareness of Privacy (AP) are observable variables

that are central to both usability and security in MFS. Also, the study identified four latent components that affect usability and security in MFS. To analyse the model fit and analyse the impact of the six component on the trustworthiness of the system we conducted a CFA and an SME The result showed that both usability and security have an impact on end-user trust, with security having a higher effect than usability. When considering a trade-off between usability and security, it should be noted that the influence of security on end-user trust is much higher than that which usability has on end-user trust.

6 Conclusion and Future Work

Though user adoption of MFS has been slow due to trust, the need to reduce operational cost by Banks might unwittingly add new users to the cyberspace via MFS. It is therefore imperative to provide an instrument that will help MFS developers have a better understanding of factors that can improve usable security, improve trust and consequently safe adoption of MFS. This research has shown that MFS users prefer a more secure system to one that is easy to use. The research has identified factors that need to be addressed in order to ensure the right balance between usability and security in MFS. The study has also developed a questionnaire that can be adapted by other researchers to explore usable security factors in other mobile solutions. This research is an initial effort to conceptualising a framework specifically for the context of MFS that will help MFS developers and other ecosystem actors focus on understanding factors central to usability and security and how best to address them instead of depending.

We adopted a cross-sectional time horizon for this research, as such were limited to collecting survey data. Future studies can consider a longitudinal approach that will help observe user behaviour over time, and it might reveal more insight that will further strengthen usable security in MFS. This study was also conducted in the context of MFS users in Nigeria. Future studies should consider other jurisdiction as environmental factors might be slightly different for various countries.

7 References

Cummings, J. N., Butler, B., & Kraut, R. (2002). The quality of online social relationships. *Communications of the ACM, 45*(7), 103-108.

Hu, Y., Wood, J. F., Smith, V., & Westbrook, N. (2004). Friendships through IM: Examining the relationship between instant messaging and intimacy. *Journal of Computer-Mediated Communication*, *10*(1), 38-48.

Abdi, H. and Williams, L.J., (2010). Principal component analysis. Wiley interdisciplinary reviews: computational statistics, 2(4), pp.433-459.

Asli, D., Klapper, L., Singer D., Ansar, S. and Hess, J, (2018), The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Washington, DC: World Bank. doi:10.1596/978-1-4648-1259-0. License: Creative Commons Attribution CC BY 3.0 IGO.

Bai, W., Kim, D. Namara, M., Qian, Y., Kelley, P., and Mazurek, M. (2017). "Balancing Security and Usability in Encrypted Email", IEEE Computer Society.

Chemingui, H. and Ben lallouna, H. (2013). Resistance, motivations, trust and intention to use mobile financial services. International Journal of Bank Marketing, 31(7), pp.574-592.

Cranor, L.F. and Buchler, N., (2014), Better together: Usability and security go hand in hand. IEEE Security & Privacy, 12(6), pp.89-93.

GSMA, (2018), The Mobile Economy 2018, Retrieved May 13, 2018, from GSMA Web site: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf.

Ferreira, A. Rusu C. and Roncagliolo, S. (2009). "Usability and security patterns". In Advances in Computer-Human Interactions. ACHI'09. Second International Conferences on (pp. 301-305). IEEE.

Harrison, R., Flood, D. and Duce, D., (2013). Usability of mobile applications: literature review and rationale for a new usability model. Journal of Interaction Science, 1(1), p.1.

Hoehle, H. and Venkatesh, V. (2015) Mobile Application Usability: Conceptualization and Instrument Development. MIS Quarterly Vol. 39 No. 2, pp. 435-472.

Kainda, R., Flechais, I. and Roscoe, A.W. (2010). "Security and usability: Analysis and evaluation". In Availability, Reliability, and Security. ARES'10 International Conference on (pp. 275-282). IEEE.

Lee, Y.K., Park, J.H., Chung, N. and Blakeney, A., (2012). A unified perspective on the factors influencing usage intention toward mobile financial services. Journal of Business Research, 65(11), pp.1590-1599.

Reaves, B. Scaife, N., Bates, A.M., Traynor P., and Butler, K.R., (2015) "Mo (bile) money, mo(bile) problems: analysis of branchless banking applications in the developing world". In USENIX Security Symposium (pp. 17-32).

Sasse, M.A, Brostoff, S. and Weirich, D. (2001), "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security". BT technology journal, 19(3), pp.122-131

Shetty M., (2018), Banks warn of new mobile malware, 232 banking apps in danger. Retrieved May 12, 2018, from Times of India Web site: https://timesofindia.indiatimes.com/business/india-business/banks-warn-of-new-mobile-malware/articleshow/62436145.cms.

Stone, C.M, Chothia, T. and Garcia, F.D., (2017), Spinner: "Semi-automatic detection of pinning without hostname verification". In Proceedings of the 33rd Annual Computer Security Applications Conference (pp. 176-188). ACM.

West, R., Mayhorn, C., Hardee, J. and Mendel, J., (2009). The Weakest Link: A Psychological Perspective on Why. Users Make Poor Security Decisions.

Appendix

Section 1: Participants Details	
Age Range	a. ☐ 18-24 b. ☐ 25-34 c. ☐ 35-44 d. ☐ 45-60 e. ☐ 61 and above
Highest Qualification	a. ☐ Primary School Certificate b. ☐ Secondary School Certificate c. ☐ Diploma Holder d. ☐ 1st Degree (Bsc., Btech. HND. etc.) e. ☐ Postgraduate Degree (PGD, Msc., PhD.) f. ☐ Others (Please Specify)
Occupation	
Sector	
Average Monthly income	a. ☐ ≤ ₦ 20,000 b. ☐ ₦ 21,000 – ₦ 50,000 c. ☐ ₦ 51,000 - ₦ 100,000 d. ☐ ₦ 101,000 - ₦ 250,000 e. ☐ ₦ 251,000 - ₦ 500,000 f. ☐ ≥ ₦ 501,000
Section 2: Product type and means of use	
1. I use this phone type? a. ☐ iPhone b. ☐ Samsung c. ☐ Blackberry d. ☐ HTC e. ☐ Others (please specify)	
2. I use this Mobile Financial Services (MFS) product (select all that apply) a. ☐ Mobile Payment (e.g paga, Ezpay) b. ☐ Mobile Money (e.g teasy, readycash) c. ☐ Mobile Banking d. ☐ Others(please specify)	
3. I have been using MFS for a. ☐ ≤6 months b. ☐ 7-12 months c. ☐ ≥12 months and beyond	
4. My decision to use MFS was influenced by (select all that apply) a. ☐ lower cost of transaction compared to other means b. ☐ It is more convenient than going to the bank c. ☐ Ease of use d. ☐ I can use it anywhere and at anytime e. ☐ Others (please specify)	
5. I set up the MFS on my phone by a. ☐ Downloading from the apps store b. ☐ Installing via SDTK (SIM Development tool kit) c. ☐ Was done for me by service provider d. ☐ I am not sure e. ☐ Others (please specify)	

6. I use this connectivity option to enable me access MFS on my phone
   a. ☐ Wi-Fi only
   b. ☐ Phone Data only
   c. ☐ Both Wi-Fi and phone data, but more of Wi-Fi
   d. ☐ Both Wi-Fi and phone data, but more of phone data
   e. ☐ Others(please specify)

7. I predominantly conduct a MFS transaction via (select all that apply)
   a. ☐ Contactless(scanning)
   b. ☐ USSD(SMS like payment instructions e.g. *776#)
   c. ☐ Mobile App (app installed on phone)
   d. ☐ Others (please specify)

8. I secure my MFS through the following means (select all that apply)
   a. ☐ Token
   b. ☐ PIN
   c. ☐ Biometry
   d. ☐ Others (explain)

Section 3: Experience

9. The MFS I use is
   a. ☐ Easy to navigate
   b. ☐ Complex
   c. ☐ Meets my needs
   d. ☐ Secure
   e. ☐ Others (please specify)

10. It is difficult for me to complete a task on the MFS I use
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

11. I often experience errors in my transactions
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

12. I often perform a single task several times due to the complexity of the MFS
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

13. I often perform a single task several times due to lack of sufficient knowledge
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

14. The most frustrating part of using the product for me is

		Strongly Agree	Agree	Neither Agree Nor Disagree	Disagree	Strongly Disagree
a	I frequently forget my PIN					
b	Poor Network					
c	Unsatisfactory level of support from operators					
d	How to navigate the system					
e	How to be sure I did the right thing with my transactions					
f	Others (please specify)					

15. My financial details has been accessed by unauthorised persons via my mobile phone
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

Section 3: Awareness

16. I share my phone with friends and family
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

17. I use the same PIN for my phone and MFS
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

18. I forget my MFS PIN
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

19. I write down my MFS PIN or secret questions somewhere in my phone so I don't forget
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

20. Please select the indicator that you agree with the most for each item in the table below

		Strongly Agree	Agree	Neither Agree Nor Disagree	Disagree	Strongly Disagree
a	PIN authentication is sufficient for me to access my MFS					
b	I would need an additional level of authentication to PIN, to improve my confidence in the security of my MFS					
c	My bank/operator responds speedily to any fraud related issues I raise to them					
d	I know what to do to ensure no one accesses my sensitive financial details in the event I lose my phone					
e	I know my responsibility as a mobile account owner					
f	I know the banks/operators responsibility for ensuring I use MFS securely					
g	I know how to escalate any issue to the banks/operators					

21. I can differentiate real Mobile apps from rouge ones
    a. ☐ Yes, my bank/MFS operator showed me how
    b. ☐ Yes, it is on the FAQ from my bank/Operator
    c. ☐ Yes, due to my awareness of cybersecurity and Information Technology
    d. ☐ Yes, based on the website address
    e. ☐ Yes, based on source
    f. ☐ Yes, based on look and feel

g. ☐ No, I cannot differentiate
h. ☐ Others (Please explain)

22. Please select the indicator that tallies the most with your knowledge level of the items in the table below

		None	Basic	Average	A bit above average	Advance	Expert
a	Ransomware						
b	Spyware						
c	Smishing (SMS phising)						
d	Mobile Malware						
e	Rogue applications						
f	Cybersecurity						
e	Data Privacy						

23. I received training/ sensitization on how to use MFS before I started using it
a. ☐ yes
b. ☐ No

23b. Training/Sensitization I received was sufficient
a. ☐ yes
b. ☐ No

24. I am aware that a procedure/process exists, to guide my action in the event I misplace my phone or suspicious transactions emanate from my phone
a. ☐ Strongly Agree
b. ☐ Agree
c. ☐ Neither Agree nor disagree
d. ☐ Disagree
e. ☐ Strongly Disagree

25. No one else has access to my MFS account
a. ☐ Strongly Agree
b. ☐ Agree
c. ☐ Neither Agree Nor disagree
d. ☐ Disagree
e. ☐ Strongly Disagree

Section4: Maintenance

26. I perform an upgrade of the Operating system I use for MFS
a. ☐ As soon as it is available
b. ☐ Never
c. ☐ Seldom
d. ☐ Always
e. ☐ It is done automatically by my service provider
f. ☐ I don't know

27. I perform an upgrade of the mobile application I use for MFS
    a. ☐ As soon as it is available
    b. ☐ Never
    c. ☐ Seldom
    d. ☐ Always
    e. ☐ It is done automatically by my service provider
    f. ☐ I don't know

28. The security of my MFS transaction depends on the update of my mobile phone operating system
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

29. The security of my MFS transaction depends on the update of the mobile phone application I use for MFS
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

30. I use a phone antivirus
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

31. I update my phone antivirus
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

Section5: Usability

32. I am satisfied with the reliability of the MFS
    a. ☐ Extremely satisfied
    b. ☐ Very satisfied
    c. ☐ Somewhat satisfied
    d. ☐ Not so satisfied
    e. ☐ Not at all satisfied

33. The MFS I use is easy to navigate
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

34. I am satisfied with the available help options
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

35. The MFS I use is visually appealing
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

Section6: Security

36. The financial transactions I conduct using MFS are protected from unauthorized disclosures
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

37. The financial transactions I conduct using MFS are accurate and consistent throughout their life-cycle
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

38. The MFS service I use is available and is at the required level of performance at all times
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

Section 7: Social Context

39. I prefer a secure transaction than an easy to use MFS system
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

40. I will prefer an easy to use MFS than an MFS that is too complex to use because of security controls
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

41. I prefer an MFS system that is easy to use, yet secure
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

42. I am distracted or prone to making errors when conducting MFS transactions on my phone because of (select all that apply)
    a. ☐ In coming phone calls during transactions
    b. ☐ Environment of use
    c. ☐ Low battery life
    d. ☐ Weak network strength or poor network connectivity
    e. ☐ Others (please specify)

43. The maximum daily transactions limit set by my bank/operator on my MFS is
    - ☐ Too restrictive, I want more with same level of security
    - ☐ Too restrictive I want more with increased level of security
    - ☐ Too restrictive, I want more with reduced level of security
    - ☐ Too relaxed, I want more with increased level of security
    - ☐ Just fine
    - ☐ Others (please explain)

Section 6: Additional Information