



ADDIS ABABA UNIVERSITY
SCHOOL OF INFORMATION SCIENCE
MASTER OF SCIENCE IN INFORMATION SCIENCE

**Customers' Perception towards Mobile Banking Security:
The Case of Commercial Bank of Ethiopia in Addis Ababa.**

By

Hailieeyesus Kindie Kebede

June, 2016

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY
SCHOOL OF INFORMATION SCIENCE
MASTER OF SCIENCE IN INFORMATION SCIENCE

**Customers' Perception towards Mobile Banking Security:
The Case of Commercial Bank of Ethiopia in Addis Ababa.**

**A thesis submitted to the school of graduate studies of Addis Ababa
University in partial fulfillment of the requirements for the degree
of Master of Science in information science**

By

Hailieeyesus Kindie Kebede

June, 2016

**Customers' Perception towards Mobile Banking Security:
The Case of Commercial Bank of Ethiopia in Addis Ababa.**

By

Hailieeyesus Kindie Kebede

Name and signature of members of the examining board

Name	Title	Signature	date
_____	Chairperson	_____	_____
_____	Advisor	_____	_____
_____	Examiner	_____	_____
_____	Examiner	_____	_____

ABSTRACT

Today, the advancement of mobile technologies has provided an opportunity for financial service providers in introducing new financial innovations. One of the emerging financial innovations introduced by financial service providers is mobile banking.

This research tries to look into the customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. There are a lot of literatures available on various online banking services like internet, ATM banking, on customer' behavior and also on mobile banking adoption. However, the literature on customers' perception on the mobile banking security aspect in case of Ethiopia is very limited on the contrary to other e-banking services, so this type of research plays a great importance in the area.

In recent research and studies it was found out that while mobile banking applications have become popular in many countries and regions, these are not still widely used as expected. The main barrier that may be cited here is the concern of security by the customers' towards using the system.

The study is based on the research model that weaves two theoretical grounds. The research model includes basic constructs from the protection motivation theory (PMT) and also the two important constructs from the technology acceptance model (TAM) to be integrated with the first theory. What is more here, two important constructs were selected from the trust topology, since the PMT has a risk concept (construct), which is neglected in adoption theories, and also risk and trust are important concepts that go together. This makes our framework more comprehensive.

A survey questionnaire was developed and employed to collect data from 170 customers. An interview was also conducted with the mobile and internet banking manager. Multi stage cluster sampling technique was used (random sampling to select the branches of the bank and convenient sampling to select respondents). Pretesting of the questionnaire was also done. The results of the data analysis contributes to the body of knowledge in the area by demonstrating that some factors such as perceived ease of use, trust belief ,self-efficacy, perceived risk, and perceived vulnerability are found to be strong factors affecting customers' perception towards mobile banking security and a motivation to take protection action. The study also revealed that it is possible to determine customers' perception towards mobile banking security by integrating constructs from different theoretical models. Although the study has its limitations, the implications of the results allow by providing practical recommendations to the banking industry, and directions for further work.

Key words: Mobile Banking, Protection Motivation (PMT), Technology Acceptance Model (TAM)

ACKNOWLEDGEMENT

First, I would like to thank the almighty God and his mother, the compassionate, the most merciful and sources of knowledge and wisdom, whom bestowed upon me the health, the power of communication and the audacity to accomplish this thesis.

I would like to sincerely thank my advisor **Dr. Workeshet Lamenew** for his constructive comments, valuable suggestions and good guidance.

I would also like to thank the staffs of all the ten branches of Commercial Bank of Ethiopia in Addis Ababa who participated in this study during the data collection process and also for the manager of internet and mobile banking, Ato Mintesinot Seyoum for his willingness for the interview.

Last but not the least, my appreciation also goes to those of my colleagues who helped me and also gave me valuable support and advice to complete my study.

Hailieeyesus Kindie

June, 2016

TABLE OF CONTENTS

Titles	pages
ABSTRACT.....	IV
ACKNOWLEDGEMENT.....	V
TABLE OF CONTENTS.....	VI
LIST OF TABLES.....	X
LIST OF FIGURES.....	XII
LIST OF ACRONYMS.....	XIII
CHAPTER ONE.....	1
1. INTRODUCTION.....	1
1.1. Background of the study.....	1
1.2. Statement of the problem.....	3
1.3. Research questions.....	5
1.4. Objectives of the study.....	5
1.4.1. General objective.....	5
1.4.2. Specific objectives.....	5
1.5. Scope of the study.....	6
1.6. Significance of the study.....	6
1.7. Structure of the Study.....	7
CHAPTER TWO.....	8
2. LITRATURE REVIEW.....	8
2.1. Introduction.....	8
2.2. Introduction to Mobile banking.....	8
2.3. Mobile banking in Ethiopia.....	10
2.4. Customers' perception towards mobile banking.....	15

2.4.1. Aspects of Risk and security.....	16
2.4.2. Aspects socio-economic background and culture.....	17
2.4.3. The characteristics of the service.....	17
2.4.4. The service and device costs.....	18
2.4.5. The mobile Device features.....	18
2.5. Different Models used for Customers' Perception on Mobile banking Adoption and online security.....	18
2.5.1. Theory of Reasoned Action (TRA).....	19
2.5.2. Technology Acceptance Model (TAM).....	20
2.5.3. Theory of Planned Behavior (TPB).....	20
2.5.4. Innovation Diffusion Theory (IDT).....	21
2.5.5. Unified Theory of Acceptance and Use of Technology Model (UTUAT) Model.....	22
2.5.6. Protection Motivation Theory (PMT).....	22
2.6. Related Works using different theoretical models.....	24
2.7. Summary of related researches.....	29
2.8. Theoretical framework(Protection Motivation Theory).....	33
2.8.1. The Protection Motivation Theory and its constructs.....	35
2.8.2. Threat appraisal.....	35
2.8.3. Coping appraisal.....	36
2.8.4. Protection motivation.....	37
2.9. Trust and perceived risk.....	37
2.8.1. Perceived risk and trust belief.....	38
2.8.2. Perceived risk and structural assurance.....	39
2.10. Perceived ease of use and perceived usefulness.....	39
2.11. The model.....	40
CHAPTER THREE.....	41

3. RESEARCH METHODOLOGY.....	41
3.1.Introduction.....	41
3.2.Overview of the methodology.....	41
3.3.Research purpose	42
3.4.Research Approach.....	43
3.4.1. Qualitative and Quantitative Approaches.....	43
3.4.2. Deductive and Inductive Approach.....	44
3.5.Research strategy	44
3.6.Types of research.....	45
3.7.Research Instruments	46
3.8.Pre-testing of the questionnaire	47
3.9.Sample and Data collection	47
3.10.Data Collection Procedure.....	49
3.10.1. The Bank customers.....	49
3.10.2. The bank workers.....	50
3.11.Methodological limitations	50
3.12.Data analysis tools and techniques	50
3.13.Research model and hypotheses	51
3.14.Related works and their methodologies.....	55
3.15.Quality of Research	59
3.15.1. Reliability of the Research.....	59
3.15.2. Validity of the Research.....	60
3.16.Conclusion.....	60
CHAPTER FOUR.....	61
4. DATA ANALYSIS AND RESULTS.....	61
4.1.Introduction.....	61
4.2.Research and Statistical Tools Employed.....	61
4.3.Analysis of the data.....	61
4.4.Respondents Demographic Characteristics	62
4.5.Customers' perception towards the theoretical model factors. (Analysis results from the yes/no questions).....	64
4.6.Reliability and Validity of the questionnaire items and the model factors...	74

4.6.1. Reliability	74
4.6.2. Validity.....	76
4.7.Hypotheses testing and discussion of results.....	76
4.8. Qualitative Data Analysis.....	86
4.9.Summary of the chapter.....	88
CHAPTER FIVE.....	89
5. SUMMARY, CONCLUSION AND RECOMMENDATION.....	89
5.1.Introduction.....	89
5.2.Summary of findings.....	89
5.3.Conclusion.....	94
5.4.Recommendation.....	95
5.5.Limitation and future research.....	97
REFERENCES.....	99
APPENDICES.....	107
Appendix 1 – Questionnaire.....	107
Appendix 2 – Semi-structured interview questions presented for the bank’s internet and mobile banking manger.....	114
Appendix 3-Letter of cooperation written by the university to the bank.....	115
Appendix 4-Letter of cooperation from the bank to any other branches of the bank.....	116
Appendix 5 - Results of linear regression for Perceived vulnerability, Perceived severity and Perceived risk.....	117
Appendix 6- Results of linear regression for Perceived risk and Protection Motivation in Mobile Banking.....	117
Appendix 7 - Results of linear regression for Response efficacy, Self-efficacy, Response cost and Protection Motivation in Mobile Banking.....	117
Appendix 8- Results of linear regression for Perceived ease of use, Perceived usefulness, and Protection Motivation in Mobile Banking.....	118
Appendix 9- Results of linear regression for Trust belief, Structural assurance, and perceived risk in mobile banking.....	118
Appendix 10– Sample size calculation.....	119

LIST OF TABLES

Table 2.0: Some summary of empirical and theory-based empirical researches.....	32
Table 3.0. Characteristics of different research strategies.....	45
Table 3.1: Summary of some related works and their methodologies.....	58
Table 4.0: Gender of respondents.....	62
Table 4.1: Age of respondents.....	63
Table 4.2: Educational status of respondents.....	63
Table 4.3: Marital status of respondents.....	63
Table 4.4: occupation of respondents.....	64
Table 4.5: Frequency distribution of respondents about Perceived vulnerability.....	64
Table 4.6: Frequency distribution of respondents about Perceived Severity.....	65
Table 4.7: Frequency distribution of respondents about Perceived risk.....	66
Table 4.8: Frequency distribution of respondents about Response efficacy.....	67
Table 4.9: Frequency distribution of respondents about Self-efficacy.....	67
Table 4.10: Frequency distribution of respondents about Response cost.....	68
Table 4.11: Frequency distribution of respondents about Perceived ease of use.....	69
Table 4.12: Frequency distribution of respondents about Perceived usefulness.....	70
Table 4.13: Frequency distribution of respondents about Trust belief.....	71
Table 4.14: Frequency distribution of respondents about Structural assurance.....	72
Table 4.15: Frequency distribution of respondents about Protection motivation in mobile banking.....	73
Table 4.16: Reliability of questionnaire items.....	75
Table 4.17: Reliability of the model factors.....	75
Table 4.18: Results of linear regression for Perceived vulnerability, Perceived severity and Perceived risk.....	78
Table 4.19: Results of linear regression for Perceived risk and Protection Motivation in Mobile Banking.....	78
Table 4.20: Results of linear regression for Response efficacy, Self-efficacy, Response cost and Protection Motivation in Mobile Banking.....	80

Table 4.21: Results of linear regression for Perceived ease of use, Perceived usefulness, and Protection Motivation in Mobile Banking.....	81
Table 4.22: Results of linear regression for Trust belief, Structural assurance, and perceived risk in mobile banking.....	83
Table 4.23: Summaries of the above results.....	83
Table 4.24. Attitude towards mobile banking in Africa.....	84

LIST OF FIGURES

Figure 2.1. Theory of Reasoned Action (TRA).....	19
Figure 2.2. Technology Acceptance Model (TAM).....	20
Figure 2.3. The Technology Acceptance Model, version 1.....	20
Figure 2.4. Theory of Planned Behavior (TPB).....	21
Figure 2.5. Unified Theory of Acceptance and Use of Technology Model (UTUAT) Model.....	22
Figure 2.6: Technology-Organization-Environment framework.....	27
Figure 2.7. The theory of planned behavior.....	28
Figure 2.8. The theoretical/conceptual/research model adapted from PMT and TAM.....	40
Figure 3.1: Framework for the research paradigm.....	42
Figure 4.1. The research model and relationship between the factors.....	85

LIST OF ACRONYMS

ATM –Automatic Teller Machine.

CBE –Commercial Bank of Ethiopia.

CRM –Customer Relationship Management.

GPRS - General Packet Radio Services.

ICR- Internal consistency reliability.

ICT –Information Communication Technology.

IDT –Innovation Diffusion Theory.

ITU - International Telecommunication Union.

MB -Mobile Banking.

MFIs –Microfinance Institutions.

NBE -National Bank of Ethiopia.

PCI –Per Capital Income.

PDA –Personal Digital Assistant.

PEOU –Perceived Ease of Use.

PMT –Protection Motivation.

PR -Prior Studies.

PU –Perceived Usefulness.

SMS –Short Message Service.

SPSS –Statistical Package for Social Sciences.

TAM –Technology Acceptance Model.

TOE –Technology Organization Environment.

TPB –Theory of Planned Behavior.

TRA –Theory of Reasoned Action.

UMTS - Universal Mobile Telecommunication System

UTUAT - Unified Theory of Acceptance and Use of Technology Model

WAP –Wireless Application Protocol.

XHTML –Extreme Hypertext Markup Language.

CHAPTER ONE

INTRODUCTION

1.1. Background of the study

The rapid development of information technology has affected the banking industry globally. An impact of information technology in the banking sector is the introduction of mobile banking. Earlier studies have shown the usefulness of mobile banking in facilitating the financial transactions between banks and their customers (Mattila, 2003).

Mobile banking is more easily and fast banking today, but its challenges related to security is still an apparent issue. Many organization or financial institutions are now incorporating mobile banking and financial services as a key component of their growth strategy, and use of the mobile phone to conduct banking and financial service tasks continues to rise among early adopters.

Mobile banking can be categorized as the latest advancement in electronic banking. Mobile banking refers to provision and availing of banking and financial services with the help of mobile telecommunication devices. What attracts customers to mobile banking is the round clock availability and ease of transactions (Ashta, 2010).

Mobile banking today is most often performed via SMS or the mobile internet, but it can also use special programs called clients downloaded to the mobile device. Mobile banking is most often performed by SMS and hence is also known as SMS banking. Commercial banks are exploring this avenue to make their services more convenient for their customers. The growing number of mobile subscribers in any country forms the most valuable support base for the growth and success of mobile banking. Though mobile banking is synonymous with the word convenience banking, its usage is not anywhere close to its potential.

Together with the advent of smart phones and ever growing usage of internet on mobile handsets, application based banking has emerged as a new concept within this space. Other than SMS banking, banks are now also offering banking services on mobile handsets through WAP-based internet websites and application based mobile banking services. (Mehta, 2012).

Mobile applications have been rapidly changing the way business organizations deliver their services to their customers and how customers can interact with their service providers in order to satisfy their needs. The use of mobile applications increases rapidly, and has been used in many segments including the banking segment. Mobile banking involves mini-statements and checking of account history; alerts on account activity or passing of set thresholds; monitoring of term

deposits; access to card statements; mutual funds/equity statements; insurance policy management; pension plan management; access to loan statements; status on cheque, bill payment processing; peer to peer payments; and deposit at banking agent (Mohammad, 2010).

On the other hand customers' have different perceptions towards this mobile banking services. Mobile banking security perception is related to customers' view point, how they think of the service in terms of safety, threats or attacks, hacks, risks ,trust on the bank and also on the transmission channel(wireless platform) etc.

Commercial Bank of Ethiopia's (CBE's) mobile banking service enables customers to access their bank accounts, make fund transfers, payments and balance inquiries, as well as get instant notifications on all their accounts linked with MB(mobile banking) services using the SMS, XHTML and DOWNLOADABLE application channels. Similarly through CBE's Internet Banking, many transactions can be carried out from the comfort of customers' home or office. The online services include: viewing account balances and transactions, making fund transfers between a customers' own current accounts and savings accounts, effecting payments to third parties, including bill payments to predefined CBE customers within Ethiopia, viewing and downloading current and saving account statements, requesting for stop payments on cheques, applying for a letter of credit and more.

Currently there are more than 16 banks in Addis Ababa (Mengistu, 2011). Mobile banking in Ethiopia is a recent phenomenon. Commercial Bank of Ethiopia is a pioneer state owned banking industry that introduce modernization through the introduction of various e-banking services. It is the leading bank in Ethiopia, established in 1942. It is also a pioneer to introduce modern banking to the country. It has more than 970 branches stretched across the country. It is the leading African bank with assets of 303.6 billion Birr as on June 30th 2015. It plays a catalytic role in the economic progress & development of the country. Currently CBE has more than 11 million account holders and the number of mobile and internet banking also reached more than 460,000 as of June 30, 2015.

The motivation for studying the security perception of customers' towards mobile banking services stems from issues such as the need to attract potential users, retaining existing users, and also for determining the elements that may influence the customers' perception towards mobile banking security. There are so many constraints that need to be explored as they can create the barriers for the customers' to use mobile banking, such as low level of infrastructural development, lack of

suitable legal and regulatory framework, high rates of illiteracy, frequent power interruption and security issues. Among these constraints the one which is considered as the main barrier for the adoption and use of the service by the customers is the concern of security (Gardachew, 2010). Similarly a study conducted by Wondwossen and Tsegai (2005) revealed that an adequate legal structure and security framework could encourage the use of e-payments or e-banking in Ethiopia. So, if having an adequate legal structure and security framework can encourage the use of e-payments or e-banking in Ethiopia, it leads to the need to determine the perception of customers' towards mobile banking security in order to forward practical recommendation for the bank. The other motivation is, the innovation is new in Ethiopia and knowing how it is perceived or accepted by customers' is important, especially on the security perspective as it is explained earlier.

1.2. Statement of the problem

Internet technology is rapidly changing the way personal financial services are being designed and delivered. Electronic banking in Ethiopia started before 10 years with the adoption of ATM cards and other services (Mengistu, 2011). Recently because of the increasing adoption of cellphones in developing countries, it creates the opportunity for mobile banking. Ethiopia is now seeking in adopting new technologies that will modernize the service industries (banks-Commerce, e-Shopping, e-Governments, etc.). All these services require a strong banking system, and this cannot now be achieved without adopting new technology. However, traditional branch based retail banking remains the most widespread method for conducting banking transactions in Ethiopia as well as any other country. Ethiopian banking industry is quite underdeveloped in comparison to the rest of the world (Gardachew, 2010). The predominant medium of exchange in transactions is still cash, although the rapidly growing ICT technologies are poised to revolutionize the banking sector in Ethiopia (FORTUNE, 2013) that is going through modernization initiatives to support real-time financial services.

Now, Commercial Bank of Ethiopia is doing too much to introduce mobile banking to improve their operations and to reduce costs. Despite all their efforts aimed at developing better and easier mobile banking systems, these systems remained largely unnoticed by the customers, and certainly these were underused in spite of their availability. Therefore, there is a need to understand users' acceptance of mobile banking, and a need to identify the factors that can affect their intention to use mobile banking. This issue is important because the answer holds the clue that will help the banking industry to formulate their marketing strategies to promote new forms of mobile banking systems in the future. Mobile banking also helps banks to form good relations with their customers.

In mobile banking, banks get valuable data about the customers which help them for effective customers' relationship management practices. It facilitates quick feedback and helps in customer retentions and customer loyalty. When banks have customer database, they can use SMS advertising to give information about their service to their existing customers. This helps in the communication and promotion of new customers. Customers enjoy anytime anywhere banking with the help of their mobile phones. They need not stand in the queues or face the employees to get their banking needs. Mobile banking is cost-effective for bankers and customers. The information can also be stored automatically in the mobile phones in the form of SMS as a proof, whether sent or received.

As the number of mobile phone users in Ethiopia is increasing day by day, there is a great scope for mobile banking. Therefore the customer should be made aware of mobile banking. when we look at the context of our country, the comparison from mobile phone users and the mobile banking users, there is a big gap between the two, that is even if the mobile banking technology is easiest and fast way of doing banking activities online, the customers number is less when it is compared with the real mobile phone users for the normal day to day conversations or communication services. From this there can be a deduction why customers are not using this mobile banking service without losing their time and effort. Even if there is no particular local study that indicates why this gap exists, there are so many researches done on related aspects in general, which make customers not to use this service. This gap arises due to lack of awareness, fear of the service being expelled for errors that is concerns related to security and the other may be efforts taken by the banks themselves to reinforce customers to use the technology properly without being fear of it (Gardachew, 2010; Wondwossen and Tsegai, 2005).

In Ethiopian mobile banking related works are too limited. Most of the researches done still are focused more on the adoption of e-banking, opportunities and challenges of e-banking and also factors affecting the adoption of e-banking in general in which mobile banking related researches receive little attention, so our particular research tries to look on perception of customers' specifically to the security concerns of mobile banking. Therefore, to address the current gap in the literature, this study is designed to identify the customers' perception of mobile banking security particularly at the Commercial Bank of Ethiopia in Addis Ababa. According to researchers it is recognized that research is scarce in the domain of individual security related behaviors about online banking in which mobile banking one of these to be investigated.

Nowadays Commercial Bank of Ethiopia is doing too much tasks to announce mobile banking usage to the customers using different mechanisms like Medias, newspapers, and also through social networks. But still it remains a lot to be done on the area, particularly the concern of security issues about mobile banking services by the customers ‘and also about other e-banking services.

1.3. Research questions

Based on the statement of the problem described, the research aims to answer the following questions which are central to the study being conducted:-

1. What are the factors associated with customers’ perception towards mobile banking security?
2. Does a relationship exist among different factors of the existing adoption models and individual security related models together with trust topology?
3. What are the security perception factors that will help the mobile banking service providers to expand the reach of mobile banking service to desired number of customers?

1.4. Objectives of the study

1.4.1. General objective

The general objective of the study is to explore customers’ perception towards mobile banking security at the Commercial Bank of Ethiopia in Addis Ababa.

1.4.2. Specific objectives

To achieve the general objective of the study the specific objectives are identified as:

1. To generate the theoretical frame work for the study after a detail literature review.
2. To identify existing gaps and relationship of the different theoretical models.
3. To find the factors associated with customers’ perception towards the security of mobile banking.
4. To determine the mobile banking security perceptions of customers’.
5. To find out factors which then explored can help to deepen the reach of mobile banking services to more customers.
6. To draw conclusions and forward recommendations for further study.

1.5. Scope the study

The study is intended to identify customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa and it contributes a theoretical framework for the study being conducted. Currently there are a number of banks which provide mobile banking services and there are also so many services being offered by the mobile banking service providers in which customers have different viewpoints on these services. But due to time and financial constraints, this particular study will have its own scope, so the scope of the study will be on the customers of Commercial Bank of Ethiopia in Addis Ababa only and the study will be confined to perception of customers' on mobile banking security.

1.6. Significance of the study

The mobile banking usage at Commercial Bank of Ethiopia is a recent phenomenon and there are also some related researches done on this particular issue in the banking industries, but still there remains a lot of work to be done to make this technology to be used in the proper manner by customers. The things that have been done in this area were limited for identifying the customers' perception towards the mobile banking security. So researches to be done like this will have a contribution to what have been done and also to what will be done next regarding technologies to be born out in relation to the mobile banking industry and customer perceptions. Therefore, the research is expected to have significances like showing directions of improvements and also the things to be done towards the perception of customers on mobile banking security. The findings from the research/study/ will lead one step forward to what will be done in terms of customers perceptions in the area of mobile banking security. The workers will also be capable of or being aware of customers' perception towards this mobile banking security after the study is conducted. Again it helps Commercial Bank of Ethiopia to implement the mobile banking service properly to its customers. It also contributes too much to the users of the mobile banking who are the customers, to use the technology properly without being fear of it. The security perceptions of customers to be identified or determined after the completion of the study will contribute a lot to the providers of the mobile banking services to adjust their marketing strategy.

So the findings and the recommendations of the study will contribute to reach at proper utilization of the mobile banking technology and helps the Commercial Bank of Ethiopia to proceed as the leading banking sector in Ethiopia. In addition lessons learned from the use of mobile banking by

Commercial Bank of Ethiopia will help other banks to understand how these technologies are built or put into practice.

1.7. Structure of the Study

This study paper will be structured to contain five chapters.

Chapter one contains background of the study, statement of the problem, objective of the study; it goes further to highlight scope of the study and the significance of the study.

Chapter two contains the literature review that talks about mobile banking, mobile banking in Ethiopia, and perception of customers' towards mobile banking. It will also look at some basic aspects on mobile banking services in order to have more understanding on the issue of customers' perception on mobile banking security. It goes further to review other studies about mobile banking, which will serve as a basis for the research framework.

Chapter three explains the research methodology, the method used and the purpose of using such method by taking into consideration its strength and weaknesses. It also looks at the way the data will be analyzed and also the methodological limitations in the research work. It goes further to explain the research model and the hypothesis development.

Chapter four contains the analysis and the interpretation of data. It goes further to compare the findings of the present research with the past once and it puts forward the proposed and also recommended solutions to increase the awareness of customers' on the perception of mobile banking security. Similarly an interview result from the bank's internet and mobile banking manager will be added.

Finally, **chapter five** will contain the summary, the conclusion, recommendations, directions for future work and limitations of this study.

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This chapter contains the literature review which begins with the introduction of mobile banking, Mobile banking in Ethiopia, and customers' perception towards mobile banking services in the literature of mobile banking with other related researches conducted in the past years and the recent once. Similarly different models used for customers' perception and technology adoption will be discussed. Again related works on customers' perception and mobile Banking adoption using those models will also be discussed. The PMT (Protection Motivation) with its constructs will also be clarified. Finally trust and perceived risk, perceived ease of use and perceived usefulness will also be discussed in detail. This will serve as a frame work for our research work.

2.2 Introduction to Mobile banking

In recent times the industry of banking has been undergoing radical changes and all these things are taking place in every aspects of the banking sector. Among these new changes one thing to be mentioned is the information technology as a system as a whole and it is mainly used by most of the banks to reduce the turnaround time and also to improve business operation in general. Again the introduction of mobile technology and also mobile devices have indeed brought about efficiency and effectiveness in the manner which commercial and business activities are been carried out (Tiwari and Buse, 2007; UNCTAD, 2007). One of this technological development is the production of mobile telephones. Mobile telephones serve as a platform for launching out innovative mobile phone applications and also services (UNCTAD, 2007). In addition the use of mobile technologies for commercial purposes has generated the concept of mobile commerce. Mobile banking is an application of mobile commerce which enable customers to bank virtually at any convenient time and place (Suoranta, 2003). There has been evidence for the increase in the number of users subscribing for mobile telephones in both developed and developing countries (UNCTAD, 2007). There is also indication that the fastest growing market in the world is now the mobile industry.

The recent innovations in telecommunications have enabled the launch of new access methods for banking services; one of these is mobile banking; whereby a customer interacts with a bank via mobile phone devices (Barnes & Corbitt, 2003). But even if there is a launch of new accesses due to the recent innovations in telecommunications, according to Clark (2008) he suggested that as a

channel the mobile phone device can augment the number of channels available to customers, thereby giving customers a more low-cost self-service options by which to access funds, banking information and make payments. Mobile as a channel also delivers convenience, immediacy and choice to customers. But there are a large number of different mobile phone devices and it is a big challenge for banks to offer Mobile banking solution on any type of device. Some of these devices support Java2Micro Edition (J2ME) and others support Wireless Application Protocol (WAP) browser or only SMS; presetting a serious challenge to the provision of mobile banking service.

Mobile banking is the type of banking services that allows customers to perform banking services (i.e. alerts, banking transactions and balance enquiries) with the use of their mobile devices (Corbitt and Barnes, 2003). This mobile banking technology could be defined as a service which provides the banking services such as balance enquiries, fund transfer, bill payment and transaction history through a user's mobile devices (Stair and Reynolds, 2008). Tiwari et.al (2006) believes that "corner stone of m-commerce is built by m-banking"; many banks are taking advantage of this new technology in order to increase customers' satisfaction, manage costs, increasing profits and bring about positive transformation of banking payment systems in the economy(ThridayLive 2011).The name of mobile banking itself indicates it is "banking on the move" with the help of mobile telecommunication devices in which this devices can be used for a different purpose at any time and also anywhere. This mobile banking allows customers to receive short text messages(SMS) using their telephone devices, wireless application protocols(WAP) and also Java enabled phones support other banking activities using GPRS(General Packet Radio Services) like direct payments confirmation and funds transfer (Mallat et.al 2004). For example from earlier conducted researches 30% of households in the United Kingdom use their mobile devices to perform banking activities (MMA 2009). Mobile devices show promising path to the future which can reach larger population of customers irrespective of their location and this also can lead to customers' loyalty. Mobile Banking, also known as M-Banking, can perform various functions like mini statement, checking of account history, SMS alerts, access to card statement, balance check, mobile recharge etc. via mobile phones (Vinayagamoorthy and Sankar, 2012). Banks are constantly updating their technology and want to increase their customer base by reaching to each and every customer. There are many advantages of using mobile banking, such as people in the rural or remote areas can also get an easy access to mobile banking whenever required. Again Vinayagamoorthy and Sankar, (2012) have also discussed about the mobile banking and according

to them it is a term that is used for performing various banking transactions like fund transfer, balance check, payments etc. via mobile phones.

The mobile banking technology has been said to have brought about positive shift in customers' perception but this couldn't be true in the case of Ethiopia. There is no much attention which is given to the area and also there is lack of empirical research on the adoption and also the usage of mobile banking in the context of Ethiopia. Therefore our research aims to bridge the gap in the area. According to many researchers they have given proof of the advantage that can be obtained from using mobile banking services (Barnes and Corbitt, 2003), which customers can get when there is a desire to adopt the facility of the services. In the past years there has been several challenges in which the banks have been facing because of poor information technology systems, but with the introduction of the new technological development like the universal mobile telecommunication system (UMTS), the banks can fully adopt the advantage of this new technology or platform for realistic mobile applications which have been made available (Tiwari et.al 2006). So in general, by definition mobile banking is one form of banking transaction carried out through mobile phones. This mobile banking allows bank customers to do banking tasks like checking their account balances, performing credit card transactions and also providing information on the latest transaction made by customers. Mobile banking is also a subset of e-banking in which customers access a range of banking products like savings accounts, credit instruments, and also others via electronic channels.

2.3. Mobile banking in Ethiopia.

The history of modern banking in Ethiopia goes back to 1900 when an agreement was reached in 1905 between Emperor Minilik II and Mr.Ma Gillivray, representative of the British owned National Bank of Egypt. Currently as per National Bank of Ethiopia estimates, there are 18 private and 3 state owned banks. Out of these 19 banks, the state owned Commercial Bank of Ethiopia (CBE) is the largest and leading bank in financial operations.

Commercial Banks as such provide all the banking services including ATM facility, Internet Banking, Telephone Banking, SMS banking and Mobile Banking beside the traditional banking activities. The appearance of E-banking in Ethiopia goes back to the late 2001, when the largest state owned, Commercial Bank of Ethiopia (CBE) introduced ATM to deliver service to the local users. Electronic banking facilities provided by most Ethiopian Banks are very basic. However e-banking facilities provided are at par (similar) with those in the region.

On 1 January 2013, the National Bank of Ethiopia (NBE) issued a long-awaited directive that allows transaction-based mobile banking for the country's unbanked citizens (Elissa Jobson (2013)). Four major players: Commercial Bank of Ethiopia, M-BIRR, BelCash and Zemen Bank's Z-Birr were expected to begin operations later that year, making Ethiopia the last but one African country to adopt this technology.

The rapidly growing information and communication technology (ICT) is knocking the front door of every organization in the world, where Ethiopian banks would never be exceptional. In the face of rapid expansion of electronic payment (E-payment) systems throughout the developed and the developing world, Ethiopian's financial sector cannot remain an exception in expanding the use of the system (Gardachew, 2010).

Though it is true that traditional banking has grown steadily over the years, in terms of technological based financial service/product, the Ethiopian banking sector didn't fully benefit from ICT in general and M-banking in particular. Currently there are six commercial banks that commenced M-banking service, although the M-banking regulation directive was issued in January 2013 (Henok Arega Asfaw, 2015).

At the end 2013/14 fiscal year, there were eighteen commercial banks operating in Ethiopia, of these sixteen are private commercial banks while the rest two are state owned banks. Despite a rapid increase in the number of financial institutions since financial liberalization, the Ethiopian banking system is still underdeveloped compared to the rest of the world. The Ethiopian banking industry as a whole had a network of 2,323 branches as of September 30, 2014, in which the number of population being served by a single branch was around 37,861.8. Commercial Bank branch (per 100,000 adults) ratio in 2012 was 2.94 which is lower than Sub-Saharan Africa, that is 3.71 (World Bank, 2012).

With urban skewed branch network it is hard to ensure efficient flow of financial resources and optimize the contributions of the entire financial system to the development processes. The mobile banking development in Ethiopia is at its starting stage. Currently m-banking practice in Ethiopia can be considered as accessing the core banking system within the bank. Hence, only a customer of a given bank can access some banking services via his/her mobile phone. Moreover, there are only six commercial banks that have got license to operate mobile and agent banking services as per the Directives No. FIS /01/2012.

In 2013/14 there were about 28.3 million mobile phone subscribers, recording an annual growth rate of 19.2 percent. The mobile phone subscribers' penetration rate is increasing in each year. During the same period the penetration rate reached at 33.3 percent. Such development in mobile phone subscribers implies there is an immense potential in reaping the benefits from m-banking service. Moreover, the continual increase in PCI (per capital income) of the nation can be considered as another potential for banks to reap the full benefits derived from M-banking.

As of December 2014 there are about 151,425 active number of mobile subscriber customers in these six banks. The mobile banking development in Ethiopia is not full-fledged in terms of exhaustively utilizing all the mobile services that one can get. Currently, of all the types of mobile banking services, most customers of the bank use notification or alarm inquiry. Five Micro-Finance Institutions (MFIs), namely Amhara Credit and Savings Institution, Addis Credit and Savings Institution, Dedebit Credit and Savings Institution S.C, Oromia Credit and Savings and OMO Microfinance render M-Birr mobile money service in their respective regional states. M-BIRR aims to develop a mobile banking services, allowing people to conduct basic financial transactions from their mobile phone, including sending and receiving money, paying bills, receiving salaries and other government or non-governmental, and repaying loans. According to Directive No FIS/01/2012, a persons' balance in his/her mobile account shall not exceed Birr 25,000 and daily mobile banking transaction shall not exceed Birr 6,000. As mobile money is a new phenomenon in the banking sector development, and hence fear of unknown, and the service heavily rely on ICT, which is vulnerable to hacking, such limit by NBE(national bank of Ethiopia) is considered to minimize the risk associated with money laundering and financing terrorism. M-Banking requires the customer to hold a deposit account to and from which payments or transfers may be made. M-banking reduces the transactions costs of payments because there is an electronically accessible store of value.

Mobile payments are a small but growing subset of the broader world of electronic payments. While customers may initiate and authorize e-payments through a number of other electronic channels such as the internet and card based devices like ATMs (automatic teller machines), mobile payments are made using a mobile device such as a cell phone or PDA (personal digital assistant). Despite the natural conservatism of the banking industry, M-banking innovation has proceeded to become a rapidly growing tool across developing countries. (Porteous, D. 2006).

With the nine successful private banks in Ethiopia and the largest state owned bank, CBE, all thriving due to economic growth, (Economist Intelligence Unit Country Report 2007 “Ethiopia”) m-banking will no doubt increase due to competition. Factors affecting customers’ intention to adopt e-banking service channels have been at the forefront of several research works in the developed world (Lassar, 2005; Lichtenstein & Williamson, 2006). Nevertheless, there is very much limited published works that investigate the factors influencing the adoption of e-banking from the viewpoint of customers in the context of developing countries like Ethiopia. To date there have been very few such studies, a remarkable exception to this is the study conducted by (Gardachew, 2010) who studied electronic banking practices, opportunities and challenges in Ethiopia. Despite the growth of e-banking worldwide, commercial banks in Ethiopia continue to conduct most of their banking transactions using traditional teller based methods. So some of the factors that may be raised as contributors for the lagging behind of e-banking or mobile banking in Ethiopia can be cited below.

Banking operation is still under developed and backed by low level of infrastructural development, lack of suitable legal and regulatory framework, high rates of illiteracy, frequent power interruption and security issues (Gardachew, 2010). Moreover, e-banking is a new technology in Ethiopia which needs a lot of effort and resources to be easily adopted by customers. Hence, in order to help the banks to improve e-banking adoption by their customers, it is necessary to examine the hindrance factors that influence customers’ intention to adopt e-banking service channels.

Some of the hindrance factors include, lack of appropriate infrastructure for e-payment, lack of internet facilities with customer and learning how to interact with bank’s website. Moreover, the factors that can affect adoption of e-banking in the country are regarding the technological factor, organizational factor and Environmental factor. Even Though problems are plenty, a study conducted by Wondwossen and Tsegai (2005) revealed that an adequate legal structure and security framework could encourage the use of e-payments or e-banking in Ethiopia.

Again low literacy rate is a serious impediment for the adoption of e-banking in Ethiopia as it hinders the accessibility of banking services. For citizens to fully enjoy the benefits of e-banking, they should not only know how to read and write but also possess basic ICT literacy (Gardachew 2010). Again risks related with security issue, lack of competition among local & foreign banks and social awareness on the e-banking system were not also addressed.

Africa's least developed countries, including Ethiopia, lag behind other more developed countries on the continent. Between 1986 and the end of the 1990s, the poorest African states' share of the world's telephones was constant at about 0.8%. After 1998, this share rose sharply because of the introduction of mobile phones, reaching 0.4% in 2002 and it has been estimated that this number has increased to 0.6% at the end of 2006. There is no question that the mobile industry accounts for a major portion of the GDP in Sub-Saharan Africa. Africa is now the world's fastest growing mobile phone market and, according to latest research by telecommunications analyst firm Informa Telecoms & Media, there are now more than 100 million mobile phones in use on the continent one for every nine Africans.

Literature also supports that the level of user's acceptance of electronic banking is largely determined by their perceptions of its effectiveness in terms of costs and benefits (Olatokun & Igbinedion 2009).

Robinson (2000) argued that the online banking extends the relationship with the customers through providing financial services right into the home or office of customers. The banks may also enjoy the benefits in terms of increased customers loyalty and satisfaction. However, Nancy, Lockett, Winklhofer, and Christine (2001), viewed the same situation differently and argued that customers like to interact with humans rather than machines. As it is stated in different e-banking literatures some of the problems related with adoption of e-banking are generally: Low level of internet penetration and poorly developed telecommunication infrastructure. According to Jensen (2003), most countries in Africa, except South Africa, have Internet infrastructure only in their major cities.

Lack of suitable legal and regulatory framework for e-commerce and electronic payment is another impediment for the adoption of new technology in banking industry. According to Ayana Gemechu (2014), the major barriers that Ethiopian banking industry faces in the adoption of Electronic banking are: security risk, lack of trust, lack of legal and regulatory framework, Lack of ICT infrastructure and absence of competition between local and foreign banks.

Wondwossen & Tsegai (2005) observed the following reasons which may be considered as hindrance factors for the use of electronic payment system in Ethiopia.

The regulatory framework could limit m-banking's progress. Paper receipts will be required for every transaction, necessitating the use of a printer and a consistent electricity supply, both of which may not be easily available in remote rural areas. The transfer limit is 6,000 birr (\$324),

other countries have a ceiling of \$1,000. In addition, foreign-owned companies are disqualified from acting as agents. The exclusion of non-domestic players from the m-banking market is consistent with Ethiopia's policy for the sector as a whole. The government's line is that foreign banks are barred because the country's central bank, the NBE, does not yet have the capacity to deal with sophisticated global institutions. Other analysts say that the NBE could impose whatever regulations it wanted. A second reason given for the prohibition is that the country's nascent financial services industry which was first opened to private ownership in 1994 needs time to mature before being exposed to international competition. Therefore a study of customers' perception towards mobile banking security here in Ethiopia is relevant since mobile banking is one of the e-banking services.

2.4. Customers' perception to mobile banking

There are researches on customer attitude and adoption of mobile banking that showed the several factors predetermining the customers' attitude towards online banking/mobile banking/ such as person's demography, motivation and behavior towards different banking technologies and individual acceptance of new technology. From these researches it has been found that customers' attitudes toward online banking are influenced by the prior experience of computer and new technology (S. Laforet and X. Li, 2005). The adoption of electronic banking forces customers to consider concerns about password integrity, privacy, data encryption, hacking, and the protection of personal information (J. Peppard, 2000). Electronic banking requires perhaps the most customer involvement, since it requires the web service technology. A key component of many initiatives to be considered here is the implementation of Customer Relationship Management (CRM) software. Many companies in the financial services sector have been quick to implement internet capabilities, and electronic service which is becoming a viable option for interaction between financial service providers and their customers. Customer satisfaction and customer retention are increasingly developing as key success factors in e-banking (E. E. Ibrahim, M. Joseph, and K. I. N. Ibeh, 2006). Technology, in particular, has been increasingly employed in service organizations to enhance customer service quality and delivery, reduce costs, and standardize core service offerings.

A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking".

In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services. (“Consumer and Mobile Financial Services,” 2012). From this two unclear points there is a need to know whether security issue is customers concern or not, to identify clearly the customers perception towards mobile banking security.

Hayat (2009) suggests that for a banking regulator, it is important to provide adequate protection for customers, ensure economic stability, provide interoperability of electronic systems and guarantee security of transactions and Anti Money Laundering and also knowing your customer principles must be applied to mobile payments.

Sharma and Singh (2009) found that Indian mobile banking users are especially concerned with security issues like financial frauds, account misuse and user friendliness issues, difficulty in remembering the different codes for different types of transaction, application of software installation and also updating techniques due to lack of standardization. Some of the customers’ perception towards mobile banking are discussed below:

2.4.1 Aspects of risk and security

Security and trustworthiness of a service was identified as one of the most important factors within every target customer consideration when deciding on the use of banking service delivery channels. Some customers agreed that “using of mobile phones in the banking industry is trustworthy” (Mattila, 2002). According to Fain and Roberts (1997) they defined “risk is a perception of customer, not a characteristics of a product”. It was also found out that the security factor could influence customers’ attitudes towards online banking in China (Laforet & Li 2005). Furthermore, it was considered to be one of the greatest concerns in adoption of mobile banking services (Luarn & Lin, 2004), as the individuals may worry about safety issues during mobile banking service transactions such as data input and output mechanisms (Laukkanen & Lauronen, 2005), loss of connection risk (Kuisma et al., 2007) and personal performance mistakes (Laukkanen & Lauronen, 2005; Kuisma et al., 2007). As a result, many people may decide not to use this service and ignore the extra benefits obtained from using mobile banking. *However, some previous studies have argued that, on the contrary, security issues were not major obstacles for customers in adopting mobile banking (Suoranta, 2003; Laukkanen & Lauronen, 2005). So it can be concluded that the security aspect is to be investigated as an important element which influences the use of mobile banking.*

2.4.2. Aspects of Socio-economic background and culture

According to Laforet and Li (2005) they have found out that the lack of understanding the concepts and benefits was the main barrier to customers using mobile banking, furthermore, users of mobile banking were not intended to be highly educated and were typically younger people in China; this was on the contrary to the situation in the western countries as explained by Karjaluoto, Mattila, and Pento, (2002). As discussed by Trappey and Trappey (2001), the Chinese were used to carrying cash, and have little confidence in traditional financial management. When it is compared with other Asian customers, Chinese customers seem to be more traditional and less affected by new technological advancements. Some customers simply prefer to deal directly with a bank clerk instead of using “arms-length technology” (e.g. mobile banking). In addition, earlier related studies indicated that males used mobile banking more than females, and mobile banking users tended to come from high-income groups such as small business owners, salaried employees and also senior managers. Furthermore, a negative, hard-to-use imagination (Fain & Roberts, 1997) of these technologies and computers may have been perceived by customers when thinking about using mobile banking. Therefore, the socio-economic background and culture of potential users could be factors that influence the usage of mobile banking.

2.4.3 The characteristics of the service

The account balance service is one of the most promising mobile banking services, and it is designed to help customers to check their account balances and also latest transactions immediately anytime/anywhere (Laukkanen, 2007). Luakkanen and Lauronen (2005) found out that location free access by the mobile banking created convenience in requesting account balances. Furthermore, accessibility and portability of the services are classified as dimensions of convenience in the customer behavior studied literatures. Consequently the spatial and temporal distance between need recognition and need satisfaction can be considered as an important element for doing banking via mobile phone devices. The ability of the technology to allow customers to have more control over their financial situation is one attraction of mobile banking services (Laukkanen & Lauronen, 2005), as the customer prefers to act for himself/herself when dealing with his /her own monetary transactions through his/her mobile devices. Luakkanen (2005) again found out that the flexibility of being able to use the service wherever and whenever the users want enables immediate completion of banking tasks (transferring money or paying a bill). So this would save time and be perceived as convenient and efficient. The SMS service is the easiest way to check account balances and latest transactions via mobile phone devices (Laukkanen, 2007).

Laukkanen et al (2007) also found out that speed of data transmission and the user interface impaired, the added value of mobile services. Therefore, the characteristics of the service as perceived by the user or the customer and the characteristics of the service provided by the banking institution and also the service provider are important factors influencing the usage of mobile banking.

2.4.4. The service and device costs

According to Nah, Siau, and Sheng (2005), the cost of mobile devices and mobile services was identified as an investment concern. Again Luarn and Lin (2004) argued that financial cost to be incurred was one of the greatest concerns in adoption of mobile banking services. The cost of banking services may have an opposite effect with respect to the adoption of mobile banking, which may result in customers preferring the traditional banking services (Laukkanen et al, 2007). Customers agree to pay a reasonable fee to use this service; however this would depend on both the banking and service provider. Provision of a lower service cost is also a major benefit for users using mobile banking and performing banking transaction functions through their mobile devices; so it can be understood that the “value for money” barrier may be another factor influencing the adoption of mobile banking services.

2.4.5. The mobile device features

The other very important factor to be considered is, the limited input and display capability of current mobile devices can be seen as limiting factor for the use of mobile banking applications (Laukkanen, & Lauronen, 2005). For example, a mobile phone’s small screen cannot accommodate enough information about an account, and also scrolling up and down would be needed. However, the mobile phone device itself may have little effect to provide the required facilities; Laukkanen (2007) found out that, when customers had experience in using a mobile phone service, they did not stress the importance of screen size in the service, but rather they focused their attention on the spatial issues in the service consumption. Therefore compared to others described above, device features may not be an issue for bank customers when considering using mobile banking.

2.5. Different Models used for Customers’ Perception on Mobile banking Adoption and online security

Researchers have come across many different models that help them in determining the important factors that affect the attitude and intention of the mobile banking users. These models include

various attributes that judge the intention of the mobile banking user and his/her attitude towards it. In the next section those models will be discussed.

These models are: 1) Theory of Reasoned Action (TRA) 2) Technology Acceptance Model (TAM) 3) Theory of Planned Behavior (TPB) 4) Innovation Diffusion Theory (IDT) 5) Unified Theory of Acceptance and Use of Technology Model (UTUAT).

2.5.1.Theory of Reasoned Action (TRA)

In the model proposed by Fishbein and Ajzen (1975) it was suggested that person's actual behavior can be determined by the behavioral intention along with the belief and subjective norms that the person has for the behavior. Subjective norms refer to *“an individual's perception of other's opinion about his/her particular behavior, if he should perform a particular behavior or not”* and attitude towards action is defined as *a person's positive or negative attitude towards this performed behavior*. Thus, TRA is a useful model that can explain the actual behavior of an individual. In 1985 Davis took the same model and extended it to the TAM and linked it to the user acceptance of an information system.

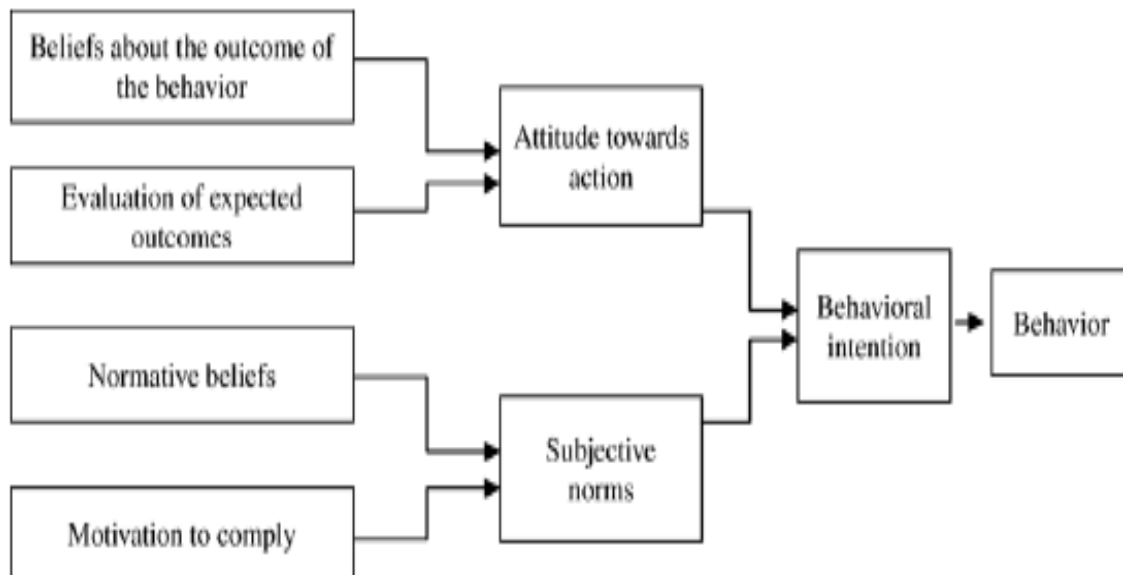


Figure 2.1. Theory of Reasoned Action (TRA)

2.5.2. Technology Acceptance Model (TAM)

Technology Acceptance Model (TAM) proposed by Fred Davis in 1986. Davis (1986) defined Perceived usefulness as “*The degree to which an individual believes that using the particular system would enhance his or her performance*” and Perceived ease of use is defined as “*the degree to which a person believes that using a particular system would be free of effort*”. According to him attitude of the user towards the acceptance of new technology or information system is determined by perceived usefulness and perceived ease of use.

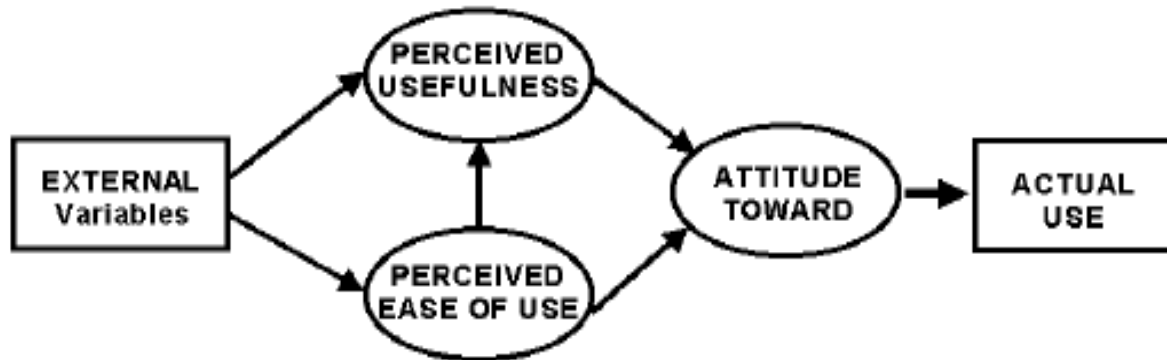


Figure 2.2. Technology Acceptance Model (TAM)

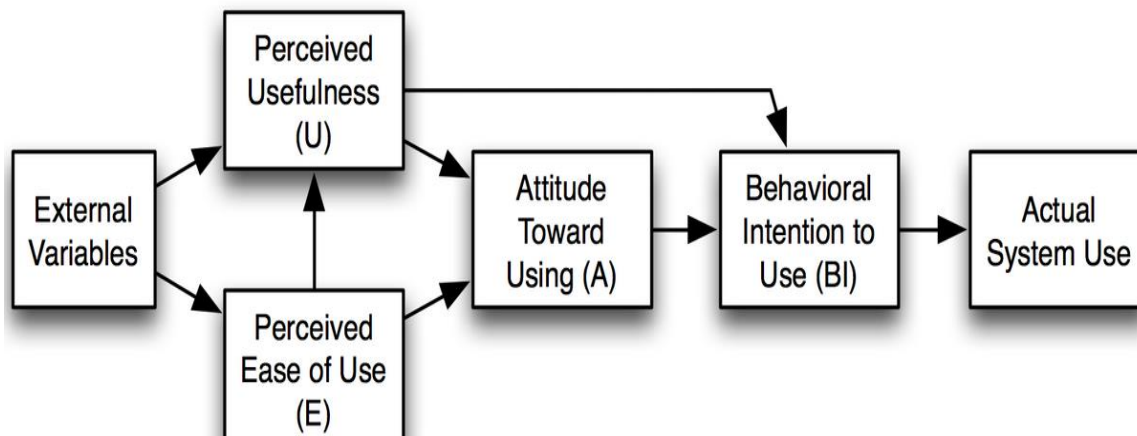


Figure 2.3. The Technology Acceptance Model, version 1. (Davis, Bagozzi & Warshaw 1989)

2.5.3. Theory of Planned Behavior (TPB)

Theory of Planned Behavior is an extension to TRA, it has taken into account one additional construct i.e. Perceived Behavioral Control (PBC). Perceived behavioral control refers to the people's perceptions of their ability to perform a given behavior in a controlled manner. PBC is further influenced by control beliefs and perceived Power or perceived facilitation. Control beliefs refer to the perceived presence of those factors that may facilitate or impede the performance of

behavior. Perceived power specifies the power to have the resources that are required to use a specific system.

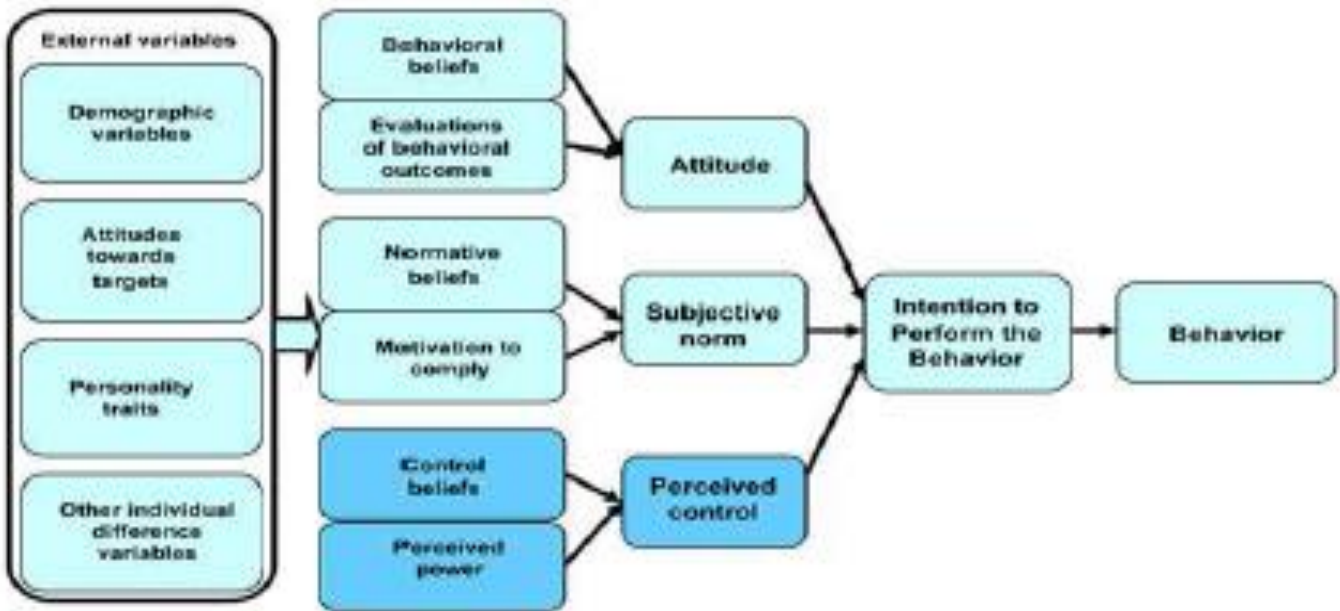


Figure 2.4. Theory of Planned Behavior (TPB)

2.5.4. Innovation Diffusion Theory (IDT)

Rogers (2003) described the innovation-diffusion process as “an uncertainty reduction process” and he proposes attributes of innovations that help to decrease uncertainty about the innovation. Attributes of innovations include five characteristics of innovations:

- Relative advantage
- Compatibility
- Complexity
- Trial ability
- Observability

Rogers (2003) stated that “individual’s perceptions of these characteristics predict the rate of adoption of innovations”. Rogers (2003) defined the rate of adoption as “the relative speed with which an innovation is adopted by members of a social system”, Relative advantage as “the degree to which an innovation is perceived as being better than the idea it supersedes”, “compatibility is the degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters”, complexity as “the degree to which an innovation is perceived as relatively difficult to understand and use”, “trial ability is the degree to which an

innovation may be experimented with on a limited basis”, observability as “the degree to which the results of an innovation are visible to others”.

To summarize, Roger argued that innovations that offer a more relative advantage, compatibility, simplicity, trial ability, and observability will be adopted much faster as compared to others.

2.5.5.Unified Theory of Acceptance and Use of Technology Model (UTUAT) Model

This model is based on the theories of individual acceptance that are synthesized by Venkatesh, Morris, and Davis, (2003),which includes the Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Motivational Model (MM), Theory of Planned Behavior (TPB), Model Combining the Technology Acceptance Model and Theory of Planned Behavior (C-TAM-TPB), Model of PC Utilization (MPCU), Innovation Diffusion Theory (IDT), and Social Cognitive Theory (SCT). Venkatesh (2003),defined Performance expectancy as the degree to which an individual believes that using the system will help him/her to attain gains in job performance, Effort Expectancy as the degree of ease associated with the use of the system, Social Influence as the degree to which an individual perceives what important others believe, he or she should use the new system and Facilitating Conditions as the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system.

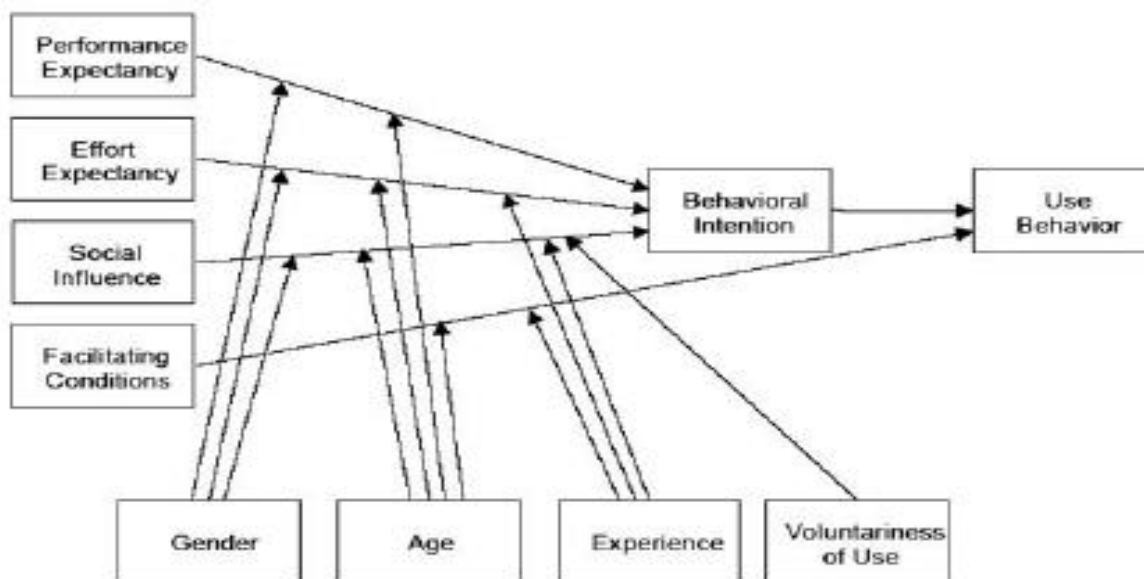


Figure 2.5. Unified Theory of Acceptance and Use of Technology Model (UTUAT) Model

2.5.6.Protection Motivation Theory (PMT)

Towards investigating the protective behavior of mobile banking users, this study mainly adopt protection motivation theory (PMT). PMT, originally rooted in the health filed, is a useful theoretical framework that explains a socio-cognitive phenomenon that the individual go through

in deciding a security behavior to exercise (Floyd, et al., 2000; Crossler & Belanger, 2014). PMT has been used as a lens to understand the behavior of individual about the performance of security measures (Lee and Larsen, 2009 ;), policy compliance (Ifinedo, 2012), data backup (Crossler, 2010), securing home networks (Woon et al., 2005), and adoption of anti-plagiarism software (Lee, 2011). In a cross-cultural context, Chen (2012) adopted PMT to investigate how individuals in US and China perceive and dealt with online security threats. Further, recently Jansen (2015) developed a conceptual model based on PMT to study the safe online banking behavior (Jansen, 2015). Similarly, in this study we can claim the applicability of PMT to examine how bank customers perceive and dealt with mobile banking security threats.

The basic assumption of PMT is that the individual protection motivation arises from the cognitive process (known as threat appraisal) that a threatening event is dangerous and likely to occur, together with the belief that a suggested coping appraisal can effectively avert its occurrence (Milne et al., 2000; Lee & Larson, 2009; Floyd, et al., 2000). Threat appraisal is associated with the individual evaluation of the likelihood and impact of a threatening event (danger), while coping appraisal is associated with the individual evaluation of possible coping strategy against the threatening event. According to the theory the cognitive process is usually driven by information source, which could have environmental and interpersonal source (Crossler & Belanger, 2014). In this study we are arguing that these cognitive processes affect the individual protection motivation in mobile banking security.

Threat appraisal, which concerns with the individual estimation of the degree of threatening security event, is described by two construct - perceived vulnerability and perceived severity. These in turn form the individual perceived risk. In this study in line with the definition by Yousafzai et al. (2003) perceived risk is defined as “the potential of loss in the pursuit of a desired outcome from using” mobile banking services. It is the assumption that changes in individual behavior is directly affected by the degree of perceived risk. Perceived vulnerability concerns with the individual beliefs that a threatening event is likely to occur (Yousafzai et al., 2003; Jansen, 2015). It has a direct effect on individual risk perception (Jansen, 2015). In our case it can be the individual perception of how likely he/she would be the victim of mobile banking fraud. Increased perceived vulnerability will likely increase the individual perceived risk, which in turn motivate the individual for more secured practices. Perceived severity is “an individual’s assessment of the severity of the consequences resulting from a threatening security event” (Crossler, 2010). When the individual perception of the consequence of a threat is increased, it is likely that this will

increase perceived risk, which in turn increases the motivation of individual to protective action (Jansen, 2015).

According to the PMT, the individual threat appraisal usually followed by a cognitive process called coping appraisal. Coping appraisal, according to Crossler (2010) is:

An individual's assessment of his ability to perform a given behavior and his confidence that a given behavior will be successful in mitigating or averting the potential loss or damage resulting from a threatening security event, at a perceived cost that is not too high.

It is related to the individual's assessment of the effectiveness of the proposed adaptive behavior to avert the threat (i.e., response efficacy) and the perceived ability to conduct the advocated behavior (i.e., self-efficacy), and associated cost (i.e., response cost). Based on the idea of Milne et al., (2000) and Jansen (2015), response efficacy can be conceptualized as the individual belief that applying the bank's recommended coping strategy is more likely reduce the mobile banking threat. Self-efficacy is concerned with the individual ability and confidence to perform the recommended coping measures or actions (Milne et al, 2000). In this line, when the individual self-efficacy increased, this will likely increase the individual safe behavior in using mobile banking. Response cost deal with the cost that the individual is likely to incur while perusing the recommended response (Milne et al., 2000). According to Jansen (2015), the cost could be anything from financial to time sacrificed. High response cost is likely to decrease the individual willingness to demonstrate the recommended response. In our case response cost can be conceptualized as the individual belief that practicing the bank's recommended activities will cost me much in terms of money and time.

2.6. Related Works using different theoretical models

Customers' Perception of M-banking adoption in Kingdom of Bahrain: An Empirical Assessment of an Extended TAM model.

This research aims at extending the Technology Adoption Model (TAM) to incorporate the role of factors in influencing customers' perception towards M-banking adoption. The results reveal that the intention to adopt is mainly affected by specific factors which are: Perceived Usefulness and Ease of Use. On the other hand, some factors such as perceived cost and perceived risk did not show any effect on the users' intention to use mobile banking. The result of this research is beneficial for banking service managers to consider the factors that can enforce the Mobile Banking services adoption and increase the take-up of their mobile services. With intensive banks competition and the popularity of mobile device use, there is an urgent need to understand the

factors that would attract customers to adopt Mobile banking. Thus, understanding the essentials of factors that determine user Mobile banking adoption can provide great management insight into developing effective strategies to remain competitive and hold market share. So, in their research they aimed to propose an extended Technological Adoption Model for Mobile Banking (ETAMMB) to incorporate the role of factors influencing customers' perception towards M-banking adoption. In addition, the extended TAM was evaluated empirically to measure its impact on M-banking adoption. To conclude all the relations, their study shows that the intention to use mobile banking is mainly affected by the perceived usefulness, perceived risk and ease of use.

An analysis of Mobile Banking Acceptance by Malaysian Customers.

The researchers here argued that there is a need to understand the extent of acceptance of mobile banking by customers and to examine the factors affecting intentions to use it for financial transactions. In order to determine the factors influencing the acceptance of mobile banking by customers, this study adopts the Technology Acceptance Model (TAM) as one of its research instruments. TAM was chosen in this study for two main reasons. First, TAM is based on its predictive power which makes it easy to apply in different information system devices (Luarn and Lin, 2005; Kleijnen *et al.*, 2004). Second, TAM helps to better understand the relationship between six important constructs of the study, notably, perceived usefulness, perceived ease of use, perceived credibility, perceived self-efficacy, normative pressure and behavioral intention. In this study, perceived credibility, perceived self-efficacy and normative pressure are added to enhance the understanding of customer acceptance of mobile banking beyond the general constructs used in TAM. Thus, the study aims to obtain insights into the factors that can influence the adoption of mobile banking among bank customers in Malaysia. It is hoped that the results of this study will extend current knowledge on technology acceptance and in mobile banking, in particular. Furthermore, the study may provide deeper insights into what is needed in order for bank customers to accept this emerging technology and, thus, allow for improvement in bank strategies to attract potential users of mobile banking. Perceived usefulness and perceived ease of use are the fundamental elements of TAM.

Based on previous findings, it is highly predictable that the general causalities found in TAM are also applicable to mobile banking.

Factors influencing the use of M-banking by Academics: Case Study SMS-Based M-banking.

There are several advantages with M-banking. Several related studies have shown that M-banking and indeed SMS-based mobile banking applications have become popular in many countries in

Europe and America. The phenomenon remains not widely used in many others such as Nigeria. This study identified and investigated the factors that influence academics in Nigeria to use M-banking with focus on the evaluation of SMS-based mobile banking. The research model was adopted from the Unified Theory of Acceptance and Use of Technology model (UTAUT). A survey questionnaire was administered to collect data from 150 academic staff and 350 university students of the University of Ilorin, Nigeria. The results show a positive correlation between customer service, type of bank and perceived ease of use and the use of M-banking. The implications of the results are crucial for technology adoption research and managers of banks in Nigeria. The main purpose of this study was to investigate the influence of factors such as customer service, bank /brand, perceived usefulness (PU) and perceived ease of use (PEOU) on the use of M-banking by academics in the context of Nigeria.

Constructs of the modified UTAUT model such as facilitating conditions, effort expectancy (perceived ease of use), performance expectancy (expectations) and social influence (social factors) constitute the variables for the this research undertaken.

Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry.

In this study a research framework was developed based on technology-organization environment model (TOE) which was developed by Tornatzky and Fleischer. The result of the study indicated that, the major barriers Ethiopian banking industry faces in the adoption of Electronic banking are: security risk, lack of trust, lack of legal and regulatory frame work, Lack of ICT infrastructure and absence of competition between local and foreign banks. Many researchers have been used different frame works in the study of adopting new technological innovation. Among frameworks that have been developed based on the past studies includes, the Technology-organization-Environment framework (TOE) (Tornatzky & Fleischer 1990), which identifies three basic Factors for the adoption of technological innovation, i.e., technological factors, organizational and environmental factors. TOE framework was proposed by Tornatzky and Fleischer; it is designed for studying the likelihood of adoption success of technology innovations. The technology adoption within an organization is influenced by factors pertaining to the technological context, the organizational context, and the external environment. Based on this, the researcher adopts the TOE framework to summarize possible key factors affecting E-banking adoption.

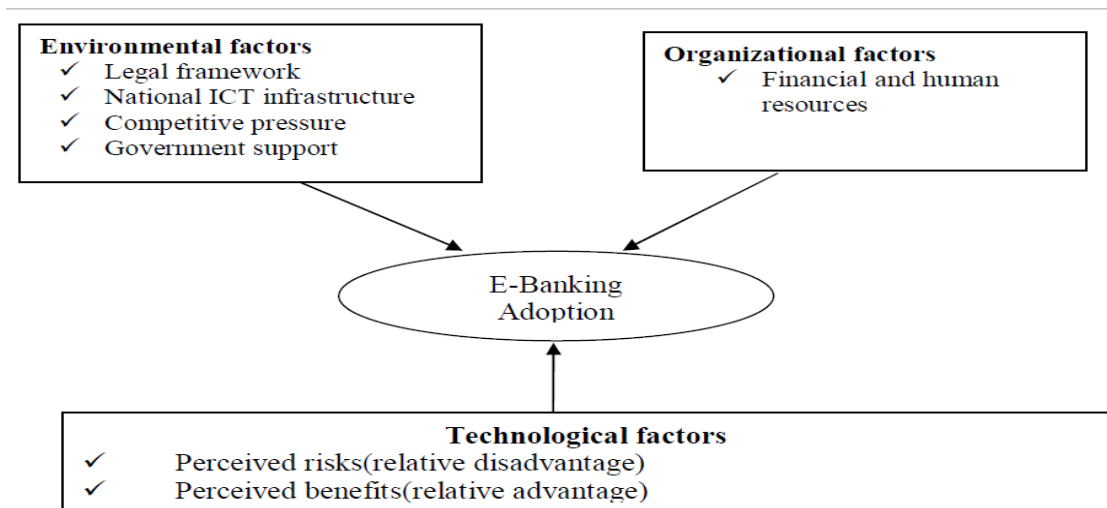


Figure 2.6: Technology-Organization-Environment framework

Analysis of Factors Influencing Customers’ Intention to the Adoption of E-Banking Service Channels in Bahir Dar city: An integration of TAM, TPB AND PR.

In this study a conceptual framework was developed by integrating six variables from theory of planned behavior, technology acceptance model and previous studies. The findings from this study revealed that attitude, subjective norm, perceived behavioral control, perceived usefulness and perceived ease of use and perceived risk were significant in affecting users’ intention to use e-banking service channels.

The construct perceived behavioral control emerged as a dominant factor followed by attitudes and perceived usefulness in predicting an individual’s intention to adopt e-banking service channels. Finally, attitude is jointly predicted by perceived behavioral control, perceived usefulness, perceived ease of use and perceived risk while perceived ease of use contributed more for the variation in attitude.

The measurement of customers’ intention of to adopt e-banking service channels in Bahir Dar city is undertaken with the aid of TAM, TPB and PR variables.

The extension of the original theory of reasoned action had led to the formation of the theory of planned behavior with the introduction of a new construct; perceived behavioral control to the earlier variables of TRA (attitude and subjective norms). According to this theory, perceived behavioral control is a situation in which the resources and opportunities available to a person must to some extent dictate the likelihood of behavioral achievement. But the greater psychological interest than actual control, however, is the perception of behavioral control and its impact on intentions and actions (Ajzen, 1985).

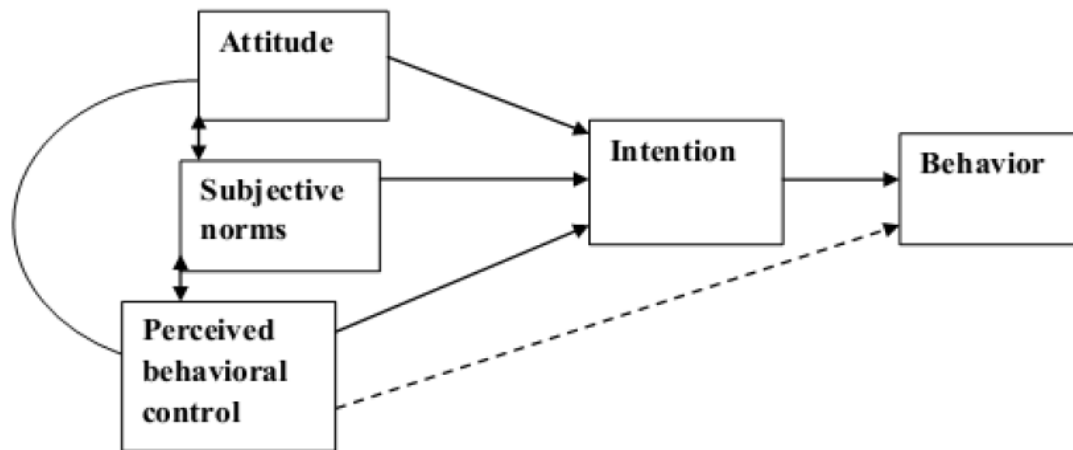


Figure 2.7. The theory of planned behavior.

2.7. Summary of related researches

Literature reveals that research on electronic banking has focused on Internet banking, whereas research focusing on mobile banking receives little attention. Table (2.0) presents a summary of empirical and theory-based empirical researches done about customers' perception on mobile banking adoption and on the mobile banking technology in general.

Authors	Theories	Sampling	Main findings
Laforet and Li(2005)	Attitude, motivation and behavior	300 respondents randomly interviewed	Awareness, confidential, and security, past experience with computer and new technology are salient factors affecting mobile banking adoption.
Luam and Lim(2005)	Extended TAM	180 respondents surveyed at e-commerce exposition and symposium.	Perceived self-efficacy, financial costs, credibility, ease of use and usefulness had remarked influence on the intention to adopt mobile banking.
HANUDIN AMIN , RICARDO BABA, MOHD ZULKIFLI MUHAMMAD(2006)	TAM	Purposive sampling is done for 250 customers.	Determinants are perceived usefulness, perceived ease of use, perceived credibility and perceived self-efficacy. Normative pressure was found to be a weak determinant in explaining bank customers' intention to use mobile banking. The study also demonstrates the significant effect of perceived ease of use on behavioral intention through perceived usefulness.

Laukkanen (2007)	Mean -end theory	20 qualitative in-depth interviews conducted	Perceived benefits (i.e. location free and efficiency) are the main factors encouraging people to adopt mobile banking.
Amin et.al(2008)	TAM	156 respondents surveyed via convenient sampling	Perceived ease of use, perceived usefulness, credibility, amount of information and normative pressure significantly influence the adoption of mobile banking.
Koenig-Lewis et al(2010)	TAM and IDT	155 customers aged 18-35 surveyed online.	Perceived usefulness, compatibility and risk are significant factors while perceived costs, ease of use credibility and trust are not salient factors for the adoption of mobile banking.
Sripalawat et al(2011)	TAM and TPB	195 questionnaires collected via online	Subjective norm is the most influential factor, and the next are perceived usefulness and self-efficacy for the mobile banking adoption.
Dasgupta et al(2011)	TAM	325 usable questionnaires were gathered	Perceived usefulness, ease of use, image value, self-efficacy and credibility significantly affect intentions towards mobile banking usage.
Gbolahan Olasina(2015)	UTAUT	A survey questionnaire To 150 academic staff and 350 university students.	The results show a positive correlation between customer service, type of bank and Perceived ease of use and the use of m-banking.

Yitbarek Takele and Zeleke Sira(2013)	Integrating six variables from TPB, TAM and previous studies.	A moderately representative sample was obtained by stratified sampling technique	The findings revealed that attitude, subjective norm, perceived behavioral control, perceived usefulness and perceived ease of use and perceived risk were significant in affecting users' intention to use e-banking service channels.
Ali AlSoufi1 and Hayat Ali2(2014)	extended TAM	The model Was evaluated using a sample survey of 372 customers.	The results reveal that the intention to adopt mobile banking is mainly affected by specific factors which are: Perceived Usefulness and Ease of Use. On the other hand, some factors such as perceived cost and perceived risk did not show any effect on the users' intention to use mobile banking.
Ayana Gemechu Bultum(2014)	TOE	The study statistically analyzes data obtained from the survey questionnaire.	The result of the study indicated that, the major barriers Ethiopian banking industry faces in the adoption of Electronic banking are: security risk, lack of trust, lack of legal and regulatory frame work, Lack of ICT infrastructure and absence of competition between local and foreign banks.
Mohammed Arif Shaikh(2014)	This study was conducted using attributes identified after a detailed literature review.	The study used a questionnaire for 78 respondents.	As per the findings of this study it is observed that bankers perceive a means to save time and minimize inconveniences as the most and the least advantage of electronic banking, whereas Need for expertise and training and charge a high cost for services are considered as the most and the least risk associated with electronic banking.

Henok Arega Asfaw(2015)	An exploratory research design is utilized.	In-depth interview with 6 Vice-Presidents of System and E-banking.	The study reveals that there are no operational challenges that hinder the flourish of m-banking development in Ethiopia. However, lack of timely approval of new products by regulatory body, lack of interoperability system and lack of aggregators between service provider and retail agents were the major problems observed in the study.
----------------------------	---	--	---

Table 2.0: Some summary of empirical and theory-based empirical researches.

Most of the researches from the above table indicated that there is a lot of work done on the mobile banking adoption, on other e-banking services , on different factors affecting these services and also about perception of customers' towards these services. Where as a research that focuses particularly on the individual security related behaviors towards online banking services receives little attention unlike the other online banking services. So a research trying to identify these individual security related behaviors towards online banking services more specifically mobile banking, will have too much contributions towards the area.

2.8. Theoretical framework (Protection Motivation Theory)

In Ethiopian context the mobile banking related works are too limited. Most of the researches or studies explained above focused more on the adoption of mobile banking and customers' perception towards mobile banking, similarly on the mobile banking technology in general, so our particular research tries to look on perception of customers specifically to the security concerns of mobile banking. Therefore, to address the current gap in the literature, this study is designed to identify the customers' perception of mobile banking security particularly the Commercial Bank of Ethiopia in Addis Ababa. *It is recognized that research is scarce in the domain of individual security related behavior (Liang and Xue, 2010).* Anderson and Agarwal (2010) stated for example: "there is limited Understanding of what drives home computer users to behave in a secure manner online, and even less insight into how to influence their behavior". Based on these, (Jansen, 2015) concluded that the PMT is a suitable theory to take as a starting point for further study. In literature, no further studies were found that applied the PMT to online banking to identify individual security related behavior, but in a cross-cultural context, Chen (2012) adopted PMT to investigate how individuals in US and China perceive and dealt with online security threats. By applying the PMT to a new territory, it can be assessed whether the PMT, extended with additional variables, maintains its value.

Therefore by adding additional variables to PMT, which are the main important factors/variables/ (perceived ease of use and perceived usefulness) from TAM as indicated from the previous literatures and researches, we can assess whether the PMT when extended with additional variables maintain its value or not. So our particular research will be the other to apply PMT with some additional variables from TAM model to study the customers' perception towards mobile banking security. This makes our particular study more comprehensive since it adapts the two important determinant variables from TAM model.

So our study will utilize the PMT model and some basic constructs of TAM to investigate customers' perception of mobile banking security. Moreover, this study outlines the details of each construct and its relevance toward the research issue.

On the other hand there should be a reason for selecting PMT primarily to our particular study. So when we look at available researches or studies much is done on the adoption of the technology and customers' behavior. There is an indication that it remains a lot to be done on the perception

of customers (individual security related behavior) towards online banking security of which our particular focus is mobile banking security.

According to Floyd et al. (2000) there are several theories that try to explain and predict behavior. For example, in information systems research already much is known about the adoption of technology. Technologies that have been studied are often beneficial technologies (Chenoweth et al. 2009), of which online banking is an example. Regarding the use of protective technologies, which are focused on preventing negative outcomes, less is known (Chenoweth et al. 2009). Few studies have been conducted on security behavior of end users/customers/ and on how such behavior can be changed (Ng et al. 2009). Research has shown that there are significant differences between the use of beneficial and protective technologies (Dinev and Hu, 2005). Therefore, other theories than adoption theories may be more appropriate. After evaluating several psychological theories, the PMT (Rogers, 1975) is chosen as the basis for the study of safe online banking behavior, a social cognitive theory that predicts behavior (Milne et al. 2000). According to Jansen (2015) the main reasons for this choice are as follows. The PMT has been successfully applied to understand and predict the use of various protective measures (Milne et al. 2000) and is considered one of the most powerful explanatory theories for safe behavior (Floyd et al. 2000). The theory is applied, sometimes in an adjusted form, to the field of information systems and has been found useful in predicting individual computer security behavior in both home (Crossler, 2010 ;) and working situations (Ifinedo, 2012; Lee and Larsen, 2009), making it a useful theory for studying safe online banking behavior. Strength of the PMT is that it includes the concept of risk, which is neglected in adoption theories (Jansen, 2015). Furthermore, attention is not only paid to the predicting variables, but also to how these variables are related. Finally, the theory is useful for the development of interventions (Floyd et al. 2000). The Protection Motivation Theory functions as the core of the model. The model is extended with additional variables, making it suitable for the whole online banking context. The coping perspective, which is central to the Protection Motivation Theory, seems to be valuable to study behavior in information systems.

By taking a cognitive behavioral perspective, it can be examined how individuals cope with threats, which may contribute to the development of effective intervention programs aimed at safe online banking in general. It thus become appropriate that we utilize the conceptual research model proposed to study safe online banking behavior. As exhorted by J. Jansen (2015), studying Safe Online Banking Behavior: A Protection Motivation Theory Approach, our research using PMT as

the core of the model also serves as a part of that continued effort to ensure confirmatory application of the model in new technology and country settings to explore the factors that affect customer perception towards mobile banking security in Ethiopia.

2.8.1. The Protection Motivation Theory and its constructs

There are two cognitive processes which are central to the PMT, namely threat appraisal and coping appraisal. In the threat appraisal process, individuals evaluate the likelihood and impact of a threat. This is followed by the coping appraisal process in which individuals evaluate possible coping strategies against the threat. This process is driven by the effectiveness of a strategy or measure, the degree to which the individual is able to perform the required action and the costs involved. The cognitive processes are initiated by receiving information, which is called sources of information, and includes environmental and interpersonal sources. Both processes in their turn affect the protection motivation, i.e. the intention to perform certain behavior.

2.8.2. Threat appraisal

In the threat appraisal process, an estimate is made about the threat event. This is performed initially, because a threat must be observed first before one can assess coping strategies (Floyd et al. 2000; Liang and Xue, 2009).

Crossler (2010) defines this threat appraisal process as “an individual’s assessment about the level of danger posed by a security event”. Threat appraisal consists of the constructs perceived vulnerability and perceived severity, which both make up perceived risk. The rewards construct is also part of the threat appraisal process. However, rewards are barely operationalized in PMT studies (Milne et al. 2000). This is mainly because the conceptual difference between the value of a reward for risky behavior and the response costs for a security measure is not always clear (Abraham et al. 1994). Therefore, this construct is dropped. For threat appraisal one additional construct is added, namely trust in online banking in our case trust in mobile banking. In the context of online banking, perceived risk is defined as “the potential of loss in the pursuit of a desired outcome from using electronic banking services” (Yousafzai et al. 2003). When a risk is perceived, individuals will change their behavior based on how much risk they are willing to accept for the particular threat (Workman et al. 2008). Based on this notion, it is expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures. Perceived vulnerability is “an individual’s assessment of the probability of a threatening security event occurring” (Crossler, 2010). This involves an individual’s believe on how likely it is to be

victimized by online banking fraud. It is expected that perceived vulnerability has a positive influence on perceived risk. The perceived impact of a threat is “an individual’s assessment of the severity of the consequences resulting from a threatening security event” (Crossler, 2010). This involves how serious the consequences of online banking/mobile banking/ fraud are perceived. It is expected that perceived severity of a threat has a positive influence on perceived risk.

Liang and Xue (2010) argued that perceived vulnerability and perceived severity have an interaction effect on the formation of perceived risk. They state that perceived risk is a calculation of probability multiplied by impact and that when one of the two is zero, the perceived risk disappears. Literature on online banking adoption such as mobile banking has repeatedly shown that a high level of trust reduces the perception of risk (e.g. Yousafzai et al. 2009).

2.8.3. Coping appraisal

Assessing of threats by itself is not enough. When individuals feel vulnerable and think that the potential severity of a threat is high, this does not change their behavior immediately. There are additional barriers that must be overcome (Furnell et al. 2006). The coping appraisal process includes an evaluation of the estimated coping strategies to avoid or minimize the threat. Crossler (2010 p.2) defines this process as “an individual’s assessment of his ability to perform a given behavior and his confidence that a given behavior will be successful in mitigating or averting the potential loss or damage resulting from a threatening security event, at a perceived cost that is not too high”. Threat appraisal consists of the constructs response efficacy, self-efficacy and response costs.

Response efficacy “concerns beliefs about whether the recommended coping response will be effective in reducing threat to the individual” (Milne et al. 2000). If the individual is sufficiently satisfied that the protective measure will actually work, then that is an incentive to apply it. Liang and Xue (2010) argued that it is possible that response efficacy, what they call safeguard effectiveness, interacts with perceived risk. Self-efficacy “concerns an individual’s beliefs about whether he or she is able to perform the recommended coping response” (Milne et al. 2000).

Rhee et al. (2009) studied self-efficacy and its impact on safe behavior by end users and also Rhee et al. (2009) speak of self-efficacy in information security, which they define as “a belief in one’s capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability”. The assumption is that the higher the self-efficacy in terms of taking safety measures, the more an individual will be inclined to take such

measures. Response costs “concern beliefs about how costly performing the recommended response will be to the individual” (Milne et al. 2000). This involves both tangible and intangible costs. When the costs of applying safety measures exceed the costs of a potential threat, then the response costs have a negative influence on protection motivation.

2.8.4. Protection motivation

The protection motivation is the decision or intention to proceed to, continuation of, or the avoidance of the studied behavior (Floyd et al. 2000). “Protection motivation is an intervening variable that has the typical characteristics of a motive: it arouses, sustains, and directs activity” (Rogers, 1975). The protection motivation can manifest itself in an adaptive or maladaptive coping response. An adaptive response implies that customers protect themselves. A maladaptive response is the opposite, namely that customers do not protect themselves. This response suggests that an individual is at risk.

In our study, the PMT is applied to explain why mobile banking customers adopt the desired behavior, i.e. an adaptive coping response. The desired behavior is compliance with the unified rules for safe online banking/in our case trust in mobile banking/, the outcome variable of the conceptual model. Thus, the independent variable consists of multiple actions. This is, however, not an issue considering that securing online banking/mobile banking/, as is the case with securing a computer, “is about performing a number of different practices, not one in particular” (Crossler and Belanger, 2014). These authors furthermore state that a more holistic view on safe behavior is acquired when measuring multiple behaviors instead of one. In information systems research, it is preferred to measure actual behavior instead of intentional behavior (Anderson and Agarwal, 2010; Workman et al. 2009). However, this will be difficult to achieve. Therefore, it is chosen to measure intentional behavior. Anderson and Agarwal (2010) who also studied intentional behavior instead of actual behavior justified their choice by findings from earlier studies which indicated that the relationship between intentional and actual behavior is strong, consistent and theoretically grounded.

2.9. Trust and Perceived risk

Prior studies, Jansen, (2015), and Luo, Li, Zhang, & Shim (2010), also found out that trust also play a vital role in the acceptance of mobile banking adoption. In the current study we also claim that trust in mobile banking is likely to decrease the individual perceived risk. This will increase the willingness of the individual to pursuit his transaction using mobile banking.

Trust plays a central role in exchange relationships involving unknown risks (D. Gefen, E. Karahanna, D. Straub (2003), S.L. Jarvenpaa, N. Tractinsky. (1999)). In case of wireless banking, like mobile banking, customers need to rely on trust to overcome their risk perceptions. The potential risks may come from multiple sources such as the vulnerability of wireless and Internet communication platforms and the technical capability of banks.

Based on the suggestion of McKnight et al. (2001), I selected two dimensions of trust from the trust topology which I think are important for my particular study. These are structural assurance, and trust belief.

Structural assurance (SA) is the trust perception about the institutional environment (D.H. McKnight, N.L. Chervany, C. Kacmar. (2002)). In the context of mobile banking, SA is the perception about the availability of the necessary legal and technical structures such as encryption, promises/guarantees, insurances, regulations, or other procedures in the wireless Internet to ensure the successful completion of financial transactions with a bank.

Trust belief is the perception that the trustworthiness of the vendor consists of a set of specific beliefs about integrity, benevolence, and competence (D. Gefen, E. Karahanna, D. Straub. (2003), D.H. McKnight, N.L. Chervany, C. Kacmar. (2002)).

2.9.1. Perceived risk and trust belief

Trust belief has been found helpful in explaining how customers may overcome perceived risk and engage in online transactions (S.L. Jarvenpaa, N. Tractinsky. (1999), N.K. Malhotra, S.S. Kim, J. Agarwal. (2004)). Trust plays a critical role in mitigating perceived risks, especially for transactions involving uncertainty (S.L. Jarvenpaa, N. Tractinsky. (1999)). Because MB(mobile banking) is still in the initial adoption stage, customers are unclear about the technical capability of their banks to provide MB service and about the reliability and security of the Internet and wireless communication channels in delivering their sensitive financial data, among other concerns. The existing trust beliefs toward a bank are relied on as one of the major leverage points for customers to assess the potential risks involved in the wireless banking service provided by that bank. Customers who believe in the technical capability, integrity, and benevolence of their banks are more likely to overcome their risk perceptions toward new services such as the wireless banking situation. Therefore, considering the uncertainties in MB, the stronger the trust a customer has toward a bank, the lower the risk he or she anticipates in adopting mobile banking.

2.9.2. Perceived risk and structural assurance

Online transactions, in general, raise security and privacy concerns among users (T. Teo, M. Tan, and SN. Peck. (2004)). Similar to trust belief, structural assurance such as promises, guarantees, and contractual protections should also help alleviate customers' perceived risk in the unfamiliar, open airwave environment. MB service providers can draft customer service policies, use advanced encryption technologies, and make promises (e.g. 100% satisfaction guarantee, monetary refund, protection of privacy, and accurate transaction information) to relay structural assurance information to MB users. As such, customers who trust the legal and technology structures of the wireless Internet will be more likely to believe their financial data will be protected against loss or theft along transmission. Such belief in the structural soundness of the wireless Internet platform is anticipated to lower the perceived risk in wireless banking. Trust is not often integrated in PMT studies. However, it is an important construct in risk literature.

2.10. Perceived ease of use and perceived usefulness

The widely used adoption model for technology is technology acceptance model (TAM) which is developed by Davis in 1989. TAM is technology acceptance model that measures people perception towards using the technology. To measure user's perception towards the technology TAM use three main factors which are perceived ease of use, perceived usefulness and attitude towards using the system. The two most important component of TAM are perceived usefulness (PU) and perceived ease of use (PEOU), Perceived usefulness in relation to IS was defined by Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance". And perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free from efforts".

Hu et al. (1999) suggested that many factors influence initial acceptance of technology, but fundamental determinants like perceived ease of use and perceived usefulness play a greater role in continued acceptance.

Perceived usefulness: It is believed that an innovation perceived to be useful is more likely to be adopted and customers will take advantage of the innovation such as mobile banking which they find useful to them (Luarn & Lin 2005). Perceived usefulness is one of the two most important factors affecting the acceptance of new technologies or information system.

Perceived ease of use: It is believed that a customer will adopt an innovation or a particular system if it is easy to learn and use (Davis, 1985). An innovation perceived to be difficult to use by customers will be less adopted (Rogers, 1983). According to Cooper and Zmud (1997), ease of use of an innovation is one the most important characteristics for adoption of an innovation. Adoption of mobile banking is more likely to occur if the process of usage is easy for customers. So the two important factors of TAM, PU and PEOU also play an important role during mobile banking usage.

2.11. The model

The arrows in this model indicate which variables have an impact on what other variables. A minus-sign means that a negative relationship is expected. In other cases, the expected relationship is positive. So our particular model takes primarily the constructs of PMT, then the two most important elements of TAM and also some constructs are taken from the concept of trust. These our framework will be more comprehensive to study customers security related behavior.

The final proposed conceptual model that will be adopted in this research will be as follows:

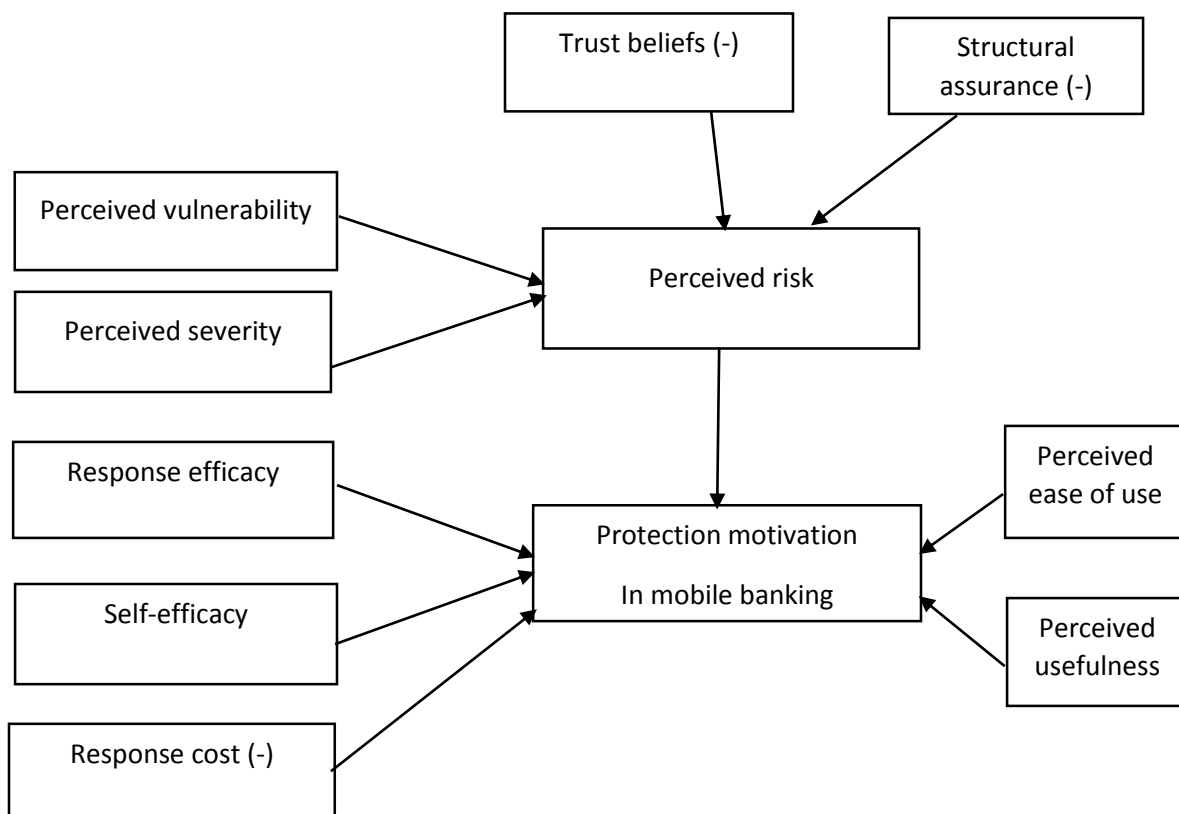


Figure 2.8. The theoretical/conceptual/research model adapted from PMT and TAM.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Introduction

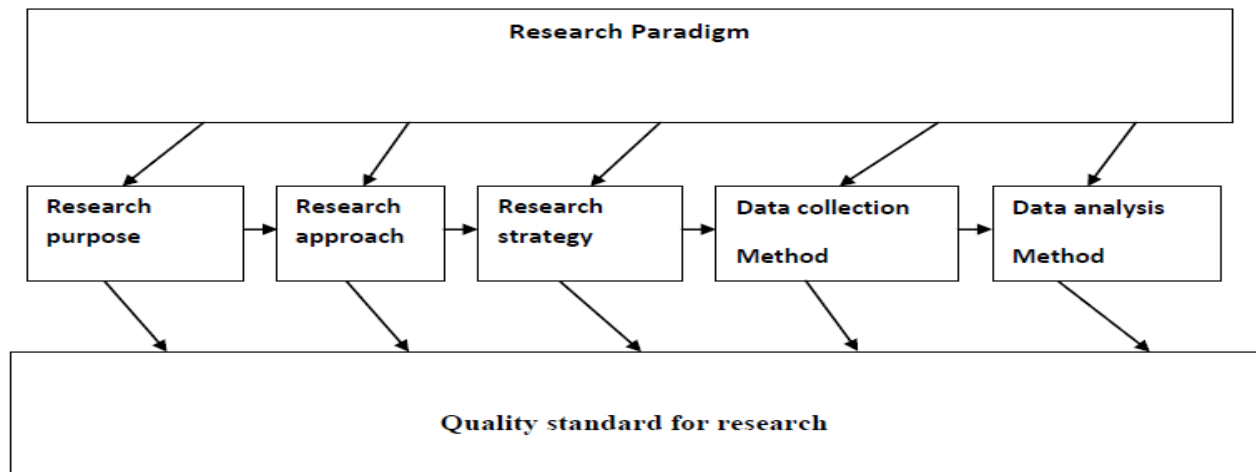
In the previous chapter, the literature review, which shows customers perception towards mobile banking security and review of issues related with mobile banking, has been presented. Accordingly, this chapter discusses about the methodology by which the researcher has used to conduct this study. Thus, overview of the methodology, research purpose, research approach, research strategy, types of research, research instruments, sample and data collection, data collection procedure, methodological limitations, data analysis tools and techniques, research model and hypotheses, related works and their methodologies, quality of research and finally conclusion are presented below respectively. So this chapter outlines the method that were used in answering the research questions.

3.2. Overview of Methodology

Many researchers have written extensively on research methodology. The underlying factor in most of the studies on research methodology is that the selection of methodology is based on the research problem and stated research questions. Methodologies cannot be true or false, only more or less useful (Silverman, 2001). Naichiamas *et al.* (1996) for instance states that methodologies are considered to be systems of explicit rules and produced, upon which the research is based, and against which claims for knowledge are evaluated. Conducting any type of research should be governed by a well-defined research methodology based on scientific principles. Research methodology can be again defined as a method or way to systematically solve the research problem (Blaxter et al 2006). In one way or another methodology is the overall approach which underpins the research process (Blaxter et al 2006).

The research method is the significant part of a research, because it helps researchers to decide how to achieve the specified objective, what data to collect, how to collect and analyze the data in order to solve the target problem. Therefore, it needs much attention on choosing the appropriate methods which can provide the desired outputs. The general objective of this research as described earlier is determining the factors that affect customers' perception towards mobile banking security and constructing a theoretical model for customers' perception towards mobile banking security.

According to Eldabi (2002), he suggested that a series of steps as a research paradigm to be followed in a methodology part of a research. Based on his suggestion our research followed the basic framework of research paradigm developed by Foster.



Source: Foster (1998)

Figure 3.1: Framework for the research paradigm

3.3. Research purpose

There are basically three types of academic researches depending on the problem area and the nature of the phenomenon that is to be studied. The purpose of the research can be Exploratory which deals with unknown problem, Descriptive in which there is an awareness of the problem and Explanatory, where the problem is clearly defined (Ahmed 2011).

The purpose of this research is to conduct an exploratory and descriptive research in order to gather as much information as possible concerning customers' perception towards mobile banking security. Our research is focused on describing the current situation of the problem and answer the research questions which are in the form of "what", and to highlight the most important factors that can negatively or positively affect the customers' perception towards mobile banking security. Moreover, this research aims to explain the phenomenon and assess the current situation of mobile banking. Therefore, Descriptive research was used for the purpose of our research.

Whereas exploratory research according to Yin (1994) is designed to allow a researcher to just look around with respect to some phenomenon, with the aim to develop suggestive ideas. Exploratory research is often used when a problem is not well known, or the available knowledge

is not absolute. The technique that is best suited for information gathering when performing an exploratory research is interview (Yin, 1994). It has also been demonstrated that exploratory research provides suggestive ideas through reviewing information from problem area. So this exploratory can also be used for the purpose of our research.

3.4. Research Approach

There are different approaches that are used when conducting a research. The most commonly used approaches in most of the research works are the quantitative and qualitative approaches and also inductive and deductive approaches (Amaratunga et al. 2001). These approaches will be briefly described below.

3.4.1. Qualitative and Quantitative Approaches

Our research mainly uses quantitative approach and to some extent qualitative methods were also used to increase the researchers' insights. In order to attain the objective of the study and answer the research questions; this research adopt both quantitative and qualitative (Mixed) research approach. The rationale of using such a mixed approach is to gather data that could not be obtained by adopting a single method and for triangulation (Creswell 2003). The quantitative research method involves gathering information and data which is evaluated through a statistical analysis. Quantitative research method gives clear presentation of finding and the result could be used for a larger population if it's well carried out. So to have a better understanding and detailed information about our research, quantitative approach was mainly used as it provides respondents to answer or explain their feelings and their opinions without being fear of their responses. Additionally qualitative approaches were also used. So this makes our research a little bit mixed approach type. When we look at Qualitative approach it is a participant observer research and this method involves getting information from respondents. Again this method can provide timely and detailed information if it is carried out appropriately (Denzin & Lincoln 2003).

Therefore we can say our research has used quantitative method as its primary approach and also qualitative method to increase the researchers' knowledge about the problem to be investigated. Generally by considering the research aim for this particular study, the quantitative and qualitative approaches were used through questionnaire distribution and interview respectively by taking into consideration at the proposed research framework.

3.4.2. Deductive and Inductive Approach

This research approach can be categorized into two, either deductive or inductive. Deductive approach is the testing of theories while inductive is building of theories (Perry 1998; Blaikie 2000; Gamage et al. 2008). When theories are formulated, it is tested to prove or falsify hypothesis which is deduced from the relationship of variables of past formulated theories (Gill & Johnson 2010; Saunder et al. 2009). The hypothesis should be tested in order to check if the data of the hypothesis matches the hypothesis (Blaikie 2000). Inductive approach is building up of theories as a result of data analysis collected, which could be obtained through observation of the empirical world (Saunder et al. 2009; Gill & Johnson 2010). The deductive approach was used in this research work because, the research sought to use existing theory which was adopted from the research framework to test the research hypothesis and, this is fast to carry out and is less risky (Saunder et al. 2009).

3.5. Research strategy

The most important condition for differentiating among the various research strategies is to identify the type of research question being asked (Creswell, 2003; Hair *et al.* 2006). It is possible to identify some situations in which all research strategies might be relevant and other situations in which two strategies might be considered equally attractive. We can also use more than one strategy in any given study. To this extent, the various strategies are not mutually exclusive. But we can also identify some situations in which a specific strategy has a distinct advantage (Yin, 1989). According to Yin (1994), there are five strategies to collect data and get results: experiment, survey, archival analysis, history and case study. In addition, there are three criteria to determine the research strategy: types of research questions, control over behavioral events, and focus on present events. But it is important to notice that boundaries among the above methods are not completely clear, they may overlap each other. The relevant situation for different research strategies are summarized in a table as follows:

Strategy	Nature of questions	Requires control over behavioural events	Focus on contemporary event
Experiment	How, Why	Yes	Yes
Survey	Who, what ,where, How, many, How	No	Yes
Archival Analysis	Who, What, Where ,How many, How much	No	Yes/No
History	How, Why	No	No
Case Study	How, Why	No	Yes

Source: Ahmed, 2011

Table 3.0. Characteristics of different research strategies

In our study, Survey approach has been chosen, because the research questions are focused on: What are factors that affect customers' perception towards mobile banking security. So the types of questions are in the form of "what". This research does not require control over behavioral events, but it focuses on current issues.

3.6. Types of research

Research types can be classified into two types and this could either be primary or secondary research depending on how the data collected was used (Various 2007). Secondary data collection has been the most common method of research and it involves the use of data which has already

been collected for other purposes (Nargundkar 2008), while Primary research is the collection of data for the specific purpose of study which is from the original source and this can be directly from customers (Various 2007). Primary data can be collected through survey (personal interview, telephone interview mailing of questionnaires and through schedules) or experiment (observation of quantitative measurement). Primary data is very important for the purpose of our research due to its relevant to our study and the richness of information that can be collected. Secondary data was also used in our research due to easy access to books, web sites, and materials from different libraries, related journal articles, etc. The data collected was used to review the individual security behavior and the data collected were also used to analyze and answer the research questions in order to achieve the research aim and objective. The secondary data serves as a help for the primary researches (Maria 2008). So our research has used both secondary and primary data in achieving the purpose of our research.

3.7. Research Instruments

As described earlier, the primary instrument that was used in this research study was questionnaire and interview. The Questionnaire is prepared after extensive review of literatures in this area, the questionnaire items focused on the research problems, objective and research questions. Pretesting of the questionnaires was conducted. Thus, to ensure content validity of the scales, some of the items chosen for the constructs were adapted from previous researches to ensure content validity and most of the other items were designed by the researcher.

The questionnaire contains three sections. But before this, it began with the introduction statement that is written parallel with the research questions and which shows the aim and the importance of the research study, in which it gives the respondents the assurance of confidentiality for every information provided. Section one contains the personal data which includes gender, age and occupation etc. Section two shows the perception of the respondents' towards mobile banking security based on the constructs derived from the theoretical frame work using yes/no and open ended questions. These questions were designed to give respondents more opportunity for an in depth answers; which they feel had influence their decision either positively or negatively.

Section three shows the questions that aim to identify the perceptions of customers towards mobile banking security or the factors that affect/influence the customers' perception towards mobile banking security using a five point Likert scale questions.

Similarly, interview was also used in this research work. An interview could either be structured

or unstructured. Structured interviews is a pre-planned discussion where questions are asked to get specific answers from respondents while unstructured interview is conducted by allowing respondents to bring up ideas which might lead to further investigation (McNabb 2002). So in order to improve the quality of the research work and for the researcher to have a better understanding of the subject matter, semi-structured interview was conducted first with the bank's internet and mobile banking manager and also telephone interview was conducted with some of the bank workers. It was consisting of a pre-determined open-ended question.

3.8. Pre-testing of the questionnaire

The questions were straight forward and easy to understand by taking a pre-test which was carried out on some individuals. It was pre-tested in order to detect any error and also for further improvement that may be needed in the questionnaires design (Willis 2005). It is also done to determine if the questionnaires are understandable and if the adopted survey procedure works or not (Crask, et al., 1995). The questionnaire may show some gaps such as ambiguity in the question, too many questions under each research framework, or some questions may be too long, etc., and adjustment was made on the research questions before it was finally distributed to the target respondent. The final questionnaires was distributed through in person that is face to face to the customers or respondents.

3.9. Sample and Data collection

The questionnaire was used as a survey instrument for this research work by collecting data from previous studies on customers' perception on mobile banking adoption. A survey is a powerful and effective tool that can be used to collect data about human attitudes, behaviors, and characteristics. The survey questionnaire is often adopted by researchers as an effective hypothesis testing method (Cavana et al., 2001). For example, in their prior study on mobile banking in Taiwan, Luarn and Lin (2004) used a questionnaire in the data collection phase. Data was collected via personally-administered questionnaires from different sources such as customers and bank workers, as they are also customers. The advantage of this method was that both the cost and the time required were low (Cavana et al., 2001). Reviewing prior studies on mobile banking, e-commerce and information systems, it was found out that many studies used questionnaires to collect data for analysis and research objective investigation. In this study a survey with questionnaires was implemented to explore customers' perception towards mobile banking

security. There was no technical jargon or difficult words in the questions, and closed-ended questions was used largely in the questionnaire. This is quite helpful as respondents could make a quick decision when answering the questions (Cavana et al., 2001), and it provided greater uniformity, thereby making data processing easier. Similarly defining the target population is an important step in designing the research project (Crask, et al., 1995). Target population is the specific population about which information is desired. According to Ngechu (2004), a population is a well-defined set of people, services, elements, events, group of things or households that are being investigated and to which the findings will be generalized. The target population of the study is customers of Commercial Bank of Ethiopia in Addis Ababa, particularly those having the mobile banking account. On the other hand selecting a sample is also a very important step for a positivistic study. Larger Sample size calculation is concerned with how much data we require to make correct decision on particular research. If we have more data, then our decision will be more accurate, but Greenfield et al. (2002) stated that this does not necessarily mean that more is always best in sample size calculation.

For example Hussey and Hussey (1997) noted that the sample should be unbiased and large enough to satisfy the needs of the research. It is impossible to survey the entire population of a particular study because of limited funding and time. Therefore it is necessary to survey a sample of the population as an alternative in order to formulate predictions about the entire population. So for our study as a sampling design we followed multistage cluster sampling. In stage one, ten branches of the bank are randomly selected (namely Silasie, St. Marry, Megenagna, Gurd Shola, Gerji, Yerer Ber, Jackros area, CMC, Saris, Gotera Shell Dipo branches). In stage two, 17 respondents are selected from each selected branch. For the selection of respondents a convenient sampling techniques was used due to difficulty of getting the bank customers or respondents as they are required, at some time and at some location. For the qualitative study purposive sampling method was used, which helps the researcher to select the appropriate person for the interview, for this study the central branch manager whom monitors the whole branches activity was considered since the service is controlled by the central bank.

The sample size is determined by the following formula:

$$\text{Initial sample size (No)} = \frac{P * (1-P) * Z^2}{D^2}$$

Final sample size (N1) = design effect*initial sample (No), so a total of 170 sample size is

determined. (See appendix 10 for the sample size calculation)

The Commercial Bank of Ethiopia was chosen as our study area because it is the pioneer state owned bank to start modern banking and e-banking services like ATM, internet banking and mobile banking (Mengistu, 2011) and questionnaires were distributed to bank customers and bank workers in capital city Addis Ababa, because majority of bank customers are located in the city (Yohannes, 2010). The samples of respondents will actually represent customers of banks who are users of mobile banking at Commercial Bank of Ethiopia in Addis Ababa. In order to ensure its suitability, a total of 150 respondents were considered out of 170 questionnaires that were sent out, because 150 of the questioners were properly filled and returned and 20 of the questioners were discarded. The questionnaires consisted of close ended and open ended questions and these were used in order to have a proper understanding, accurate and genuine information of the subject matter. The open-end questions will allow respondents to give their exact opinions (Russell & Jarvis 2008; Gratton & Jones 2004). In the closed ended questions a yes/no questions and also a five-point Likert scale, with anchors ranging from “strongly agree” to “strongly disagree”, was used in the questionnaire like Strongly Agree (SA) = 1; Agree (A) = 2; Neutral (N)=3, Disagree (D) = 4; and Strongly Disagree (SD) = 5.

3.10. Data Collection Procedure

A brief invitation and introduction to this research was provided to respondents before they started filling out the questionnaires. If they accepted the invitation, questionnaires will be handed out to them. Otherwise, they would not receive any questionnaires. If possible, after 30 minutes the completed, anonymous questionnaires will be directly collected by the researcher, otherwise it will be by scheduling.

3.10.1. The Bank Customers

Since our focus of the study is the Commercial Bank of Ethiopia and the branches of the bank are too many in number only 10 branches of the bank were chosen, since there was time constraint and cost. The main important data collection procedure is questionnaires which were distributed to customers and bank workers themselves in person or face to face. It is important to collect data from the customers and bank workers face to face as it is reliable and trustworthy. The other was the questionnaires was given to a friend to make them distributed to the customers. The respondent includes any respondent who is the bank’s customer. As we said earlier the Commercial Bank of

Ethiopia is chosen because, it is the pioneer bank in introducing modern banking or e-banking service to its customers and it is also the bank with large number of customers. So the need to use other banks may not be necessary and also the time frame is limited to complete this research work, which is short. Generally several questions was constructed based on the objectives of the research work.

3.10.2. The bank workers

Even if today there are so many other banks which launch mobile banking service to their customers, due to time constraint and cost, the largest state owned bank that is Commercial Bank of Ethiopia will be considered, because of its large number of customers and its biggest capital (Yohannes,2010). Interview were conducted with open ended questions to the bank's internet and mobile banking manager.

Additionally interview was conducted using telephone with the bank workers. Some of the questions were specific and some were general information regarding mobile banking usage and customers' perception of mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. These gives the researcher a better understanding of the past and present challenges of the mobile banking industry and how best to be in preparing the research questions. In other cases since the workers themselves are also customers of the bank some of the questionnaires were given for them.

3.11. Methodological limitations

There was several challenges that came up during the research work in regards to the chosen approach, these are highlighted below.

Sample size: The sample size is considered not to be too large which could affect the extent to which the findings may be generalized for the whole customers and branches of the bank and to other banks in general at a country level.

Time and cost: The time required to complete the research was very small and this had an influence on the researchers' decision to pick a small sample size. The short time did not permit an in-depth search for more information. There was also cost associated with the research work which involves telephone calls, transportation, internet and other related costs.

3.12. Data analysis tools and techniques

The data taken from the respondents were properly checked and input into the Statistical Package

for Social Science (SPSS) software which was used to analyze the responses from the collected data. This allows the frequency and percentage distribution to be developed from the analysis of the collected data. The frequency and percentage distribution was used to calculate the personal data information of respondents, and additional statistical measurements like regression analysis, reliability and validity of model factors were used to find the relationship between the factors influencing customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. Factor analysis is done to test construct validity. Factor analysis more specifically principal component analysis is a data reduction technique which reduces variable or items to one or few component of factors that explains the relationship about the variables. The qualitative data analysis is conducted in order to clarify the findings obtained from the survey about the general attitude of customers' towards mobile banking security. This was conducted with the bank's internet and mobile banking manager. As the service is new to the country the whole system is controlled or administered by the central bank branch. Because of this the interview was conducted with one person, who is the manager for the whole branches of the bank offering mobile banking services. Finally the research framework was used to predict the research hypothesis and these are highlighted below.

3.13. Research model and hypotheses

1. Perceived vulnerability concerns with the individual beliefs that a threatening event is likely to occur (Yousafzai et al., 2003; Jansen, 2015). It has a direct effect on individual risk perception (Jansen, 2015). In our case it can be the individual perception of how likely he/she would be the victim of mobile banking fraud. Increased perceived vulnerability will likely increase the individual perceived risk, which in turn motivate the individual for more secured practices.

Hence, we posit that:

H1: Perceived vulnerability is positively associated with the individual perceived risk in mobile banking.

2. Perceived severity is "an individual's assessment of the severity of the consequences resulting from a threatening security event" (Crossler, 2010). When the individual perception of the consequence of a threat is increased, it is likely that this will increase perceived risk, which in turn increases the motivation of individual to protective action (Jansen, 2015).

Hence, we hypothesize:

H2: Perceived severity is positively associated with the individual perceived risk in mobile banking.

3. In the context of online banking, perceived risk is defined as “the potential of loss in the pursuit of a desired outcome from using electronic banking services” (Yousafzai et al. 2003). When a risk is perceived, individuals will change their behavior based on how much risk they are willing to accept for the particular threat (Workman et al. 2008). Based on this notion, it is expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures.

Therefore, we hypothesize:

H3: Perceived risk is positively associated with the individual protection motivation in mobile banking.

4. Based on the idea of Milne et al., (2000) and Jansen (2015), response efficacy can be conceptualized as the individual belief that applying the bank’s recommended coping strategy is more likely reduce the mobile banking threat.

Hence, we hypothesize:

H4: Response efficacy is positively associated with the individual protection motivation in mobile banking.

5. Self-efficacy is concerned with the individual ability and confidence to perform the recommended coping measures or actions (Milne et al, 2000). In this line, when the individual self-efficacy increased, this will likely increase the individual safe behavior in using mobile banking.

Therefore, we hypothesize:

H5: Self-efficacy is positively associated with the individual protection motivation in mobile banking.

6. Response cost deal with the cost that the individual is likely to incur while perusing the recommended response (Milne et al., 2000). According to Jansen (2015), the cost could be anything from financial to time sacrificed. High response cost is likely to decrease the individual willingness to demonstrate the recommended response. In our case response cost can be conceptualized as the individual belief that practicing the bank’s recommended activities will cost me much in terms of money and time.

Hence, we hypothesize:

H6: Response cost is negatively associated with the individual protection motivation in mobile banking.

7. Perceived usefulness and perceived ease are the two components of Technology Acceptance Model (TAM). According to (Davis, 1989), they are very important factors affecting the adoption of new innovation. There exist a positive relationship between Perceived usefulness and perceived ease of use and they are very important factors on the use of electronic banking (Poon, 2008). Therefore, an innovation perceived to be useful to customers which is equally easy to use is more likely to be better accepted by customers. These can be applied into mobile banking security context and protection motivation theory.

Hence, we hypothesize:

H7: Perceived ease of use is positively associated with the individual protection motivation in mobile banking. And

H8: Perceived usefulness is positively associated with the individual protection motivation in mobile banking.

8. Trust belief has been found helpful in explaining how customers may overcome perceived risk and engage in online transactions (S.L. Jarvenpaa, N. Tractinsky. (1999); N.K. Malhotra, S.S. Kim, J. Agarwal. (2004)). Trust plays a critical role in mitigating perceived risks, especially for transactions involving uncertainty (S.L. Jarvenpaa, N. Tractinsky. (1999)). Because MB(mobile banking) is still in the initial adoption stage, customers are unclear about the technical capability of their banks to provide MB service and about the reliability and security of the Internet and wireless communication channels in delivering their sensitive financial data, among other concerns. The existing trust beliefs toward a bank are relied on as one of the major leverage points for customers to assess the potential risks involved in the wireless banking service provided by that bank. Customers who believe in the technical capability, integrity, and benevolence of their banks are more likely to overcome their risk perceptions toward new services such as the wireless banking situation. Therefore, considering the uncertainties in MB, the stronger the trust a customer has toward a bank, the lower the risk he or she anticipates in adopting mobile banking.

Therefore, we hypothesize:

H9: Trust belief toward a bank will have a negative effect on perceived risks in mobile banking.

9. Online transactions, in general, raise security and privacy concerns among users (T. Teo, M. Tan, and SN. Peck. (2004)). Similar to trust belief, structural assurance such as promises, guarantees, and contractual protections should also help to alleviate customers' perceived risk in the unfamiliar, open airwave environment. Mobile banking service providers can draft customer service policies, use advanced encryption technologies, and make promises (e.g. 100% satisfaction guarantee, monetary refund, protection of privacy, and accurate transaction information) to relay structural assurance information to mobile banking users. As such, customers who trust the legal and technology structures of the wireless internet will be more likely to believe their financial data will be protected against loss or theft along transmission. Such belief in the structural soundness of the wireless internet platform is anticipated to lower the perceived risk in wireless banking (mobile banking in our case).

Hence, we hypothesize:

H10: Structural assurance has a negative impact on perceived risk.

3.14. Related works and their methodologies

Local and international Works	Titles	Research Strategy	Sampling	Data Collection Method	Analysis Techniques
International works	An analysis of mobile banking acceptance by Malaysian customers.	survey	Purposive sampling	questionnaires	The frequency and percentage distribution was used to calculate the personal data information of respondents, and regression analysis was used to test the hypothesis, reliability and validity were checked by alpha value.
	Factors influencing the use of m-banking by academics: case study SMS-based M-banking.	survey	a simple random sampling	questionnaire	Frequency counts and percentages are used and descriptive statistics are calculated and relationships among the factors are analyzed using, Pearson Product Moment Correlation (PPMC) and multiple regression analysis. Reliability and validity tests were also done.
	Effect of bank innovations on financial performance of commercial banks in Kenya.	descriptive survey	a purposive sampling	questionnaires	Besides using frequencies and descriptive analysis, the study used multiple linear regression analysis to test the statistical significance of the various independent variables
	Customers' perception of mobile banking: an empirical study in national capital region Delhi	structured survey	Convenience sampling	questionnaire	The reliability of the data was carried out by using Cronbach's Alpha Value. ANOVA was employed to find the significant factor. Factor analysis is done to test

International works					construct validity. Bartlett's test of sphericity and measure of sampling adequacy (MSA) were also carried out to ensure that the requirements of factor analysis were met.
	A study on customer perception towards mobile-banking: technology adoption and challenges.	structured survey	convenience sampling	Questionnaire	The frequency and percentage distribution was used to calculate the personal data information of respondents, ANOVA was employed to find the significant factor.
	To study consumer awareness & perception towards usage of mobile banking.	A survey research	Convenience sampling method	Structured Questionnaire and Interviews	The frequency and percentage distribution was used to calculate the personal data information of respondents, cross tabulation was also used and factor analysis was done. Finally chi – square test to test the hypothesis.
	Factors hindering consumer adoption of internet banking in commercial banks in Kenya.	descriptive survey	Stratified Proportional sampling	a survey questionnaire	Quantitative data collected was analyzed by the use of descriptive statistics such as mean, standard deviation, frequency and percentages. The findings were displayed by use of bar charts, graphs and pie charts and in prose-form. Content analysis was used to test data that was qualitative in nature or aspect of the data collected from the open ended questions.
	Factors influencing the adoption of internet banking.	Survey	Random sampling	Questionnaire	Partial least square method /PLS/ was applied for analyzing the collected data. Similarly the frequency and percentage distribution was used to calculate the personal data information of respondents.

International works	Customers' perception of m-banking adoption in kingdom of Bahrain: an empirical assessment of an extended tam model.	survey	random sampling	questionnaire	The frequency and percentage distribution was used to calculate the personal data information of respondents, and additional statistical measurements like regression analysis, reliability and validity of model factors.
----------------------------	--	--------	-----------------	---------------	--

Local works	Factors affecting adoption of electronic banking system in Ethiopian banking industry.	Survey	purposive sampling	Questionnaire and semi-structured interview	Data obtained from survey were analyzed by using descriptive statistics such as median, mode etc.
	Analysis of factors influencing customers' intention to the adoption of e-banking service channels in Bahir Dar city: an integration of TAM, TPB AND PR.	survey	a stratified sampling technique	questionnaire	The study used simple descriptive statistics, computation of ANOVA and multiple regression analysis.
	The impacts of e-banking services on customer satisfaction: the case of selected commercial banks in Addis Ababa.	survey	multi- stage sampling technique	Questionnaire and semi structured interview	The study employed multiple linear regressions models and chi-square independency test to see the relationship between demographic characteristics and satisfaction of e-banking users.
	Electronic-banking in Ethiopia- practices, opportunities and challenges	survey	-	Document analysis	It is simply based on the analysis of documents. No further analysis techniques used
	Electronic payment adoption in the banking sector of low income countries.	cross-sectional survey	Convenient sampling technique	questionnaire	The study mainly employed Partial Least Squares (PLS) methods for the analysis of data. Reliability tests and validity tests were also done using Cronbach's Alpha value.

Local works	Assessment of the opportunities and challenges for the adoption of e-banking services in Ethiopia.	survey	Purposive or convenience sampling technique	Questionnaire and unstructured interview	The collected data was analyzed by using descriptive analysis such as tables and percentages.
--------------------	--	--------	---	--	---

Table 3.1: Summary of some related works and their methodologies.

N.B. From the table above we can understand and see that most of the local researches are done about the e-banking adoption and also challenges, whereas international works show that there is an attempt or researches which are done on customers perception and mobile banking adoption. So our particular research in this limited local work will contribute a lot to the mobile banking service providers and also to the researchers whom want to proceed on the area. Again our research is trying to look the individual customer perception towards mobile banking security, in which it makes our research comprehensive in particular to other researches.

The other thing that we can observe from the table is the methodologies that most of the researches used are almost similar, this means that the methodologies they have used were appropriate for their study. From this we can say that for our study the methodology that we are going to adopt is reasonable based on the review of related works that is indicated above.

3.15. Quality of Research

Reliability and validity are mostly raised in conducting quantitative research. While preparing the questionnaire, ambiguous or vague wording was avoided to ensure that respondents would read and answer the question consistently on different occasions in the same context. Moreover, reliability and validity of the study is acquired through analyzing data from different sources. The data from different sources can help for crosschecking the information obtained. At the same time, the reliability can be gained during the analysis part when those proved information would interpret in consistent manner.

3.15.1. Reliability of the Research

According to Greenfield et al. (2002) they defined Reliability as “the consistency or repeatability of the measure”. Reliability is especially important if the measure is used for an on-going basis to detect change. Convenience sampling such as timing of data collection, structure of interviews and data triangulation makes this research reliable. Similarly the Cronbach’s alpha value for the model factors and the questionnaire items can be determined.

3.15.2. Validity of the Research

Similarly validity as it has been stated by Greenfield (2002) is a way of checking that the study is “measuring what was intended to measure”. There are different types of validity measurements including content validity and construct validity. The content validity will be assured when the questionnaire is to be prepared based on extensive reading of literature review. According to Kumar (1999) Construct validity is a data reduction technique and principal component analysis method which explains the relationship between variables. Here construct validity can be determined by checking the item loadings using principal component analysis and by reducing items having low loadings.

3.16. Conclusion

The methodology for this research work was appropriate as it was compared or cross checked with the previous researches. An improvement can be made by expanding the research to more advanced level. The questionnaires were both quantitative and qualitative in nature for the gathering of necessary data that was useful for the research work and also semi structured interview was taken into consideration. The limitation for the research work was mentioned. In addition to this, method of data analysis and interpretation was given with the research model and hypotheses developed from the research frame work. So the next chapter shows data analysis and interpretation.

CHAPTER FOUR

DATA ANALYSIS AND RESULTS

4.1. Introduction

This chapter will focus on the analysis of the results obtained from the questionnaires that was distributed to respondents using the research framework and also the interview conducted with the manager of mobile and internet banking at Commercial Bank of Ethiopia in studying customer's perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa.

4.2. Research and Statistical Tools Employed

The research and statistical tools employed in this study are simple frequency distribution, reliability and validity tests, and regression analysis. SPSS 20.0 was used to perform statistical analysis. The reliability of the data was carried out by using Cronbach's Alpha Value.

In this research a questionnaire was employed to assess the developed model. Customers who have experience, ability, or knowledge in using mobile applications, especially in using mobile banking were selected. The sample size was determined based on the method explained earlier in the methodology section. So based on the formula a sample size of 170 respondents were determined. The survey questionnaire consisted of three parts. The first section was about the subject's demographic information. The second section was about customers' perception of each factor in the model using yes/no questions. The third section asked each subject to indicate his or her degree of agreement with each item, here data were collected using a five point Likert-type scale.

4.3. Analysis of the data

This study has proposed a research framework developed from previous findings which will be used to analyze the data. Customer's perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa will be analyzed using the research framework using the sample that was selected.

The analysis of this data was divided into following section:

- Respondents Profile:
- Frequency and percentage distribution of respondents on the model factor questions:

- Reliability and Validity Analysis:
- Hypotheses testing: using linear regression analysis:

4.4. Respondents Demographic Characteristics

The frequencies were used to determine how often respondents made a certain response in answering questions, and this allow general information about the information collected to be analyzed. Questionnaires were also distributed to the customers of Commercial Bank of Ethiopia in Addis Ababa. The demographic detail shows gender, age, current educational status, marital status, and occupation and these are shown in the tables below. Secondly, the perception of respondents about mobile banking security at Commercial Bank of Ethiopia in Addis Ababa was also discussed.

4.4.1. Gender

Table 4.0 below shows the gender of respondents in number and in percentage terms.

Gender	Frequency	Percent	Cumulative Percent
Valid Male	110	73.3	73.3
Female	40	26.7	100.0
Total	150	100.0	

Table 4.0: Gender of respondents Source. Primary Data

As reflected in the table above, 73.3 percent (110) of the entire respondents were male and 26.7 percent (40) were female. This indicates that there are more male respondents than female. The majority of users being male is also consistent with the finding of Singh's (2004) on the adoption of internet banking in South Africa.

4.4.2. Age

Table 4.1 below; reflects the age groups that participants falls into. 1.3% (2) is the lowest age group which is above 51 while the majority of the respondents 66.0% (99) are between ages of 20-30, with 27.3% (41) in the age group of 31 to 40, 5.3 % (8) in the age of 41 to 50 group. The study shows that, respondents between the ages of 20-30 are in the dominant group.

Age		Frequency	Percent
Valid	From 20-30	99	66.0
	From 31-40	41	27.3
	From 41-50	8	5.3
	From 51-60	2	1.3
	Total	150	100.0

Table 4.1: Age of respondents

Source. Primary Data

4.4.3. Educational status

As we look from the table below the majority of respondents 66.7%(100) are degree holders then followed by diploma holders which are 13.3%(20) and those who are under elementary and TVET are fall under the same number that is 7 which is 4.7% where as those who are under secondary education are 3.3%(5) and lastly there were 2 of the respondents who are doctorate holders who constitute 1.3% of the respondents.

Educational status		Frequency	Percent
Valid	Elementary	7	4.7
	Secondary	5	3.3
	TVET	7	4.7
	Diploma	20	13.3
	Degree	100	66.7
	Masters	9	6.0
	Doctorate	2	1.3
	Total	150	100.0

Table 4.2: Educational status of respondents

Source. Primary Data

4.4.4. Marital status

Table 4.3 shows the marital status of respondents, in which the majority of respondents were unmarried 61.3 %(92) and 38.7 %(58) of them are married. As we observe from the table we don't have respondents who are under the widowed category.

Marital status		Frequency	Percent
Valid	Unmarried	92	61.3
	Married	58	38.7
	Total	150	100.0

Table 4.3: Marital status of respondents

Source. Primary Data

4.4.5. Occupation

The occupation distribution of the participants differs from one another. Table 4.4 reflects that the highest number is the employed with 73.3% (110) respondents followed by the students with 14% (21) of respondents, 8.0% (12) are business man and other 4.7 % (7) of respondents are unemployed persons.

Occupation		Frequency	Percent
Valid	Unemployed	7	4.7
	Student	21	14.0
	Employed	110	73.3
	Business Man	12	8.0
Total		150	100.0

Table 4.4: occupation of respondents

Source. Primary Data

4.5. Customers' perception towards the theoretical model factors.(Analysis results from the yes/no questions)

Here the questions are designed to get the general perception of respondents towards the constructs derived from the theoretical model. Accordingly we have eleven constructs in the theoretical framework, so we have eleven questions based on the constructs and the feeling of respondents will be analyzed using one of the SPSS tools like frequency and percentage.

1. Perceived vulnerability

Question: Do you think using mobile banking is vulnerable to threats or attacks and does this makes you to think of risk in mobile banking security?

Perceived vulnerability

		Frequency	Percent	Cumulative Percent
Valid	Yes	125	83.3	83.3
	No	25	16.7	100.0
Total		150	100.0	

Table 4.5: Frequency distribution of respondents about Perceived vulnerability

Source. SPSS Result

When we look at the above table, the responses of the respondents from the investigation conducted shows that, the customers' perception of vulnerability towards mobile banking security

is high. This also indicates that majority of the customers' think of risk due to this vulnerability perception. From table 4.5 above, it shows that the majority of the mobile banking users 83.3% agreed that using of mobile banking service is vulnerable to threats, whereas 16.7% of the users said that using the service is not that much vulnerable to threats. Most of this category explained that if we use the service properly it is not vulnerable to threats and they also added that still now they didn't face any kind of threats when using the service. But majority of the respondents are still concerned of vulnerability even if they are still using the service. This finding is similar with the findings of (Yousafzai et al., 2003; Jansen, 2015), in addition (Jansen, 2015) and Liang and Xue (2010) said that perceived vulnerability has a direct effect on individual risk perception.

2. Perceived severity

Question: Do you think threat or failure in mobile banking service is sever if it happens and does this makes you to think of risk in mobile banking security?

Perceived severity				
		Frequency	Percent	Cumulative Percent
Valid	Yes	116	77.3	77.3
	No	34	22.7	100.0
Total		150	100.0	

Table 4.6: Frequency distribution of respondents about Perceived Severity

Source. SPSS Result

Similarly the table above shows responses of customers from the data collected which shows the severity perception of respondents about mobile banking security. The customers were asked whether the threat or problem is sever if it happens at the time of using mobile banking services and due to this perception does they think of risk or not. So when we look at the response of customers the majority of them agreed with this question which constitute 77.3 %(116) of the total respondents. Whereas the remaining 22.7 %(34) didn't agree with the question. From this number we understood that majority of the respondents still think of the severity of mobile banking security even if they are using the service. The other respondents' whom do not agree with the question said additionally that, if the treat or problem happens it will not be that much sever since the bank that we are a customer is reliable, trustworthy and also government bank. But generally the above data show that still the majority of customers are concerned about its severity, this is similar with the findings of (Crossler, 2010; Jansen, 2015) and Liang and Xue (2010) in which when the

individual perception of the consequence of a threat is increased, it is likely that this will increase perceived risk, which in turn increases the motivation of individual to protective action.

3. Perceived risk

Question: Do you perceive there is risk in using mobile banking and does this enforces or pushes you to take protection motivation/action/ when using mobile banking so as to avoid risks?

Perceived risk

	Frequency	Percent	Cumulative Percent
Valid Yes	112	74.7	74.7
No	38	25.3	100.0
Total	150	100.0	

Table 4.7: Frequency distribution of respondents about Perceived risk

Source. SPSS Result

Again when we look at the above table which shows the responses of customers in relation to the risk perception of them that may lead to the protection motivation activity, majority of respondents 74.7%(112) said that they perceive risk when using mobile banking services and this enforces them to take or to be ready to take protection action in order to avoid risk as per the capacity of them. On the contrary 25.3 %(38) of the respondents said that even if we perceive risk we don't have the knowhow how to take protection action. So according to them even if we think of risk we will not be motivated to take action because of our perception. But still the figure shows that most of the customers agree with the question. This is in line with the findings of (Yousafzai et al. 2003; Workman et al. 2008) in which when a risk is perceived, individuals will change their behavior based on how much risk they are willing to accept for the particular threat and it is also expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures.

4. Response efficacy

Question: Are you ready or willing to perform the bank's recommended actions properly so as to avoid risks and does this will help you to take protection motivation/action/ when using mobile banking?

Response efficacy

	Frequency	Percent	Cumulative Percent
Valid Yes	111	74.0	74.0
No	39	26.0	100.0
Total	150	100.0	

Table 4.8: Frequency distribution of respondents about Response efficacy

Source. SPSS Result

The response efficacy of the customers was one construct in which respondents were asked. The customers were asked whether they are ready or willing to perform the banks recommended actions so as to avoid risks and whether this helps them to take protection action when using mobile banking services. As we look from the frequency table 74.0 %(111) of the respondents' agreed with the question, whereas 26.0 %(39) of the respondents still don't agree with this question. When they explain about their disagreement the said that even if we are willing or capable to perform the banks recommended actions this doesn't help us to take protection action, because we don't know from where the threat or failure comes and we believe that we can't protect it if it happens. They added that our only guaranty is the bank itself. This finding is similar with the findings of (Milne et al., 2000; Jansen ,2015)and Liang and Xue (2010) in which the individual belief that applying the bank's recommended coping strategy is more likely reduce the mobile banking threat.

5.Self-efficacy

Question: Are you capable or skilled to take the bank's recommended actions and does this will help you to take protection motivation/action/ when using mobile banking?

Self-efficacy

	Frequency	Percent	Cumulative Percent
Valid Yes	119	79.3	79.3
No	31	20.7	100.0
Total	150	100.0	

Table 4.9: Frequency distribution of respondents about Self-efficacy

Source. SPSS Result

Similarly self-efficacy was one construct in which the customers were asked. The customers were asked whether they have skill or experience in using electronic devices like mobiles and also

computers, and does this helps them to take protection action when using mobile banking services. From the table above it is observed that again most of the customers 79.3 %(119) agree that they have capability or skill in manipulating those devices and their skill helps them to manage or protect threats that may happen. On the other hand 20.7%(31) of the respondents didn't agree with this idea, they said that still even if we have skill of using those devices and we are also capable of taking the banks recommended actions, this doesn't help us to protect ourselves because the threats may be even beyond the technical security of the banks themselves. And in addition they said that we can't say that we are 100% skilled and capable. Generally the findings from this data shows that majority of the customers agreed that their self-efficacy helps them to protect threats or problems. This result is parallel with the findings of (Milne et al, 2000) in which when the individual self-efficacy increased, this will likely increase the individual safe behavior in using mobile banking. Similarly with the findings of (Rhee .et al, 2009) whom studied self-efficacy and its impact on safe behavior by end users.

6. Response cost

Question: Do you think that doing or following the bank's recommended actions will have some expenses in terms of time and cost and does this will not push you to take protection motivation/action/ when using mobile banking?

Response cost

		Frequency	Percent	Cumulative Percent
Valid	Yes	116	77.3	77.3
	No	34	22.7	100.0
Total		150	100.0	

Table 4.10: Frequency distribution of respondents about Response cost

Source. SPSS Result

When we look at the responses of customers on the basis of the expense or the cost that the customers think when applying or following the banks recommended actions and whether this cost or expense perception doesn't motivate them to take protection action. Similar to the above data the majority of respondents 77.3 %(116) said or agreed that the expense in terms of cost and time will make us not to be motivated to take protection action. But the remaining respondents 22.7%(34) of respondents said that this cost or expense doesn't prohibit us from taking protection action that is recommended by the bank, because if we follow the recommended actions it will

save us from the threat or problem that may happen that is the cost that we may incur will be less than the threat or problem that may occur on us. So even if there will be some cost to be incurred this doesn't be much more than the problem that may happen. But still large number of respondents' said that if there is accost on us when applying the banks recommended actions we will be demotivated to take protection action. This is similar with the idea or findings of (Milne et al., 2000; Jansen, 2015) in which High response cost is likely to decrease the individual willingness to demonstrate the recommended response.

7. Perceived ease of use

Question: Do you think mobile banking is easy to use and does this will help you to take protection motivation/action/ when using mobile banking?

Perceived ease of use			
		Frequency	Percent
			Cumulative Percent
Valid	Yes	122	81.3
	No	28	18.7
Total		150	100.0

Table 4.11: Frequency distribution of respondents about Perceived ease of use

Source. SPSS Result

On the above table the construct is derived from the well-known technology acceptance model TAM to test whether this will have impact on the customers to take protection action or not. From the responses collected it is shown that most of the respondents 81.3 %(122) said mobile banking is easy to use and they agreed that this easiness helps us to protect ourselves when using mobile banking services. Whereas 18.7%(28)of the respondents said the easiness of mobile banking service doesn't help us to protect ourselves when using mobile banking, because they added that the easiness is for the use purpose only, but it doesn't that much help us to take protection action. But from the above data we still understood that majority of the respondents agreed that the easiness of the service will help them for taking protection action. This result is similar with the findings of (Davis, 1989; Poon, 2008) in which they said that an innovation perceived to be easy to use is more likely to be better accepted by customers. When we bring to our construct the easiness of mobile banking will have an effect on the protection action of the customers, if the

service is accepted by customers due to its easiness. So we can apply this into mobile banking security context and protection motivation theory. This is again similar with Luarn and Lin's (2005) finding on behavioral intention to use mobile banking and also with the findings of Adesina et al. (2010) on electronic banking in Nigeria.

8. Perceived usefulness

Question: Do you think mobile banking is useful and does this will help you to take protection motivation/action/ when using mobile banking?

Perceived usefulness		Source. SPSS Result		
		Frequency	Percent	Cumulative Percent
Valid	Yes	97	64.7	64.7
	No	53	35.3	100.0
Total		150	100.0	

Table 4.12: Frequency distribution of respondents about Perceived usefulness

Similar to the above construct this is also derived from the well-known technology acceptance model TAM to know whether the usefulness of this technology (mobile banking service) will have an effect on the customer to take protection action. Based on the question 64.7 %(97) of the respondents said that the usefulness of the service helps them to take protection motivation or to protect themselves. Similarly large number of respondents 35.3 %(53) unlike the previous construct responses don't agree with the question. The reasons that most of this category respondents said that it is not the usefulness that makes them to protect themselves from the threat that may happen rather the simplicity or the skill and also the banks recommended actions will help them in doing so. From this data we can understood that even if the respondents that agree with the question are larger than those whom do not agree, there is a question on the construct that the usefulness is not that much helpful for the customers to take protection action when using mobile banking service. But based on the data, this finding is to some extent similar with the findings of (Davis, 1989; Poon, 2008) in which they said that an innovation perceived to be useful is more likely to be better accepted by customers. When we bring this concept to our model construct the usefulness of mobile banking will have an effect on the protection action of the customers, if the service is accepted by customers due to its usefulness. So we can apply this into mobile banking security context and protection motivation theory. Others also said that even if the service is useful, still they concerned with security issues, additionally this concern is going to

make them to stop being the user of the service rather than to protect themselves, this response of customers' is consistent with that of Mattila (2003), and Luarn and Lin (2005) that the issue of security still have an impact on the perceived usefulness.

9. Trust belief

Question: Do you have any trust on the bank that provides mobile banking service to you and does this will make you not to think of risks in mobile banking?

Trust belief

		Frequency	Percent	Cumulative Percent
Valid	Yes	127	84.7	84.7
	No	23	15.3	100.0
Total		150	100.0	

Table 4.13: Frequency distribution of respondents about Trust belief

Source. SPSS Result

Another very important construct which is derived from the concept of trust is that the trust belief (trust on the bank itself). Based on this construct customers were asked about the trust belief towards the bank and their perception of risk. From the table above it is indicated that majority of the respondents 84.7 % (127) said that they do have trust towards the bank that provides the service and this trust on the bank makes them not to worry about the risk that may happen. On the other hand some of the respondents 15.3% (23) said that even if they have trust on the bank still they are worried about the risk that may happen, because those customers said that sometimes the risks or problems that may happen may be beyond the capacity of the bank itself. In addition they added that our countries system of the new technologies is not that much well strong to protect those hackers and experience sharing with those countries developed with the technology is mandatory. But the data shows that most of the customers have trust on the bank and due their trust they are not that much concerned with risk. This result is similar with the findings of (S.L. Jarvenpaa, N. Tractinsky. (1999), N.K. Malhotra, S.S. Kim, J. Agarwal. (2004)) in which trust belief has been found helpful in explaining how customers may overcome perceived risk and engage in online transactions (in our case mobile banking transactions). Similarly with (S.L. Jarvenpaa, N. Tractinsky. (1999)) in which trust plays a critical role in mitigating perceived risks, especially for transactions involving uncertainty. Again this is similar with Jansen, (2015), and Luo, Li, Zhang,

and Shim (2010), whom also found out that trust plays a vital role in the acceptance of mobile banking adoption.

10. Structural assurance

Question: Is the bank is a legislative or a legal institution that will be responsible for the problems or risks that may happen on you and have a good transmission channel for successful completion of financial transactions with it and does this makes you not to think of risks in mobile banking?

Structural assurance

		Frequency	Percent	Cumulative Percent
Valid	Yes	92	61.3	61.3
	No	58	38.7	100.0
Total		150	100.0	

Table 4.14: Frequency distribution of respondents about Structural assurance

Source. SPSS Result

Another important construct which is also derived from the concept of trust is structural assurance (trust towards the bank's legal frame work and also the transmission channel (wireless platform that the bank is using). This is mainly concerned with the transmission channel and insurance system employed by the bank. Based on this notion customers were asked to judge whether the bank's legal frame work and the transmission channel is trust worthy and also does this makes them not to think of risk in using mobile banking service. As we look from the table large number of respondents 61.3 %(92) agree with this question that they trust the bank's transmission channel and also the insurance mechanism that the bank is using. Due to this they also agreed that this makes them not to think of risk when using mobile banking service. Similarly large number of respondents also said that they don't have trust on the bank's transmission channel and also they are not sure of the bank's insurance system that is adopted. The reason that they cite here is that the transmission channel is being controlled by telecommunication, so the bank is dependent on the service of this company. Network breakup is high, and also power interruption is also the other factor that makes the transmission channel not to be safe. Due to this and other factors they said we don't trust the bank as secured and it is insured in terms of the wireless platform breakup or interruption. This construct is under question like the perceived usefulness to be considered exactly for our theoretical model. This result is similar with the findings of (T. Teo, M. Tan, and SN. Peck.

(2004)) in which similar to trust belief, structural assurance such as promises, guarantees, and contractual protections should also help to alleviate customers' perceived risk in the unfamiliar, open airwave environment. Such belief in the structural soundness of the wireless internet platform is anticipated to lower the perceived risk in wireless banking (mobile banking in our case). Trust is not often integrated in PMT (protection motivation theory) studies. However, it is an important construct in risk literature, so we include it in our model to see the effect in the risk construct.

11. Protection motivation in mobile banking

Question: Are you concerned with security issues when using mobile banking services and does this leads you have motivation to take protection action?

Protection motivation in mobile banking

		Frequency	Percent	Cumulative Percent
Valid	Yes	126	84.0	84.0
	No	24	16.0	100.0
Total		150	100.0	

Table 4.15: Frequency distribution of respondents about Protection motivation in mobile banking.

Source. SPSS Result

This is the main construct in our theoretical model which is dependent on most of the other constructs. Again similar to the other constructs, customers were asked to answer the question related to this construct. The question is whether they are motivated or forced to take protection action when they feel of insecure at the time of using the mobile banking service. Based on the data from the table above majority of the respondents 84 %(126) agreed to the question that they will be motivated to take protection action when they feel of insecure at the time of using mobile banking services. On the other hand 16 %(24) of the respondents said that even when they feel insecure they try to quit using of the service rather than taking protection action. Additionally they also said that it is not only when they feel insecure, that they need to take protection action rather they are happy if they can protect themselves at any time. They also stressed that knowing to protect oneself is not only important when one feels insecure, but it is important for everyone to protect oneself at any time when using of the service. Lastly they also said that even if they feel insecure, since they don't have knowledge how to protect themselves they will not be motivated to take protection action during using the service. This result is in line with the thoughts of (Rogers, 1975) in which protection motivation is an intervening variable that has the typical characteristics

of a motive: it arouses, sustains, and directs activity. Similarly it is also similar with the thoughts of (Floyd et al. 2000) in which protection motivation is the decision or intention to proceed to, continuation of, or the avoidance of the studied behavior. When we bring their thoughts to our question, the perception of insecurity will result is the avoidance or continuation of taking the protection action and also perception of insecurity arouses, motivates and leads to take protection action.

4.6. Reliability and Validity of the questionnaire and the model factors

4.6.1. Reliability

The alpha values were calculated to evaluate the internal consistency reliabilities of the scales. The first factor, Perceived vulnerability, was loaded with two variables ($\alpha = 0.794$). The second factor, Perceived severity, was loaded with two variables ($\alpha = 0.826$). The third factor, Perceived risk, contained four variables ($\alpha = 0.750$). The fourth factor, Response efficacy, was loaded with two variables ($\alpha = 0.829$). The fifth factor, Self-efficacy, was loaded with two variables ($\alpha = 0.831$). The sixth factor, Response cost, was loaded with two variables ($\alpha = 0.815$). The seventh factor, Perceived ease of use, was loaded with two variables ($\alpha = 0.711$). The eighth factor, Perceived usefulness, was loaded with two variables ($\alpha = 0.827$). The ninth factor, Trust belief, was loaded with three variables ($\alpha = 0.828$). The tenth factor, Structural assurance, was loaded with two variables ($\alpha = 0.873$). The dependent variable, Protection motivation in Mobile Banking was loaded with 2 variables ($\alpha = 0.836$).

Table 4.17 shows the result of reliability analysis- Cronbach's Alpha Value. This test measured the consistency between the survey scales. The Cronbach's Alpha score of 1.0 indicate 100 percent reliability. Cronbach's Alpha scores were all greater than the Nunnally's (1978) generally accepted score of 0.7. In this research we attempted to examine the customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa by employing PMT (Protection motivation theory) and by adopting some constructs from TAM model and trust concept.

The PMT (Protection motivation theory) as a model is developed in order to verify the relations between the dependent variables and independent variables and to test the hypotheses.

SPSS analysis technique was used to assess the validity and reliability for each factor that determine customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa.

As K. Cherry (2013) stated that the reliability is referring to the consistency of a measure, and a test is considered reliable if the tester get the same result on repeated trails. There are many types of reliability including inter-ratter reliability, Test-retest reliability, parallel-forms Reliability and internal consistency reliability. In this research, the internal consistency reliability was tested as for the factors and all questionnaire items. Internal consistency reliability (ICR) is used to evaluate the reliability (Venkataesh et al., 2003). The total Cronbach's Alpha for all the questions is shown in the table 4.16. From this table it indicates that the internal consistency (reliability) of all the questionnaire items is above 0.7 which is good internal consistency. Similarly table 4.17 shows the results of alpha coefficients for each factor with reliability analysis. All factors are above 0.7 which indicate that good internal consistency of the questionnaire items, as (J. C. Nunnally, 1978; Wixom and Watson, 2001) recommended that what is equal to 0.7 or above is acceptable.

Table 4.16: Reliability of questionnaire items

Cronbach's Alpha	N of Items
.876	25

Table 4.17: Reliability of the model factors

Factors	Cronbach's Alpha
Perceived vulnerability	0.794
Perceived severity	0.826
Perceived risk	0.750
Response efficacy	0.829
Self-efficacy	0.831
Response cost	0.815
Perceived ease of use	0.711
Perceived usefulness	0.827
Trust belief	0.828
Structural assurance	0.873
Protection motivation in Mobile Banking	0.836

4.6.2. Validity

Validity is defined as the extent to which data collection methods or methods accurately measure what they were intended to measure (Saunders and Thornhill, 2003). It is concerned with whether the findings are really about what they appear to be about.

The two elements convergent validity and discriminant validity are components of a larger scientific measurement concept known as construct validity (Straub et al., 2004). These two validities capture some of the aspects of the goodness of fit model, i.e., how well the measurement items relate to constructs.

Convergent validity is shown when each measurement item correlates strongly with its assumed theoretical construct. Discriminant validity is shown when each measurement item correlates weakly with all other constructs except for the one to which it is theoretically associated. For this study from the two validity measures we use convergent validity.

On the other hand, K. Cherry (2013) defines the validity as the extent to which a test measures what it claims to measure. For all the constructs with multiple reflective measures, all items have high loadings, with majority above 0.8 therefore demonstrating convergent validity.

Besides, all factors in the measurement model have adequate convergent validity because the average of loadings for each variable item were greater than 0.7, which is an acceptable level.

4.7. Hypotheses testing and discussion of results

In order to do the hypothesis test we use linear regression statistical method. So with regards to the data analysis, the dependent variables (Protection motivation in Mobile Banking and perceived risk) was aggregated with the independent variables. Similar approach was also applied for the independent variables for aggregation (i.e. Perceived vulnerability, Perceived severity, Perceived risk, Response efficacy, Self-efficacy, Response cost, Perceived ease of use, Perceived usefulness, Trust belief and Structural assurance). As it is indicated earlier in order to test the 10 hypotheses, the study used linear regression.

4.7.1. HYPOTHESES TESTING

In this research, hypothesis testing was performed on the basis of linear regression analyses. Linear regression is a method to find a relationship between one dependent variable and an independent variables (J. F. Hair. et al, 1992). The independent variables and the dependent variable are integrated and tabulated in SPSS for hypothesis testing. Hypothesis testing is based and relies on

the standardized coefficient significant (P value) and also the standardized coefficient (Beta value). To support the hypothesis, the significant of the standardized coefficient should be below the 0.05 level (the minimum probability to reject or accept the hypothesis) and the standardization coefficient should be greater than 0.1 which is the accepted rate. In order to calculate standardized coefficient (Beta value) and the significant of the standardized coefficient (P value) the following steps were followed:

1. *Independent variables:* Perceived vulnerability, Perceived severity are individually regressed against the dependent variable Perceived risk. (Hypotheses H1, H2).
2. *Independent variables:* Perceived risk, Response efficacy, Self-efficacy and Response cost are individually regressed against the dependent variable Protection motivation in Mobile Banking (Hypotheses H3, H4, H5 and H6).
3. *Independent variables:* Perceived ease of use and Perceived usefulness are individually regressed against the dependent variable Protection motivation in Mobile Banking (Hypotheses H7 and H8).
4. *Independent variables:* Trust belief and Structural assurance are individually regressed against the dependent variable Perceived risk (Hypotheses H9 and H10).

Accordingly, the following results were obtained:

Perceived vulnerability and Perceived risk: Hypothesis 1, that is Perceived vulnerability is positively associated with the individual perceived risk in mobile banking that is accepted because of standardization coefficient that equals to 0.419, which is greater than the accepted rate 0.1 and the significant is 0.000, which is lower than the accepted rate 0.05. This result is similar with the findings of (Crossler, 2010) who said that it is expected that perceived vulnerability has a positive influence on perceived risk. Similarly with Liang and Xue (2010) whom argued that perceived vulnerability has an effect on the formation of perceived risk.

Perceived severity and Perceived risk: Hypothesis 2, that is Perceived severity is positively associated with the individual perceived risk in mobile banking that is accepted because of standardization coefficient that equals to 0.232 which is greater than the accepted rate 0.1 and the significant is 0.003 that is lower than the accepted rate 0.05. This result is again similar with the findings of (Crossler, 2010) who said that it is expected that perceived severity has a positive influence on perceived risk. Similarly with Liang and Xue (2010) whom argued that perceived severity has an effect on the formation of perceived risk.

Table 4.18: Results of linear regression for Perceived vulnerability, Perceived severity and Perceived risk.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.117	.034		3.403	.001
1 Perceived vulnerability:	.488	.089	.419	5.500	.000
Perceived severity	.241	.079	.232	3.050	.003

a. Dependent Variable: Perceived risk

Source. SPSS Result

From the above two hypotheses (H1 and H2): Perceived vulnerability (H1) has the strongest effect in the perceived risk, because standardization coefficient is equal to 0.419 that is greater than the other factor Perceived severity that affect perceived risk.

Perceived risk and Protection motivation in Mobile Banking: Hypothesis 3, Perceived risk is positively associated with the individual protection motivation in mobile banking that is accepted because of standardization coefficient that equals to 0.415 which is greater than the accepted rate 0.1 and the significant is 0.000 that is lower than the accepted rate 0.05. This finding or result is similar with the findings of (Workman *et al.* 2008, Yousafzai *et al.* 2003) whom said that when a risk is perceived, individuals will change their behavior based on how much risk they are willing to accept for the particular threat. According to them, it is expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures.

Table 4.19: Results of linear regression for Perceived risk and Protection Motivation in Mobile Banking.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
1 (Constant)	.071	.032		2.251	.026
Perceived risk	.350	.063	.415	5.545	.000

a. Dependent Variable: Protection Motivation in Mobile Banking

Source. SPSS Result

Response efficacy and Protection Motivation in Mobile Banking: Hypothesis 4, that is Response efficacy is positively associated with the individual protection motivation in mobile banking, but it is rejected because of standardization coefficient that equals to 0.084 that is lower than the accepted rate 0.1 and the significant is 0.333 that is greater than 0.05. This finding or result is on the contrary to the findings of (Milne *et al.* 2000) in which the recommended coping

responses will be effective in reducing threat to the individual. Again this contradicts with the findings of Liang and Xue (2010) whom argued that it is possible that response efficacy, what they call safeguard effectiveness, will have a positive effect on the protection motivation that an individual can perform. This opposite result may be because of the customers' feeling that only following the banks recommended action doesn't guarantee them for taking protective actions. This result may be again because of the bank's themselves that doesn't inform the customers well about how to protect themselves from threats when it happen.

Self-efficacy and Protection motivation in Mobile Banking: Hypothesis 5, Self-efficacy is positively associated with the individual protection motivation in mobile banking that is accepted because of standardization coefficient that equals to 0.475 which is greater than the accepted rate 0.1 and the significant is 0.000 that is lower than the accepted rate 0.05. This finding is similar with the findings of (Milne *et al.*, 2000, Rhee *et al.*, 2009) whom speak of self-efficacy in information security, which they define as "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability". From their finding they argued that the higher the self-efficacy in terms of taking safety measures, the more an individual will be inclined to take such measures. Luarn and Lin (2005) also found that perceived self-efficacy had a significant positive influence on behavioral intention to use an Information System (IS), in our case to take protection action. The result is also supported by the study of Wang *et al.* (2003) who found that computer self-efficacy had a significant positive influence on behavioral intention to take protection action.

Response cost and Protection motivation in Mobile Banking: Hypothesis 6, Response cost is negatively associated with the individual protection motivation in mobile banking that is accepted because of standardization coefficient that equals to 0.173 which is greater than the accepted rate 0.1 and the significant is 0.037 that is lower than the accepted rate 0.05. This finding is also similar with the findings of (Milne *et al.* 2000) whom said the cost of performing the recommended response to the individual will have an effect on the individual's protection motivation action. According to him when the costs of applying safety measures exceed the costs of a potential threat, then the response costs have a negative influence on protection motivation. From this result we understood that customers are thinking of the response costs they perceive will demotivate them in taking protective actions. This may be again because of the lack of information providing by the bank that this cost will not be by no means greater than the threat that may happen.

Table 4.20: Results of linear regression for Response efficacy, Self-efficacy, Response cost and Protection Motivation in Mobile Banking.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
1	(Constant)	.019	.027	.677	.500
	Response efficacy	.070	.072	.084	.971
	Self-efficacy	.430	.078	.475	.000
	Response cost	.152	.072	.173	.037

a. Dependent Variable: Protection Motivation in Mobile Banking. **Source. SPSS Result**

From the above four hypotheses (H3, H4,H5,H6): Self-efficacy (H5) has the strongest effect in the protection motivation in mobile banking, because standardization coefficient is equal 0.475 that is greater than the other factors that affect protection motivation in mobile banking.

Perceived ease of use and Protection Motivation in Mobile Banking: Hypothesis 7, Perceived ease of use is positively associated with the individual protection motivation in mobile banking that is accepted because of standardization coefficient that equals to 0.591 that is greater than the accepted rate 0.1 and the significant is 0.000 that is lower than 0.05. The result is supported by previous research in which there is a positive relationship between perceived ease of use and usage intention (Guriting and Ndubisi, 2006; Luarn and Lin, 2005; Kleijnen *et al.*, 2004; Wang *et al.*, 2003 and Ramayah *et al.*, 2003). Guriting and Ndubisi (2006) also found out that that perceived ease of use had a significant positive effect on behavioral intention to use online banking in Malaysia. Similarly, in the study of Kleijnen *et al.* (2004) about wireless finance in Netherlands, they concluded that perceived ease of use was a significant measure in the development of people's intention to use wireless finance. Ramayah *et al.* (2003) showed that perceived ease of use has a significant impact on the development of initial willingness to use internet banking. The result is also supported by the findings of Wang *et al.* (2003), Adams *et al.* (1992), Davis *et al.* (1989) and Ramayah *et al.* (2002). This finding is also in line with another previous research which revealed the significant relationship between perceived ease of use and intention to use new technology, in which in our case it may be the intention to take protective measures (Kleijnen *et al.*, 2004). Again according to (Davis, 1989), it is an important factor affecting the adoption of new innovation. Similarly it is also an important factor on the use of electronic banking (Poon, 2008). So when we bring to our context it may be applied for the intention to take protective actions at the time of

using mobile banking. Thus, the greater the perceived ease of use, the more likely to be aware of taking protective measures.

Perceived usefulness and Protection Motivation in Mobile Banking: Hypothesis 8, Perceived usefulness is positively associated with the individual protection motivation in mobile banking that is rejected because of the significant that equals to 0.107 that is greater than the accepted rate 0.05. Even if earlier studies have shown that there is a positive relationship between perceived usefulness and usage intention or protection motivation (Luarn and Lin, 2005; Cheong and Park, 2005; Chiu *et al.*, 2005; Wang *et al.*, 2003; and Venkatesh and Morris, 2000). This result is in contradiction with this finding and also with the findings of (Kleijnen *et al.*, 2004) in which there is a significant relationship between perceived usefulness and use of new technology. Similarly this contradicts with the findings of (Davis, 1989; Poon, 2008) in which perceived usefulness is an important factor affecting the adoption of new innovation and also on the use of electronic banking. On the other hand this was to mean it is an important factor for motivating oneself to take protective actions when using mobile banking services, even if the hypothesis is rejected based on the survey. This result may be due to the fact that customers may think the usefulness of the service but they believe that its usefulness doesn't help them for protecting themselves, rather the simplicity and the skill they have will help them to protect themselves from threats. This is the information obtained from the survey questionnaire result.

Table 4.21: Results of linear regression for Perceived ease of use, Perceived usefulness, and Protection Motivation in Mobile Banking.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.026	.029		.895	.372
1 Perceived ease of use	.556	.064	.591	8.689	.000
Perceived usefulness	.085	.052	.110	1.621	.107

a. Dependent Variable: Protection Motivation in Mobile Banking

Source. SPSS Result

From the above two hypotheses (H7 and H8): Perceived ease of use (H7) has the strongest effect for the Protection Motivation in Mobile Banking, because standardization coefficient is equal to 0.591 that is greater than the other factor Perceived usefulness(H8) which is even rejected.

Trust belief and Perceived risk: Hypothesis 9, Trust belief toward a bank will have a negative effect on perceived risks in mobile banking that is accepted because of standardization coefficient that equals to 0.487 which is greater than the accepted rate 0.1 and the significant is 0.000 that is lower than the accepted rate 0.05. This result is similar with the findings of (S.L. Jarvenpaa, N. Tractinsky. (1999); N.K. Malhotra, S.S. Kim, J. Agarwal. (2004)) in which they said that trust belief has been found helpful in explaining how customers may overcome perceived risk and engage in online transactions. According to them Trust plays a critical role in mitigating perceived risks, especially for transactions involving uncertainty. They also added that customers who believe in the technical capability, integrity, and benevolence of their banks are more likely to overcome their risk perceptions toward new services such as the wireless banking situation.

Structural assurance and Perceived risk: Hypothesis 10, Structural assurance has a negative impact on perceived risk that is rejected because of standardization coefficient that equals to -0.033 which is lower than the accepted rate 0.1 and the significant is 0.675 that is greater than the accepted rate 0.05. This result is a contradiction to the findings of (T. Teo, M. Tan, and SN. Peck. (2004)) whom said that similar to trust belief, structural assurance such as promises, guarantees, and contractual protections should also help to alleviate customers' perceived risk in the unfamiliar, open airwave environment. According to them, customers who trust the legal and technology structures of the wireless internet will be more likely to believe their financial data will be protected against loss or theft along transmission. Such belief in the structural soundness of the wireless internet platform is anticipated to lower the perceived risk in wireless banking (mobile banking in our case). But the finding from the survey indicated the opposite result, this may be because of the customers' thinking that they are not sure of the structural soundness of the wireless platform or the bank which provides the services to them. From the survey some of the customers said that even if they think of the assurance of the bank as good, still they have a fear towards the threats that may happen. In one way or another customers do not agree with the structural assurance of the bank and also this doesn't help them not to think of risk when using mobile banking services. Another reason here may be the bank may not work strongly to make customers aware of the bank's structural soundness through different mechanisms, because this may increase the customers' trust toward the structural soundness of the bank.

From the above two hypotheses (H9 and H10): Trust belief (H9) has the strongest effect in the perceived risk in Mobile Banking, because standardization coefficient is equal to 0.487 that is greater than the other factor Structural assurance (H10) which is even rejected.

Table 4.22: Results of linear regression for Trust belief, Structural assurance, and perceived risk in mobile banking.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.175	.041		4.301	.000
1 Trust belief	.587	.093	.487	6.297	.000
Structural assurance	-.029	.069	-.033	-.425	.672

a. Dependent Variable: Perceived risk

Source. SPSS Result

Table 4.23: Summaries of the hypothesis tests.

Hypothesis	Standardization coefficient	Significant	Acceptance/rejection of the hypothesis
H1	0.419	0.000	Accepted
H2	0.232	0.003	Accepted
H3	0.415	0.000	Accepted
H4	0.084	0.333	Rejected
H5	0.475	0.000	Accepted
H6	0.173	0.037	Accepted
H7	0.591	0.000	Accepted
H8	0.110	0.107	Rejected
H9	0.487	0.000	Accepted
H10	-0.033	0.672	Rejected

To conclude all the relations, the study shows that customers' perception towards mobile banking security and a motivation to take protection action is mainly affected by the perceived vulnerability, perceived risk ,self-efficacy ,perceived ease of use and trust belief, even if the perceived severity and also response cost affect the customers' perception towards mobile banking

security. Among all the factors based on our result perceived ease of use is the strongest factor to take protection motivation as it has the largest standard coefficient of 0.591 which is larger than the others.

Generally speaking the attitude of customers' towards mobile banking in Ethiopia is very low as compared to the other African countries. Ethiopians would trust mobile banking least among other African countries. This could be explained by the low bank account and mobile penetration in Ethiopia (Research ICT Africa).

Table 4.24. Attitude towards mobile banking in Africa

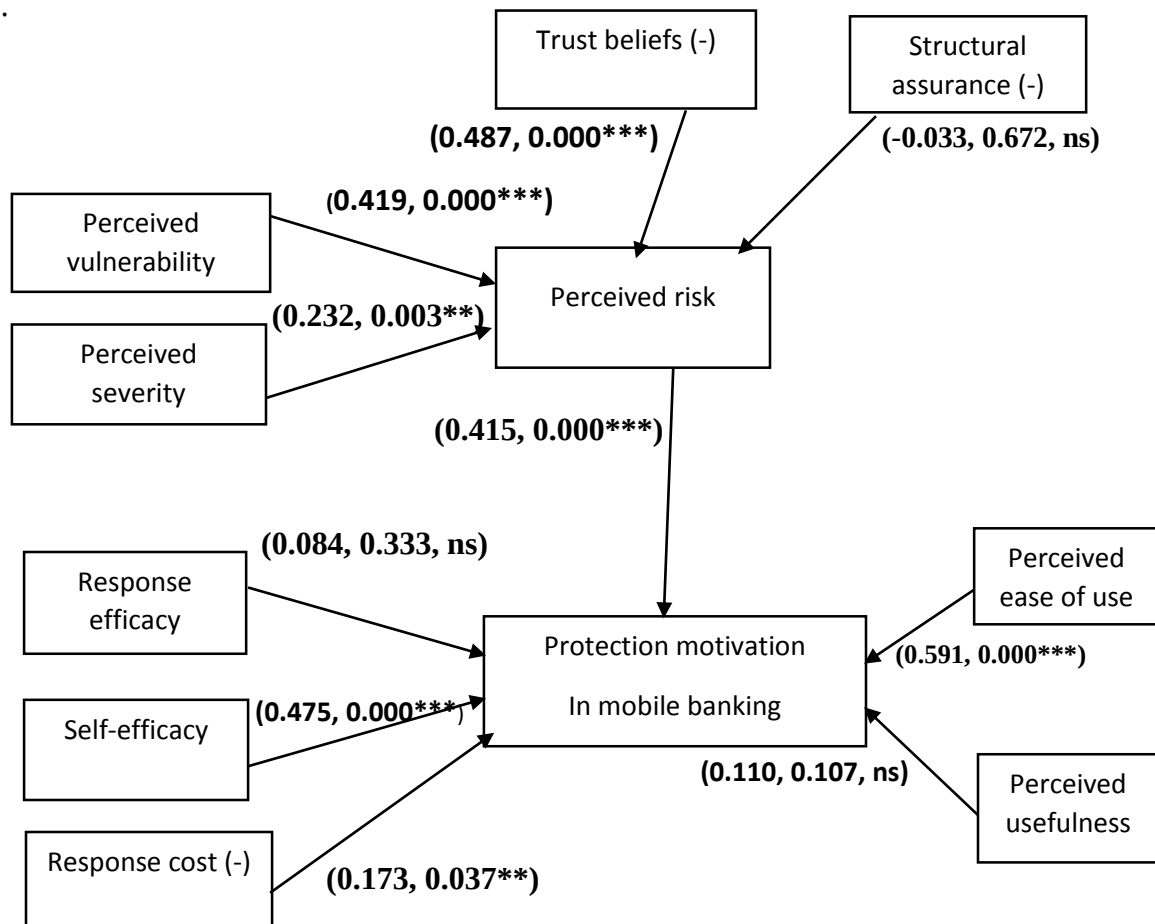
	Mobile phone banking can be trusted if backed by a mobile phone operator	Mobile phone banking can be trusted if backed by a bank	You would consider having your salary (or your main source of income) paid into mobile phone bank account
Benin	12.4%	10.3%	10.2%
Botswana	19.7%	26.3%	44.4%
Burkina Faso	17.6%	13.0%	9.6%
Cameroon	21.0%	21.0%	12.6%
Côte d'Ivoire	10.7%	9.5%	4.5%
Ethiopia	1.9%	1.8%	3.5%
Ghana	39.3%	50.9%	45.7%
Kenya	38.1%	38.7%	38.4%
Mozambique	49.7%	47.7%	47.1%
Namibia	21.3%	20.2%	17.9%
Nigeria*	26.9%	38.0%	19.9%
Rwanda	7.9%	6.9%	4.2%
Senegal	16.0%	15.1%	36.0%
South Africa	30.1%	32.3%	49.4%
Tanzania	14.7%	13.3%	10.9%
Uganda	16.6%	14.9%	22.3%
Zambia*	22.1%	25.3%	16.5%

Source: M-banking the Unbanked, Volume 1, 2008, Policy Paper 4. Research ICT Africa By Alex Comminos, Steve Esselaar, Ali Ndiwalana & Christoph Stork.

From the table above we can understand that the attitude of customers towards mobile banking is very low in Ethiopia as compared to other African countries. This indicates that there is a lot to remain to study and investigate the mobile banking industry in Ethiopia. One of the reasons for

this very low rate of customers' attitude is the perception of insecurity that is what our research tries to address or identify from the various reasons that make customers not to use the technology without being fear of the security concern.

The findings from the linear regression analysis indicates that seven hypotheses were accepted in which three of them were rejected. The rejected ones were hypothesis on response efficacy, perceived usefulness, and structural assurance, the remaining constructs and hypothesis were in line with our research model. The following figure shows the relationship between the model factors.



**** =good *** =very good ns =not significant**

Figure 4.1.The research model and relationship between the factors.

4.8. Qualitative Data Analysis

In addition to the quantitative study, qualitative data analysis is conducted in order to clarify the findings obtained from the survey about the general attitude of customers' towards mobile banking security. This was conducted with the bank's internet and mobile banking manager. As the service is new to the country the whole system is controlled or administered by the central bank branch. Because of this the interview was conducted with one person, who is the manager for the whole branches of the bank offering mobile banking services. So in addition to the questionnaires collected from the customers, an interview was conducted with the bank's internet and mobile banking manager. The interview was taken in the manager's office by scheduling the time and date in prior so that the manager will be free to express his idea. In addition, the interview was taken before and after the collection of the questionnaire so as to clarify some issues that were vague in questionnaire analysis. Before starting the interview sessions, the interviewer first introduced himself and then continued by explaining the aims of the study and how the interview would be carried out. The interviewer assured the informant that all information would be treated with confidentiality. The interview topics included the complains by customers related to mobile banking services, activities that are done by the bank to fully fledge the mobile banking service, the mobile banking development at the bank in general and also others.

According to the manager Ato mintesinot seyoum he said that mobile banking at Commercial Bank of Ethiopia has been started at the end of 2013. He added that the number of subscribers at the time of launching the service was 38,000 in number, but now the number of registered customers reach to 800,000, even if the active users or subscribers are 570,000 in whole country, but in Addis Ababa the number of active subscribers are 355,832 in number. There was also question to the manager related to customers usage and also complains or feedbacks from those customers, and he said that most of the complains by the customers are the transmission channels (network related issues). According to him since the technology is new, customers are not that much comfortable with the service. By looking at the feedback from the customers he said that the bank is trying to do a lot of things including upgrading of the service jointly by working with Ethio-telecom, and he added that the two companies have SLA (service level agreement) in order to upgrade the technology.

According to the manager there are different kinds of channels that are to be provided for the customers, the first channel is the easiest of all that is web based (browser based) which have its

own security system. The other is the application based that the banks application will be installed on the customer's mobile phone in order to do banking activities. These two channels require internet connection to be available. He also said that they are working to improve the band width (smoothing of network break up) for the two channels. The other channel type is SMS (short message service) based. But he said that this service has stopped before two years in which its progress was medium. As described earlier the above two channels require internet connection and also smart phones to be used by customers. They are not SIM card dependent, if the SIM is changed to the other phone as far as there is internet connection it will work, but practically this is not comfortable.

The other channel to be provided or used by customers according to his explanation is USSD (unstructured supplementary data) this works with any type of phone, even if the security system is low for this channel as compared to the others.

Another point raised by the manager related to customer complains was connectivity issue and lack of trust by the customers (due to poor awareness). In order to solve these problems (complains) he said that we do have our own survey department to study customer service satisfaction. According to him he said that they are working on promotion intensively through Medias, friends, brochures and also others.

He also added about the burden on the customers at the time of usage (and also to use the service), according to him, there will be no burden on the customers since there is notification (validation at the time of filling the data system). When he was asked about the development of the service in general, he replied that the development of the service is generally good as compared to other banks. He also added justification about the development, which within the last six months the transaction done using mobile banking had reached to 1.5 billion birr (from July to December 2015).

He also said that there is also training to be given for the customers at the time of registration about activation code, PIN code usage and also change of PIN code and in addition there will be different guidelines that will be given through different brochures. Generally there will be 10 minutes orientation or training at the time of registration. The manager stressed that now a day's mobile banking is working with any type of phone as compared to before, which selects or prefers the use

of smart phones. This makes the service unique at Commercial Bank of Ethiopia as compared to other banks in which the service still selects(depends)on the phone type. But the channel to be selected or used by the different phones will be different. In all other cases mobile banking at Commercial Bank of Ethiopia works with any type of phone.

Finally the manager concluded that we are striving to be the best and the first in our banking services particularly with regard to mobile and internet banking. CBE has a total of 1100 branches all over the country and also 12.4 million account holders. He added that currently in Addis Ababa and near Addis Ababa there are four districts, each district has around 70 branches, so totally in Addis Ababa and near Addis Ababa we have 280 branches and when we focus on the Addis Ababa city only we have around 200 branches which makes our bank the leading bank in terms of customers number and also capital.

4.9. Summary of the Chapter

This chapter details the results of the data analysis based on the data collected from the survey conducted and also from interview. The demographic profile and the perception of respondents towards mobile banking security are described based on the constructs derived from the theoretical model. The reliability and validity of the model factors was also checked using the appropriate statistical tool.

Linear regression analysis techniques are applied to test the predicting capability of the model and to investigate the research hypotheses. The result of the hypothesis testing supports all variables in the research model except response efficacy, structural assurance and perceived usefulness. The results from the linear regression analysis suggest that perceived ease of use, trust belief, self-efficacy, perceived risk, perceived vulnerability are the strongest factors having the highest influence on the customers' perception towards mobile banking security and also for the motivation to take protection action.

Finally, additional related finding which was done on the attitude of customers towards mobile banking in Africa was included to show the general picture of how mobile banking is perceived and used by the customers in Africa, particularly in our country Ethiopia and an interview result was also discussed.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1. Introduction

This chapter presents the summary of key data findings, conclusion drawn from the findings and also the recommendations forwarded, the conclusions and recommendations drawn were focused on addressing the objective of the study. The researcher is intended to determine customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. The contributions and recommendation given in this research work can be used for future research and enhance further development in the mobile banking sector especially for the customers' perception towards mobile banking security. The limitations of the study are also discussed with a conclusion.

5.2. Summary of findings

The study was conducted to determine the customers perception towards mobile banking security with the use of the protection motivation theory (PMT) and also using the two basic constructs of the technology acceptance model (TAM) that are perceived ease of use and also perceived usefulness. Similarly some important constructs of trust which are always in line with the risk concept were also used (these are trust belief and structural assurance).

Bamoriya and Singh (2012) found out in their study that 'security concern' is a significant barrier in using mobile banking, it means banks should focus on the security aspect and need to create awareness that it is as secured as traditional banking channel. As this is the main barrier in using mobile banking our research tries to identify this security perception of customers on the mobile banking usage. To determine the customers' perception the researcher followed some procedures of data collection. Questionnaire was the main tool of data collection, in addition interview was conducted with the bank's internet and mobile banking manager. The questionnaire was consisted of questions like demographic variables and also questions directly related to the constructs of the model. As Bamoriya and Singh (2012) found out that mobile banking usage is not associated with demographic variables except age and education in their respective studies, similar to their finding this research didn't focus on the demographic variables in order to determine the customers' perception towards mobile banking security, since we gave much attention on the constructs or factors that were tested based on the theoretical model and the hypothesis generated. Actually when we look at the frequencies and percentages of the demographic variables there is some

indication on the respondents' age and also educational status in which it indicates the trends of mobile banking usage. From this figure we understood that most of the mobile banking users are between the ages of 20-30 and also they are educated on a degree level. The other demographic variables doesn't have that much important in our research or the analysis results that were generated.

This study was undertaken to create a better understanding of customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. The result indicated that 3 out of 10 hypotheses were rejected. It was found out that after the analysis process, the research results are in line with (Jansen, 2015) and the Chen (2012) study in US and China to investigate how individuals perceive and dealt with online security threats, except that some of the constructs or hypothesis were failed or rejected based on our data collected. From our study it has been revealed that there are some important factors that can determine the perception of customers' towards security and also the motivation to take protection action. The result of our study revealed that customers' perception towards mobile banking security and a motivation to take protection action is mainly affected by the perceived vulnerability, perceived severity, perceived risk, self-efficacy, perceived ease of use and trust belief. Among all the factors based on our result perceived ease of use is the strongest factor to take protection motivation as it has the largest standard coefficient of 0.591 which is larger than the others. The rejected factors or constructs for the failed hypothesis were response efficacy, perceived usefulness, and also the trust construct (i.e. structural assurance).

In order to do the hypothesis test a linear regression analysis was used. The dependent variables (Protection motivation in Mobile Banking and perceived risk) was aggregated with the independent variables. Similar approach was also applied for the independent variables for aggregation (i.e. Perceived vulnerability, Perceived severity, Perceived risk, Response efficacy, Self-efficacy, Response cost, Perceived ease of use, Perceived usefulness, Trust belief and Structural assurance). Hypothesis testing was based and relied on the standardized coefficient significant (P value) and also the standardized coefficient (Beta value). To support the hypothesis, the significant of the standardized coefficient should be below the 0.05 level and the standardization coefficient should be greater than 0.1 which is the accepted rate.

As we said our research model studied or tested 10 constructs such as Perceived vulnerability, Perceived severity, Perceived risk, Response efficacy, Self-efficacy, Response cost, Perceived ease

of use, Perceived usefulness, Trust belief and Structural assurance and also protection motivation towards mobile banking.

It was found out that Perceived vulnerability is positively associated with the individual perceived risk in mobile banking with standardization coefficient that equals to 0.419, and the significant which is equal to 0.000. This result is similar with the findings of (Crossler, 2010) who said that it is expected that perceived vulnerability has a positive influence on perceived risk. Similarly with Liang and Xue (2010) whom argued that perceived vulnerability has an effect on the formation of perceived risk.

Similarly Perceived severity is positively associated with the individual perceived risk in mobile banking with standardization coefficient that equals to 0.232, and the significant which is equal to 0.003. This result is again similar with the findings of (Crossler, 2010) who said that it is expected that perceived severity has a positive influence on perceived risk. Similarly with Liang and Xue (2010) whom argued that perceived severity has an effect on the formation of perceived risk.

Perceived risk is positively associated with the individual protection motivation in mobile banking as standardization coefficient that equals to 0.415 and the significant is equal to 0.000. This finding or result is similar with the findings of (Workman *et al.* 2008, Yousafzai *et al.* 2003) whom said that when a risk is perceived, individuals will change their behavior based on how much risk they are willing to accept for the particular threat. According to them, it is expected that the higher the perceived risk, the more likely a customer will be inclined to take protective measures.

Response efficacy is positively associated with the individual protection motivation in mobile banking. This hypothesis was rejected since standardization coefficient is equals to 0.084 and the significant is 0.333. This finding or result is on the contrary to the findings of (Milne *et al.* 2000) in which the recommended coping responses will be effective in reducing threat to the individual. Again this contradicts with the findings of Liang and Xue (2010) whom argued that it is possible that response efficacy, what they call safeguard effectiveness, will have a positive effect on the protection motivation that an individual can perform. This result is obtained based on the responses of the customers that they doesn't think that the response efficacy doesn't motivate them to take protection action. Here there is an indication that the bank is expected to do a lot to inform customers about how their response efficacy will help them in protecting themselves from threats.

Self-efficacy is positively associated with the individual protection motivation in mobile banking as standardization coefficient that equals to 0.475, and the significant is equal to 0.000. This finding is similar with the findings of (Milne *et al.*, 2000, Rhee *et al.*, 2009), they argued that the higher the self-efficacy in terms of taking safety measures, the more an individual will be inclined to take such measures. Luarn and Lin (2005) also found that perceived self-efficacy had a significant positive influence on behavioral intention to use an Information System (IS), in our case to take protection action. The result is also supported by the study of Wang *et al.* (2003) who found that computer self-efficacy had a significant positive influence on behavioral intention to take protection action.

Response cost is negatively associated with the individual protection motivation in mobile banking as standardization coefficient that equals to 0.173, and the significant is equal to 0.037. Prior studies (Luarn & Lin, 2004) strongly support perceived cost (in our case response cost) is important factor influencing user behavior. This finding is also similar with the findings of (Milne *et al.* 2000) whom said the cost of performing the recommended response to the individual will have an effect on the individuals' protection motivation action. Here the banks should provide as much information as possible so as to inform the customers' that this cost will not be by no means greater than the threat that may happen.

Perceived ease of use is positively associated with the individual protection motivation in mobile banking as standardization coefficient that equals to 0.591, and the significant is equal to 0.000. The result is supported by (Luarn and Lin, 2005; Kleijnen *et al.*, 2004; Wang *et al.*, 2003 and Ramayah *et al.*, 2003). Similarly this result is supported by Guriting and Ndubisi (2006). Similarly this result is supported by Ramayah *et al.* (2003). So many researches support that the easiness of the service will make users to use it freely and also this easiness motivates them to take protection action.

Perceived usefulness is positively associated with the individual protection motivation in mobile banking. This is rejected according to our finding as the significant that equals to 0.107. This result is in contradiction with (Luarn and Lin, 2005; Cheong and Park, 2005; Chiu *et al.*, 2005; Wang *et al.*, 2003; and Venkatesh and Morris, 2000) whom argued that there is a positive relationship between perceived usefulness and usage intention or protection motivation. Similarly it contradicts with the findings of (Kleijnen *et al.*, 2004) in which there is a significant relationship between perceived usefulness and use of new technology. It is also in contradiction with (Ali and

Bharadwaj, 2010) whom argued that adoption (in our case protection motivation) will not take place unless customers perceive the service to be useful. Even if perceived usefulness is one important component for the acceptance of new technology, it is in contrast to this incase of our finding, because our research is not on the acceptance of the technology rather on the perception of the security of mobile banking and the motivation to take protection action. So in our finding respondents said that it is not the usefulness rather the simplicity of the service that motivates us to take protection action.

Trust belief toward a bank will have a negative effect on perceived risks in mobile banking as standardization coefficient that equals to 0.487, and the significant is equal to 0.000. This result is similar with the findings of (S.L. Jarvenpaa, N. Tractinsky. (1999); N.K. Malhotra, S.S. Kim, J. Agarwal. (2004)) in which they said that trust belief has been found helpful in explaining how customers may overcome perceived risk and engage in online transactions.

Structural assurance has a negative impact on perceived risk. This is rejected because as standardization coefficient that equals to -0.033, and the significant is 0.675. This result is a contradiction to the findings of (T. Teo, M. Tan, and SN. Peck. (2004)) whom said that similar to trust belief, structural assurance such as promises, guarantees, and contractual protections should also help to alleviate customers' perceived risk in the unfamiliar, open airwave environment. But the finding from the survey indicated the opposite result, this may be because of the customers thinking that they are not sure of the structural soundness of the wireless platform or the bank which provides the services to them. From the survey some of the customers said that even if they think of the assurance of the bank as good, still they have a fear towards the threats that may happen. Here there is an indication that the bank is expected to do a lot of tasks regarding the awareness creation activity and also making the customers to be reliable on the bank by giving them trainings and also community based education on the service.

To conclude all the findings the bank or the concerned body should work strongly to enhance the customers' perception towards mobile banking security based on these important factors and also a great attention should be given for the other factors like response efficacy, perceived usefulness and also structural assurance.

5.3. Conclusion

It is well recognized that mobile phones have immense potential of conducting financial transactions thus leading the financial growth with lot of convenience and much reduced cost. For inclusive growth, the benefits of mobile banking should reach to the common man at the remotest locations in the country. For this all stakeholders like Regulators, Government, telecom service providers and mobile device manufactures need to make efforts, so that penetration of mobile banking reaches from high-end to low-end users and from main cities to the middle towns and rural areas. Inclusion of non-banking population in financial main stream will benefit all. There is also need to generate awareness about the mobile banking so that more and more people use it for their benefit.

As the mobile banking technology is new in Ethiopia it is good to understand customers' perception towards mobile banking security, since the number of users or subscribers is too limited compared to the number of actual mobile phone users(from the interview). The findings in this study offer insights to the Commercial Bank of Ethiopia and also other private and government banks in the country in promoting the use of mobile banking among bank customers. In order to achieve this, it is important for the Commercial Bank to take into account the factors that this study had found to impact on perception of customers towards mobile banking security.

This research seeks to answer the questions in line with the research objectives. The quantitative and qualitative approach were used which contained opened and close-ended questions, semi-structured interviews were also conducted. There was a use of statistical analysis to determine the results of the collected data. Looking at the research question for this study, which was to assess the customers' perception towards mobile banking security at Commercial Bank of Ethiopia in Addis Ababa, in comparison with the present or current customers' usage trends, it clearly shows that, the customers' perception towards mobile banking security is affected by important factors like perceived vulnerability, perceived severity, perceived risk, self-efficacy, response cost, perceived ease of use and trust belief. This shows that, customers are truly affected by the factors which have been described in the research framework. Similarly the research result clearly shows that there exists relationship between factors that affect the customers' perception towards this mobile banking security. Among these factors the main important factors that affect customers perception towards mobile banking security are mainly five of the factors these are perceived

vulnerability, perceived risk, self-efficacy, perceived ease of use and trust belief. These factors can be utilized to formulate good promotional strategies in enhancing the use of mobile banking among the customers of the bank.

This research findings are in line with the findings of (Jansen, 2015), Chen (2012), Davis (1989), and (Luarn & Lin 2005) whom tried to explore the individual security behaviors in different contexts and also whom explored about the two basic constructs of TAM (perceived ease of use and perceived usefulness) respectively. But the research result has also draw backs, in which it contradicts with the findings of the above mentioned scholars, because as it was previously mentioned there were three hypothesis or constructs which were rejected and there is an indication for the researchers to investigate further on these factors by adding some other constructs to the used or tested theoretical framework.

The study also leads to the following conclusions:

1. First, it successfully confirms the applicability of the PMT and also TAM with trust constructs to mobile banking security context. From the model it was found that self-efficacy, perceived vulnerability, perceived severity, perceived risk, response cost, and perceived ease of use and also trust belief were significant factors for the motivation to take protection action when using mobile banking, making self-efficacy as the strongest factor for the motivation of customers to take protection action.
2. Second, this study supports Wang *et al.*'s (2003) research findings that there is a significant direct relationship between perceived self-efficacy and behavioral intention to use online banking, and may extend its generalizability to mobile banking context; and also the motivation to take protection action when using mobile banking.

5.4.Recommendation

This study have found out seven dimensions on the security perceptions of mobile banking service. Banking practitioners and mangers can use these dimensions to measure the effectiveness of service provided by them. The finding can be used to manage organization resources and provide higher quality of services to their customers. This will result in retaining of customer and thereby lowering the cost of acquiring new customer. They may give special attention to the factors such as self-efficacy, perceived ease of use, perceived risk, trust belief, and also perceived vulnerability

aspects, which will further enhance the confidence levels of the customer in using this facility and which will have a positive impact on the customers' perception.

The findings of this study have implications for developing usable mobile banking systems for the bank. Research and development associated with mobile banking systems involves too much investments in terms of money and also time. So it is very important for the bank to ensure that bank customers use mobile banking as a new form of banking without being fear of the technology. In order to achieve this goal, the following suggestions/recommendations/ may render ways to attract bank customers to utilize mobile banking in the future:

1. The bank should give more attention to the awareness creation about the mobile banking service, especially to those factors like response efficacy, perceived usefulness and also structural assurance.
2. The bank should develop the belief of usefulness, response efficacy, and structural assurance by providing sufficient information on the benefits of mobile banking. In order to achieve this, banks should provide user manual that contains details on mobile banking, including usefulness, response efficacy and structural assurance.
3. The Bank should also have counters for mobile banking customers. These counters can offer advice and assistance to bank customers, focusing on the usefulness, response efficacy, and structural assurance factors of mobile banking. By having these counters, bank customers will be able to learn about mobile banking. This, in turn, will influence customers' decision to use the mobile banking without being concerned of security issues.
4. Attention should be given to the risks which could affect day-to-day transactions performed through mobile devices. Thus, it should be eliminated or reduced in order to enhance customers trust in the banking services being offered. So creating trust on the customers is having acritical value.
5. The Bank should ensure safety measures such as firewalls, intrusion detection and other related security devices which are properly developed and incorporated in the mobile banking systems. In addition, banks should also stress the importance of confidentiality of personal identification number (PIN) in mobile banking. This also enhances the perception of customers towards mobile banking security positively. Again this strongly influences the customers trust towards the bank.

6. To motivate customers to use this technology without fear of security, the bank should try to increase the level of service expansion periodically as it should offer versatility in its offerings.
7. The Bank can be more focused on the development of self-efficacy. In order to promote a bank customers' perception towards mobile banking security and protection motivation, enhancing the self-efficacy of the customer for using mobile banking is important. So the bank should organize training courses in various mobile commerce applications. This will increase bank customers' familiarity and understanding of mobile banking and this may influence their perception of security towards mobile banking and use the service freely.
8. Technical infrastructure of mobile banking services should be sophisticated and developed in order to ensure reliable and timely offering of services to customers.
9. There is a need to change the customer's perception through a well-structured advertisement and staff interaction in order to make them realize that the service is safe to use.
10. The bank should also ensure that the cost of mobile banking service is reasonable and affordable for students, officer workers, business person, etc. in order not to discourage current users and the intending users.
11. Attention should be given to students in educational institutions as they consist of a larger population of the country due to their favorable attitude towards new innovation and this is also evident that the majority of our respondents were students.
12. The bank staffs should be trained and be knowledgeable about how to use the self-service, so as to provide support for customers.

5.5. Limitation and future research

Although this research is primarily based on the primary data from the users of mobile banking, the findings cannot be generalized. This study has successfully examined the major factors responsible for mobile banking based on respondents' perception of security on the technology; future research may include examining the factors importance.

The further research of this study's frame work can be useful to advance knowledge about the perception of customers' towards mobile banking security. A number of issues remain to be addressed. First, the investigation of mobile banking security perceptions in this study suggests ten constructs only to gauge customers' perception towards mobile banking security and also the

protection motivation associated with it. However, these constructs can be integrated with others to provide a more comprehensive understanding of mobile banking security perception of customers' and also the protection motivation associated with it. In our theoretical model the whole PMT constructs were not used and also the basic constructs of the TAM model were only used with some additional constructs of trust. There is a need, therefore, to explore additional constructs that can predict customers' perception towards mobile banking security and also protection motivation more accurately. For a suggestion, new measures such as attitude, demographic variables, and prior computing experience can be applied in the model for future research. The location and the sample of this study is only confined to Addis Ababa city and Commercial Bank of Ethiopia and this may not represent the whole customers of the bank country wide and also for other banks. Future research can improve on this limitation by increasing the sample size and performing future research across the whole country in Ethiopia and also among other banks operating in Addis Ababa. Furthermore the study could go for a better understanding on other segments of the industry such as M-Health, M-Education and M-Government to support mobile technology and its services and abilities. Further researches could be conducted by looking at the customers' demographic characteristics with the model constructs to determine the perception of mobile banking security by the customers.

Despite these limitations, the present study serves as a pilot study to explore bank customers' perception towards mobile banking security. This research work has been able to contribute to the literature on customers' behavior and mobile banking security and it can also bridge the gap which exists between developed countries and developing countries with particular reference to Ethiopia. The study will be able to add to the limited knowledge available on mobile banking studies in Ethiopia particularly the individual security behaviors.

Perceptions of users may change over time when users have gained more experience (Mathieson et al., 2001; Venkatesh & Davis, 1996). So it may be useful to redo and re-evaluate this research and the study after a certain period of time as the results may be expected to be affected by the time.

REFERENCES

- Ahmed, H 2011, "E-banking Adoption Model in Palestine", MA thesis, An-Najah National University, Palestine.
- Amaratunga, D., Baldry, D., Sarshar, M. & Newton, R 2001, "Quantitative and qualitative research in the built environment: application of mixed research approach." *Management*, vol. 17, no. 1.
- Anderson, C.L. and Agarwal, R 2010, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34, No. 3, pp613–643.
- Ashta, A 2010, *Evolution of Mobile banking Regulations*.
- Ayana Gemechu 2014, *Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry* *Journal of Management Information System and E-commerce*, Vol. 1, No. 1; June 2014 1.
- Banzal S 2010, *Mobile Banking & M-Commerce and Related Issues*.
- Barnes, S.J. & Corbitt, B 2003, Mobile banking: "concept and potential." *International Journal of Mobile Communications*, vol. 1, no. 3, pp. 273-288.
- Blaxter, L., Hughes, C., & Tight, M. 2006, *How to Research*, 3rd edn, Open University Press, England.
- Chen, Y 2012, *Three essays on internet security-understanding users' security perceptions and behaviors* (Doctoral dissertation, The University of Wisconsin-Milwaukee).
- Clark, Adam 2008, *Mobile banking & Switching*.
- Consumer and Mobile Financial Services, Board of Governors of the Federal Reserve System, March 2012.
- Creswell, W 2003, "Research Design: Qualitative, Quantitative and Mixed Approaches" 2nd edition. Sage publication, California.
- Crossler, R. and Belanger, F 2014, "An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument", *ACM SIGMIS Database*, Vol. 45, No. 4, pp51–71.

Crossler, R. E 2010, Protection motivation theory: Understanding determinants to backing up personal data. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on* (pp. 1-10). IEEE.

D. C. Fonchamnyo 2013, "Customers' Perception of E-banking Adoption in Cameroon: An Empirical Assessment of an Extended TAM". *International Journal of Economics and Finance*, vol. 5, no. 1, pp. 166-176. Edition, Prentice-Hall, Englewood Cliffs, NJ.

D. Gefen, E. Karahanna, D. Straub 2003, Trust and TAM in online shopping: an integrated model, *MIS Quarterly* 27 (1) 51–90.

D.H. McKnight, N.L. Chervany, C. Kacmar 2002, Developing and validating trust measures for e commerce, *Information Systems Research* 13 (3) 344–359.

Davis, F.D 1989, "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology." *MIS Quarterly*.

Dinev, T. and Hu, Q 2005, "The centrality of awareness in the formation of user behavioral intention toward preventive technologies in the context of voluntary use", *Proceedings of the International Conference of Information Systems*, pp1–5.

E. E. Ibrahim, M. Joseph, and K. I. N. Ibeh 2006, "Customers' Perception of Electronic Service Delivery in the UK Retail Banking Sector," *International Journal of Bank marketing* vol. 24, no. 7, pp. 475- 493.

Elissa Jobson 2013, The mobile banking game-changer in Ethiopia.

Fain, D., and Roberts, M. L 1997, Technology vs. consumer behavior: the battle for the financial services customer. *Journal of Direct Marketing*, 11(1), 44-54.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W 2000), "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 2, pp 407–429.

Furnell, S.M., Jusoh, A. and Katsabas, D 2006, "The challenges of understanding and using security: A survey of end-users" *Computers & Security*, Vol. 25, No.1, pp27–35.

Gardachew, W 2010), 'Electronic -banking in Ethiopia: practices, opportunities and Challenges', *Journal of internet Banking and commerce*, 15(2):2-9.

H. H. Bauer, M. Hammerschmidt, and T. Falk 2005, “Measuring the Quality of E-Banking Portals”, *International Journal of Bank Marketing*, vol. 23, no. 2, pp. 153-175, 2005.

Hair, et al. 2006, *Marketing Research*, with in changing information environment, 3rd edition, Tata McGraw-Hill Publishing Company limited, New Delhi.

Hayat Muhammad Aslam 2009, *Mobile payments: Will Colombo keep its leadership in South Asia?*

Henok Arega Asfaw 2015, *Financial Inclusion through Mobile Banking: Challenges and Prospects*. Monetary and Financial Analysis Directorate, National Bank of Ethiopia, Addis Ababa

Herath, T., and Rao, H. R 2009, Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, 18(2), 106-125.

Hussey, J., & Hussey, R 1997, *Business Research*, Basingstoke: Macmillan Press Ltd.

Ifinedo, P 2012, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31, No. 1, pp83–95.

International Telecommunication Union 2007, *Telecommunication/ICT markets and trends in Africa*, ITU.

J. C. Nunnally 1978, *Psychometric Theory*, 2nd edition New York: McGraw-Hill, 1978.

J. Peppard 2000, “Customer Relationship Management (CRM) in Financial Services,” *European Management Journal*, vol. 18, no. 3, p. 312–327.

Jansen, J 2015, *Studying Safe Online Banking Behavior: A Protection Motivation Theory Approach*.

Johnston, A. C., and Warkentin, M 2010, Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 34(3), 549-566.

K. Cherry 2013, *What is reliability?*

Kim, G., Shin, B., and Lee, H.G 2009, Understanding dynamics between initial trust and usage intentions of mobile banking. *Information Systems Journal*, 19(3), 283–311.

- Kuisma, T., Laukkanen, T., and Hiltunen, M 2007, Mapping the reasons for resistance to Internet banking: a means-end approach. *International Journal of Information Management*, 27(2).
- Laforet, S., & Li, X.Y 2005, Consumers' attitudes towards online and mobile banking in China. *International Journal of Bank Marketing*, 23 (5).
- Lassar, W.M 2005, The Relationship between Consumer Innovativeness, Personal Characteristics, and Online Banking Adoption. *International Journal of Bank Marketing*, 23(2), 176-199.
- Laukkanen, P., Sinkkonen, S., Kivijarvi, M., and Laukkanen, P 2007, Segmenting Bank Customers by Resistance to Mobile Banking. The Sixth International Conference on the Management of Mobile Business (ICMB 2007).IEEE.
- Laukkanen, T 2005, Comparing Consumer Value Creation in Internet and Mobile Banking. *Proceedings of the International Conference on Mobile Business*. IEEE.
- Lee, Y 2011, Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361-369.
- Lee, Y. and Larsen, K.R 2009, "Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software", *European Journal of Information Systems*, Vol. 18, No. 2, pp177–187.
- Liang, H. and Xue, Y 2009, "Avoidance of information technology threats: A theoretical Perspective", *MIS Quarterly*, Vol. 33, No. 1, pp71–90.
- Lichtenstein, S., Williamson, K 2006, Understanding consumer adoption of internet banking: an interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, 7 (2), 50–66.
- Luarn, P. and Lin, H-H 2005, "Toward an understanding of the behavioral intention to use mobile banking." *Computers in Human behavior*, vol. 21, no. 6.
- Luo, X., Li, H., Zhang, J., & Shim, J. P 2010), Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision support systems*, 49(2), 222-234.

Mallat, N., Rossi, M. and Tuunainen, V. K 2004, "Mobile Banking Services." *Communications of the ACM*, vol. 47, no. 5, pp. 42-46.

Maria 2008, "Advantages and disadvantages of secondary research" vol. 1, pp.1-5.

Mattila, M 2003, Factors affecting the adopting of mobile banking services. *Journal of Internet Banking and Commerce*, vol. 8, no. 1.

Mehta Shalini 2012, "Mobile banking in India does not need a one-size-fits-all solution".

Mengistu, A 2011, Customer service satisfaction: The case of Commercial Bank of Ethiopia. Addis Ababa University. <http://www.aau.edu.et/>

Michael Ardovino 2007, Mobile Phones and Mobile Banking in Ethiopia. USAID KNOWLEDGE SERVICES CENTER (KSC) 9, 2007.

Milne, S., Sheeran, P. and Orbell, S 2000, "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory", *Journal of Applied Social Psychology*, Vol. 30, No. 1, pp106–143.

MMA 2009, Mobile Banking Overview.

Mohammed Arif Shaikh 2014, Ethiopian Banker's Perception of Electronic Banking in Ethiopia – A Case of Adama City.

N.K. Malhotra, S.S. Kim, J. Agarwal 2004, Internet Users' Information Privacy Concerns (IUIPC): the construct, the scale, and a causal model, *Information Systems Research* 15 (4) 336–355.

Nah, F., Siau, K., and Sheng, H 2005, The Value of Mobile Applications: A Study on a Public Utility Company. *Communications of the ACM*, 48 (2), 85-90.

Ng, B-Y., Kankanhalli, A. and Xu, Y.C 2009, "Studying users' computer security behavior: A health belief perspective", *Decision Support Systems*, Vol. 46, No. 4, pp. 815 825.

Olatokun, W. M and Igbinedion, L.J 2009, "The Adoption of Automatic Teller Machines in Nigeria: An Application of the Theory of Diffusion of innovation", *Issues in Informing Sciences and Information Technology*, 6(1), pp373-393.

Porteous, D 2006, The Enabling Environment for Mobile Banking in Africa, *Bankable frontier*.

Regulation of Mobile and Agent Banking Services Directives No. FIS /01/2012, National Bank of Ethiopia.

Rhee, H.-S., Kim, C. and Ryu, Y.U 2009, "Self-efficacy in information security: Its influence on end users' information security practice behavior", *Computers & Security*, Vol. 28, No. 8, pp816–826.

Rogers, E. M 2003, *Diffusion of Innovations*. New York: Free Press.

Rogers, R.W 1975, "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol. 91, No. 1, pp93–114.

S. Laforet and X. Li 2005, "Consumers' attitudes towards online and mobile banking in China," *International Journal of Bank Marketing*, vol. 23, no. 5, pp. 362-380.

S.L. Jarvenpaa, N. Tractinsky 1999, Consumer trust in an internet store: a cross-cultural validation, *Journal of Computer-Mediated Communication* 5 (2) 1–35.

Saunders, M., Lewis, P. and Thornhill, A 2009, *Research methods for business students*, Financial Times/Prentice Hall.

Saunders, M., Thornhill, A 2003, Organizational justice, trust and the management of change an exploration, *Personnel Review* Vol.32, No.3, pp.360-375

Siau, K., and Shen, Z 2003, Building customer trust in mobile commerce. *Communications of the ACM*, 46(4), 91-94.

Silverman, D 2001, *Interpreting qualitative Data*, 2nd Ed. Sage Publication Ltd. London.

Stair, R.M. and Reynolds, G 2008, *Fundamentals of Information Systems*, 5th edn, Course Technology, USA.

Straub, D., M.-C. Boudreau, and D. Gefen 2004, "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (14) pp. 380-426.

T. Teo, M. Tan, S.N. Peck 2004, Adopters and non-adopters of Internet stock trading in Singapore, *Behavior & Information Technology* 23 (3) 211–223.

- Teshome, A., Tridib, B., and Solomon, N 2014, Electronic payment adoption in the banking sector of low income countries. Addis Ababa University. <http://www.aau.edu.et/>
- Trappey, C.V., Trappey, A.J.C 2001, Electronic commerce in Greater China. *Industrial Management and Data Systems*, 101(5), 201-220.
- UNCTAD 2007, Science and Technology for Development: A New Paradigm for ICT, Information Economy Report, New York.
- Various 2007, Principles of marketing, Global Media, India.
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D 2003, User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 425-478.
- Vinayagamoorthy, A., Sankar, C 2012, Mobile Banking—An Overview. *Advances in Management*. 5(10), 24-29.
- Wang, Y.S., Wang, Y.M., Lin, H.H., and Tang, T.I 2003, Determinants of user acceptance of internet banking: An empirical study. *International Journal of Service Industry Management*, 14(5), 501-519.
- Willis, G. B 2005, Cognitive interviewing: A tool for improving questionnaire design, Sage Publications, USA.
- Woon, I., Tan, G. W., Low, R 2005, A protection motivation theory approach to home wireless security. *ICIS 2005 Proceedings*, 31.
- Workman, M., Bommer, W.H. and Straub, D 2008, "Security lapses and the omission of information security measures: A threat control model and empirical test", *Computers in Human Behavior*, Vol. 24, No. 6, pp2799–2816.
- Y, Shi 2009, Factors influencing the use of mobile banking: The case of SMS based mobile banking.
- Yohannes, A 2010, Key factors that determine adoption of internet banking in Ethiopia. Addis Ababa University. <http://www.aau.edu.et/>

Yousafzai, S., Pallister, J. and Foxall, G 2009, "Multi-dimensional role of trust in Internet banking adoption", *The Service Industries Journal*, Vol. 29, No. 5, pp591–605.

Zelege Sira and Yitbarek Takele 2013, Analysis of factors influencing customers' intention to the adoption of e-banking service channels in Bahir Dar city: an integration of TAM, TPB AND PR.

APPENDICES

Appendix 1 – Questionnaire.

March, 2016.

Questionnaire to be filled by Customers

Dear Sir/Madam

I am conducting research on customers' perception towards mobile banking security at Commercial Bank of Ethiopia for my master's degree in information science at Addis Ababa University. Here I kindly request you to attempt all the questions in the questionnaire, as this will help me to complete my study.

The use of mobile phone to make transaction such as fund transfer, viewing of account balance, notification of account balance, payment of bill, etc., is known as mobile banking. Mobile banking security perception is related to customers view point, how they think of the service in terms of safety, threats or attacks, hacks, risks ,trust on the bank and also on the transmission channel(wireless platform) etc.

The information given will be treated as confidential and for the purpose it is been collected for. Please, your assistance will be highly appreciated. There is no need to write your name.

I thank you in advance.

Hailieyesus Kindie

Tell: 0911-812378

E-mail: hahem2012@yahoo.com

If you have any question with regard to the questionnaire please contact me using the above mentioned address.

General Instruction

This questionnaire contains three sections and 8 pages. Please provide your responses to the questions based on the instructions under each section. If you have any comments or if you want to provide further explanations, please use the space provided at the end of the questions.

Section I: Demographic profile of respondents

Instruction I: Please answer the following questions by ticking (✓) on the boxes in front of the response options:

1. Gender: Male: ☐ Female: ☐
2. Age: 20-30 ☐ 31-40 ☐ 41-50 ☐ 51-60 ☐
above 60 ☐
3. Current educational level:

Illiterate ☐ Primary ☐ High school ☐ TVET ☐

Diploma ☐ Degree ☐ Masters ☐ Doctorate ☐

Above doctorate ☐
4. Marital status: Single ☐ Married ☐ Divorced ☐ Widowed ☐
5. Occupation: Unemployed ☐ Student ☐ Salaried ☐ Business man/woman ☐

Pensioner ☐ Other ☐

Section II: Questions related with customers' perception towards mobile banking security at Commercial Bank of Ethiopia. (Yes/No questions)

Instruction II: Please answer the following questions by ticking (✓) on the boxes in front of the response options:

Perceived vulnerability:

1. Do you think using mobile banking is vulnerable to threats or attacks and does this makes you to think of risk in mobile banking security?

Yes ☐ No ☐

If no, explain why

.....
.....

Perceived severity

2. Do you think threat or failure in mobile banking service is sever if it happens and does this makes you to think of risk in mobile banking security?

Yes ☐ No ☐

If no, explain why

.....
.....

Perceived risk

3. Do you perceive there is risk in using mobile banking and does this enforces or pushes you to take protection motivation/action/ when using mobile banking so as to avoid risks?

Yes ☐ No ☐

If no, explain why

.....
.....

Response efficacy

4. Are you ready or willing to perform the bank's recommended actions properly so as to avoid risks and does this will help you to take protection motivation/action/ when using mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Self-efficacy

5. Are you capable or skilled to take the bank's recommended actions and does this will help you to take protection motivation/action/ when using mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Response cost

6. Do you think that doing or following the bank's recommended actions will have some expenses in terms of time and cost and does this will not push you to take protection motivation/action/ when using mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Perceived ease of use

7. Do you think mobile banking is easy to use and does this will help you to take protection motivation/action/ when using mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Perceived usefulness

8. Do you think mobile banking is useful and does this will help you to take protection motivation/action/ when using mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Trust belief

9. Do you have any trust on the bank that provides mobile banking service to you and does this will make you not to think of risks in mobile banking?

Yes ☐ No ☐

If no, explain why

.....
.....

Structural assurance

10. Is the bank is a legislative or a legal institution that will be responsible for the problems or risks that may happen on you and have a good transmission channel for successful completion of financial transactions with it and does this makes you not to think of risks in mobile banking?

Yes ☐

No ☐

If no, explain why

.....
.....

Protection motivation in mobile banking

11. Are you concerned with security issues when using mobile banking services and does this leads you have motivation to take protection action?

Yes ☐

No ☐

If no, explain why

.....
.....

12. In order to enhance subscribers' confidence and avoid threats in using mobile banking could you suggest how the bank can improve mobile banking service?

.....
.....

Section III: Questions related with customers perception about mobile banking security at Commercial Bank of Ethiopia in Addis Ababa. (Using a 5 point Likert scale)

Instruction III: Below are lists of statements or pertaining Questions related with customers' perception towards mobile banking security. Please indicate whether you agree or disagree with each statement by ticking (✓) on the spaces that specify your choice from the options that range from "strongly agree" to, "strongly disagree". Each choice was identified by numbers ranged from 1 to 5.

Note: SA- Strongly Agree, A- Agree, N- Neutral, D- Disagree, SD- Strongly Disagree

No	Questions related with customers perception about mobile banking security.	SA 1	A 2	N 3	D 4	SD 5
	I. PERCIVED VULNERABILITY					
1.	Using of mobile phones for banking transactions is vulnerable to threats.	()	()	()	()	()
2.	Due to this vulnerability I think of risk in mobile banking security.	()	()	()	()	()
	II. PERCIVED SEVERITY					
3.	If I make mistakes in time of using mobile banking, the risk will be sever on me.	()	()	()	()	()
4.	Due to this severity I always think of risk in mobile banking security	()	()	()	()	()
	III. PERCIVED RISK					
5.	There is risk in using mobile phones for banking transactions.	()	()	()	()	()
6.	As a mobile banking user if I lose the mobile phone, in the meantime I will lose my money as well.	()	()	()	()	()
7.	Mobile banking is unreliable because I afraid that my personal or transaction detail would be leaked during message passing.	()	()	()	()	()
8.	Mobile banking is one of new useful technology applications, but I am still aware of its security during the transactions.	()	()	()	()	()
	IV. RESPONSE EFFICACY					
9.	I am ready or willing to take the banks recommended actions.	()	()	()	()	()
10.	Taking the bank's recommended actions will help me to protect myself from threats.	()	()	()	()	()
	V. SELF EFFICACY					

11.	I do have prior experience in using computers and other devices.	()	()	()	()	()
12.	I am fully confident and skilled to take protective actions to the threats that may happen.	()	()	()	()	()
	VI. RESPONSE COST					
13.	There will be cost that may be incurred during an attempt to protect my self	()	()	()	()	()
14.	Following the banks recommended actions will increase my banking costs.	()	()	()	()	()
	VII. PERCEIVED EASE OF USE					
15.	Easiness of mobile banking have made me to protect myself from threats.	()	()	()	()	()
16.	Learning to use mobile banking is easy for me.	()	()	()	()	()
	VIII. PERCIVED USEFULNESS					
17.	I find mobile banking useful for my banking needs.	()	()	()	()	()
18.	Usefulness of mobile banking have made me to protect myself from threats.	()	()	()	()	()
	IX. TRUST BELIEF					
19.	The bank is reliable, competitive and have a good will.	()	()	()	()	()
20.	Since I do have trust on the bank, I use mobile banking without fear of threats.	()	()	()	()	()
21.	Since the bank is government bank I trust it.	()	()	()	()	()
	X. STRUCTURAL ASSURANCE					
22.	The mobile banking transmission channel is trustworthy.	()	()	()	()	()

23.	Even if threat or failure happens, I am guaranteed since the bank has strong legislation in terms of communication platforms and insurance.	()	()	()	()	()
	XI. PROTECTION MOTIVATION					
24.	My perception of risk in mobile banking makes me to protect myself in time of usage.	()	()	()	()	()
25.	Perception of insecurity enforces me for protection.	()	()	()	()	()

26. In order to enhance subscribers' confidence and avoid threats in using mobile banking could you suggest how the bank can improve mobile banking service?

.....

Appendix 2: Semi structured interview questions.

1. What are the frequent or the most complains by customers related to mobile banking service?
2. Do you think customers at your bank feel comfortable about the mobile banking service that the bank is providing?
3. What are the main activities that are done by the bank to fully fledge the mobile banking service to the customers to fully enjoy the technology without being fear of attacks, or security concerns?
4. What are the things that make customers feel of vulnerable to threats related to mobile banking?
5. How you rate your mobile banking security system?(high, medium, low)
6. What will be the consequence or the cost that may happen on the customer, if there comes some mistake or problem at the time of using mobile banking service?
7. Do you think customers get using mobile banking is easy for them and also useful for them?
8. How is the mobile banking development at your bank in general?
9. How your bank is doing to increase trust of customers on the mobile banking service and also on the bank itself as a legislative institution?
10. What are the things that are done by your bank to make customers protect themselves from threats or failures when using the mobile banking service?

Appendix 3-Letter of cooperation written by the university to the bank.

አዲስ አበባ ዩኒቨርሲቲ
የተፈጥሮ ሳይንስ ኮሌጅ
የኢንፎርሜሽን ሳይንስ ት/ቤት



ADDIS ABABA UNIVERSITY
College of Natural Science
School of Information Science

Date December 21, 2015

Ref: -SIS/ 26 /2015

To: Commercial Bank of Ethiopia HRD (Human
Resource Directorate)
Addis Ababa

Dear Sir / Madam

Student Hailieyesus Kindie (ID. No. GSR/1454/07) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting a MSc. thesis research under the title "Customer's perception to words mobile banking security. The case of commercial bank of Ethiopia (CBE)".

I would like to thank you in advance for all the assistance that you would provide to the students.

With Regards


Martha Yifiru (PhD)
Head, School of Information Science

☎: 1176

☎: +251-(11)-122-91-91 ☎:2122- 91-92

Appendix 4-Letter of cooperation from the bank to any other branches of the bank.



የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA
Inter Departmental Memorandum

DATE ቀን	:	Mar. 08, 2016
TO ስ	:	To whom it may concern
FROM ከ	:	Manager -Learning and Development
SUBJECT ጉዳይ	:	Request for Research Work

Addis Ababa University College of Natural Science School of Information Science has requested our bank to assist and cooperate Student Haileyesus Kindie, who is an postgraduate student to grant him access to the required information to the research work entitled "customers perception towards mobile Banking security: The case of Commercial Bank of Ethiopia" as part of the fulfilment of MSc. in Information Science.

This is, therefore to request you to provide him the required assistance and cooperation without compromising confidentiality.

With Regards

Getu Bedilu

/yt

Appendix 5: Results of linear regression for Perceived vulnerability, Perceived severity and Perceived risk.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.117	.034		3.403	.001
	Perceived vulnerability:	.488	.089	.419	5.500	.000
	Perceived severity	.241	.079	.232	3.050	.003

a. Dependent Variable: Perceived risk

Source. SPSS Result

Appendix 6: Results of linear regression for Perceived risk and Protection Motivation in Mobile Banking.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.071	.032		2.251	.026
	Perceived risk	.350	.063	.415	5.545	.000

a. Dependent Variable: Protection Motivation in Mobile Banking

Source. SPSS Result

Appendix 7: Results of linear regression for Response efficacy, Self-efficacy, Response cost and Protection Motivation in Mobile Banking.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.019	.027		.677	.500
	Response efficacy	.070	.072	.084	.971	.333
	Self-efficacy	.430	.078	.475	5.499	.000
	Response cost	.152	.072	.173	2.100	.037

a. Dependent Variable: Protection Motivation in Mobile Banking. **Source. SPSS Result**

Appendix 8: Results of linear regression for Perceived ease of use, Perceived usefulness, and Protection Motivation in Mobile Banking.

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.026	.029		.895	.372
1 Perceived ease of use	.556	.064	.591	8.689	.000
Perceived usefulness	.085	.052	.110	1.621	.107

a. Dependent Variable: Protection Motivation in Mobile Banking. **Source. SPSS Result**

Appendix 9: Results of linear regression for Trust belief, Structural assurance, and perceived risk in mobile banking

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.175	.041		4.301	.000
1 Trust belief	.587	.093	.487	6.297	.000
Structural assurance	-.029	.069	-.033	-.425	.672

a. Dependent Variable: Perceived risk
Source. SPSS Result

Appendix 10. Sample size calculation

The sample size is determined by the following formula:

$$\text{Initial sample size (No)} = \frac{P * (1-P) * Z^2}{D^2}$$

Where:

Z= Z value (e.g. 1.96 for 95% confidence level).

P= percentage picking a choice, expressed as decimal (0.5 is used for the sample size needed).
(This is proportion method)

D = is confidence interval, expressed as decimal (e.g. 0.09, ± 9), this the margin of error. (Mostly 0.1(10%) is used as margin of error), but below 0.1(10%) can be used as far as the required initial sample size is determined. So for our case we use 0.09 margin of error, which is 9%.

$$\frac{0.5 * (1-0.5) * (1.96)^2}{(0.09)^2}, \text{ this gives approximately } \sim 118$$

Final sample size (N1) = Design effect*initial sample (No).

N1=1.5(default value)*118 = 1.5*118, so this gives us approximately ~170 sample size.

The confidence interval (also called margin of error) is the plus-or-minus figure usually reported in newspaper or television opinion poll results. For example, for this study confidence interval of 5.0 is used which means if 50% percent of the sample picks an answer it can be generalized that if the entire relevant population were asked the question between 41% (50-9) and 59% (50+9) would have picked that answer.

The confidence level tells how sure one can be. It is expressed as a percentage and represents how often the true percentage of the population who would pick an answer lies within the confidence interval. The 95% confidence level means one can be 95% certain; the 99% confidence level means you can be 99% certain. For this study 95% is used since most researchers use the 95% confidence level.

Declaration

I, the undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university, and that all source of materials used for the thesis have been duly acknowledged. ,

Hailieeyesus Kindie

June. 2016

Confirmation

This thesis can be submitted for examination with my approval as a university advisor

Workeshet Lamenew (PhD)

June. 2016