Trust, Security and Perceived Risk Models for Designing Internet Banking

Ahmed Massoud Alsuwiey Massoud

The Software Technology Research Laboratory

De Montfort University Leicester UK

A doctoral thesis submitted to

De Montfort University

In partial fulfilment of the requirements for the

Degree of Doctor of Philosophy

August 2015

ACKNOWLEDGEMENTS

First and foremost, I would thank ALLAH (GOD) the Almighty, for all blessings, guidance and for providing me patience, guidance and perseverance throughout this academic journey to complete this research.

I extend my deepest gratitude to my parents, my brothers and my sisters for their prayers, constant love support and encouragement. My small family (my wife and my daughters) was the foundation of my strength and inspiration. My deepest gratitude and my thank goes to "my wife" for her unflagging support throughout my studies.

I would like to take this opportunity to thank persons who have encouraged and supported me during my doctoral of studies at university of De Montfort and them: My supervision team, I owe a lot of gratitude to my supervisor Professor. Duska Rosenberg; also I owe considerable thanks to Professor. Hussein Zedan for their guidance during my research study, and their continuous energy and enthusiasm in research have motivated me.

Acknowledgment also goes to all STRL team, all the staff and colleagues at De Montfort University, as well as acknowledgment strongly goes to my brother " Zaid Nagarseth" and all my friends, and participants in the survey of the study sample. I would thank all above, without their cooperation, encouragement and support this study would not have been possible and this enabled me to complete this work.

AHMED MASSOUD

ABSTRACT

This research assesses the behaviour patterns of existing bank customers towards Internet banking service in the UK (non-adopters and adopters), and their continuing usage or abandonment of service. The study also develops a theoretical model for trust, risks and Internet banking security, to achieve safety in the area of Internet banking services.

Specifically, the majority of existing studies neglect patterns of post-adoption (continued use and abandonment of use) of Internet banking; focusing instead on either adoption or acceptance of internet banking (pre-adoption).

The research in this thesis responds to this gap in the existing literature, offering a reassessment of the authentic use of Internet banking services in the UK. It does so by exploring the influence of trust, perceived risk, and security concerns, on customers' behaviour and intention to use or not use Internet banking services.

To address the study aims, it first develops conceptual frameworks. These encompass trust, security and perceived risk factors, and identification, and determine what influences consumers in their non-adoption, adoption, continued use, or abandonment of Internet banking.

The study investigates customers located in Leicester city, and applies a quantitative research design, using a survey as the primary means of data collection. There were eight hundred and thirty eight valid copies (838) of the questionnaire, comprising a sample of 503 Internet banking users, 291 non-users of Internet banking and 44 abandoners of Internet banking.

A combination of simple regressions, correlation coefficients and frequencies (Categorical Variables), was used to analyse the data, by subjecting it to statistical analysis software SPSS. Initial statistical results displayed that 34.7% of the study sample were non-users of Internet banking, with Internet banking services abandonees being a minority. They represented just 5.30%, i.e. 44 customers from an overall study sample of 838. For them, trust, security and perceived risk were significant influences.

Similarly, in adoption and continuity models, 60% of active users mentioned that trust has a low effect on their intentions for Internet banking adoption, while security and perceived risk had a very low influence on service adoption. On the other hand, the findings demonstrated that one-third of the users sampled mentioned other Internet banking adoption factors besides trust, namely: convenience, ease of use, saving time, ease of access, good monitoring and control of accounts, and speed when performing transactions.

With regard to the continuity of usage, 87% of service users agree, or strongly agreed, about their future intentions regarding continuity. Reasons for continued use of Internet banking were trust, security and perceived risk. Additionally statistical analysis found weak relationships between perceived intentions and three factors. Further, the findings also highlighted that the relationships between demographic characteristics and customers' trust, security and perceived risk were weak in three areas (Non-users, Abandoners and Users).

One of the main contributions of this study is the development of a safety area model for Internet banking usage. The safety aspects identified were trust, security and low-risk degree between 53%, 51% and 9%, according to customers' recommendations.

This model will serve as a basis for future studies, to determine safety area in which to exercise Internet banking. However, the usefulness of this may vary from one environment to another and by time.

Overall, the research contributes to knowledge and understanding of Internet banking patterns during two phases: pre-adoption and post-adoption of services (non-adoption, abandonment, adoption and continuity of use).Moreover, the research findings and insights will help bank executives, developers, academics, managers, and stakeholders, to formulate strategies and service frameworks to induce clients to accept services. Furthermore, maximising productivity and profitability through the creation of sustainable relationships in the long term with users will improve their satisfaction and retention. Bank administrators and decision makers should take advantage of the safety area model, and consider the views and recommendations of customers.

Table of Contents

List of Figures

List of Tables

CHAPTER 1: INTRODUCTION

1.1 INTRODUCTION

This chapter introduces the research area, namely trust, risk and security within UK internet banking, which underpins the development of consumer adoption, non-adoption, abandonment and safety area models. A description of the problem is followed by a discussion of the research objectives and research questions. A brief description of the need, contribution and significance of the overall research field is also presented. Measures of success and evaluation are explained in this chapter in addition to the methodology. Finally, an overview of the study is presented.

1.2 PROBLEM DESCRIPTION/ DISCUSSION

The growing phenomenon of Internet banking has been observed in both developed and developing economies. Naturally, it is not without difficulties and obstacles, which hinder its overall adoption, development and growth (Salih, 2009).

Research indicates that the United Kingdom is one of the leading countries in the distribution and engagement of Internet banking services. Nevertheless, in recent years notable and extensive studies have described curbing indicators and a reduction in the rate of uptake of Internet banking. Jayawardhena and Foley (2000) argue that uptake of Internet banking services in the UK is slow and fluctuating.

Reports from the Office for National Statistics (ONS, 2013) confirm that compared to the statistics for 2009-2010, there was a steady increase in the number of Internet banking users in 2011 in UK, whilst a clear decrease was predicted in 2012, as

illustrated in Figure 1. Moreover, statistics the Office for National Statistics (ONS, 2012) show that in 2012 7.82 million adults, equating to 16 percent of the UK's population, had never used the Internet.

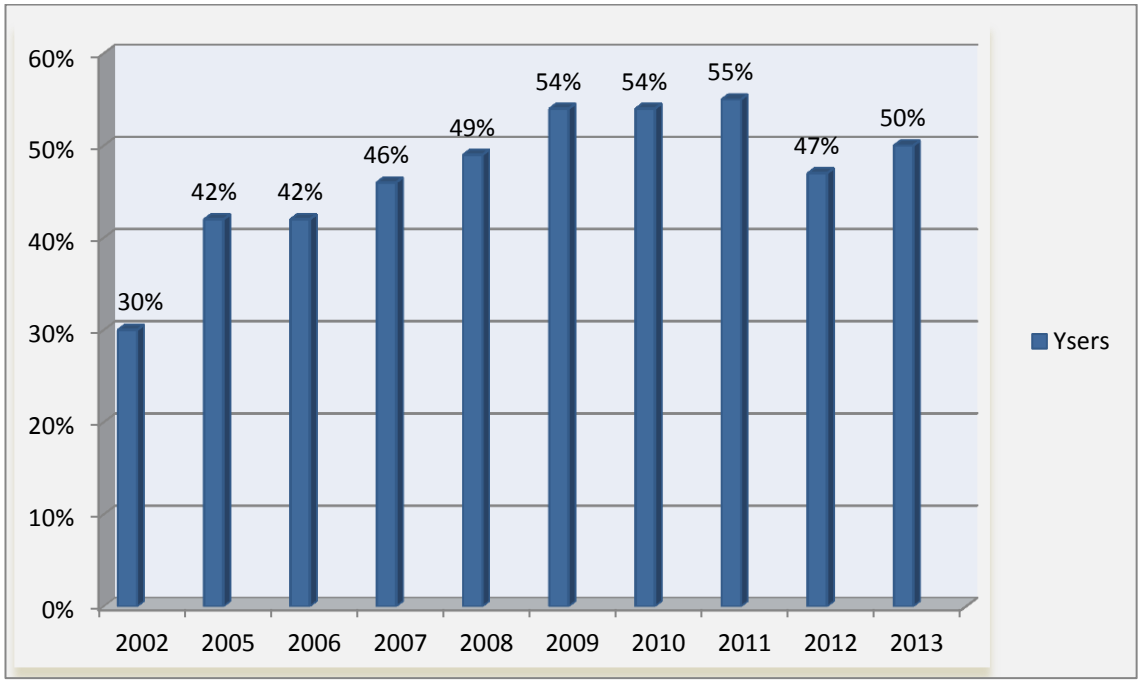


Figure (1) Numbers of Internet banking users in the UK
Source: (Office for National Statistics, 2013; 2012; 2011)

Additionally, Giovannini and Ensor (2006) note that approximately 5.5 million Europeans, mostly in Germany and the UK, have ceased to use Internet banking. Although more than half of all European adults use the Internet, it is estimated that 75 million have yet to use Internet banking, as shown in Figure 2.

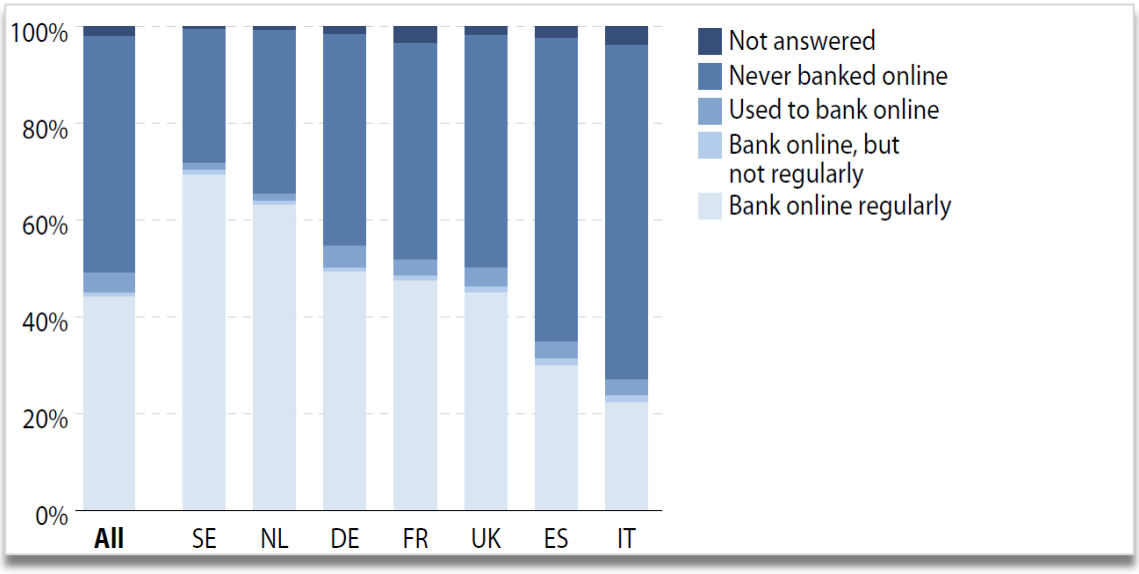


Figure (2) European Banks Are Losing Out On 80 Million Potential Internet Banking Users. Source: (Giovannini and Ensor, 2006).

Moreover, Yousafzai and Yani-de-Soriano (2012) classify Internet banking in the UK as being slow and lagging behind the US, Germany and France. Furthermore, it appears that roughly two million people have ceased to use Internet banking and that half of UK clients still visit their banks every month.

White and Nteli (2004, p.49) observe that despite "an increase in the number of Internet users recorded by various agencies, the level of increase of Internet usage for banking purposes has not increased at the same rate".

Studies demonstrate customers' lingering security concerns, despite evident advances in Internet banking service security systems in the UK. Conversely, studies have shown that a considerable level electronic fraud has taken place in the United Kingdom, notably during the 2008-2009 period (Chambers and Turksen, 2010; Mahdi et al., 2010).

Statistics indicate losses in the region of £580 million in 2007 within the United Kingdom (Francois, 2013). The National Fraud Authority's Annual Fraud Indicator (Harrison, 2013, p.46) states that, "Financial Fraud Action UK reported that in 2011 Internet banking fraud losses totalled £35 million; a 24 per cent reduction compared with losses in 2010." These facts have been confirmed by Financial Fraud Action in UK (2014). Figure 3 shows the losses to Internet banking fraud over the period from 2004 to 2013 in the UK.

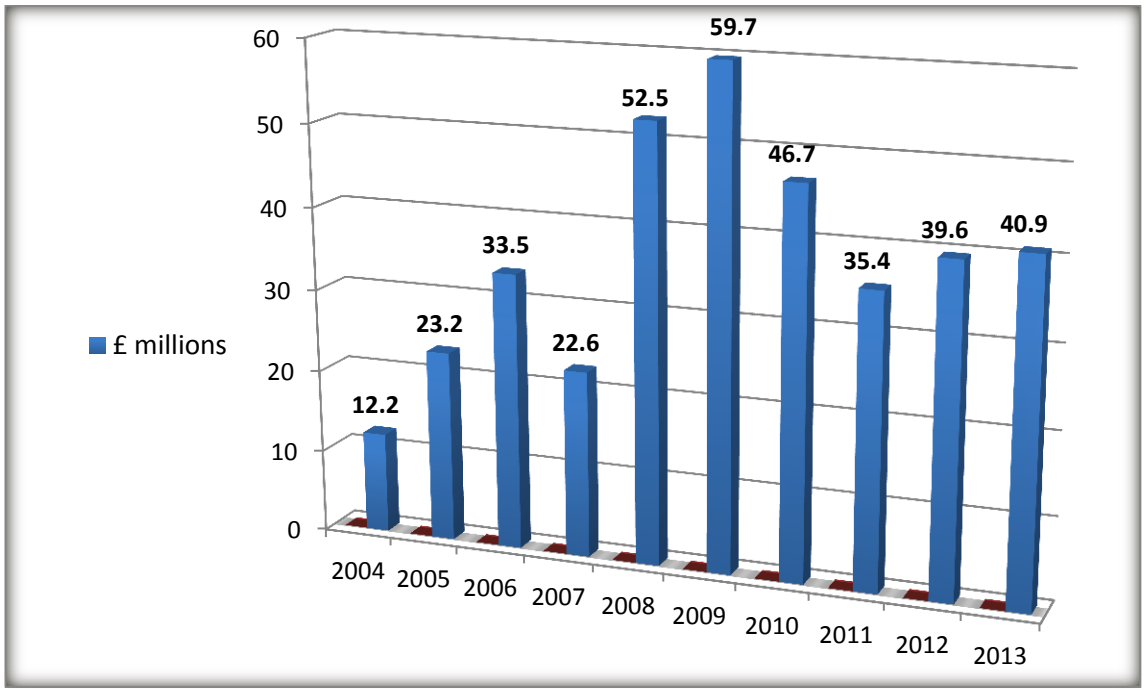


Figure (3): Internet banking fraud losses in the UK.
Source: (Financial Fraud Action UK, 2014)

In light of the above, there appear to be varying degrees of engagement in branch and Internet banking services. There is variation in behaviour ranging from banking user purists (branch) to pre-adoption and post-adoption amongst Internet banking users. Supporting literature on Internet banking tends to reaffirm patterns of global growth in

Internet banking, with previous studies focusing on user acceptance and adoption of Internet banking and its underlying governing factors for user service populations (Govender and Wu, 2013; Hong et al., 2013; Muzividzi et al., 2013; Janahi et al., 2013; Delafrooz et al., 2013; Takele and Sira, 2013). Interestingly, few studies have examined the behaviour of post-adoption customers (Adapa, 2011). Moreover, Adapa (2011) investigated the influential factors on the behaviour of pre-adoption and active users of Australian Internet banking. This has laid the foundation for further research into continued user behaviour patterns in different geographical areas and to extend the scope of research to include dormant users and those who have ceased to use Internet banking. More hybrid paradigms could be developed to understand consumers' decision-making processes.

Yousafzai and Yani-de-Soriano's (2012) study of 435 UK Internet banking services provides an integrated yet singular behavioural model of Internet banking, embedding demographic variables (such as age and gender) and encompassing constructs of willingness to use technology and technology adoption models. As a result, this should provide a comprehensive view of customers' Internet banking acceptance attitudes given an absence of behavioural variables, which include perceived risk, trust and insight into the adoption process.

However, it should be noted that only existing Internet banking customers were examined in this study. It would hence be useful for future research to include current non-users of the service in order to define acceptance propensity and predictability. As UK studies have shown (Forrester Research, 2008 cited in Yousafzai and Yani-de-Soriano, 2012), around two million people have ceased to use Internet banking. It is

therefore easy to see that Internet banking usage in the UK lags behind its international counterparts.

Based on the above, the purpose of this study is to investigate the current position of Internet banking in the UK along a trust, risk and security matrix analysis in order to gauge user reluctance in terms of adoption, continued use, cessation of usage, overall usage behaviour and the rates of use of Internet banking.

Moreover, customers need to feel safe when using Internet banking if they are to continue use the service. This study will therefore develop a framework to based on safety aspects that help customers use relevant services.

The safety area in this study is defined as a region that displays the most favourable level of customer confidence, by providing acceptable security and reducing the levels of risks, in order to maximize the effectiveness of Internet banking services. This region is located between the three-dimensional factors of trust, security and risk, with a percentage scale for each factor. The safety area model aims to achieve the best and most favourable degrees for trust and security and to lower the level of risk. More details about this model in chapter 4, especially in 4.2.3.4 Internet banking safety area model.

The factors described above were selected based on the recommendations made in the literature on the interrelationship between these three dimensions, for example (Jayawardhena and Foley, 2000; White and Nteli, 2004; Yousafzai, et al., 2009; Zhao et al., 2010; Yousafzai and Yani-de-Soriano, 2012; Kesharwani and Bisht, 2012; Al-Rfou, 2013). As the majority of studies in this field revolve around several factors, this study focuses on security, perceived risk, and trust.

Research into Internet banking has shown that trust, security and risk generally have a significant and obvious direct and indirect influence on both the non-adoption and adoption of Internet banking services (Hanzaee and Alinejad, 2012; Riffai et al., 2012; Subsorn and Limwiriyakul, 2012; Taleghani and Taban, 2012; Moga et al., 2012 ; Jham and Van Genderen, 2012; Nasri and Charfeddine, 2012; Twum and Ahenkora, 2012; Hassanuddin et al., 2012; Mughal et al., 2012; Ashtiani and Iranmanesh, 2012; Alsheyyab and Singh, 2013; Joubert and Belle, 2013; Farzianpour et al., 2014).

In particular, some studies focusing on the UK recommend further investigating the effect of trust, security and perceived risks on the adoption and non-adoption of Internet banking. Such as: (Jayawardhena and Foley, 2000; White and Nteli, 2004; Chambers and Turksen, 2010; Yousafzai and Yani-de-Soriano, 2012). Moreover, Internet banking services in the UK are still subject to security concern issues, according to the National Fraud Authority in Annual Fraud Indicator (Harrison, 2013) and Financial Fraud Action in UK (2014). The above provided the motivation for the selection of these factors.

To sum up, users who first take up Internet banking and then abandon it have not been studied in any detail. This is the main focus of this study. Generally, it is clear that there is ambiguity surrounding the reality of Internet banking services, in which more research is needed. This study aims to explore these issues in order to contribute to research in this field. The next section will therefore present the objectives of this study and the research questions.

1.3 RESEARCH AIMS AND OBJECTIVES

The main aim of this study is to determine in what way and to what extent trust, perceived risk and security influence the adoption, non-adoption and abandonment of Internet banking. The research objectives of this study are follows:

a) To assess current customer behaviour and related intentions towards engagement with Internet banking services. The survey will therefore attempt to explore the influence of trust, risk and security on the non-adoption, adoption and cessation of Internet banking behaviour. Accordingly, the behaviour of post-adoption users, in terms of branch to Internet migration, engagement sustainability and abandonment behaviour will be examined. In short, the study intends to develop the following three theoretical frameworks for studying customers' behavioural models: non-adoption, adoption and abandonment of Internet banking.

b) To design a model (theoretical model) of trust, risks and security for Internet banking in order to reach a safety area (Internet banking safety area model).

c) To discover correlations between trust, security and risk that influences the adoption of Internet banking in the UK.

1.4 RESEACH QUESTIONS

To satisfy the research aims and objectives, as stated in Section 1.3, the following research questions were formulated:

a) Do trust, security and risk have an effect on customers' decisions or intentions regarding the non-adoption of Internet banking?

b) Do trust, security and risk have an effect on customers' decisions and intentions regarding the abandonment (giving up) of Internet banking?

c) Do trust, security and risk have an effect on a customers' decisions and intentions regarding the adoption of Internet banking?

d) What constitutes 'significant' degrees of trust, risk and security when considering customers' decision-making processes in relation to Internet banking engagement sustainability (continuity of use)?

e) Does perceived risk related to Internet banking affect customers' levels of trust?

f) Does the security of Internet banking affect customers' levels of trust?

g) Does the security of Internet banking affect perceived risk?

h) What is the optimum safety combination of trust, security and perceived risk that would determine desired levels of usage and degrees of satisfaction with Internet banking services?

1.5 NEED FOR AND SIGNIFICANCE OF THE RESEARCH

The current research stems from the necessity to provide a comprehensive and meticulous insight into user behaviour in order to aid, develop and optimise bank management strategies and commercial products. This research follows on from several studies that are of significance with the context of the Internet banking research field.

It should be noted that tracing users' pre-adoption and post-adoption of Internet banking, as well abandonment behaviour, is likely to be invaluable to banking managers, decision-makers, academics and practitioners in this area. Moreover, this research contributes to the existing body of knowledge by investigating pivotal trust, security and risk factors that influence users' continued adoption, non-adoption and abandonment behaviour, as opposed to just proposing a conceptual framework based partly upon the findings of previous research into Internet banking.

1.6 RESEACH CONTRIBUTION

This research contributes to both theory and practice by providing a detailed analysis of Internet banking, which is the subject of considerable academic and commercial interest. This study has the following objectives:

1. To provide a further contribution to the literature on UK Internet banking.
2. To bridge the gap in the existing literature, which focuses heavily on factors affecting consumers' adoption intentions and respective adoption actions in terms of Internet banking. To a lesser extent, other research has compared adoption studies or investigated factors that hinder consumers' adoption of Internet banking. The present research thus aims to examine UK Internet banking customers' non-adoption, continued use and abandonment behaviour.

3. To clarify ambiguity clarity faced by the researcher. Despite developments in the spread of Internet services, Internet banking is still characterised by user reluctance, slow uptake and rising abandonment in the UK, as described in the literature cited earlier.

4. Current literature on Internet banking highlights the user perspective either through theoretical technology acceptance models or the application of the diffusion of innovations theory. This study will hence contribute to new theoretical model designs based on three- dimensional trust, risk and security in Internet banking. It is necessary to ensure safety in the work of the bank in order to achieve the desired degree of customer trust, an appropriate level of security and a low-risk environment. The safety area identified is located between 53%, 51% and 9% for trust, security and risk respectively. This model can therefore serve as a basis for future studies as well as determining the safety area in which to utilise Internet banking, as this may vary between environments, time periods, and circumstances.

5. The study reinforces the importance of comprehensive testing by developing conceptual frameworks in order to obtain an understanding of the factors (trust, security and risk) in influencing the adoption, continued use non-adoption and abandonment behaviour by users of Internet banking.

1.7 MEASURE OF SUCCESS AND EVALUATION

Many studies have examined user adoption and acceptance of Internet banking. However, relatively little research has been carried out into post-adoption behaviours in the UK and the field in general. As previously stated, this research thus aims to bridge the gap in the literature with relevant model conceptualisations and developments.

Accordingly, the study evaluates the current position of UK Internet banking. This entails a three-stage review of UK Internet banking user behaviour, non-adoption, adoption and post-adoption.

The investigation was supported and underpinned by quantitative data collections (questionnaires) completed by a representative defined sample of the UK Internet banking population. Results expressly measured trust, security and the impact of risk on Internet banking user intentions, non-adoption and abandonment behaviours across perceived values drivers. Consequently, factors influencing the adoption of Internet banking and acceptance behaviours and sustainability were examined.

Numerous innovative theoretical model designs have therefore found to be associated with key performance indicator scales. Countering, advancing and enriching comprises a previously existing problem in the field, namely a three-dimensional model of trust, risks and security in Internet banking behaviour. Additionally, the safety of Internet banking is equally important in order to provide a comprehensive life-cycle of non-adoption, adoption and post-adoption. In summary, this should provide useful information for bank managers, decision-makers, academics and practitioners.

1.8 RESEARCH METHODOLOGY

Research methods refer to the devices that may be used for systematic data collection in order to answer research questions (Johnson et al., 2007). The two distinct methodologies for conducting research are qualitative and quantitative. This study adopted quantitative methods coupled with theoretical information from published reports and studies. Empirical data were gained from questionnaires.

The literature review was conducted in accordance with the research objectives, which led to the generation of numerous hypotheses. These were based on the synthesis of available literature on Internet banking. Accordingly, cited research questions were tested during the course of this study. As a result, initial pilot results were collected and evaluated as a measure of instrument efficiency and initial models were constructively developed.

The main study surveyed 1,400 Internet banking service users and non-users. A questionnaire was distributed across the city of Leicester, including at the High Cross shopping centre, universities, public libraries and in front of banks. About 890 respondents answered survey questionnaires, of which 838 were valid. The results encompassed 503 users, 291 non-users and 44 former users. This study consists of seven chapters. The next section discusses the previous chapters and includes an overview of the thesis.

1.9 OVERVIEW OF THE THESIS

This thesis consists of seven chapters, as illustrated in Figure 4. The introductory chapter includes the research study blueprint. It provides an overview of the research problem, and describes the research objectives and research questions. The significance and contributions of the research coupled with evaluation measures of success are presented alongside the methodology.

Chapter Two provides a general literature review of Internet banking services, focusing specifically on the definition and perceived benefits of Internet banking. Additionally, the challenges facing Internet banking and trends in global Internet banking (in the USA, Africa, the Middle East, Asia, Australia, New Zealand, Europe and the UK) are

also reviewed. Moreover, factors affecting the adoption and non-adoption of Internet banking services are reviewed and a summary of the chapter provided.

Chapter Three reviews the literature on trust, security and perceived risks in Internet banking as well as the factors affecting online services. Furthermore, it includes a review and assessment of theoretical models, namely the Theory of Reasoned Action, Theory of Planned Behaviour and Technology Acceptance Model. Lastly, research issues and a summary of this chapter are presented.

Chapter Four discusses the information relating to the theoretical framework (research models) and the models developed for the purpose of this research, namely the Internet banking non-adoption model, the Internet banking abandonment model, the Internet banking adoption and prediction model for continued behaviour and the Internet banking safety area model. In addition, research hypotheses are formulated based on the survey questions and the study paradigms are discussed. Moreover, the research methodology constructs methods and designs to develop and widen conceptual frameworks and to refine the scope of the research. The chapter provides all the details of the design process of the research instrument and the operation of the pilot study. Finally, the process of sampling design and obtaining ethical approval are explained.

Chapter Five describes the implementation of frameworks, starting with data collection procedures, before discussing data analysis, which includes constructs abbreviations, descriptive statistics of the sample and demographic profile analysis. In addition, the chapter discusses the relationship between trust, security and risk, demographic characteristics of customers and general Internet usage trends. As well as testing the

assumption of normality, checking for outliers and the reliability and validity of the instrument are described in this chapter, which concludes with a summary.

Chapter Six discusses the data analysis techniques used to address the hypotheses and an explanation of model outcomes, which include a non-adoption model, abandonment model, a model to predict continued use and a safety area model. In addition, the significant findings of these models are discussed before summarising this chapter.

Chapter Seven comprises the conclusions of the research, starting with a brief introduction, followed by the key findings of this research and the research implications (theoretical, methodological and practical). In addition, the contributions and limitations of the research are discussed. Lastly, the scope for future work and conclusion are presented.

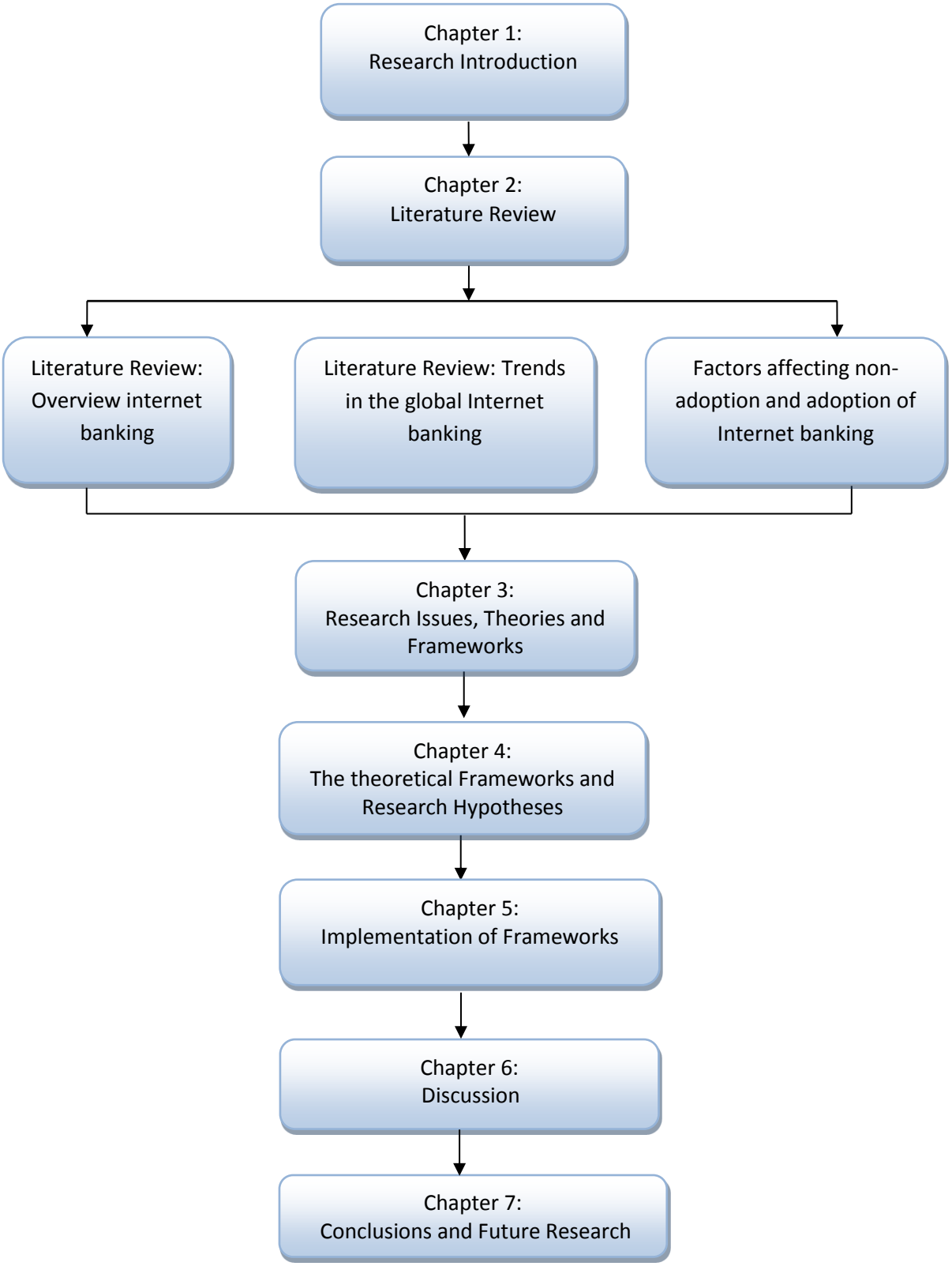


Figure (4): Thesis outline.

1.10 CHAPTER SUMMARY

Chapter One introduced the topic under investigation and discussed the purpose and structure of the study. Firstly, the research problem and discussion was presented, with special attention given to consumers' abandonment of service, non-adoption and the continued use of the Internet banking service delivery channel in the UK. The key research objectives for the present study were then discussed and followed by the research questions. The need for and significance of the research was discussed.

The contribution of this study to existing research was presented on the basis of the development of conceptual frameworks explaining the influence of trust, security and perceived risk factors on the propensity of consumers to abandon Internet banking, or in terms of the non-adoption or continued use of Internet banking services. Moreover, a brief description of the measure of success and evaluation was provided. Finally, overview of the thesis was presented at the end of the chapter.

The research used quantitative methods as it aimed to explore a new phenomenon by developing conceptual frameworks to investigate the issue. This research should be of benefit to managers, marketers and banking employees as well as academics working in this field.

The following chapter will review and discuss some points in the literature, such as Internet banking services, followed by trends in the global Internet banking industry. Finally, the literature review chapter will discuss the factors affecting the non-adoption and adoption of Internet banking services.

CHAPTER 2: LITERATURE REVIEW

2.1 INTRODUCTION

At the present time, information technology is considered to be important to industries, and Internet services are of particular significance (Alsaffar and Sun, 2009). In the context of the digital age, Internet banking has become essential, as it enables customers to complete electronic transactions more easily. This chapter will explore the realm of Internet banking as described in the introductory chapter. It will discuss the historical and contemporary trends in Internet banking, in addition to describing trends in the global Internet banking industry. A brief summary will be offered to explain the relevance of this context to UK researchers, and a review of service factors affecting the adoption and non-adoption of Internet banking will also be included.

2.2 OVERVIEW OF INTERNET BANKING SERVICES

2.2.1 INTRODUCTION

This chapter aims to provide a comprehensive explanation of the activities surrounding Internet banking: its definition, the development of the main electronic banking channels, the perceived benefits of Internet banking, trends in the global Internet banking industry, and factors affecting the adoption and non-adoption of Internet banking services.

The content provided in this chapter will provide a better understanding of global Internet banking trends from the perspective of the consumer, enabling the researcher to identify the gap in the literature and attempt to address this issue. Moreover, this chapter

will focus on the theoretical foundations of the survey method and introduces the main concepts that will be discussed.

2.2.2 INTERNET BANKING DEFINITIONS

"Electronic banking (E-banking) is the newest delivery channel of banking services and it has some platforms such as Internet banking" (Keivani et al., 2012, p.62). This section will first define electronic banking and then go on to provide a definition of Internet banking.

In the light of the above definition, Shannak (2013, p.242) defines electronic banking in general as "the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels". Takele and Sira (2013, p.403) offer a broader definition, describing electronic banking as "the mechanism of action that enables banks to deliver customers accessibility of accounts to complete transactions and obtain information through electronic communication channels such as ATMs, telephone banking, home banking, mobile banking and Internet banking". This study will use a narrower definition of electronic banking services and will focus primarily on Internet banking

The Basel Committee on Banking Supervision gives the following definition of Internet banking: "such products and services include deposit-taking, lending, account management, the provision of financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money" (1998, cited in Osei and Seth 2015, p.84).

Internet banking is also defined as "the delivery of banks' information and services to customers via different delivery platforms that can be used with different terminal devices such as a personal computer and a mobile phone with browser or desktop software, telephone or digital television" (Tandrayen-Ragoobur and Ayrga, 2011, p.4).

Daneshgadeha and Yildirima (2014, p.323) give the following definition "Any use of information and communication technology and electronic means by a bank to conduct transactions and have interaction with the stakeholders".

Alternative definitions have been provided by Martins et al. (2014, p.2), who note that "Internet banking is defined as the use of banking services through a computer network (the Internet), offering a wider range of potential benefits to financial institutions due to more accessibility and user friendly use of the technology" (2014, p.2), and also by Nwogu and Odoh, who defined Internet banking as "a facility provided by banking and financial institutions that enables the user to execute bank related transactions through Internet" (2015, p.21).

This study has defined Internet banking as the process of conducting all banking transactions and operations electronically via the Internet between the bank and the customer, easily at any time and place, and the subsequent transfer within the banking industry from the use of traditional to electronic methods, via the Internet. The following sections will briefly describe the evolution of electronic banking service channels.

2.2.3 ELECTRONIC BANKING CHANNELS

In the 1980s, significant expansions in banking and financial services took place, including advances in the delivery of services. This paved the way for financial transactions of a varied nature to be conducted electronically, including but not limited to: transferring money, reimbursements, checking bank accounts, and administrative services noted in the previous section (Wu et al., 2012). As a result of technological advancements such as ATMs and mobile banking, and the increasing number of these devices, the service reach to customers has been improved and extended (Ramya et al., 2013). Figure 5 below summarises four types of electronic banking.

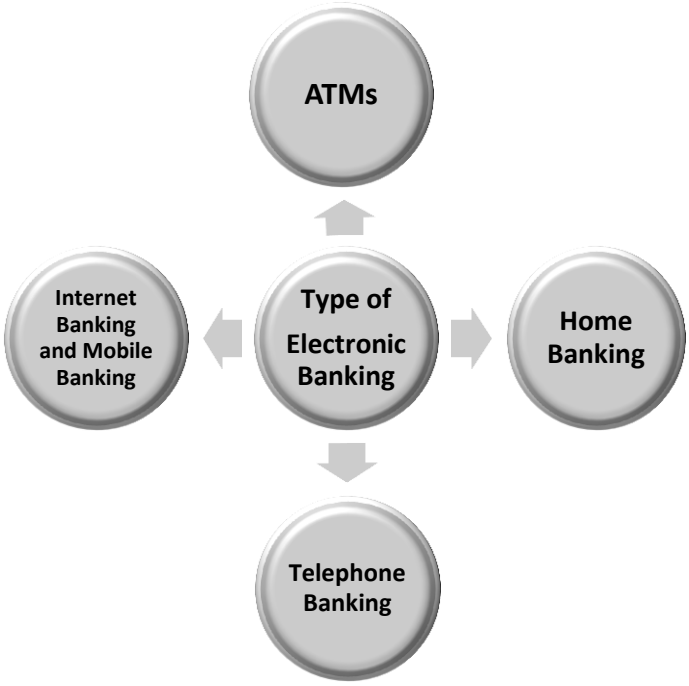


Figure (5) Type of Electronic Banking
(The source: Ramya et al., 2013, p.15)

2.2.3.1 AUTOMATIC TELLER MACHINE (ATM)

A familiar hallmark of traditional branch banking was extended waiting times, which were spent queuing and administrating banking transactions. After this period, a remarkable development in computer networks took place, with first wave introductions of cash dispensers, commonly referred today as automated teller machines (ATMs) (Chang, 2005). Cash machines are defined as computerised telecommunications devices offering accessible financial transactions such as withdrawals, deposits, making payments, and money transfers to consumers in public places. The Chemical Bank in Rockville Centre, New York, USA was a pioneer of cash machines in 1969, offering the public dispensing of cash to customers (Shannak, 2013). Lloyds Bank followed suit in the UK, with the introduction of ATMs in 1972 (Chan et al., 2009). Thus, from 1980 onwards, ATMs became one of the most successful models for the global adoption of electronic banking (Shannak, 2013).

2.2.3.2 TELEPHONE BANKING

Telephone banking, one of the principal forms of electronic banking, is a service provided by banks whereby they allow clients to access their accounts and perform transactions over the telephone at any time of day (Trivedi, 2010). Several service options are available, including transferring funds, checking account balances, paying bills and making stock exchange transactions. However, cash withdrawal and deposit services are not provided (Donner and Tellez, 2008). Telephone banking services can be divided into two types. The first of these is operator services; there are complicated questions that cannot be answered by automated services, and some customers need to have a direct discussion with a human being. The second type of service offered over

the telephone is automated services, which can be used for all services that can be performed by the automated system without the need for human operators (Shannak, 2013; Ramya et al., 2013).

2.2.3.3 HOME BANKING

As stated previously, the world of technology provides numerous examples of the continuous innovation of computer telecommunications and new financial distribution channels which continue to expand rapidly (Biswas et al., 2011). The fundamental step that paved the way for the evolution of home banking services was telephone banking, which became available from the beginning of the 1970s. There are three requirements for performing home banking, namely a telephone line, a personal computer and a modem.

In addition, it is necessary to install banking application software to perform various banking functions (Siu-cheung and Lu, 2004). By the mid-1980s, banks began to provide home banking services to clients by allowing them to install software, which enabled them to connect to their banks (Ramya et al., 2013).

2.2.3.4 INTERNET BANKING

Internet banking, often referred to as online banking, can be defined as customers being able to carry out their transactions via the Internet. Using either a computer or a mobile phone with an Internet browser, customers are able to access developed banking services at any time on their bank's website (Shannak, 2013).

Internet banking provides financial services to customers 24 hours a day throughout the year, at any location where they are able to gain access to the Internet (Hoehle et al.,

2012). Many researchers indicate the importance of Internet banking services, and the next section will attempt to provide a brief summary of its importance for banks and customers. In this age, Internet banking services are an important channel for customers and banks, therefore banks need to implement strategies which expand the adoption and increase the usage of this low cost channel. Thus, the next section will discuss the benefits for banks and customers.

2.2.4 THE PERCEIVED BENEFITS OF INTERNET BANKING

The benefits of Internet banking can be divided into two categories: benefits related to the banks and benefits related to customers.

2.2.4.1 THE PERCEIVED BENEFITS FOR BANKS

Many financial entities are motivated to adopt Internet banking due to the potential it offers for increasing their market share and competitiveness by countering geographical stigmas previously attached to classical branching, and due to the universal nature of Internet banking services. Hence, technological service advances have provided a safe haven for users to perform transactions seamlessly around the clock. The absence of traditional labour and stationery, and the reduction in human error, have both improved operational efficiency (Mermod, 2011).

The subsequent market coverage amplifications have led to the enhancement of value chains, offerings and competitive positions, (Ndlovu and Sigola, 2013). As a result of satisfying multiple demographic segments, banks are able to attract and enhance extended and elongated customer relationships (Martins et al., 2014; Kaleem and Ahmad, 2008).

2.2.4.2 THE PERCEIVED BENEFITS FOR CUSTOMERS

In today's challenging social structures, Internet banking services present a ray of much needed sunshine; they provide convenience and simplicity, and the service is securely accessible 24 hours a day (Adepoju and Alhassan, 2010; Radojevic and Radovanovic, 2010). Users are able to view balances, print statements, transfer money, and make payments and information transparency. Frequently, there are no additional fees for services, even if those services are excellent. It is also worth noting that Internet banking services provide the best rate of interest on credit cards and savings accounts (Mahmood, 2009; Salehi and Alipour, 2010). Due to the importance of evolution in this service, the following sections briefly describe the development of the Internet banking service channel from a global perspective.

2.3 TRENDS IN THE GLOBAL INTERNET BANKING INDUSTRY

2.3.1 INTRODUCTION

The literature review represents a pivotal point in academic research, and is considered to be the main base upon which useful research efforts can be built. This undoubtedly confirms that academic studies are not developed in a vacuum. They form a cumulative process of knowledge emanating from previous studies and efforts, with the aim of achieving progress and adding to the sum of human knowledge.

The principal advantages of the literature review, which will be explored in this section, are the fact that it enables the researcher to access to the knowledge gap, and to gain an insight into the aspects that have attracted the attention of previous researchers globally and locally in the field of Internet banking. Moreover, it helped to identify the

importance of the study and determine the scientific contributions of previous studies. Consequently, the researcher was in a position to go beyond the submissions of other researchers in order to contribute to the development of scientific knowledge and increase the value of the study. Furthermore, the literature review was a key factor in the development, evaluation, and subsequent reformulation of study questions, and it was also an important source for the interpretation of the findings as it gave the researcher the possibility to examine examining the views and comments that previous researchers had applied to similar situations.

There were two main reasons for the inclusion of a review of international literature in this study: firstly to help identify general weak points in this field and shed light on Internet banking services in the UK in particular; secondly, because relatively few studies already exist relating to this field in the UK. The following section will present a brief history and trend analysis of the global evolution of the Internet banking industry and an examination of the geographical impact of Internet banking in seven broad groupings of countries: the USA, Europe, Africa, the Middle East, Asia, Australia, New Zealand, and also the UK.

2.3.2 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN THE USA

In the USA, Eighty- seven per cent of banks provided electronic banking services in 2003 (Delong and De Young, 2007). It is evident from the existing literature that consumers have accepted electronic banking services with phenomenal intensity, especially with regard to the service delivery channel of the Automated Teller Machine. ATMs have been in use for more than 29 years and they are used by a wide variety of

customers (Kolodinsky et al., 2004). During the 1970s, customers started using the ATMs we know today and the banks also developed 24-hour cash machines. In addition to the withdrawal process, they can be used to make deposits, provide cash advances from a credit card, take payments and transfer money (Hayashi et al., 2003). In the USA, individuals prefer to use ATMs: there are approximately 1.65 million ATMs, and this number is expected to increase by 1.7 million in 2010. Similarly, in Canada 75% of consumers prefer to use ATMs (Adapa, 2011). In 2010, fifty-eight per cent of Internet users also reported that they bank online, and in 2011, 18% of mobile phone owners indicated that they had used their phone to access their bank account (Fox, 2013). These statistics clearly indicate there has been a rapid increase in the number of Internet users who have cited the usefulness of adopting Internet banking services.

On the other hand, several studies demonstrate the existence of factors which cause customers to have concerns about the use of Internet banking (Yoon and Steege, 2013); a survey of 5,000 US adults by Finextra (2006) revealed that 46% were concerned about the issue of security. Moreover, the study found that fraud had a negative impact on the use of Internet banking in 2006; online shoppers lost approximately £660 million to fraud during sales processes.

This has caused approximately 9 million US adults to abandon the use of Internet banking, while 23.7 million do not use this service due to fears about security. Other studies found that Internet banking services in the USA require improvement and development, for example by enhancing security, usability, customer awareness and interface (Yang et al., 2009).

An investigation by Joseph and Stone (2003) pointed out that the most significant factor for customers in the USA is accuracy, followed by security and convenience. Kolodinsky et al. (2004) highlighted other factors which have an effect on the adoption of Internet banking services in the United States, namely: the relative advantages of the service, its level of simplicity or complexity, its compatibility with users' devices, its observability, the risk tolerance of the consumer, and the level of product involvement.

2.3.3 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN EUROPE

The UK, Spain, France, Germany and Italy account for a massive 77% of the ATMs in Europe (Adapa, 2011). Nearly two-thirds of Internet banking users report that they are satisfied with branches and ATMs, with customer satisfaction levels reportedly highest among German and UK customers, but still high throughout Europe (Giovannini and Ensor, 2006). Ravoet (2010) confirmed that in Spain, ATMs are the most frequently used channel for interactions, followed by branches and Internet banking. In addition, studies have also found that the number of ATMs in the European Union has been steadily increasing, reaching a total of almost 434,000 by the end of 2009.

The literature on this subject tends to focus on the issues relating to Internet banking in Europe, with several studies revealing that this is a phenomenon which has been in constant evolution over the past few years, with solid evidence of stable growth in all European countries (Floros, 2008). In Greece, where nearly every bank provides Internet banking services, it has been reported that there are 226 000 active users divided between the four leading banks, i.e. 73% of the total banking population (Adapa, 2011). In France, there were over 34.7 million active Internet banking users

over the age of 11 in December 2009; although mobile usage in France, at 26%, is slightly below the global average, it is close to some of its European peers. Nevertheless, trust, security, and other factors have an effect on the usage of Internet banking services (Sanchez and Jean-Baptiste, 2010). In Poland, the advent of electronic banking can be dated back to 1990, when Bank Pekao S.A. installed the first ATMs in the country, and the introduction of Internet banking followed eight years later when Powszechny Bank began to offer the service in October 1998. As is the case in other countries, concerns about security have a significant influence on Polish customers' decisions about the adoption of Internet banking (Polasik and Wisniewski, 2009).

In Romania, despite the fact that several banks provide an Internet banking service, only 1% of service users are active (Radulescu and Serbanescu, 2009). However, figures from 2012 indicate that the rate of use has increased (Fratila et al., 2013). Thirty-nine per cent of customers in this country still prefer to use traditional services and 27.3% of them prefer to use ATMs; once again, security is still the main reason for this phenomenon (Bartlett and Prica, 2011).

In Italy, Internet banking has been positioned as a major distribution channel for financial institutions since the 1990s (Capece and Campisi, 2013), with Italian users reporting a high level of satisfaction and trust in Internet banking. In addition, there are some variables such as accessibility, trust, ease of use and satisfaction of customers has influence on acceptance Internet banking services (Liebana-Cabanillas et al., 2013).

This contrasts with the situation in Germany, where the increase in Internet banking users over the last few years has been moderate, due to security concerns, lack of trust, poor customer acceptance of the service, website design, and user-friendliness. In 2010,

there were only slightly more than 27 million German Internet banking service users (Dapp, 2013).

In addition, there were 80 million Europeans who had either not used, or given up using, Internet banking in Europe. 5.5 million Of those, primarily German and UK residents, ceased using the service "due to a mix of poor service design, security fears, satisfaction with existing channels and marketing messages". By contrast, 75 million customers of Swedish and Dutch banks have never banked online. Italy remains the leading European country in terms of the uptake of Internet banking services: 69% of Italians use Internet banking, in comparison with only 28% of Swedes (Giovannini and Ensor, 2006, p.1).

In brief, customers in European countries still worry about online security, especially in Sweden, the UK (Giovannini and Ensor, 2006) the Nordic region, Switzerland, the Benelux countries (Polasik and Wisniewski, 2009) and Germany (Dapp, 2013). This has a significant impact on the non-adoption, adoption, and the continuity of usage of Internet banking in Europe. The following section will review the literature on the Internet banking industry in Africa.

2.3.4 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN AFRICA

In South Africa, Internet banking services only became available from 1996, and in 2002, there were still only four banks offering this service. Internet banking got off to a slow start, as 92% of consumers mainly depended on ATMs. Internet banking services in South Africa were first provided by ABSA, Nedcor Standard Bank, First National Bank and Mercantile Bank (Singh, 2004). Sixty-nine per cent of consumers did not use Internet banking; the main reasons for non-adoption were concerns about security and

lack of awareness of the benefits (Adapa, 2011). Similarly, in Zimbabwe, the first appearance of electronic banking was in 1990, when Standard Chartered Bank installed ATMs. This gave rise to a sequence of service deliveries in Zimbabwean banks, such as Electronic Funds Transfer Systems, telephone banking, and recently, Internet banking services (Thulani et al., 2009).

Popola (2013) informs us that Nigeria's first bank, the African Banking Corporation, was established in 1892. ATMs still remain the most widely used form of electronic banking service in Nigeria: almost 100 million financial processes are conducted monthly with cash machines, by about 30 million ATM card holders (Ayo et al., 2010). There are 9000 ATMs across 36 states in this country (Aliyu et al., 2012). In addition, most banks now offer Internet banking, although usage levels have remained relatively low because concerns about security dissuade customers from adopting this service (Ndlovu and Sigola, 2013). It is apparent that users' main concerns relate to security and confidentiality; and these issues constitute an obstacle to the adoption of service (Aderonke and Charles, 2010).

In Ethiopia, the majority of people still use cash; Dashen Bank installed more than 40 ATMs in June 2009. However, electronic payment is in its infancy and Internet infrastructure exists only in the main cities (Worku, 2010).

Regarding North Africa, Tunisia was ranked 38th out of 134 countries for information technology in the Global Information Technology Report of 2008-2009. At the beginning of 2009, there were approximately 2.8 million Internet users in Tunisia, and on the 30th of March of the same year, there were 19,123,336 credit cards in use and 1289 ATMs available. However, Tunisian customers still experience concerns about

security (Azouzi, 2009). With Egyptian clients, perceived ease of use has an influence on follow-up usage of Internet banking services, while perceived risk has had no impact on customers' intentions to continue using the service (El-Kasheir et al., 2009). Twati (2008) mentioned that in Libya, most businesses have Internet access, although there are concerns about the security of electronic transactions and people have limited trust in online trading systems. Furthermore, e-shopping and e-banking are all new in Libya and a lack of experience on the part of both businesses and customers affects their adoption (Hunaiti, 2009). Other factors which have a negative effect on the adoption of Internet banking are the lack of Internet banking facilities and the absence of laws relating to electronic services in Libya (Abukhzam and Lee, 2010).

A similar picture of Internet banking services can be seen in other African countries. For example, in Nigeria, the majority of customers prefer to use ATMs, despite the fact that security is still a major concern to them (Aderonke and Charles, 2010; Auta, 2010). Moreover, perceived usefulness and ease of use have a significant influence on customers' adoption of Internet banking (Ayo et al., 2010).

Internet banking in Ethiopia and Zimbabwe is not currently in an optimal state as the level of use is low, significant security concerns exist, and the telecommunications infrastructure is insufficient (Thulani et al., 2009). As for Mauritius, perceived ease of use and perceived security were considerable factors that have an impact on customers' choices to adopt Internet banking (Tandrayen-Ragoobur and Ayrga, 2011).

In summary, Internet banking is a significantly new phenomenon in African countries, where the spread level is very low. A lack of data and the limited number of studies available prevented further examination of the current state of mobile banking services.

The next section will review the literature on the Internet banking industry in the Middle East.

2.3.5 EVOLUTION OF INDUSTRY INTERNET BANKING IN THE MIDDLE EAST

In the Middle East, a client preference for the use of ATMs has been observed. Customers have perceived electronic banking services, such as ATMs, to be an appropriate transition in the banking sector, and 50% of transactions are conducted outside of bank branches (Adapa, 2011).

In Turkey, the rate of Internet usage in the financial service sector has recently increased (Aktan et al., 2009). 1980 saw the first usage of ATMs, followed by the introduction of telephone banking in 1995. Internet Banking began to be used in the early 2000s (Boyacioglu et al., 2010).

According to the Turkish Banking Association, Internet banking services were offered for the first time in 1987 by Isbank Bank and Garantibank Bank. Later, 22 banks in Turkey offered Internet banking services (Mermod, 2011). Celik (2008) states that Turkish customers are strongly influenced by ease of use and usefulness when making decisions about the adoption of Internet banking services, with income and education levels also having a significant impact on Internet banking usage. However, most Turkish Internet users have confidence in protection systems and security (Boyacioglu et al., 2010; Mermod, 2011).

In the case of Saudi Arabia, subscriptions for wireless Internet access reached 11.5 million by the end of 2011, representing 40.5% of the population (Baabdullah et al., 2013). The vast majority of people use ATMs, with Internet banking being the second

most preferred method of conducting transactions (Mahdi, 2011). On the other hand, studies revealed the existence of problems related to credit card security; these cards were insecure during online shopping and this led to lack of trust in their use (Mahdi, 2011). The significant factors which affect customer attitudes towards Internet banking, adoption and acceptance are: perceived usefulness (Alsajjan and Dennis, 2010), awareness, social factors, perceived ease of use, trust, resistance to change, effectiveness of infrastructure, and computer self-efficacy (Al-Somali et al., 2009).

In Iran, the government and the Iranian banks set up all the necessary infrastructures (organisational and software) for fully launching electronic banking services in Iran by 2005, in addition to the ATMs that are now commonplace (Sadeghi and Farokhian, 2010). However, research indicates that knowledge of the internet banking sector is not widespread amongst Iranian customers (Salehi and Alipour, 2010). Likewise, a relationship exists between Internet service and customer satisfaction; this relationship was measured according to the following criteria: efficiency, reliability, responsiveness, fulfilment, security and empathy (Doost and Ashrafi, 2014).

Between 2000 and 2008, the number of banks in Jordan offering Internet banking services increased from two to fourteen (Migdadi, 2008). The existence of Internet banking in this country dates back to 2000, when the Jordan Kuwait Bank made this service available for the first time, and it developed rapidly from that point. However, the use of Internet banking services is still weak, mainly due to concerns about security (Al-Rfou, 2013). Social influence, perceived trust and awareness are the significant factors that have an impact on the acceptance of Internet banking by customers (AL-Majali, 2011). The three leading countries in the Middle East for the adoption of Internet banking are Bahrain, the United Arab Emirates and Kuwait, with usage rates of

17%, 21% and 29% respectively. In Saudi Arabia, although 25% of banks have websites and offer full services over the Internet, the use of Internet banking services in this country is a marginal activity. As for Oman, there are few banks offering Internet banking services, though the banks maintain an informational website with basic interactive capability (Adapa, 2011). The next section will review the literature relating to the Internet banking industry in Asia.

2.3.6 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN ASIA

In India, Internet banking services were first offered by ICICI bank in 1998, and approximately 89% of the population prefer to conduct transactions using ATMs (Adapa, 2011). In 2005, research by the Internet and Mobile Association of India (IAMAI) revealed that customers are reluctant to conduct their transactions through the banks' websites, due to concerns about security and a preference for face-to-face banking transactions (Kesharwani and Bisht, 2012).

In 2010, Dixit and Datta confirmed that there had been a slow but steady increase in the adoption of Internet banking services in India, although worries about the security of the service persist. Additionally, a number of studies agree that the factors which are expected to affect Internet banking adoption in India are: expected risks, expected benefits, ease of use, trust and awareness (Joshua and Koshy, 2011; Safeena et al., 2011).

In China, the Internet payment system was launched for the first time by China's Merchants Bank in 1997. Thereafter, services of Internet and telephone banking proliferated across the region. Although there are about 40 million Internet banking

users to date in China, this number is low in comparison to the vast number of Internet users in that country (Yuan et al., 2010). In short, Internet banking in China is still in its early stages, and security is still the biggest obstacle to the acceptance of Internet banking (Hua, 2009).

There is a significant relationship between trust and perceived risk, and both of these factors affect the likelihood of Chinese consumers to adopt Internet banking (Zhao et al., 2010). Security had the greatest influence on users' acceptance of Internet banking, followed by privacy and perceived ease of use (Hua, 2009). Kurnia et al. (2010) argue that the barriers to the adoption of Internet banking in China include security concerns, limited infrastructure and lack of trust, whilst also noting the drivers, such as expected benefits and strong support from top management and government. Finally, the effectiveness and quality of Internet banking sites in terms of expected ease of use have an influence on customers' adoption of the service in this country (Liu et al., 2008).

In Malaysia, the information and communications technology revolution in the banking sector began in the 1970s. ATMs started to be used in 1981, while telephone banking was first offered in 1990. The Malaysian Central Bank allowed commercial banks to offer Internet banking services to their customers in 2000 (Raman et al., 2008) and by 2008, almost 23 banks were offering this service. Suki (2010) noted that customers' consciousness of Internet banking and its benefits is a critical variable affecting their adoption of Internet banking, while Nor and Pearson (2007) observed that trust is the factor which has the most significant impact on customers' adoption of Internet banking in Malaysia.

In Pakistan, Allied Bank was the first bank to provide an Internet banking system in 2004 (Omar et al., 2011). However, Mughal et al. (2012) mentioned that ease of use, security, trust, and awareness have an effect on the adoption of Internet banking by Pakistani customers. Similarly, the major factors which influence the adoption of Internet banking are: usefulness, security concerns, difficulties with navigating the websites and concerns that spying on the information is taking place (Akhlaq and Shah, 2011). In contrast, Zahid et al. (2010) found that the security and quality of Internet services do not have any considerable influence on Internet banking.

In Thailand, the Internet became available for the first time in 1987, with Internet banking services first being offered by the Siam Commercial Bank Plc. in 1999. By 2000, many banks in Thailand had begun to offer online transactions, with the average penetration of Internet users reaching 5.64% in 2001. The key factors which hinder the acceptance of this service relate to problems with the quality of the website, its usefulness, and the external environment (Jaruwachirathanakul and Fink, 2005).

Furthermore, it has been demonstrated that the ability to access services at any time, complete a transaction accurately, contact staff immediately, update information, and also the speed of transactions, all have a significant influence on the customer satisfaction levels (Nochai and Nochai, 2013). Security, risk awareness, ease of use, and quality of Internet connection were factors which affected the likelihood of customers in Thailand to adopt Internet banking (Kasemsan and Hunngam, 2011).

In Taiwan, although approximately one-third of banking transactions in 2002 were performed online, the data for May 2002 revealed that 1.25 million Taiwanese customers did not visit Internet banking websites during that month (Wang et al., 2003).

In order to attract and retain users of Internet banking services in Taiwan, the banks should provide better information which demonstrates the utilitarian advantages of this service (Chuang and Hu, 2011). Moreover, perceived usefulness and perceived ease of use have exerted a strong influence on the adoption of Internet banking (Chang and Hamid, 2010). Security plays a significant role in discouraging clients from using Internet banking, alongside accessibility, convenience, and the availability of features in Taiwan (Chuang and Hu, 2011).

With regard to Hong Kong, the adoption of Internet banking is affected by perceived usefulness, perceived ease of use and perceived risk (Yiu et al., 2007). In Bangladesh, Baten and Kamil (2010) found that customers' security and privacy had an impact on the adoption of this service. Jahangir and Begum (2008) agreed with this result and they also highlighted the importance of perceived usefulness and ease of use. According to Mondal and Saha (2013), customers are satisfied with the bill payment and money transfer services, but they are still worried about the security of Internet banking.

Overall, it clear that there has been slow but stable growth in Internet banking in Asian countries, such as India, China and the Republic of Korea. In Southeast Asia, notable growth in the Internet banking sector has taken place in Thailand, Malaysia, Singapore, the Philippines and China, despite the ongoing concerns that customers in those countries have about security (Hasan et al., 2010). A review of the literature on the Internet banking industry in Australia and New Zealand will follow in the next section.

2.3.7 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN AUSTRALIA AND NEW ZEALAND

In New Zealand, Internet banking services were introduced for the first time by the Auckland Savings Bank in 1996, followed by their subsidiary, Bank Direct. Since its introduction, there has been an obvious growth in Internet banking in New Zealand: in 2001, there were about 480,000 regular users of Internet banking services. A study indicates that the number of service users in this country will reach over one million in 2008 (Gan et al., 2006). Data from the Market Intelligence Strategy Centre revealed that over 7.2 million customers' accessed 27 million accounts online in Australia (Adapa, 2011). In 2002, Twenty- five per cent of adults in Australia were using Internet banking services; demand for these services is on the rise in spite of consumers' concerns about security. The factors which have been shown to have a negative effect on the adoption of Internet banking in Australia are: accessibility, a lack of awareness of services and their benefits, diminished trust, and risks relating to security and privacy (Lichtenstein and Williamson, 2006). In addition, usability and perceived trialling have had a significant influence on the attitudes of Australian consumers towards Internet banking. Moreover, social factors and convenience have an influence on consumers' choices regarding the adoption of Internet banking (Adapa, 2011).

In a study by Yeow et al. (2008), the respondents strongly believed that using Internet banking services would be beneficial to them; nevertheless, they encountered many obstacles to using these services, such as concerns about security and anxieties about the use of technology, all of which decrease their sense of self-efficacy. Conversely, Subsorn and Limwiriyakul (2012) concluded that there was a lack of information about the security of Internet banking on the banks' websites; this information could possibly

have an influence on current and potential future customers' level of trust in the banks. Consequently, this this study will focus on customers in the UK in order to explore the effects of concerns about security on customer trust, and will include users, non-users, and former users of Internet banking.

Furthermore, perceived risks, marketing communications and Internet access all have an impact on customers' decisions to adopt Internet banking (Clemes et al., 2012). The next section will review the literature on the Internet banking industry in the United Kingdom.

2.3.8 THE EVOLUTION OF THE INTERNET BANKING INDUSTRY IN THE UK

In 1983, the Bank of Scotland became the first bank in the UK to adopt the concept of electronic banking services (Shannak, 2013). By the end of 1989, telephone banking was commonly used in the UK (Nasir et al., 2015). In 2014, approximately 68% of customers had used devices such as tablets, mobile phones, and laptop or desktop computers to access Internet banking.

In same year, 76% of adults in Great Britain (approximately 38 million people) accessed the Internet every day. A survey by the Office for National Statistics (ONS, 2014) revealed that adults aged from 25 to 34 used the Internet more than other age groups to perform banking transactions, with 71% of people in this age group being users of Internet banking services; this survey also indicated that 54% of Internet banking users was men and 47% were women. Overall, 50% of the population of the UK use Internet banking according to Office for National Statistics (ONS, 2014).

While the percentage of Internet users increased, there was an associated steady increase in Internet banking usage. The figures from the Office for National Statistics prove that the rate of use was stable between 2009 and 2011, but indicate that a significant decrease in numbers of Internet banking users in the UK took place in 2012. The same report also highlighted the fact that, in 2012, 7.82 million adults, equating to 16% of the UK's population, had never used the Internet (ONS, 2013). According to the Annual Fraud Indicator, total losses resulting from Internet banking fraud reached £46.7 million in 2010 and £35 million in 2011 (Harrison, 2013).

Between 2005 and 2006, there was a steady rise in the use of Internet banking in the UK; and in the same period there was a significant increase in electronic fraud, which rose from £23.2 million to £33.5 million. Likewise, electronic fraud in the UK experienced another significant increase (up from £22.6 million to £52.5 million) between 2007 and 2008; during this period there was also an increase in the use of Internet banking (Chambers and Turksen, 2010). This is confirmed by Mahdi et al. (2010), who showed that Internet banking fraud had increased in 2008. In 2009, losses resulting from Internet banking fraud totalled £59.7 million in the UK (Randall, 2010).

In UK studies, the findings indicate that usefulness has a significant influence on younger males' attitudes, whilst ease of use had a significant effect on older females' behaviour with regard to the acceptance of Internet banking by customers in the UK. "Despite the steady growth of Internet banking services in the United Kingdom in the past few years, customers still visit a branch regularly"(Yousafzai and Yani-de-Soriano,2012,p.60). Research carried out by Finextra (2011) revealed that 42% of respondents prefer traditional human contact with their banks, compared to 38% who expressed a preference for email contact, 11% who preferred to use a website, and 3%

who wished to receive text messages by mobile phone. In 2009, the UK was lagging behind in the Internet banking figures, falling well behind the USA, Germany and France. Moreover, the data shows that there were approximately two million users who had left Internet banking services (Forrester Research, 2008).

In addition, Kamarulzaman (2007) hinted that by promoting trust in online services, banks could allay customers' fears about the perceived risks, owing to the fact that trust has a negative relationship with risk. Therefore, risk still had an impact on British customers' intentions to use electronic services at the time of the study. It has also been shown that perceived risk and lack of knowledge both exert an influence on the adoption of Internet banking in the UK (Gerrard et al., 2006; Bauer and Hein, 2006).

A study of the Woolwich bank found that security had an effect on the adoption of Internet banking services, alongside other factors such as availability of resources, brand name, effective administration and support from senior administration (Shah and Siddiqui, 2006).

Joseph et al. (2005) found that customers were generally satisfied with Internet banking services in the UK, but they also expressed a preference for personal (face-to-face) service, even when the same service is available online. Similarly, despite the fact that the majority of banks in the UK offer Internet banking services, most clients prefer using bank branches. The literature also confirms that there has been a steady increase in Internet users, with security being cited as the reason for non-use of Internet banking (Borland and Nteli, 2005). The Halifax Bank of Scotland asserts that perceived usefulness, trust, and perceived risk have a significant impact on the intentions of British customers to adopt and continue to use Internet banking services (Yousafzai et al., 2005)

In a broader sense, there are several obstacles which prevent people in Great Britain from using electronic government services, namely: lack of trust, lack of awareness, problems with accessibility, and language difficulties.

A study by Weerakkody and Choudrie (2005) found that that awareness and demand for e-services is modest in the UK. Clients were prevented from adopting Internet banking services by their wish to have stronger control over their financial transactions, and by the possible technical challenges encountered while using the service (Jayawardhena and Foley, 2000). O'Donnell et al. (2002) proved that customers in the UK preferred face-to-face interaction, which all customers considered to be more important than technological methods, such as Internet banking, email and web sites. In addition, British customers have a preference for a mix of delivery channels such as email, face-to-face services and telephone services, rather than using one single channel. They did not have a general predisposition to change their attitudes and adopt widespread usage of Internet banking (Howcroft et al., 2002).

This was further exemplified by a study conducted by Daniel (1999) in the UK and the Republic of Ireland, which found that banks were facing several challenges (e.g. security) when attempting to diffuse their services and motivate customers to accept and maintain Internet banking services.

All of these points lead to the conclusion that a significant number of British bank customers prefer personal services (face-to-face), while others tend to favour a mix of delivery channels. Nevertheless, customers were generally satisfied with Internet banking services in the UK. Furthermore, it is apparent that there is still a correlation between the issues of security, trust, and ease of use, and the uptake of Internet banking services: this is evidenced by the fluctuation and stagnation in demand for Internet

banking. The next section will discuss the global Internet banking trends that have discussed early in summary form.

2.3.9 DISCUSSION OF GLOBAL INTERNET BANKING TRENDS

From the analysis of the state of Internet banking in the countries discussed above, it is evident that banks and their consumers encounter challenges and worries with regard to the demand for and the adoption of Internet banking services. The relative modernity of Internet banking services and their total dependence on the World Wide Web give rise to concerns on the part of the consumers about security issues and access to their accounts. Moreover, several studies have conclusively shown that the acceptance and non-adoption of Internet banking services are influenced by security.

Financial institutions in general, and banks in particular, seek to provide new services in order to gain a significant market share and maintain a competitive advantage. Although Internet banking has created opportunities, it is clear that it also presents some challenges and obstacles to banks and consumers. The existing studies point out that almost all of the main banks have been quick to adopt Internet banking services, irrespective of whether or not they had the necessary infrastructure in place for the provision of this service, and also of the readiness of the population of their country to use such a service.

In spite of the rapid introduction of services by the banks, it took a relatively long time for clients in developed countries to accept Internet banking; this is due to issues relating to the development of the infrastructure for this service and also due to consumers' uncertainty about new technologies. The findings of previous studies show that there has been an uptake of the Internet banking service delivery channel around the

world: many countries have started to provide Internet banking services and are encouraging their customers to adopt them.

Therefore, bank managers now face the challenge of encouraging non-users to adopt the service, whilst also retaining existing users and motivating them to continue using Internet banking services.

From an economic perspective, an increase in the number of Internet banking users leads to a reduction in costs. As far as marketing is concerned, banks should continually research the views, proposals and requirement of customers, in order to retain current users of Internet banking and motivate non-users to adopt the service.

Thus, further research is required to investigate the potential factors that influence a customer's pre-adoption and post-adoption use of Internet banking services. Specifically, research into of post-adoption (continued use and abandonment of use) patterns of Internet banking use have been neglected, as most existing studies focus on either the adoption or acceptance of Internet banking (pre-adoption). The studies have also highlighted the existence of several indicators about abandonment of service. Moreover, the UK is lagging behind its international peers, especially other European countries, in terms of Internet banking usage. Nevertheless, it is clear that some ambiguity still exists with regard to the actual numbers for Internet banking use and abandonment of service in the UK.

The research in this thesis is a response to this gap in the existing literature: it offers an assessment of the reality of adoption and non-adoption of Internet banking services in the UK. It does so by exploring the influence of trust, perceived risk, and security concerns on customers' behaviour and on their intention to use, or not to use, Internet banking services. Moreover, it will highlight and explore the phenomenon of service

abandonment. Thus, the remainder of this literature review chapter focuses on the factors which influence the adoption and non-adoption of Internet banking services.

2.4 FACTORS AFFECTING THE NON-ADOPTION AND ADOPTION OF INTERNET BANKING

A review of the literature on Internet banking at both the global and local levels provides the researcher with broad prospects concerning the factors that have been studied and their impact on Internet banking services in the pre- and post-adoption periods, and also gives rise to recommendations for future studies in this area. Of particular significance are the variance of service delivery and the impact of factors from one environment to another. Moreover, an investigation of convergent cultural and economic environments will help the researcher to make comparisons with the environment under study and highlight significant features. Since there have been relatively few studies on Internet banking in the United Kingdom, this thesis will review the factors which affect the universal and local acceptance or rejection of Internet banking services . The purpose of this section is to review previous studies conducted in this context, with the aim of identifying factors affecting the adoption and non-adoption of Internet banking.

2.4.1 FACTORS INFLUENCING THE ADOPTION OF INTERNET BANKING

There are several factors which influence the acceptance and adoption of Internet banking. Since many international studies have evaluated Internet banking and the

factors that influence its adoption, it is vital that this investigation takes these factors, which are discussed below, into account.

Yoon and Steege (2013) identified three factors that influence Internet banking users in the USA. These factors are security, openness and website usability, which are significantly and positively related to Internet banking adoption. In addition, Kolodinsky et al. (2004) state that complexity, compatibility, observability and risk tolerance are associated with adoption. However, revenue, education level, sex, age and marital status also have an effect on acceptance of the service. The Federal Reserve Bulletin mentioned that socioeconomic and demographic characteristics of customers, and the ease with which the service can be used, have an influence on the acceptance and adoption of Internet banking in the USA (Anguelov et al., 2004). In Canada, Montazemi and Saremi (2013) showed that trust, perceived usefulness, and perceived ease-of-use influenced consumers towards initial use of Internet banking. Furthermore, Mangin et al. (2011) indicate that price and convenience variables have an impact on the usefulness of Internet banking services in Canada.

In Mexico, the factors that affected the acceptance of Internet banking were trust, security, social influence, compatibility and computer skills (Mansumitrchai and Al-Malkawi, 2011). In the same way, research conducted in the UK (White and Nteli, 2004; Ochuko et al., 2009) found that Internet banking security remains the key concern for consumers, and it influenced the diffusion and adoption of Internet banking. Liebana-Cabanillas et al. (2013) discovered that accessibility, ease of use, trust and usefulness all had a positive effect on customers' acceptance of, and satisfaction with, Internet banking services in Spain. In the same continent, Internet experience and connection mode, perceived security, and socio-demographic characteristics influenced

customers in Poland to adopt this service (Polasik and Wisniewski, 2009). Martins et al. (2014) found that effort expectancy, performance expectancy, social effects, and risk were considerable factors affecting users' acceptance of this service in Portugal.

With regard to New Zealand, Clemes et al. (2012) revealed that ease of use, marketing communications, perceived risks, price, and accessibility had an influence on customers' decisions to adopt Internet banking services.

In Malaysia, the findings of the Goudarzi et al. (2013) indicated that trust has a significant effect on the adoption of Internet banking. The same study also revealed that several factors have a relationship with trust in electronic services. In addition, Al-Fahim (2012) showed that trust, ease of use, awareness and security have had a positive impact on use of Internet banking in Malaysia. In the same country, Eze et al. (2011) found that perceived ease of use, perceived usefulness, self-efficacy, perceived credibility and trialability incited consumers to accept this service in Malaysia.

In Iran, numerous studies confirm that usefulness, security, trust and perceived ease of use had an influence on customers' acceptance and adoption of Internet banking (Salari and Salajegheh, 2011; Rahmati et al., 2013).

Moghadam et al. (2012) show that Internet advertisements have an influence on customers' acceptance of Internet banking, whilst also creating a positive attitude towards Internet banking. In a further study relating to Iran, Farzianpour et al. (2014) showed that risk and willingness to accept innovation have a direct effect on the adoption of Internet banking. In addition, Akbari et al. (2013) found that tangibility, reliability, responsiveness, assurance, empathy and convenience affect customers' satisfaction and their adoption of Internet banking services.

A study by Salari and Salajegheh (2011) revealed that trust, ease of use, usefulness and attitude all have an influence on the adoption of Internet banking, whereas Shafiee et al. (2013) observed that the complexity or simplicity of the process, security, existing appropriate legal infrastructure, ease of use, and users' levels of IT literacy have an influence on the acceptance of Internet banking by users in Iran.

In Pakistan, Ilyas et al. (2013) found that the quantity of information, security, and privacy have an impact on the behaviour of customers in relation to the acceptance of Internet banking. Azim et al. (2011) showed that trust had an important effect on customers' behaviour with regard to Internet banking. In China, findings indicate that trust and perceived risk have a significant influence on Internet banking usage (Zhao et al., 2010). Other studies also show that service quality has a significant effect on users' trust and satisfaction with the service, and on their adoption and continued usage of Internet banking (Zhou, 2013).

In Taiwan, Lee (2009) indicated that the decision to use Internet banking services is influenced by perceived benefit, attitude, and perceived usefulness. Moreover, Tsai et al. (2013) highlight the fact that risk, social issues, performance expectancy and effort expectancy all affected customers' adoption of the service in this country.

Lee et al. (2013) mention that Internet banking users in South Korea are still concerned about security issues. In Hong Kong, Yiu et al. (2007) found that there was an obvious effect of usefulness, ease of use, and risk on the acceptance of Internet banking In Vietnam, a study by Chong et al. (2010) found that usefulness and trust have an influence on the adoption of Internet banking.

In the Philippines, Lim (2003) showed that usefulness and ease of use positively affected customers' intention to adopt Internet banking.

As far as Arabic countries are concerned, there have been several studies in this region which have investigated this point. In Saudi Arabia, AI Somali and Ghinea (2012) confirm that the age of the user, perceived risk, perceived usefulness, social influence, facilitating conditions and the availability of an Internet connection positively influence the population's judgment of Internet banking directions. In Egypt, Hussien and Abd El-Aziz (2013) mention that service quality has a significant effect on customer satisfaction in adopting Internet banking. In Jordan, Ahmad and Al-Zubi (2011) argue that accessibility, security, convenience, website design, speed and cost have an influence on Jordanian customers' acceptance of Internet banking and their readiness to adopt this service. Whereas Al-Smadi (2012) states that perceived risk has a stronger impact on customers' attitude to using electronic banking services, a study by Al-rfou (2013) a found that there was also a significant relationship between several others factors (security, ease of use, quality of Internet connection) and Internet banking services in Jordan.

In Oman, Riffai et al. (2012) explored the significant factors that influence Omani consumers' acceptance of Internet banking. They are: trust, usability, and perceived quality. In Yemen, Al-Ajam and Nor (2013) found that perceived relative advantage, perceived ease of use, perceived compatibility, trialability and trust had an important influence on clients' adoption of Internet banking. In Tunisia, Nasri and Charfeddine (2012) pointed out the impact that security and privacy issues have on users' trust in Internet banking. In his study of Morocco, Echchabi (2011) demonstrated that perceived ease of use and perceived usefulness have a significant influence on customers' attitudes

towards the adoption of Internet banking services in that country. In Ethiopia, Takele and Sira (2013) revealed that there were some factors which had a significant influence on customers' intention to adopt services, such as perceived usefulness, attitude, subjective norm, perceived behavioural control, perceived ease of use and risk. In Nigeria, Dalhatu et al. (2014) show that trust has significant effect on Nigerian retail customers' adoption of Internet banking.

Previous research has indicated that the convenience of Internet banking is a significant reason for its adoption (Lichtenstein and Williamson, 2006; Aristeidis and Ioannis, 2010). Thus, it is one of the primary reasons for its diffusion. A number of researchers are in agreement that factor which has the second highest effect on the acceptance of service is expected ease of use, or usability (Auta, 2010; Jin and Kim, 2010).

When tracking other factors which influence Internet banking users, a number of researchers (Alsajjan and Dennis, 2010; Lee et al., 2011) found that perceived usefulness has an influence on adoption of Internet banking.

Regarding perceived risk, it is well recognised that the nature of the online environment and the uncertainty of using an open infrastructure to complete procedures throughout the world inevitably causes Internet banking services to be susceptible to risks and (Yousafzai et al., 2003). Thus, consumers have growing concerns about their ability to protect their information (Liao et al., 2011). According to several studies, perceived risk had a significant role in influencing users' decisions to use Internet banking (Takele and Sira, 2013; Tsai et al., 2013; Farzianpour et al., 2014; Martins et al., 2014).

A number of surveys show that worries about security have a significant influence on the adoption of Internet banking (Yoon and Steege, 2013; Al-Fahim, 2012; Hong et al.,

2013). As mentioned above, research also indicates that trust plays a considerable role in adoption of the service. In addition, subsequent studies confirmed the importance of this factor for the acceptance and adoption of Internet banking (Akhlaq and Ahmed, 2013; Goudarzi et al., 2013; Al-Ajam and nor, 2013).

Demographic characteristics have a significant impact on Internet banking behaviour. One such characteristic is old age: old people prefer not to use Internet banking. Gender is another important factor, as statistics confirm that women are more likely to use this service than men (Polasik and Wisniewski, 2009; Al-Somali et al., 2009; Aristeidis and Ioannis, 2010).

A further important factor is the quality of service experienced when using Internet banking services: this was investigated by Sharma and Malviya (2014) in their 2014 study which attempts to develop a model to investigate the impact of service quality on customer satisfaction. Researchers found that a positive correlation exists between service quality dimensions and customer satisfaction toward Internet banking. Other researcher also confirmed that, in order to increase acceptance and satisfaction of customers, banks should improve the quality of Internet banking services, and they also agreed that customers' satisfaction with Internet banking is affected by the quality of service (Camilleri et al., 2013; Doost and Ashrafi, 2014; Alihosseini, 2014; Sakhaei et al., 2014; Yaghubi and Seyedin, 2015). Moreover, "service quality plays a vital role to fill the gap between customer expectations and customer perceptions regarding the Internet banking services"(Saeed et al., 2015, p.1). In addition, Kaur and Kiran (2015) showed that improving the quality of Internet banking services has strong positive influence on customer loyalty. To summarise, the majority of studies show that Internet banking service quality has an influence on customer satisfaction.

Furthermore, the media have had an important impact on customers' behaviours toward Internet banking services. On the one hand, the media can have a very positive effect on the success of Internet banking; methods such as positive advertising require very little cost to achieve results. On the other hand, the media can sometimes have a very negative impact on the success of Internet banking services, for example by spreading news of electronic fraud (Al-Somali et al., 2009).

One considerable barrier to Internet banking is a lack of computers and the non-proliferation of the Internet. The non-availability of ICT infrastructure (including telecommunications networks, Internet connectivity, availability of computers and other means of help) has a negative impact on the adoption of Internet banking (Centeno, 2004). Organisational factors can also constitute a barrier to Internet banking, including the extent to which the bank is ready to provide the service, e.g. possession of infrastructure-relevant systems and the necessary technical skills (Riyadh et al, 2009). Furthermore, employee skills in speaking and debating have a role in influencing customers: a study conducted by Ashtiani and Iranmanesh (2012) on Iranian customers confirmed that positive word-of-mouth testimonials have a positive impact on service adoption.

Overall, several studies have examined the factors that influence the adoption of Internet banking service globally, and the literature review above leads to the conclusion that which have an influence on the acceptance and adoption of Internet banking services whether developed countries (for example the UAS, Canada, the UK, new Zealand and Spain) or developing countries (such as China, Malaysia, Pakistan, South Korea and Arabic and African countries), the most important of these factors are security, perceived risk, trust, ease of use, usefulness and service quality. Moreover,

majority of these factors that mentioned above have direct and indirect influence on customers' trust toward Internet banking services globally.

On the other hand, there are other factors have influence the adoption and acceptance of Internet banking services in developing countries just such as, social influence, computer skills, ICT infrastructure, awareness, self-efficacy, Organisational factors, word-of-mouth, users' level of IT literacy and facilitating conditions and the availability.

The above suggests that human nature is influenced by external factors; across different cultures and civilizations, as the instinct of fear exists within people in general. Therefore, security is a factor that still concerns customers, and has a significant influence on the acceptance and adoption of Internet banking services. Laws and regulations governing Internet banking services in order to protect customers and institutions generally still do not adequately meet the expectations of customers and organisations.

Nevertheless, there is stable and slow growth in adoption of Internet banking services, although there has been an increase in demand for Automated Teller Machines (ATM) and bank branches, to complete large transactions and money transfers, rather than online services.

With regard to demographic characteristics, it evident that these have an impact globally, and the literatures indicates that customers in older age groups prefer to use ATMs and do not use Internet banking services. It is also noted that women are more inclined to adopt these services. In addition, media influences customers, both positively and negatively, causing them to accept or reject Internet banking services.

All of this points to the conclusion that for Internet banking services, as with any economic project facing challenges and barriers to its success, the most important consideration is security, as these services depend on the World Wide Web. The following section will review the factors influencing the non-adoption of Internet banking.

2.4.2 FACTORS INFLUENCING INTERNET BANKING NON-ADOPTION

A number of studies have identified the factors influencing the non-adoption of Internet banking. For example, in the UK, Gerrard et al. (2006) observed that there were several factors behind the non-adoption of Internet banking services, namely perceived risk, lack of knowledge, and inaccessibility. By contrast, studies in Finland found that ease-of-use, usefulness, and perceived risk played an important role in the resistance of customers to use Internet banking (Laukkanen et al., 2009). Security, trust, computer skill, human communication, and social effect have an influence on the adoption of Internet banking in Mexico (Mansumitrchai and AL-Malkawi, 2011). In Malaysia, non-adopters were concerned about security and trust, with ease of use and awareness also affecting their decisions (Al-Fahim, 2012). In addition, Munusamy et al. (2012) state that ease of use, convenience, reliability, security and accessibility have an impact on customers' intention to use Internet banking. Moreover, Poon (2008) also confirmed that security issues are the main reasons for customers' dissatisfaction with the use of Internet banking.

In India, research has found that legal and security issues, socio-cultural barriers, and banking management issues are some of the most prominent challenges for the

development of Internet banking (Karimzadeh and Alam, 2012). In Taiwan, Lee (2009) found that the decision to adopt Internet banking is adversely impacted by security and risk, for example privacy risks. In Thailand, Rotchanakitumnuai and Speece (2003) found that non-users do not trust Internet banking to conduct their transactions.

In Ghana, security concerns and user privacy are the biggest challenges facing customers with regard to Internet banking (Ofori-Dwumfuo and Dankwah, 2013). In Zimbabwe, a study revealed some of the risks encountered by users of Internet banking, namely: computer literacy, security concerns, inaccessibility of services and operational problems (Ndlovu and Sigola, 2013). In Nigeria, Popola (2013) showed that Nigerian customers lack trust in Internet banking as a consequence of security issues and banks' reputations.

In addition, the results of a study indicated that the use of Internet banking services in Jordan is weak. Several factors were found to be responsible for the non-use of the service, such as ease of use, security and the quality of Internet services (Al-Rfou, 2013). This is in comparison with the situation in Sudan, where a study by Ismail and Osman (2012) highlighted that the factors leading to the non-use of Internet banking are lack of Internet access, technical problems, a lack of means of reporting faults, ambiguities in the legislation pertaining to electronic transactions, delays in correcting erroneous transactions, banks failing to play a sufficient role in raising consumer awareness, gaps in the guidelines and instructions for Internet banking, frequent power cuts, and the fact that fees are charged for Internet banking services.

Various studies have investigated the barriers to the adoption of Internet banking in developing countries.

The studies reviewed above found that the significant barriers were a tendency towards non-innovation and a lack of development, ease of use of the system, an absence of IT infrastructure, and the social and organizational culture and skills of individuals and organizations in the field of electronic commerce. Although it is clear that ease of use has a considerable effect on the acceptance of Internet banking, it cannot be considered to be an instrumental factor in the delivery of Internet banking services. In a more general sense, several issues such as the complexity and design of the website, and slow download speed, have had a strong impact on the non-adoption of the service (Hosein, 2009).

Yiu et al. (2007) also stated that risk and computer literacy had important an influence on customers' decisions about the use of Internet banking. Security also has an effect on the non-use of Internet banking services: this has been consistently demonstrated by the findings of various studies (Kim et al., 2010; Huang et al., 2011). In addition researchers have suggested that demographic and personal factors may also inhibit the adoption of Internet banking services (Almohaimmeed, 2012)

Finally, customers in the UK still experience concerns about the security of Internet banking (White and Nteli, 2004); this is also true of customers in Australia (Lallmahamood, 2007).

Overall, it is apparent that there have been growing concerns about the security of Internet banking and an increasing number of consumers are worried about the risks of using Internet banking services. This has primarily been the consequence of several fraudulent cases such as cyber hacking and e-fraud.

2.5 CHAPTER SUMMARY

Although financial institutions in some countries took steps to implement Internet banking services from the 1990s (Keivani et al., 2012), other countries are still in the first stages of this process. For this reason, this chapter has begun to highlight and review the reality of this service around the world. The majority of developed countries are considered to be the leading countries in terms of this service, but it is clear that both developed and developing countries encounter difficulties with Internet banking. For example, fraud and security risk issues are still the main concerns of customers in the USA (Yoon and Steege, 2013). Consequently, 23.7 million people in that country do not use the service and approximately 9 million American adults have abandoned the use of Internet banking (Finextra, 2006).

In addition to security, the adoption and non-adoption of Internet banking are also influenced by other factors such as trust. Similarly, security concerns are still the dominant issue for clients in European countries and ATMs are the most widely used method of conducting banking transactions. Studies have discovered indicators for customer abandonment of the service, especially in Sweden, the UK (Giovannini and Ensor, 2006) the Nordic region, Switzerland, Benelux (Polasik, and Wisniewski, 2009) and Germany (Dapp, 2013).

In the UK also the literatures concludes that more than a few British bank customers prefer face-to-face services, while others tended to favour a mix of delivery channels. Furthermore, the Annual Fraud Indicator reports by (Harrison, 2013) and Financial Fraud Action UK (2011) clearly show that the security of the Internet banking service is still a cause for concern among UK customers, who may be worried by the possibility of

fraud losses. Clearly, Internet banking users in the UK are still concerned about the security risks, privacy risks and financial risks posed by Internet banking services (Nasir et al., 2015). In addition, trust issues and ease of use have an effect on the acceptance or rejection of the service (Sankari et al., 2015).

In Asia, a similar situation with regard to Internet banking services exists in most large countries, such as India, China and, the Republic of Korea, with many similarities also existing in Pakistan. There has been a slow and steady increase in the adoption of the service. Moreover, the majority of customers in these countries prefer to use ATMs, with security risks, trust and ease of use being the significant factors influencing the adoption and non-adoption of Internet banking. Conversely, the literature has showed that there has been notable growth in Internet banking in Southeast Asia, for example in Thailand, Malaysia, Singapore, and the Philippines.

The situation in Africa is not very dissimilar from that in Asia: perceived ease of use, security and trust were factors which have a considerable impact on the adoption and non-adoption of Internet banking by customers. The majority of customers prefer to use ATMs and there is a lack of telecommunications infrastructure. In addition, trust has significant effect on customers' choices to adopt Internet banking (Dalhatu et al., 2014).

In general, it seems that several factors affect the acceptance or rejection of the service: these are security, risk, trust, ease of use, usefulness, convenience, service quality, privacy, self-efficacy, environmental factors, and social influence factors. The impact of the above factors on the adoption and non-adoption of services differs from one environment to another, although many studies in the literature review revolved around the factors of trust, security and risk and their direct influence on the non-adoption and

adoption of Internet banking, in addition to investigating the indirect effect of those factors on the acceptance and rejection of Internet banking through the relationship with and the impact on other factors.

In addition, recent research has confirmed that trust (Montazemi and Saremi, 2013; Liebana-Cabanillas et al., 2013; Goudarzi et al., 2013; Dalhatu et al., 2014), security (Yoon and Steege, 2013; Shafiee et al., 2013) and perceived risk (Clemes et al., 2012; Martins et al., 2014; Farzianpour et al., 2014) have a significant and obvious influence on the non-adoption and acceptance of Internet banking services.

It is evident from the previous review in this chapter that, even in the leading countries, Internet banking services is still a fertile field for research and exploration. The literature review highlights the existence of gaps in knowledge of various aspects of this subject, such as fluctuations in demand and indicators of abandoning the service. There is a general consensus in many previous studies that trust is one of the most important factors that exerts a direct and indirect influence on Internet banking. However, the majority of those studies focused on the influence of trust on the adoption and acceptance of Internet banking, and few studies have examined the effect of trust on non-adoption, with research into its influence on abandonment of service being almost non-existent.

Nevertheless, customers to date are still concerned about security and the perceived risk of using Internet banking services (Nasir et al., 2015) so in future, researchers in this area should concentrate on these factors. Therefore, this study will focus on these factors and their influence on the reality of Internet banking services in the UK, by investigating the influence of trust, security and perceived risk on the non-adoption,

adoption, abandonment and continuation of use of Internet banking services. Consequently, the next chapter will focus on these factors, followed by a description of the evolution of theoretical models on the acceptance of technology, in order to enable this study to build the theoretical models for addressing study issues, and the remainder of this chapter will focuses on research issues.

CHAPTER 3: RESERCH ISSUES, THEORIES AND FRAMEWORKS

3.1 INTRODUCTION

The previous chapter provided an overview of Internet banking, followed by a survey of trends in the global Internet banking industry, and concluded with a review of the factors affecting non-adoption and adoption internet banking. This chapter will provide an outline review of issues relating to trust, risk and security in Internet banking services. This will be followed by a review of these issues in online service generally. Finally, it will seek to review the relevant studies that use theoretical models of the acceptance of technology. The chapter will present the three most influential of these models, namely: the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) and the Technology Acceptance Model (TAM). These models will help the study to build theoretical models, and to attempt to evaluate consumers' decision-making behaviours towards Internet banking, in both post-adoption and pre-adoption stages. The chapter will conclude with a discussion of research issues.

3.2 CRITICAL REVIEW OF TRUST, RISK AND SECURITY

3.2.1 TRUST AND INTERNET BANKING

3.2.1.1 INTRODUCTION

It has been argued that the lack of direct physical contact in online transaction environments is accompanied by a decrease in levels of trust between parties (Yousafzai et al., 2009). Therefore, several studies have dealt with trust, and its role, impact and importance in this respect. For example, (Nor and Pearson, 2007; Chong et al., 2010) showed that trust is an important element, that has a significant influence on attitudes

towards using Internet banking. Moreover, the issue of trust is so central that it has been described as the principal focus of the system of Internet banking (Amin, 2007).

3.2.1.2 DEFINITION OF TRUST

Generally considered, trust lies at the heart of all types of relationships, whether in the online or offline world (Alsajjan and Dennis, 2006). However, some researchers have confused trust with other concepts, such as honesty, confidence, and faith. Thus, this research will focus exclusively on the concept of trust in the online world. As with conceptual analysis in other academic disciplines, there are several definitions of trust in the literature, especially concerning online transactions. In specialist Internet transactions research, a frequently cited definition is that trust "is the willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"(Aljazzaf et al., 2010,p.156).

This willingness to be vulnerable also links with the expectation that the other party will perform, according to the definition provided by Yousafzai et al. (2009, p.592). They posited that trust in Internet banking is defined as the "willingness to perform banking transactions on the Internet, expecting that the bank will fulfil its obligations, irrespective of the customer's ability to monitor or control the bank's actions on the internet".

Certainty is also a critical component of trust, in addition to willingness to be vulnerable, and to expectations of performance from the other side. In this regard, Zissis and Lekkas (2012, p.585) defined trust as "the customer's certainty that the organisation is capable of providing the required services accurately and infallibly". Ghane et al.

(2011, p.3) defined trust as "the degree of clients confidence in online dealings, or in the online exchange channel". Recently Zaglago et al. (2013, p.2) defined trust as "a psychological state that allows a person to accept vulnerability based upon positive expectations of the intentions or behaviour of others". Furthermore, it was defined as "the belief that the future actions from persons/organizations will lead to a good outcome" by Thirunarayan et al. (2014, p.184).

This study therefore defines trust *as a reliable relationship between customers and banks, built on honesty, a willingness on the part of customers, to accept all procedures and actions of a bank's online service, and the expectation that the service will meet their requirements exactly as promoted.*

3.2.1.3 THE IMPACT OF TRUST ON ADOPTING INTENET BANKING

Trust is considered an important factor in the online world, with the success or failure of online businesses largely depending upon it. Moreover, the risks associated with possible unlawful access to customer data are huge. It is therefore apposite that researchers concur on the significance of trust, in surmounting consumer resistance. For instance, Hanzaee and Alinejad (2012) argued that trust is especially significant in Internet banking, because these types of financial transaction contain very sensitive and valuable data, which all concerned are keen to safeguard; this accounts for the attention devoted to the concept of trust by many researchers and organisations. Trust is therefore an important factor in most working relationships, and it is perceived as a key dimension in the study of Internet banking acceptance (Alsajjan and Dennis, 2006). Nonetheless, researchers differ with regard to reported levels of direct or indirect

impact. For example, Esmaili et al. (2011) hinted that trust has only a moderate role in influencing customers' intentions regarding the use of online transactions. Similarly, other studies (Zhao et al., 2010; Esmaili et al., 2011; Chen, 2011) have concluded that trust plays a role in reducing customers' perception of risk, and reflects positively on their adoption of Internet banking.

A wide range of studies (Salari and Salajegheh, 2011; Alnsour and Alhyari, 2011; Widjana and Rachmat, 2011; Omar et al., 2011; Esmaili et al., 2011; Riffai et al., 2012; Alsheyyab and Singh, 2013; Sankari et al., 2015) have reinforced the view that lack of trust is one of the essential factors behind the reluctance of consumers to adopt and accept the use of Internet banking. Trust is necessary for action in diverse situations, not only in the Internet banking context; however, unless banks take strong measures to enhance security, the potential for loss, and customer uncertainty, will persist. The next section will discuss building trust towards Internet banking.

3.2.1.4 BUILDING TRUST TOWARDS INTERNET BANKING

Trust is one of the critical factors in the success of electronic business projects generally, and it plays a significant role in the acceptance and continued use of Internet banking. Consequently, attention should be paid to evolving effective steps towards gaining customers' trust, and maintaining it. In particular, electronic fraud (e-fraud) has had a significant negative impact on customers' adoption of Internet banking (Srinivasan, 2004).

Beldad et al. (2010) reported that e-fraud losses reached £59.7million in 2010, and that there were 51,000 phishing cases reported, related to Internet banking in the UK. Without doubt, security has an important role to play in improving customers' trust

towards Internet banking; Financial Fraud Action (2013) revealed that Internet banking fraud losses in 2012 and 2011 were £39.6 million and £35.4 million respectively.

Coles and Smart (2011) stressed that the perceived security and quality of a website has a significant influence on building customers' trust, as online customers often measure the risks of online action in terms of data disclosure or misuse, by penetrating the banks' websites in order to identify signs of inadequate protection, or defects in the quality of the sites. This will obviously affect the level of trust towards websites and security systems (Banakdeh and Ganginia, 2014). For instance, 88% of the sample reported that they still saw security as a source of concern relating to their personal information, and expected high levels of communications safety and security. These expectations are the first steps in building customer trust online (Coles and Smart, 2011)

Moreover, Yap et al. (2010) indicated that service quality and website advantages play a significant role in influencing trust in Internet banking. They also mentioned that new customers in Internet banking often need help from bank employees (for instance, in setting up the electronic banking account, and explaining the advantages of the system). Yousafzai et al. (2005) showed that security policy, privacy policy, web-site quality and design all enhance customers' trust in Internet banking, as well as providing them with meaningful and timely information.

Surmounting consumer fears on the safety of personal data, and achieving acceptance of Internet banking, requires a high level of trust (Nor and Pearson, 2007). Banks therefore need to develop improved policies for promoting customer confidence. However, there is still insufficient knowledge regarding the methods used by banks to develop customer trust in Internet banking (Yazdanifard et al., 2011). It is first of all important to establish

in customers' minds the perception that e-government services are secure and efficient, by ensuring that all parties provide guarantees of service efficiency and integrity. Given societal reluctances and fears of digital system engagements, failure to do this would create a major obstacle for electronic enterprises (Eanas and Sun, 2009).

In the literature, there is wide use of Chang et al.'s (2013) equation, which defined trust as the sum of credibility, reliability, and intimacy, divided by self-orientation:

(Credibility + Reliability + Intimacy)/ (Self-Orientation)

However, although Lasheng and Placide (2009, p.116) did not dispute this, they suggested that access to clients' trust can be attained by many means, the most significant being:

1) Banks should be authorised and certified by government to issue Internet banking services.

2) Clients should be certified by the banks' operational services, which are offered in a secure environment.

3) Clients requesting services need to authenticate themselves to the bank, as well as banks having to authenticate customers before beginning their dealings.

4) Each party must validate transaction documents, and keep a copy of those documents.

Lasheng and Placide provided this equation for gaining trust:

Authentication + Encryption + Certification Authority = Trust

Yap et al. (2010) showed that building customer trust in Internet banking services through service quality and website features, impacts on a bank's reputation. Hence, Chang et al. (2013) found that there were three mechanisms for building trust that had a significant positive effect on customers' trust in online services, viz. third-party certification, reputation, and return policy. In addition, Yu et al. (2015) noted that facial cues can have a powerful impact on trust-building in Internet banking services. Broadly speaking, several studies have identified ways of helping to increase trust in Internet banking services, although these suggested solutions might be more effective when used in combination with others. These studies are: Centeno (2002); Lamberti and Kawamura (2003); Srinivasan (2004); Dimitriadis and Kyrezis (2008); Urban et al. (2009); Abbass and Ibrahim (2011); and Gilaninia et al. (2011).

The following are some of the solutions proposed in various studies that can help to build customers' trust towards Internet banking: adjustment of international and national legislation to serve this sector; improving security usability; enhancement of site design and quality; transparency in dealing; establishing 'stay in touch free' policies; answering customer inquiries quickly; rectifying problems as soon as possible; emphasising truth and fairness; keeping promises made by managers; educating, guiding and advising new customers; improved marketing and advertising of services; developing strategies for maintenance and warranty contracts; promoting brand and reputation; using up-to-date technology, and developing decision-making strategies. The next section will discuss security and Internet banking services.

3.2.2 SECURITY AND INTERNET BANKING

3.2.2.1 INTRODUCTION

Internet banking is rapidly increasing; however, this increased use is accompanied by rapidly growing electronic fraud (Fatima, 2011). Thus, security and its requirements are a major preoccupation for banks, and security is considered as the main driver in financial dealings. Therefore, Internet banking security involves the protection of the system against security threats, and the control of personal data information in the online environment. Specifically, this involves the ability of the bank to protect personal information from unauthorised use or disclosure, or from being changed by third parties without permission. The importance of security to the acceptance of Internet banking has been noted in literatures relating to the banking industry (Nasri and Zarai, 2014). This section will discuss various aspects of security in Internet banking, including the definition of security, security requirements, how to make Internet banking secure, security threats facing the sector, and the role of security in the adoption and acceptance of Internet banking.

3.2.2.2 DEFINITION OF SECURITY

Security in Internet banking has been explained in different ways by numerous researchers, and thus has a number of definitions. This paragraph will review some definitions of security covered by the literatures.

Nasir et al. (2015, p.464) described security concerns as "customers' beliefs in potential uncertainties or loss caused by the vulnerability of Internet banking, which will lead to unexpected and unnecessary personal stress. This is because online transactions take

place in a generally opened virtual environment, and information through the platform may be intercepted by a third party, which might compromise users' information safety"; Reddy (2012, p.5) defined it as "the protection of data against accidental or intentional disclosure to unauthorised persons, or unauthorised modifications or destruction".

In addition, security has been defined as the situation that results from protective measures that enable organisations to perform their tasks without taking risks that threaten their use of online services (Kissel, 2011). Also, Shin (2010) defined security as the ability to protect data against unauthorised access. Sun et al. (2011, p.2853) identified security as "the combination of confidentiality, the prevention of the unauthorised disclosure of information, integrity, the prevention of the unauthorised amendment or deletion of information, and availability; the prevention of the unauthorised withholding of information".

This study defines security *as the precautionary measures adopted by all parties in the banking process (e.g., banks, customers, companies) for the protection of sensitive data; as well as the safeguarding of financial and administrative procedures from manipulation and electronic fraud reductions.*

3.2.2.3 INTERNET BANKING SECURITY REQUIREMENTS

Electronic business security generally is effective only if it is maintained as part of an organisation's overall risk administration policy (Tyagi and Srinivasan, 2011), whilst the success of Internet banking security especially depends on the quality of debate and understanding of security issues between all parties to a transaction (Koskosas, 2011). Thus security is significantly related to such aspects as confidentiality, i.e. the

prevention of unauthorised access to sensitive and private information; integrity, i.e. ensuring that during transmission information cannot be accessed or altered by a hacker; and availability, i.e. safe, continuous and uninterrupted provision of services (Abdellaoui and Pasquet, 2010; Naumann, 2009). These elements are considered to be the bedrock of the creation of secure systems (Zissis and Lekkas, 2012), and are usually abbreviated as (CIA) or the AIC triad (Pennanen et al., 2006).

As various studies have suggested, certain steps are required to enhance secure Internet banking. Many online banks throughout the United States have implemented a five-step approach for Internet banking access: in the first step, the user must enter the access ID for their account, which is provided, by the bank. The second step requires the user to enter a password to gain access. The third and fourth steps ask the user to answer security questions that were previously answered by the user. In the last step, the user identifies a picture that they have previously marked and labelled (French, 2012).

In the United Kingdom, Lloyds TSB Bank provides a phone certification service for users wishing to log in to Internet banking. Lloyds Bank also employs a range of other means to make Internet banking accounts secure.

These include fraud detection systems, automatic log-off if customers remain inactive on Internet banking for 10 minutes, or forget to log off, and the capacity to disable the account if there are a number of incorrect log-in attempts. Barclays Bank and Royal Bank of Scotland, for example, use tiered authorisation methods, involving the use of ID, password, and smart card readers, for customers' transactions and activities. In addition, Barclays Bank offers Kaspersky Internet Security Suite anti-virus computer programs (Lee et al., 2013).

Nasir et al. (2015) suggested two methods of ensuring secure access. The first proposal involved a two-factor authentication, which would include, for example, a password combined with a token, such as a smartcard. The second proposal added a third factor for authentication, which could be the use of biometrics, such as iris or thumb print recognition. Therefore, if hackers breached the first level, they would need to breach further layers of security, which would create further difficulty.

Lasheng and Placide (2009) argued that the authorisation and certification of the banks to issue Internet banking services should proceed from central government, and that customers should request services which are approved by banks, before starting their transactions. Furthermore, Reisa et al. (2011) showed that the literacy of Internet banking users has a significant role in safeguarding the continuity of security. In addition, they argued that unique passwords should be set for online accounts, and should be changed on a regular basis; and that it is best to avoid common choices such as '1234', a phone number, account number, or other easily-guessed numbers or phrases.

Customers should also be advised to be careful when using public computers to log into online banking sites, and to be aware of the people around them. Moreover, they need to be cautious of emails that may contain viruses in downloads, and should always have anti-virus software, as well as firewalls, installed and maintained (Bakar, 2011). Fatima (2011) contended that the best solution to security threats in Internet banking was the use of biometrics; this method has now been widely accepted in the consumer market. The next section will discuss security threats facing Internet banking services.

3.2.2.4 SECURITY THREATS FACING INTERNET BANKING

Internet banking is a new technology which has many possibilities and advantages, but also many potential problems; therefore customers are resistant to using the system. Moreover, the number of malicious applications targeting Internet banking dealings has increased in recent times (Fatima, 2011). The rapid spread of the Internet has meant that greater populations potentially have access to Internet banking sites, either as customers or potential customers. Along with this opportunity has come a greater threat of criminal access by hackers.

The latter are constantly evolving highly sophisticated techniques to access customer information and funds. Banks thus have had to keep ahead in the security field, in order to ensure that their portals offer the most rigorous protection available against any potential threats (Chakrabarti and Manimaran, 2002).

There are several types of fraud which threaten Internet banking, including phishing scams, a method of effecting online identity theft by sending emails or messages that look as if they come from trustworthy organisations, with the aim of tricking the target individual into submitting significant information (Delgado et al., 2008); and Crimeware, specialist softwares designed to degrade the security of computer systems/networks, and to enable the creators to gain unauthorised access, and to copy or edit, valuable information. Several forms of this software exist, including adware, malware, spyware, Trojans and viruses. These all have the potential to misrepresent and lull typical banking customers into submitting personal information, or inadvertently allowing access to the software creators (Bakar, 2011).

A third method is pharming, in which hackers attack a genuine company website, and redirect visitors/traffic to another, bogus, site, where sensitive information is then collected (Fatima, 2011). Pharming can be conducted either by changing the host's file on a customer's computer, or by exploitation of a vulnerability in the DNS server system (Delgado et al., 2008). Lastly, carding and skimming, is a practice whereby criminal entities collaborate to create markets for the purchasing, selling or exchanging of information records and databases (Altintas and Gursakal, 2007).

3.2.2.5 SECURITY ROLE IN ADOPTION OF INTERNET BANKING

Security addresses clients' fears of possible losses caused by the vulnerability of Internet banking, which can lead to concern and personal stress for customers. Internet transactions take place in a generally open environment, and information through the platform may be intercepted by other parties, which might compromise users' information security. As such, customers' expectations of perceived online security risks become a significant issue, which influences their attitude towards acceptance of Internet banking. Security issues relating to Internet technology, especially in Internet banking systems, have become more pre-eminent in recent times, due to the negative publicity caused by loss of confidentiality, integrity and privacy in networks operated by banks and their customers (Subsorn and Limwiriyakul, 2012).

The literature shows that Internet banking security is one of the most fundamental factors influencing banking customers' acceptance of the service. Some of these studies will be examined presently. Perceptions of Internet banking security, and customers' level of confidence in it, affect their decisions. For instance, Subsorn and Limwiriyakul

(2012) revealed that security is a pivotal factor in the acceptance of Internet banking service by existing and potential Australian customers. In the same vein, Dauda et al. (2007) concluded that adoption or non-acceptance of Internet banking are influenced by perceptions of electronic commerce security. Subsequent studies have also recognised the importance of security, and its influence on the adoption and acceptance of Internet banking. The differences between the studies pertain only to the degree of importance, and its role. Among these studies are:

(Omar et al., 2011; Sanayei and Jafari, 2011; Nasri, 2011; Ahmad and Al-Zubi, 2011; Chuang and Hu, 2011; Twum and Ahenkora, 2012; Mughal et al., 2012; Taleghani and Taban, 2012; Subsorn and Limwiriyakul, 2012; Moga et al., 2012; Jham et al., 2012; Hassanuddin et al., 2012; Nasri and Charfeddine, 2012 ; Nasir et al., 2015). The next section will discuss risk and Internet banking services.

3.2.3 RISKS AND INTERNET BANKING

3.2.3.1 INTRODUCTION

Internet banking is a unique type of business activity, given the ease and speed with which transactions can be concluded in the online environment. However, this can lead to an increase in the level of risk associated with financial and operational services, and also carries reputational risks (AL-Fahim, 2012). Moreover, several recent studies have confirmed that risk is a major obstacle confronting Internet services as a whole (Nasri, 2011). In the world of Internet banking, the main factors at play in risk perception are trust and ease. It is relatively quicker and easier to gain customers, but the issue is how to retain them in the presence of these risks (Mermod, 2011).

In the following section, we will be exploring some salient issues associated with risk in Internet banking.

3.2.3.2 DEFINTION OF RISK

Risk refers to the possibility that outcomes may vary from expectations in a potentially favourable or adverse direction. However, since customers are more enthusiastic to avoid adverse consequences, scholars have tended to craft their definitions in these terms. Perceived risk has been defined by Laroche et al. (2004, p.375), as “the degree to which the consumer feels the uncertainty and consequences associated with their actions”. Similarly, Maditinos (2007, p.8) argued that risk is "commonly thought of as felt uncertainty regarding possible negative consequences of using a product or service".

Azouzi (2009, p.4) pointed out that risk is “a combination of uncertainty plus seriousness of outcome involved.” Martins et al. (2014, p.8) defined perceived risk as “the potential for loss in the pursuit of a desired out-come of using an e-service”. Tsiakis (2012, p.1266) described it as “assessment of uncertainties or lack of awareness about the distribution of potential outcomes and the uncontrollability of results attainment". Meanwhile, Shafei and Mirani (2011, p.6688) saw perceived risk as "the potential or imposed financial risk which is caused by errors in Internet banking operations or misuse of bank accounts in Internet banking systems".

Hence, this study defines perceived risk *as the potential for chosen Internet banking services to result in an undesirable consumption outcome for all parties. Such potential consequences can impact on financial and administrative processes, and on service quality.*

3.2.3.3 ROLE OF RISK IN ADOPTING INTERNET BANKING

The studies reviewed above have shown that the use of Internet banking technologies is risky, due to several potential threats, such as electronic fraud and money loss. Several authors have reported findings on the influence of risk on the acceptance of Internet banking; Mohammed (2011) argued that risk is an important element of interactive technology use, and thus has a marked effect on customers' attitudes towards utilising technology. On the other hand, Featherman and Pavlou (2003) indicated that performance-based risk is the main determining factor in the adoption of electronic services; although they acknowledge perceived ease of use as a factor that helps in reducing these risk concerns.

In Tunisia, Azouzi (2009) found that several respondents still dealt with banks in the traditional way, due to transaction errors or hackers. Thus, these factors play a significant role in non-adoption of services. Simpson (2002) mentioned that another source of uncertainty relates to the fact that electronic businesses are still in the development phase. This is reflected as a further risk factor in acceptance of these services. Cho (2006) found that perceived risk was the second most important factor impacting on whether or not to accept online services, after perceived usefulness. Zhao et al. (2010) confirmed that there is an important relationship between trust and perceived risk, and that both have an influence on customers' intentions in adopting Internet banking. Lu et al. (2005) observed that risk indirectly affects peoples' intentions to use Internet banking, e.g. concerns over worms, viruses and hackers. Luo et al. (2010) also observed that risk perception has a role in the acceptance of innovative technology.

Yiu et al. (2007) concluded that risk has a positive relation to the adoption of this service. Ankit (2011) in his study showed that risk is one of the major factors that strongly affect the overall satisfaction of online consumers. Nasri (2011) mentioned that in Tunisia, security and perceived risk plays an important role in the acceptance of Internet banking services. Also Gan et al. (2006) stated that perceived risk factors, with other factors, influence consumers' choice of electronic banking.

Ashtiani and Iranmanesh (2012) noted that positive word of mouth has a negative influence on the perceived risk of using Internet banking services. The results presented by Zhao et al. (2008) indicated that there are significant risks in the Internet banking world, as have been identified; and that Chinese consumer culture plays an important role in this. Tsai and Yeh (2010) also argued that consumer intention to purchase was affected by perceived risk relating to information security and privacy on a website. Littler and Melanthiou (2006) demonstrated that although most of their sample members had concerns about security risks, nevertheless they continued to use Internet banking. Wong et al. (2009), however, showed that risk had a direct negative influence on customers' desire to use Internet banking.

However, contrary results have been reported in the USA. The results of a study conducted by Kolodinsky et al. (2004), found that risk does not play an important role in the acceptance of all Internet banking technologies. This was exemplified by their studies of areas such as automatic bill payment, phone banking, and home banking by American customers. Lichtenstein and Williamson (2006) highlighted an increase in Australian banking customers' acceptance of Internet banking risk. Further, Shafei and Mirani (2011); Joubert and Belle (2013); and Farzianpour et al. (2014) have all stated

that the perceived risk factor has a significant role to play in the adoption and acceptance of Internet banking services.

So far in the UK, Internet banking users are concerned about the security, privacy and financial risks associated with using the service. However, Nasir et al. (2015) carried out a study in the UK to explore the factors governing customers' Internet banking decisions, and concluded that social risk has no significant impact on these decisions. The next section will discuss types of Internet banking risks.

3.2.3.4 TYPES OF INTERNET BANKING RISKS

Vijesh (2011) stated that, along with the benefits of Internet banking, there are actions that carry risks for organisations and customers, but that these risks should be balanced against the advantages. The risks affecting Internet banking have engaged the attention of a number of researchers (Hong and Yi, 2012).

Eight types of risk have been covered in the literature reviews associated with Internet banking, as shown in Figure 6:

First, financial risk: the major perceived financial risk relates to possible losses due to transaction error, and weakness in the operating system, leading to fraud through unlawful hacking into the Internet banking system (Yoon and Steege, 2013). Second, operational risk: this takes the form of inaccurate processing of transactions, and unauthorised access, i.e. intrusion into systems and transactions because of the weakness of the security system. Thus, the risk of loss results from operational errors, problems in the system, the actions of people and systems, or from external events (Demirdogen et al., 2010).

Third, psychological risk: there is a risk that the client's self-perception may be adversely influenced by the acceptance of services; customers can also become concerned or stressed because of their purchasing attitude (Littler and Melanthiou, 2006; Gan et al., 2006). Fourth, strategic risk: these risks are related to how an organisation has addressed the various issues related to its business plan. Some senior managers and decision makers have a weak understanding of the strategic and technical aspects of Internet banking services, and many banks offer or expand services without an in-depth strategy study (Sarma and Singh, 2010).

Fifth, legal risk: Internet banking is a relatively new service, and the legal framework for it is still being developed. This creates a degree of ambiguity in the application of the law. Thus, banks should have a clear understanding of the law, in order to deal with all possible difficulties (Mermod, 2011). Sixth, reputational risk: this has a significant impact on the performance of the banks, due to potential negative publicity. This can be caused by poor services, security issues, limited availability, bugging software, poor response, or to customers looking for the simplest and safest Internet services. Thus, banks should develop mechanisms to address these issues.

Seventh, credit risk: financial institutions should evaluate their credit systems in line with the current challenges (Azouzi, 2009); Mermod (2011) defines a credit risk as a customer who fails to meet his/her financial responsibilities. Using Internet banking services, all types of customers can apply for credit, and banks may face some difficulties in verifying their identity. Finally, time risk: this refers to the possibility of time-wasting and delay in dealing with Internet banking transactions, and also the time taken for customers to learn how to use Internet banking services (Demirdogen et al., 2010). The main reason for adopting Internet service is to saving time; if the contrary

happens, this may lead customers to give up on the service (Lu et al., 2005). Therefore, the next section will explore further these issues of security, trust and perceived risk in online services, will attempt to discover if there is any relationship between these factors, and if there are other influencing factors.

Figure (6) Risks associated with Internet banking
The resource: (Zarei, 2011, p.135)

3.2 TRUST, RISK AND SECURITY IN ONLINE SERVICES

This research aims to consider the existence of risk, and to review the need for trust and security. It has been argued that we would not need trust or security if there was no risk (Yousafzai et al., 2003); therefore, due to the fact that risks exist, there is a need to

enhance security and to build trust. Since the emergence of the Internet, and its use as a means of providing services such as the completion of financial transactions and administration, buying, selling, and general commerce, there have emerged several accompanying risks. Therefore, there is a need to investigate whether a relationship exists between trust, risk and security. From the foregoing, several questions have been constructed:

- Is there any relationship between trust, risk and security?
- Do they affect each other?
- Are there any other factors influencing trust, security and perceived risk in online service generally, and in Internet banking services specifically?

In order to determine whether any relationship exists between the three factors, and the significance of any such relationship, this study will review the literature to attempt to discover answers to these questions.

- The research into the literature will start with the relationship between trust and security.

Several studies in the literature explore this relationship, such as Ally and Toleman (2005), whose study set out how entities attempt to build trust through the provision of efficient mechanisms for satisfying customers. The result of the study showed that security has an impact on customers' trust in electronic payment. Hussain et al. (2006) demonstrated that trust and security are complementary to each other in electronic banking. This finding has been confirmed in Spain by Flavian and Guinaliu (2006), who revealed that trust is influenced by security in online service. Chen and Barnes

(2007) observed that initial trust in online services was affected strongly by perceptions of security.

Further study of the influence of security on users' trust, and its impact on the decision to adopt Internet banking, was conducted in Iran and Malaysia. Sanayei and Noroozi (2009) found a positive correlation between security and trust in adopting Internet banking. In order to examine the paradigm of e-loyalty through the extent of its influence on satisfaction and trust, Kim et al. (2009) conducted a study on consumers who had experience in e-shopping in a south-western state of the USA. One of the important findings was that security has a significant effect on e-trust.

In Nigeria, Aderonke and Charles (2010) investigated the factors that influence acceptance and adoption of electronic banking, using TAM as a conceptual framework. A completed questionnaire was collected from 292 customers. The model measured the effect of self-efficacy, credibility, usefulness and ease of use on customer attitudes. It emerged that usefulness, and perceived ease of use, were not sufficient to define the consumers' attitudes towards using Internet banking in Nigeria. More importantly, in this aspect, the researchers arrived at the conclusion that there were worries among service users about security, and that this reflected negatively on trust.

McCole et al. (2010) carried out research aimed at examining the influence of three common trust considerations (vendor, Internet and third parties) on customers' attitudes and behaviours towards acceptance of online purchasing. They found that trust and security have a strong influence on customers' attitudes towards Internet purchasing. The findings of Kim et al. (2010) showed that security is positively related to perceived trust and e-payment systems acceptance in Korea. In Jordan, Alnsour and Alhyari (2011) highlighted that security has a significant influence on trust with regard to

Jordanian corporate customers. Moreover, Kim et al. (2011), in order to clarify factors that influence trust, conducted an Internet shopping study in South Korea, which demonstrated that security has a significant positive effect on trust in the e-commerce field. Namin et al. (2012) analysed data from 202 bank clients who use the e-payment services of Bank Melli in Iran. The results confirmed the relationship between security and e-trust. This relationship between trust and perceived security has also been confirmed by Wu et al. (2012); Taddei and Contena (2013); and Bahtiyar and Caglayan (2013).

Hanzaee and Alinejad (2012) found that perceived security was positively associated with consumers' perceived trust, and that consumers' trust also has an impact on e-payment system use. The study proposed a conceptual model for measuring the effects of perceived security and perceived trust on the use of e-payment systems. A completed questionnaire was collected from 210 online respondents in Iran. The findings further showed that perceived security in e-payment systems was positively associated with consumers' perceived trust in e-payment systems. Moga et al. (2012) conducted a survey aimed at addressing the problems of trust and security in Internet banking services in Romania. The reluctance of customers to access these services was linked to the level of security and trust in the technology used to safeguard their confidential information.

On the other hand, Yazdanifard et al. (2011) examined security and trust in e-commerce by focusing on how consumers are enabled to access electronic commerce without any constraints. The results indicated that a high level of security in online ordering is not sufficient to increase client trust.

The preceding review of studies concerning the relationship between trust and security in online services, reveals that the majority demonstrated a relationship between the two factors, both in online service generally, and Internet banking in particular. However, other studies suggested that ordering safety is not sufficient in itself to increase customers' trust.

- The next section will review the relationship between trust and perceived risk in the literature.

Ratnasingham (1999) analysed and discussed trust and risk in e-commerce from a management perspective. The study concluded that trust has a significant linkage with risk amongst traders in the e-commerce field. Kini and Choobineh (2000) presented a theoretical model of trust in www commerce systems, and confirmed this finding.

Ruyter et al. (2001) analysed the effect of reputation, relative advantage, and risk on quality of services, trust, and the behavioural attitudes of clients towards accepting e-services. They found in their study that lower risk levels promote customer trust in e-services. The results showed that perceived risk was combined with the reputation of the organisations in determining e-service acceptance. This is consistent with Gefen et al. (2003), who aimed to conceptualise the relation between trust and risk in e-commerce. They found that risk is more significant than trust. Trust reduces risk, but does not impact directly on customers' attitudes. Further, Heijden et al. (2003), in their study of online shopping in the Netherlands, asserted that trust has a direct negative influence on risk. Lim (2003) carried out a study in Queensland, Australia, in which participants confirmed the risk perceptions of consumers.

The relationship between trust and perceived risk can be summarised as follows:

Firstly, the perceived risk factor can be a moderating influence on the relationship between clients' trust, and their readiness to engage in online services. Secondly, it suggests that consumers' adoption of Internet banking is determined by a combination of trust and perceived risk, and leads to trusting behaviour by customers. Thirdly, it suggests that trust leads towards the perception of perceived risk in online services. In the fourth case, the relationship between perceived risk and trust can be seen as non-recursive. These four types of relations are summarised in Figure 7.

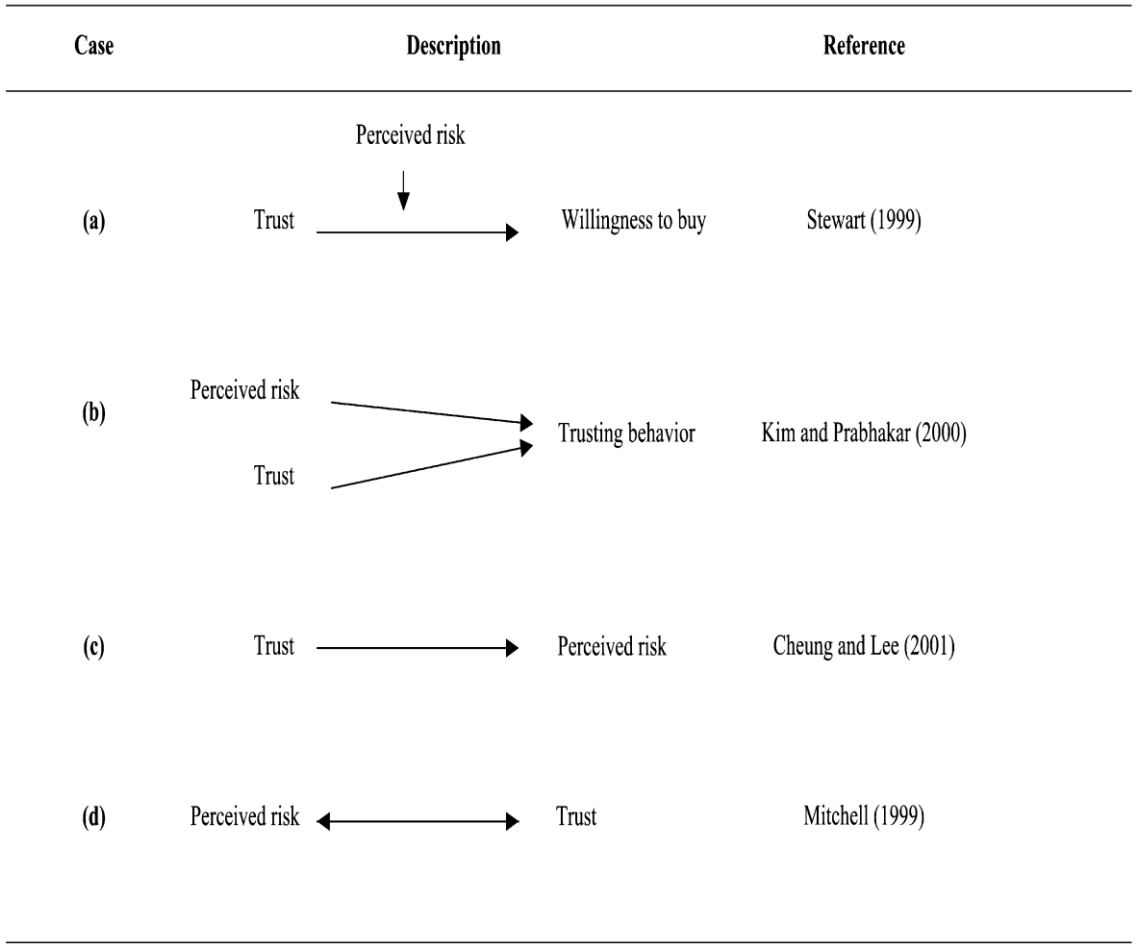


Figure (7) the relations between trust and perceived risk
Resource: (Lim, 2003, p.217)

Cho (2006) aimed to identify the significant factors impacting on Hong Kong customers' adoption of information-oriented online digital legal services. The findings observed that perceived risk reduces trust, and that trust in online services has a big influence on risk perception. An empirical study was conducted by Verhagen et al. (2006), aimed at exploring the relationship between risk and trust variables, and its effect on consumers' purchasing behaviour. The survey was conducted on 450 participants who used e-bay, and concluded that there are relationships between risk and trust, and that these factors have an effect on consumers' attitudes to the adoption of e-commerce. In addition, Lee et al. (2007) confirmed this result, with respect to the adoption of Internet banking services. Additionally, according to a study conducted on users and non-users of Internet banking services in Austrian banks, e-trust has an impact on risk perception, and on consumer attitudes to the adoption of services (Grabner-Krauter and Faullant, 2008).

Liu et al. (2008) provided an integrated model for analysing the influences of relationship stability and trust on relational risk. The hinged model of buyer-supplier relationships in the Chinese household appliances sector was examined through answers to 225 questionnaires. The research concluded that buyer trust in suppliers can reduce the relational risk. Wong et al. (2009) analysed risk as a moderator between Australian consumers' trust in Internet banking services, and their readiness to adopt these services. The research concluded that trust has an impact on the relationship between perceived risk, and the desire to use Internet banking.

Colesca (2009) investigated what factors could impact on citizens' trust in e-government services in Romania, and explored the possibility of a relationship between risk and trust in e-government. Aldas-Manzano et al. (2009) explored the factors which

impact on Internet banking use, focusing on the role of perceived risk and trust. The sample of the study included 511 Spanish service users. Findings showed that security and risk, along with other factors, have a direct effect on Internet banking acceptance. It was also suggested that trust is considered the main factor in reducing perceived risk. Zhao et al. (2010) showed that there is an important relationship between trust and risk, and that both play an important role in customers' decisions to adopt Internet service; this outcome was substantiated by Zimmer et al. (2010), and McCole et al. (2010), who highlighted that trust has both direct and indirect influences on the perceived risks of online service generally, and Internet banking in particular, and that there is a relationship between trust and perceived risk.

Zhu et al. (2010) aimed to analyse the effect of trust and risk factors on consumers' acceptance of online shopping. The study found that trust has a role in reducing online perceived risk for consumers in online shopping. In Malaysia, research by Ling et al. (2011) aimed to investigate the relationship between perceptions of technology, perceived risk and e-trust. About 250 questionnaires were distributed to undergraduate Information Technology students in Kuala Lumpur. The study found that the perceptions of technology and perceived risk have a significant influence on online trust.

Kesharwani and Bisht (2012) sought to extend a model of TAM, through investigating the influence of security and privacy on Internet banking adoption. The survey observed that risk has an important effect on the behavioural intentions of Internet banking acceptance, and that trust has an obvious influence on risk. Likewise, an important relationship between trust and perceived risk was identified, as was the influence of trust on risk perception.

In addition, Esmaili et al. (2011); Ling et al. (2011); Kesharwani and Bisht (2012); and Joubert and Belle (2013) all explored the interwoven relationships between trust and perceived risk, to explain how the two factors influence each other in online service.

In contrast, the results of a survey carried out by Belanger and Carter (2008) in the USA showed that increased risk perception did not decrease intention to use e-government services, and that risk perceptions did not affect online trust.

- The following section reviews the literature concerned with the relationship between security and risk.

The majority of consumers would adopt electronic services if they believed that privacy risks could be reduced; perceived security has an influence on perceived risk (Featherman et al., 2010). In line with this finding, Nepomuceno et al. (2014) found that security worries increase customers' perceptions of risk to the same degree, when they use Internet banking. Thus, it was concluded that security risks have an impact on Internet banking adoption. Waheed et al. (2013) explored the role of satisfaction, security and risk perception in customers' turnover intentions from traditional to Internet banking, and concluded that there is an important relationship between these factors.

- Broadly, there are several studies which consider these three factors, as detailed in the next section.

Yousafzai (2005) has been previously referenced. The study was conducted on Internet banking users of Halifax Bank of Scotland (HBOS). The results indicated that security has a significant effect on trust and risk. Gurung (2006) investigated the relationship of

trust and security to risk perception in the acceptance of online services. Data was collected from 273 undergraduate business students. Research confirmed that trust and security had an effect on risk perception. In addition, Pennanen et al. (2006) aimed to clarify the concepts of trust, risk, security and privacy, and the relation between these factors, from the consumer viewpoint in e-commerce. Findings suggested that there is a correlation between trust, risk and security. Moreover, in Thailand, Sattabusaya (2008) studied the factors which impact on Internet banking adoption. It was found that trust and risk have significant effects on actual behaviour, and that enhancing security plays a significant role in enhancing users' trust, and reducing risks.

Dolatabadi and Ebrahimi (2010) reported that, amongst the reasons for the reluctance of users to adopt online shopping, was lack of e-trust. This study investigated consumers' attitudes towards the Internet merchant, and the influence of factors such as privacy, security, and the risks and benefits of internet shopping in Iran. Their findings suggested that perceived risks and security have significant predictive value in the development of Iranian consumers' trust in e-shopping, and that security and reputation are also significant in this respect. In Malaysia, Shahibi and Fakeh (2011) showed that perceived risk and security, along with other issues, have a significant influence on online trust.

D'Alessandro et al. (2012) mentioned that security practices impact on perceived risk in online services. Furthermore, the study showed that perceived risk reduces trust in online services. Mohammadian and Ghanbar (2014) aimed to investigate the factors impacting on customers' trust in web brands in online service retailing. It was concluded that security, with other factors, has a positive influence on brand trust, although perceived risk does not have an important impact. Recently Cheng et al.

(2014) have concluded that trust has a negative influence on security and perceived risk; and moreover, that the perception of risk has a positive impact on customers' resistance to the use of Internet banking.

- In order to cover every aspect of this issue, the literatures have been reviewed in order to understand whether there are any other factors influencing trust, security and perceived risk towards online service generally, and Internet banking specifically.

For instance, perceived usefulness and perceived ease of use have an influence on security and trust, in explaining the acceptance behaviour of customers in adopting Internet banking (Alnsour and Alhyari, 2011). Ozguven (2011) found that website design had an influence on customer trust. Kim et al. (2011) found that customer satisfaction had a positive effect on trust, which, in turn, influenced customer loyalty. What is more, Wu et al. (2012) discovered a significant relationship between privacy concerns and trust in customer culture (Wu et al., 2012). Kesharwani and Bisht (2012, p.303) commented that "a well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk concerns regarding internet banking usage."

Banakdeh and Nia (2014) mentioned that to increase customer trust in their online services, banks should focus on convenience and ease of use. Moreover, Nasri and Zarai (2014) asserted that factors such as security, privacy, customers' self-efficacy and social influence, all have an effect on perceived ease of use.

By contrast, Al-Shawabkeh et al. (2015) suggested that confidentiality and availability have a significant effect on security and self-efficacy, whilst security and self-efficacy

in their turn have a moderate influence on attitudes towards confidentiality, and towards ease of usage. In addition, Sankari et al. (2015) noted that perceived ease of usage has a positive and important influence on customer trust.

In sum, with regard to the relationship between trust and security, it appears that most of the studies agreed that security impacted on customers' trust, and that the two factors had a significant and complementary relationship, in that security has a role in promoting trust, and overcoming customers' reluctance in this connection. On the other hand, some studies also showed there was a close link between trust and risk, in that levels of trust could be affected by perceived risk. On the other hand, several studies suggested that trust was a risk-reducing determinant.

Some studies combine all three factors - trust, risk and security - and examine the relationship between them. These surveys tend to confirm that risk and security play a significant role in building consumers' trust in online services. Further studies present the effects of trust and security on risk, conjoined with correlation evidence of the relationship between them. However, contrasting surveys express the relationship between trust and risk in terms of how it is influenced by security.

The present study has also reviewed the literature to determine if there are other factors affecting trust, security and risk. The studies reviewed focused mainly on the three major factors as they affect customer choice, whilst very few investigated other factors, and their possible influence on trust, security and perceived risk This could be due to the fact that Internet banking is a relatively new phenomenon; however, as Internet banking service becomes more widespread, it is important to understand all the factors which

influence trust, security and perceived risk, in order to understand why users abandon, or fail to adopt, Internet banking; or equally importantly, why they continue to use it.

As previous studies have revealed that security is an important factor in customers' decisions regarding Internet banking use, the following section will discuss this issue in more depth. In the UK, security has been identified as the most important factor underlying any decision to adopt Internet banking, as customers are specifically concerned about security risks, which might cause private data leaks, and potential losses of funds (Nasir et al., 2015).

The growth of Internet banking has raised many security issues, and resulted in increases in the cost of implementing advanced security schemes for both customers and banks. The most critical issue of service security is the protection of valuable data from illegal access by criminals. Hence, the banks must constantly improve and increase security. At the same time, however, they must manage budgets to make a profit; effective management should aim to achieve a balance between these two issues. Increased security may, of course, increase the determination of attackers to break into the bank's organisation; on the other hand a strong security system may deter some hackers.

As mentioned earlier, Internet related crimes, and the attendant security issues, are not only the concern of Internet banking, but affect all server-client Internet applications. Criminals and hackers use social phishing to gain uneducated customers, and to access their financial or personal data, usually by impersonating a trustworthy organisation. Thus, phishing attacks can cause a breakdown of trust between the banks and their customers.

Recent studies have shown that, in order to increase customer trust in their Internet banking systems, banks should focus on usefulness, ease of use, security, and the safety of transaction information. Security has a significant association with lack of trust in Internet banking services, and it has a significant influence on perceived risk as well (Banakdeh and Ganginia 2014). Furthermore, customers' perceived ease of use can be reinforced by security and social influence (Nasri and Zarai, 2014). Therefore, with regard to the security of Internet banking future research should concentrate on the extent to which other factors have an impact on the security of Internet banking services, and the customers' perceptions and intentions (Al-Shawabkeh et al., 2015). Furthermore, as Internet banking becomes more widespread, it is likely that there will be an increase in the occurrence of new security-related issues. In contrast, many customers who currently use Internet banking perceive it as having an acceptably low security risk, which does not prevent them from continuing their usage. The final point here is that the security policy of the banks should be clearly set out, regularly reviewed, and approved by higher management. It should define security objectives, and responsibilities of risk administration, with regard to risk valuation, control and mitigation.

> As a result of the above literature review, it is evident that these issues should be explored in relation to customers' behaviour, and their intentions regarding online services.

Further, it helps to know how these factors affect each other, and the influence that they have on customers' attitudes towards online services. Most studies of the relationship between trust, security and risk have been related to the adoption of online services, whereas other patterns of behaviour, such as non-adoption and abandonment of

services, have been neglected. More importantly, the majority of these studies were conducted on e-service generally, and in particular e-commerce, e-government, e-payment and e-shopping. Limited research has been undertaken to examine the relationship between these factors in the Internet banking field, especially regarding non-adoption and abandonment of services.

From all of the above it is clear that there is a gap in the literature relating to the Internet banking field in Britain. The present study aims to fill this gap, through study of the relationship between the three factors, their impact on each other, their impact on service to customers, and finally their influence on decisions regarding adoption, non-adoption, continuity, and abandonment of usage, of Internet banking.

However, there may be other factors, in addition to those being studied, that can impact on customers' intentions towards Internet banking, but have not been identified in this research. These include, but are not limited to; the effect of security and risk factors on customers' ease of use; the relationship between trust and word of mouth; social influences; and customers' self-efficacy. Therefore, research is required to identify other potential factors that may impact directly or indirectly on consumers' intentions towards Internet banking services in the UK.

The remainder of this literature review chapter focuses on the study of various theoretical models of importance, which identify the potential factors, that impact on consumers' non-adoption, abandonment, adoption and continued use of Internet banking.

3.3 THEORETICAL MODELS ON THE ACCEPTANCE OF TECHNOLOGY

3.3.1 INTRODUCTION

With the advent of the digital age, and its associated technological evolution, more and more businesses are embracing technological developments, in order to deliver value-added services to customers, and to optimise business performance and productivity. As part of these developments, the banking industries sector has developed new channels to provide services to customers, such as Internet banking (Reid and Levy, 2008).

The majority of studies on Internet banking have aimed to investigate the procedure of acceptance and adoption of the service (Yousafzai et al., 2005). Interestingly, in recent years, Internet banking has shown an increase in user adoption, albeit a marginal one (Hogarth and Anguelov, 2004).

Evidence suggests that users' behaviour shifts with their experience of the service. Thus, study of pre-adoption to post-adoption behaviours of Internet banking consumers becomes integral, in order to comprehend continued or ceased behaviour (Adapa, 2011). With this in mind, the goal of the current study is to analyse the role of trust, risk and security in customer behaviour in pre-adoption, as well post-adoption, of Internet banking, in terms of continuity or service abandonment.

Thus, research in this context will draw from current research, and possible theoretical paradigms, to provide a comprehensive understanding of user adoption or non-adoption of innovations, as well users' behaviour after adoption of services. The study will present four dominant theoretical frameworks of integrated technological models of consumer adoption, non-adoption and service abandonment, in order to explain those

trust, risk and security factors that might have an important influence on the usage patterns of customers in the banking industry in the UK.

The aim of this chapter is to lay the foundations for proposing and developing theoretical frameworks for Internet banking use, as a conceptual basis for an empirical investigation to be reported in later chapters. Therefore, this chapter examines a series of models that address technology acceptance, namely: the Theory of Reasoned Action (TRA), created by Ajzen and Fishbein in 1977, the Theory of Planned Behaviour (TPB), which is a development of TRA provided by Ajzen in 1991; and the Technology Acceptance Model (TAM), developed by Davis in 1989.

3.3.2 THE THEORY OF REASONED ACTION (TRA)

Fishbein developed this theory and Ajzen between 1975 and 1980, as a social psychology model derived from prior researches on attitude, which led to an investigation of attitudes and behaviour. This paradigm aims to forecast behavioural intention, extending to predictions of attitude and behaviour. The theory was developed in response to frustration with traditional behavioural research, much of which found only weak associations between attitude measures, and the performance of volitional behaviours (Prapavessis et al., 2015). Therefore, the paradigm aimed to examine and characterise behaviours through study of key factors, such as attitude, behaviour and beliefs.

The Theory of Reasoned Action (TRA) defines behavioural intentions as the immediate antecedents of a person's attitude or behaviour (Prapavessis et al., 2015). Yousafzai et al. (2010, p.1174) stated that the TRA supposes that: "most behaviours of social relevance are under volitional control and are thus predictable from intention". The

theory also suggests that a person's behavioural engagement is free from intent, and is underpinned by motivation and willingness. The Theory of Reasoned Action is a general model, which deals with the forecasting, rather than the results, of behaviours. Therefore, researchers using the TRA should initially identify the beliefs of participants regarding the attitudes and behaviours under research (Yousafzai et al., 2010) (see Figure 8 below).

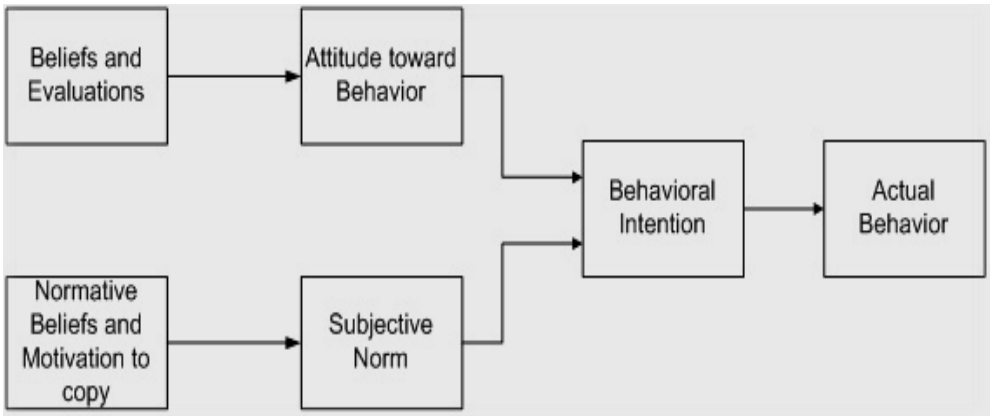


Figure (8) The Theory Of Reasoned Action (TRA).
Source: (Yousafzai et al., 2010, p.1174)

3.3.3 THE THEORY OF PLANNED BEHAVIOUR (TPB)

In psychology, the Theory of Planned Behaviour (TPB) concerns the relationship of beliefs to behaviour. The concept was developed by Ajzen between 1978-1991, in order to expand the TRA model introduced by Fishbein and Ajzen in 1975 (Swesi, 2011). It is considered to be one of the most influential theories in this field. The theory concerns behaviour, subjective norms, and control of individuals' behaviour (Nchise, 2012). These factors have a role in contributing to establishing intention, which leads to encouraging behaviour, as noted below in Figure 9.

The first version of the TPB contends that behaviour arises as a result of intention, and that intention is seen as the motivator of action. The second version considers the possibility that perceived behavioural control may have an indirect influence on behaviour. The Planned Behaviour school of thought considers that human behaviours are directed by three different kinds of belief, namely; behaviour, normative beliefs, and control (Swesi, 2011). Behavioural beliefs accordingly are positive or negative, according to the individual's attitude, whereas social pressures influence normative beliefs. Taking each of these factors into consideration, their combination may have an influence on behavioural intentions (Downs and Hausenblas, 2005).

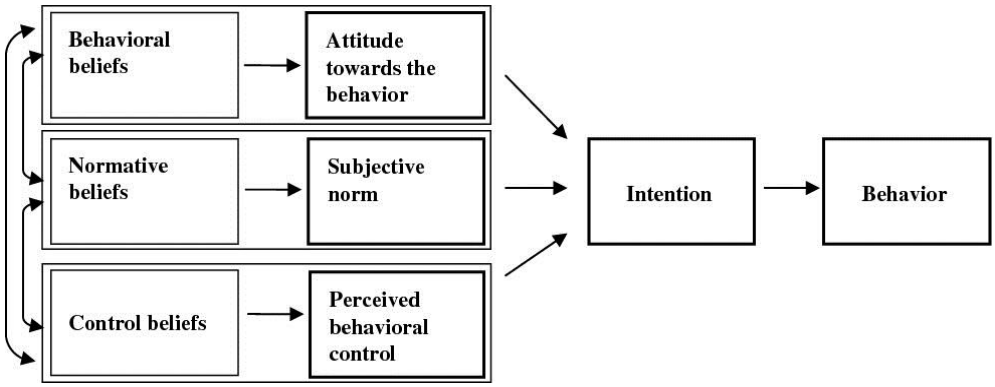


Figure (9) The Theory of Planned Behaviour (TPB).
Source: (Yousafzai et al., 2010, p.1175)

3.3.4 TECHNOLOGY ACCEPTANCE MODEL (TAM)

The Technology Acceptance Model (TAM) is an information systems (IS) theory conceived by Davis (1989), in order to demonstrate degrees of technological acceptance by users. The main objective of TAM is to offer a basis for identifying the influence of external factors on the behaviour of individuals. This model argues that, by investigating the influence of usefulness, and ease of use, on behavioural intentions and

attitudes, a prediction can be made as to whether a given technology will be adopted (Yulihasri et al., 2011).

The model proposes that when a new technology is offered, there are many factors influencing customers (users) to make decisions about how and when they will use it; this is referred to as Perceived Usefulness (PU), which was defined by Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance". Perceived Ease of Use (PEOU) was defined by Davis as “the degree to which a person believes that using a particular system would be free of effort” (Davis, 1989, p.320).

The Technology Acceptance Model (TAM) was adapted in 1989 by Davis, from the Theory of Reasoned Action (TRA), which was developed and introduced by Ajzen and Fishbein (1980). TAM is widely accepted by investigators in the information technology field as a theoretical model based on good predictive strength. As mentioned above, the model is used extensively to predict users' acceptance of corporate information technology rationales. TAM models are shown below in Figure 10. Previous research has, however, suggested that Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) are influential emotional beliefs, which determine IT user acceptance (Lin et al., 2011). Moreover, the effect of external factors on usage behaviour within the original TAM has not been well researched (Dulcic et al., 2012).

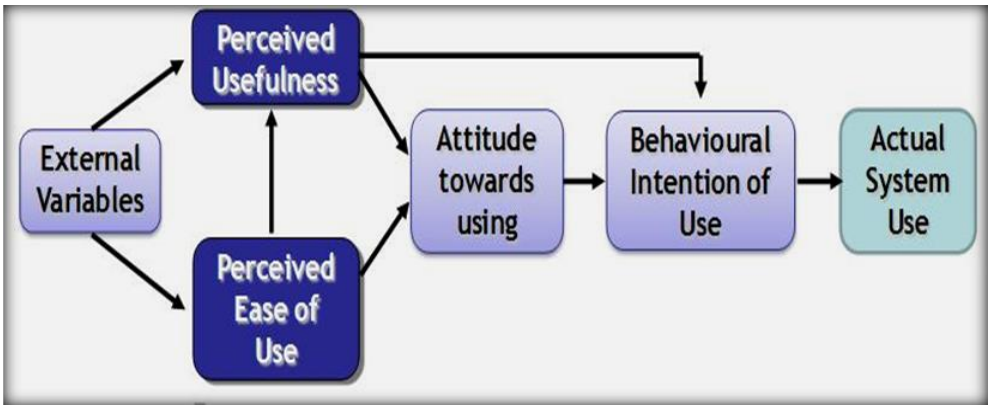


Figure (10) Technology Acceptance Model (TAM).
Source: (Park, 2009, p.151)

3.3.4.1 EXTENSION OF TAM (TAM2)

Fred Davis first proposed the TAM in 1985, since when there have been continuous expansions and studies of the model, most recently by Yousafzai et al. (2005), as shown in Figure 11. Critical re-workings include that of Venkatesh and Davis (2000), who extended TAM to TAM2, identifying in the process numerous determinants that influenced perceived usefulness, including subjective norm, job weight, image, result exaltedness, result demonstrability, and ease of use.

TAM2 proposes that the subjective norm and image will impact on perceived usefulness. In addition, TAM2 posits a direct impact of perceived usefulness on perceived ease of use. Furthermore, it emphasises the mediating influences of job relevance and result exaltedness on perceived usefulness (Venkatesh and Bala, 2008).

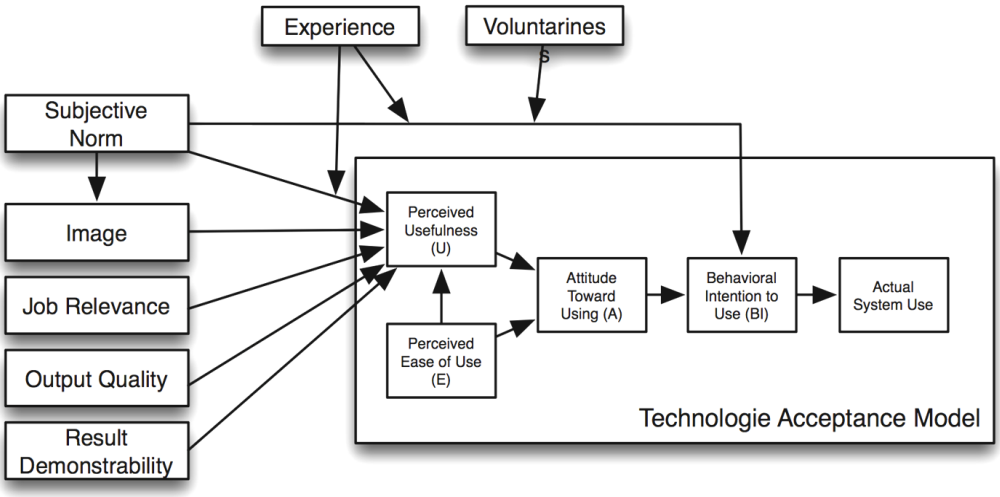


Figure (11) Technology Acceptance Model 2 (TAM2)
Source: (Venkatesh and Davis, 2000, p.188)

3.3.4.2 EXTENSION OF TAM2 (TAM3)

A second important extension of the TAM model was developed by Venkatesh and Bala in 2008. This model resulted from a combination of the TAM2 with the perceived ease of use model, called TAM3, as illustrated in Figure 12. Venkatesh highlighted two main clusters of antecedents for perceived ease of use, referred to as anchors and amendments. The former term refers to a generalised consideration of computers and computer usage, whereas the latter is based on a consideration of direct experience of system use (Chuttur, 2009).

TAM3 proposes that the determinants of perceived usefulness and perceived ease of use will not influence each other. Moreover, it suggests two theoretical relational operations between perceived usefulness and social influence, and between cognitive and instrumental processes. These processes are linked to several of the factors affecting perceived usefulness, namely: work relevance, output quality, subjective norm and

image. Ease of use is linked to individuals' self-efficacy and the procedural knowledge that derives from experience and skills. TAM3 implies that perceived ease of use determinants do not impact on perceived usefulness (Venkatesh and Bala, 2008).

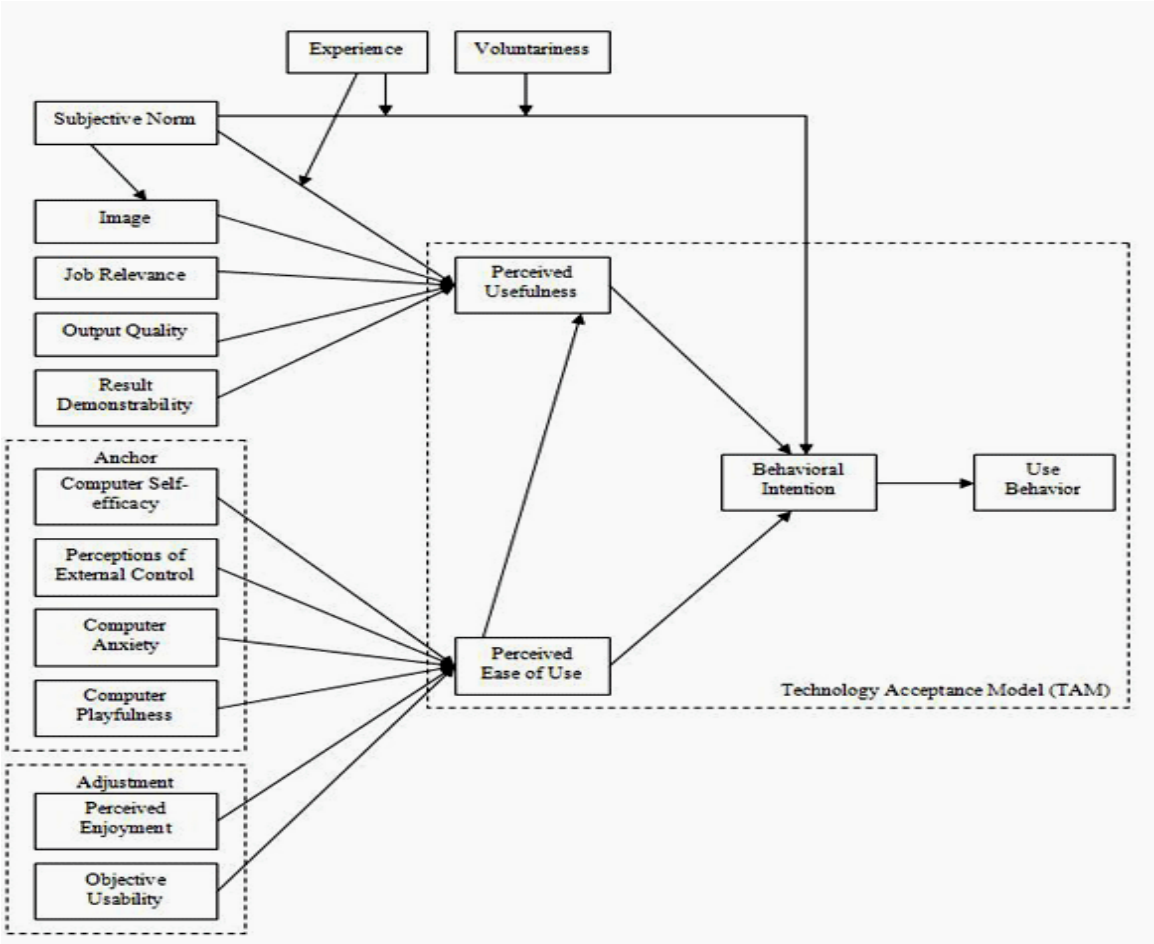


Figure (12): Technology acceptance model 3 (TAM3).
Source: (Venkatesh and Bala, 2008, p.280)

3.3.5 ASSESSMENT OF THE THEORIES

This section has discussed customers' behaviour in the case of Internet banking services, and has investigated the essential theoretical models that have been widely used in technology acceptance studies. In particular, it has reviewed three theoretical models in order to develop a basis for the theoretical models for Internet banking adoption and acceptance, which are proposed in the current study.

In this section, models have been reviewed, and some weaknesses identified, in particular with regard to the TAM. Firstly, this model highlights only the elements of intention in ease of use and usefulness, and does not pay attention to how these beliefs are developed. Secondly, the TAM does not have any social variables. Thirdly, TAM's asserts that usefulness and ease of use constructs, fully mediate the effect of outside variables on behaviour. Finally, other important factors, such as trust, perceived risk and security, have been neglected in all three-technology acceptance models.

Thus, previous researchers have agreed that these models (TRA, TPB and TAM) "did not take into account the post-adoption stage of the consumer in the internet banking usage, also all intention models seems neglect group, social and cultural aspects of decision making process" (Choudhry et al., 2013, p.23). In this study the authors criticise these models largely because they rely on simplified concepts of human emotion.

In fact, these paradigms commonly rely on a purely deterministic concept, and more often self-organisation operations are not taken into account. In addition, the above-mentioned models aim to assess clients' post-adoption decisions. Nevertheless, these theories depend on consumers' concepts of creative properties as a significant predictor of behavioural intention.

At the present time many studies still confirm that these theories are incomplete and insufficient, and other authors have suggested that integration of the theories might offer a better understanding and description of consumer evaluation of the post-adoption decision making process, than can be provided by each theory in isolation. Concerns associated with Internet banking services in particular, and with technological advances in general, often lead customers to either minimise or abandon altogether their usual

behaviour towards Internet banking. Moreover, such concerns can lead to non-adoption of the service. Likewise, usage or non-usage of the service depends upon an individual's capacity to engage with this service delivery channel. With reference to the above mentioned discussion, trust, security and perceived risk dimensions are identified as critical in influencing consumers' decision to use, continue to use, abandon or simply non-use Internet banking.

To a considerable degree, patterns of post-adoption (continued use and abandonment of use) and pre-adoption (adoption or acceptance) of Internet banking are related to technology updating mechanisms. Consequently, existing models, whilst indicative of usage attitudes toward Internet banking, are not complete in terms of all of the factors that consumers refer to in their decision making.

Consequently, this section reviewed and compared important theoretical models used in technology acceptance research, in order to gain a complete picture of the phenomenon through continuous reviewing of the literatures. In addition, it is proposed to develop a strong theoretical base for the Internet banking services models proposed in the present study.

To sum up, the three models are considered to be the cornerstone of studies in this field. In this study in particular, these models, especially TAM, have helped the researcher in the construction of study models, and have provided a basic idea of how a theoretical model should work. However, as mentioned previously, the model has neglected the post-adoption stage, whereas this study aims to include both post-adoption and pre-adoption stages of Internet banking. Furthermore, the TAM model has focused on usefulness and ease of use in determining customers' behaviour, whilst neglecting other factors, such as trust, security and perceived risk; all of which are of interest to this

study, due to their influence on all aspects of customers' behaviour. Therefore, the theoretical models developed for this study are constructed around three factors: trust, security and perceived risk. Next section will discuss research issues.

3.4 RESEARCH ISSUES

Research community has identified the following issues concerning:

1- The relationship between trust, security and risk and:

A. Customers' decisions or intentions regarding the non-adoption of Internet banking?

C. Customers' decisions and intentions regarding the abandonment (giving up) of Internet banking?

D. Customers' decision and intentions regarding the adoption of Internet banking?

E. Customers' decisions or intentions regarding the continuity of use of Internet banking?

2. Relationship between perceived risks related to Internet banking and customers' levels of trust?
3. Relationship between the security of Internet banking and customers' levels of trust?
4. Relationship between the security of Internet banking and the perceived risk related to Internet banking?

The research issues identified in the literature cover mostly adoption and non-adoption; however there is a gap in the available research concerning abandonment and continuity of usage. In addition, there is a dearth of studies relating to non-adoption in the UK. This is therefore the focus of this research.

3.5 CHAPTER SUMMARY

This chapter has reviewed a diverse range of findings on the subject of Internet banking, focusing on the three elements of trust, security and risk. The study has also discussed these issues in terms of online service in general, looking at the relationship between them, as well as assessing possible influence from other factors.

It appears that these factors have an obvious influence on the adoption of online services in general, and Internet banking in particular, and this aspect has been studied exhaustively. Although there are a limited number of studies on the influence of these factors on non-adoption of Internet banking, those reviewed provided evidence that such influence exists. Whilst investigation of the impact of these factors on Internet banking abandonment has been neglected, this study, one of the first to examine this phenomenon, has identified a relation between these factors and the abandonment of Internet banking. There was clear relationship identified between the way these factors influence each other in the Internet banking services field. However, this study recommends that the effect of other factors on trust, security and risk, and their influence on customers' behaviour towards Internet banking services in the UK, should be further investigated.

Theoretical models of technology acceptance, and consumers' decision-making processes in the context of consumer post-adoption and pre-adoption behaviour, were reviewed, and finally an assessment of the various theories was presented. Thus, this chapter aimed to lay the foundations for proposing and developing theoretical frameworks for Internet banking use, as a conceptual basis for an empirical investigation, to be reported in later chapters. The chapter reviewed and discussed the

following models of technology acceptance: the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB), and the Technology Acceptance Model (TAM). This was done in order to build and develop the theoretical models for internet banking services proposed in the present study. Chapter Four sets out the theoretical framework for this study, and will formulate research hypotheses.

CHAPTER 4: THE THEORETICAL FRAMEWORKS AND RESEARCH HYPOTHESES

4.1 INTRODUCTION

This chapter aims to discuss the theoretical frameworks, which have been developed regarding the research phenomenon, in order to establish the common ground between them in the context of the full study and its potential for wider commercial use.

These models investigate customers' intentions in patterns of service adoption, non-adoption, and abandonment of Internet banking by postulating three direct determinants: perceived trust, perceived risk and perceived security. In order to validate these models, a hypothesis was subsequently developed. In addition, this chapter will provide a more detailed discussion of the concepts of study terminologies such as trust, security and perceived risk in the field of Internet banking. Firstly, there will be a detailed explanation of the design of the study questionnaire and the process of validating the items, which will be followed by a description of the design of the sampling process.

4.2 THE APPROACH

4.2.1 RESEARCH QUESTIONS/AIMS OF THIS STUDY

- What constitutes significant degrees of trust, risk and security when considering customers' decision-making process in relation to the sustainability of Internet banking engagement (continuity of use)?

- What is the safety combination of trust, security and perceived risk, which would determine desired levels of usage and degrees of satisfaction with Internet banking services?

4.2.2 THE FRAMEWORK

After formulating the problem, the study identified some objectives, which must be accurately described in order to address these issues:

- Assessment of current customer behaviour and intentions to join Internet banking services. Thus, the research will attempt to explore the influence of trust, risk and security on non-adoption, adoption and ceased Internet banking behaviours. This will give an insight into how to control the behaviour of users in the post-adoption period, in terms of branch-Internet adoption migration, engagement sustainability and abandonment behaviours. In short, the study intends to develop three theoretical frameworks for studying customers' behavioural models, namely non-adoption, adoption, and abandonment of Internet banking.
- Design a model (theoretical model) of trust, risks and security for Internet banking to reach the safety area (Internet banking safety area model).
- Unearth the correlations between trust, security and risk which influence the adoption of Internet banking in the UK.

In order to answer these questions, the study has developed conceptual frameworks based on theoretical models in the field of technology acceptance. The conceptual models, which have been developed, encompass trust, security and perceived risk factors, and their influence on the non-adoption, adoption, continued use and abandonment of Internet banking.

4.2.3 DEVELOPED THEORETICAL FRAMEWORKS

In the following section, various conceptual frameworks will be constructed, with the aim of furthering knowledge and contributing to research in the domain of Internet banking. Accordingly, four conceptual frameworks will be posited: the Internet banking non-adoption model, the Internet banking abandonment model, the adoption model, and predictive models to promoted and enhance Internet banking behaviour. These models will be described in detail below.

4.2.3.1 INTERNET BANKING NON-ADOPTION MODEL

A number of theoretical models have been developed underlying technological acceptance or refusal. Nevertheless, the need to recognise and study technological adoption or rejection is a dominant theme in the work of many researchers (Venkatesh et al., 2012).

A minority of researchers believe that technological acceptance theorems should be favoured over alternative theorem models, due to their simplicity (Swesi, 2011). Henceforth, the study will built upon the aforementioned points about technological acceptance models, in addition to attempting to fill a gap in the literature on the non-adoption of Internet banking. As depicted in Figure 13, the aims of the model are to investigate the role of trust, security and risk among resident non-users' attitudes and intentions regarding technological non-adoption and non-acceptance within the field of Internet banking. The model is founded on three independent variables: trust, security, and perceived risk, with the non-adoption of Internet banking being a dependent variable.

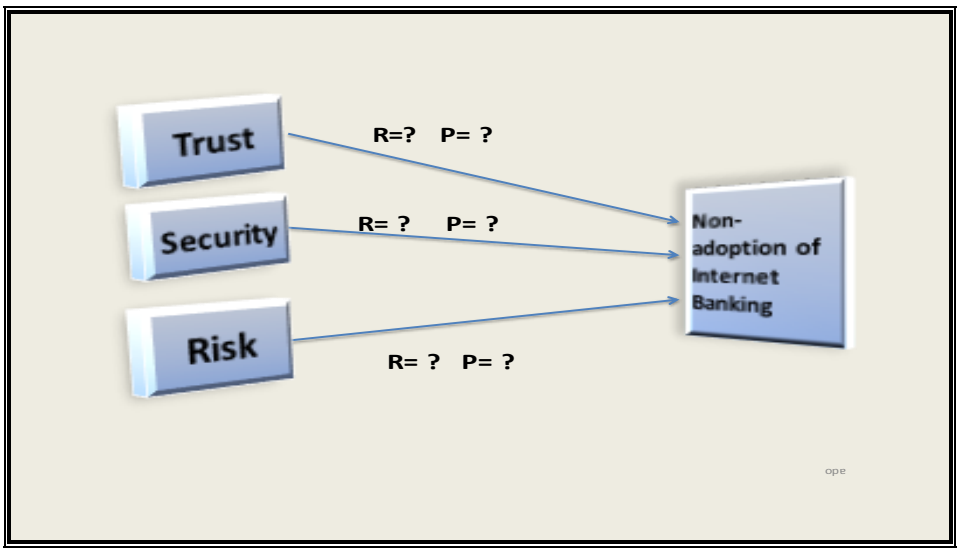


Figure (13): Research framework of customers' non-adoption of Internet banking

4.2.3.2 INTERNET BANKING ABANDONMENT MODEL

As previously noted in the introductory chapter, Yousafzai and Yani-de-Soriano (2012) claim that approximately two million Internet banking users in Britain are characterised as being inactive, or they have given up on the services. Consequently, this study needs to investigate the existence of this phenomenon in order to ascertain the impact that trust, security and risk have on the abandonment rate of Internet banking.

Therefore, this model aims to examine the role that trust, security and risk weighting play in the attitudes and intentions of Internet banking users who are resident in the UK regarding the abandonment of Internet banking services.

Theorised conceptual frameworks are used by technology acceptance models with evidence of widening gaps apparent in the literature. Thus, the model shown in Figure 14 includes three independent variables: trust, security and perceived risk.

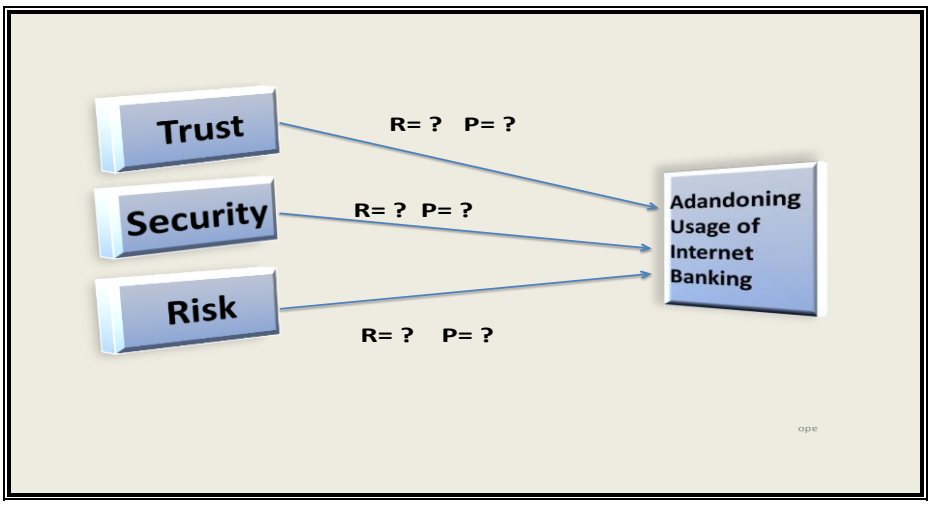


Figure (14): Research framework of customers' abandoning of Internet banking

4.2.3.3 INTERNET BANKING ADOPTION AND PREDICTION MODEL FOR CONTINUED BEHAVIOUR

The final frameworks in this study relate to customers' behaviours and intentions within the adoption- to post-adoption of Internet banking periods, with specific focus on abandonment user behaviours in Internet banking. The proposed model seeks to unearth the rationale for customers' behaviours and intentions in post-adoption in Internet banking specific to sustainability.

In the preface to his 2011 study, which aimed to investigate the influential factors responsible for sustained Internet banking behaviour in Australia, Adapa exposed the need for future research in this area, focusing past users, dormant users and non-users of Internet banking. Furthermore, the existing literature on Internet banking research reviews Internet banking from the consumer's pre-adoption perspective, whereas only a few studies have focused on customers' post-adoption behaviour. Taking all the points mentioned above into consideration, the present model is a theoretical model for

technology acceptance. It aims to examine consumers' adoption and continued usage of Internet banking, and concentrates on consumers' post-adoption behaviour by examining and exploring the influence of trust, security and risk on consumers' adoption and continued usage of Internet banking in Leicester.

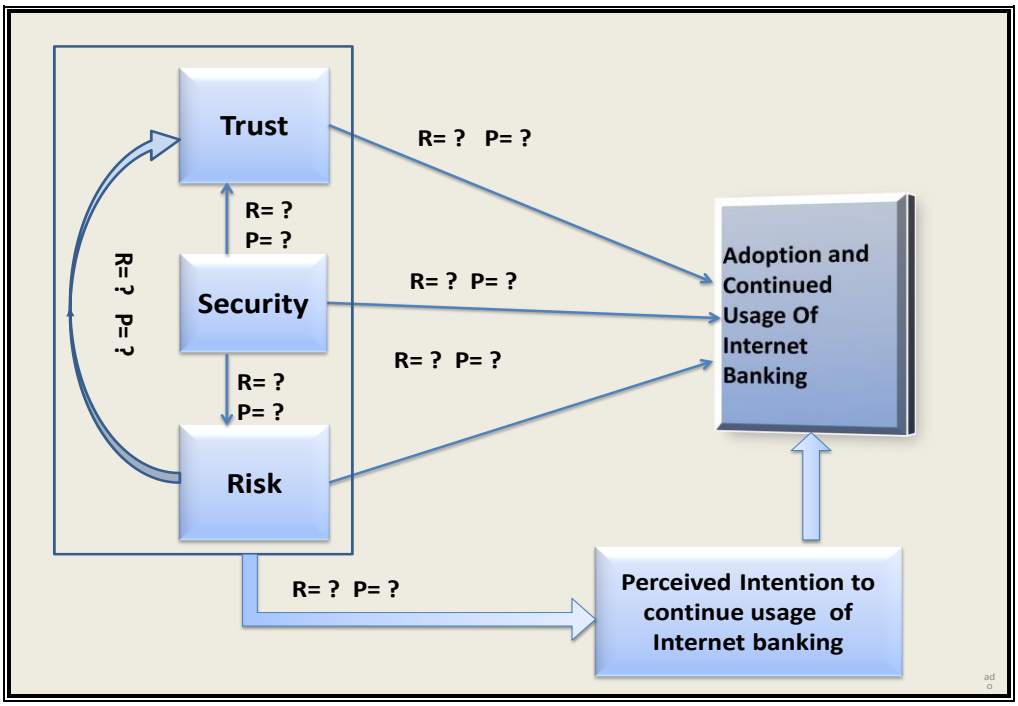


Figure (15): Model Adopting and Predicting the Continued Use of Internet Banking

The model includes three independent variables - trust, security and perceived risk - with the adoption and projected continued use of Internet banking deemed to be the dependent variable. The conceptual framework as depicted in Figure 15 above is constructed from predictive intent and consists of three steps. The first step was to study the influence of the three factors (i.e. trust, security and risk) respectively on the adoption and continued use of Internet banking.

The second step is associated with the inter-relationship between trust, security and risk, and the impacts, which they have on customers' behaviour. Finally, the third step

determines the relationship between the combination of trust, security and risk, and customers' perceived intentions towards continued use of Internet banking.

4.2.3.4 INTERNET BANKING SAFETY AREA

This section will establish the safety area model as a means of counterbalancing the limitations of previous models in this field.

- **Service Safety Cycle**

The research study defined the safety area as a region, which maximises the productivity of Internet banking services, in order to achieve the best and most favourable results along the defined matrix to forge user confidence. As demonstrated in Figure 16, this will drive performance and efficiency. Moreover, if the users are within the safety area, they will consider that it is safe enough for them to continue using the service, whereas users who feel that they are outside the safety area will abandon the use of Internet banking. In short, the safety area model aims to translate the aspirations and views of users about security, risks and trust in Internet banking services according to percentages to determine a safety zone.

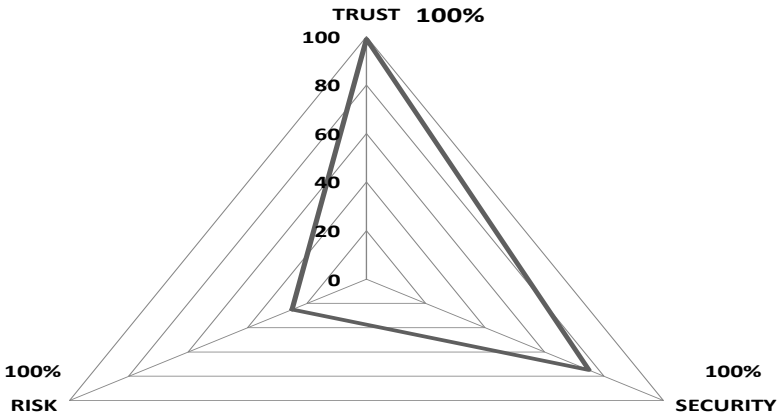


Figure (16): The Service Safety Area

More specifically, the cycled paradigm aims to discover the safe haven of Internet banking services along a three-dimensional factored net between trust, security and risk, with values attributed on a percentage scale for each respective factored state as illustrated in diagram 17 and in the exhaustive list below:

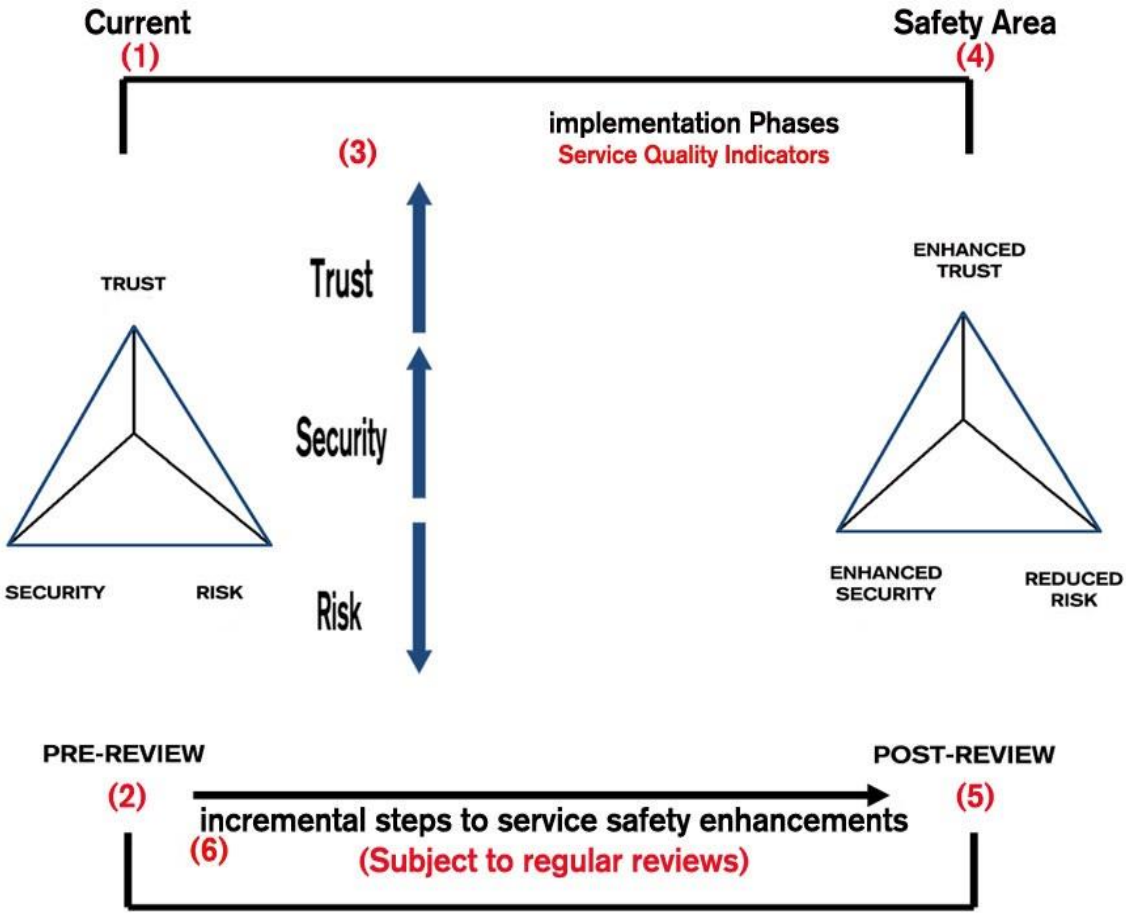


Figure (17): Safety Area Cycle

- **Current/pre-review**

In the diagrams mentioned above, items 1 and 2 considered the fundamental basis in the model toward enhance confidence. Therefore, these items enable the identification of a respective financial institution's current service position and its limitations in terms of perceived safety, as reported in the post review by items 4 and 5.

- **Service quality indicators**

These are tiered drivers of varied natures that include, but are not limited to, troubleshooting, instilling user service simplicity, and other drivers, which are perceived as paramount in user service welfare accomplishment; these are marked as item 3 in Figure 17 above. Factors are phased in a systematic manner (with their corresponding effect on safety/post review for the relevant stage) as a measure of quality control and strategic efficiency.

- **Safety/Post-review**

This will review the successful espousal of service-quality drivers, and demonstrate the change from the current position to a state of enhanced user service (annotations 5), which is reflected by an increased % valid in the line of the respective campaign wave. The essence of safety/post-review serves as a vital partner column to the current/preview, which has already taken place.

- **Incremental steps of service enhancement**

The success of the chain (iteration 6) hinges on systems to collect values from continuous users, such as feedback and renewal exercising.

This data is necessary for allowing banks to make strategic decisions, which enhance the value of the service that they offer to respective user populations, thereby aiding and developing prosperous long-term customer ties.

Overall, continuously studying data with scientific precision will result in sustainable and engaging commercial service strategies, which will lead to engaging more users to adopt the long-term use of the service, giving constancy to financial entities and allowing them to control and govern service adoption behaviour. The next section will discuss concept of trust, security and perceived risk in this study.

4.2.4 TERMINOLOGY-DEFINITION OF CONCEPTS

This research assesses the behaviour patterns of existing bank customers towards Internet banking service in the UK from two sides: patterns of post-adoption (continued use and abandonment of use) and patterns of pre-adoption (adoption or acceptance). In order to investigate those patterns and fill the gap in the existing literature on this subject, this study developed theoretical models, which focus on the three factors of trust, security and perceived risk. It does so by exploring the effect of trust, perceived risk, and security, on customers' behaviour and intentions toward Internet banking services. Therefore, it is imperative that this section gives a brief overview of the concepts of trust, security and perceived risk in this research.

- **Security**

According to several studies, security is a significant factor in customers' reluctance to use Internet banking. The majority of the clients claimed that that security is an important reason why they do not use this service (Popola, 2013). Therefore, a review of some of the respondents' answers will follow, which will examine the responses given by three categories of service users (non-users, abandoners and users) to the open question on security in the questionnaire.

One of respondents who was a non-user of Internet banking stated, “I do not have confidence in Internet banking because it is not safe and I am also afraid of losing my private financial data, which could lead to my money being stolen.”

One of respondents, who has abandoned the use of Internet banking mentioned “I think conducting transactions online is not protected and I cannot trust this service due to e-fraud: this why I have left this service.” Furthermore, one of the respondents who was a user of Internet banking said “I use Internet banking to make transactions and payments, however I still do not have full trust in the security of this service”. From all the answers above, it would appear that abandoners and non-users did not trust Internet banking for reasons which related to security issues. For them, security is a degree of feeling concerned about certain issues, such as the possibility of hackers or other parties accessing their accounts in order to transfer or steal funds. They are also worried about their sensitive personal information. In general, customers feel afraid, and e-fraud reduces their level of trust in the security of Internet banking.

In short, the concept of security in Internet banking services can be defined as the degree to which people believe in the security of Internet banking service. In addition, it is considered to be a threat which creates the circumstances that could potentially lead to the destruction or modification of data, and e-fraud to data or accounts of customers and banks in general. This sense of security, or lack thereof, influences the customers and encourages them towards the non-acceptance, abandonment after adoption, or adoption of the Internet banking service.

In summary, this study sees the concept of security in the Internet banking service as the combination of privacy, the protection offered by precautionary and protective measures

against the unauthorized disclosure of information, the prevention of unauthorized amendments or deletions of information and transfers of funds, and the prevention of the unauthorized withholding of customers' information and information relating to their bank accounts.

- **Trust**

Trust is the result of psychological tendencies that are outside the immediate control of organisations or parties and it is related to the psychological and sociological perspectives of customers (Adapa, 2011). Customers are just beginning to obtain more meaningful information about the benefits and effects of adopting Internet banking services. As a result, customers start to build a general propensity to trust or not to trust the service, and internal and external forces on the customer will also have an impact on their trust in the Internet banking service.

Similarly, some examples of the answers given by respondents in all three categories to the open question in the questionnaire concerning trust have been reviewed to evaluate the concept of confidence among customers. One non-user said "I will trust the Internet banking service if the bank guarantees that I will get my money back in the event of any e-fraud, however, right now, such a policy does not exist, which is why I do not trust the bank itself." A respondent who has abandoned the service explains, "I cannot continue to use Internet banking without a policy that assures that the bank would pay back in case of e-fraud." A respondent who was a user of Internet banking said "I use Internet banking; a policy to assure me that my money is safe would increase my trust in Internet banking."

It would appear that the definition of the concept of trust is often ambiguous and is different from one environment to another. Trust is vital and, as such, it plays a significant role in the success of the Internet banking service. Thus, the customers quoted above lack trust in Internet banking because the banks do not have any policies to protect customers if they lose their funds. They emphasized the fact that they would adopt Internet banking if the bank was responsible for any loss of customers' funds. Moreover, customers believed in the reliability of the bank and have assumed that the bank is responsible for any risk relating to their account or their online transactions. Likewise, consumer trust might be described as a function of the grade of risk involved in the situation it is basically only necessary in ambiguous cases (Kesharwani and Bisht, 2012).

In this study, the concept of trust can be summarised as a behavioural intention of customers, or their willingness to depend on the Internet banking and to believe that the bank will meet their expectations to fulfil its obligations and meet their banking needs with efficiency and effectiveness at the level of system performance. Furthermore, the bank has a responsibility to provide protection against risks. In short, customers believe that the bank's ability to provide reliable banking services will be a potential driving force for the development of Internet banking services, as this ability determines the consumers' acceptance of this service and their willingness to engage in it.

- **Risk**

It is evident that clients always tend to weigh up the possible advantages and benefits offered by Internet banking service against the potential risks. Risk has a vital role in the consumer decision-making procedure; perceived risk would often also result in their

resistance to adopt this service. Therefore, investigating the perceived risk component from a consumer's perspective helps to understand their attitudes and offers significant indicators on their acceptance or non-acceptance of the service. In order to understand how customers view the concept of risk, some of their answers to questions about risk in the questionnaire have been reviewed below.

This non-user respondent said "I can't use Internet banking because of e-fraud, but I will use it if the bank is accountable for the loss in case my money is lost." A respondent in the category of abandoners stated "I cannot continue to use this service while e-fraud still takes place. If the bank took responsibility for any risks that could occur, then I will return to use the service." Finally, a user of Internet banking explained that, I use the service, but so far, the bank does not afford any money-back guarantee. Thus, Internet banking is risky. It would be better if the bank provided policies and strategies that protect clients' savings in cases of hacking or theft. If such a policy existed, I would have complete trust in Internet banking and use it for all my banking transactions without feeling that I was at risk.

Seemingly, the concept of risk for the majority of customers is about the perceived probability of loss of funds. In addition, existing studies emphasise the importance of perceived risk in influencing online consumer behaviour towards the Internet banking service. This study has already mentioned several categories of risk associated with the Internet banking service, such as financial, performance, time and security risks. Therefore, the perception of these risks was expected to have a critical effect on customers' decisions to use the service. Based on consumers' perceptions about the Internet banking context, the most significant types of risk are likely to be financial,

security and confidentiality risks. These risks are associated with possible losses, which could be incurred due to defects in the operating, process, whereby unlawful outside access could lead to misappropriation of money and loss of individual data.

Hence, it is expected that consumers' perceptions towards risk are important in influencing their adoption and non-adoption of Internet banking. In addition, consumers' perceptions that the Internet banking service is a secure way to conduct their banking transactions encourage them to adopt this service and use it continuously. Therefore, the role of risk in the present research is of interest in light of consumers' pre-adoption and post-adoption behaviour.

The concept of perceived risk in this study can be defined as the consumers' perceptions of the uncertainty and the potential for loss in the pursuit of a desired outcome of using electronic banking services. The most significant potential adverse consequence is the misappropriation of funds and loss of sensitive personal data due to unlawful outside access. In next section the study will develop and formulate the hypotheses of study.

4.2.5 HYPOTHESES FORMULATION

Trust, security and risk factors will be hypothesised to explore the measured significance in terms of their impact on customers' perceived intentions toward non-adoption, adoption, usage continuity and abandonment of Internet banking. Thus, in order to validate these models, the study developed the hypotheses which are presented below.

H1a: Trust affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H1b: Security affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H1c: Risk affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H2a: Trust affects customers' decisions/intentions regarding the abandoning of Internet banking.

H2b: Security affects customers' decisions/intentions regarding the abandoning of Internet banking.

H2c: Risk affects customers' decisions/intentions regarding the abandoning of Internet banking.

H3a: Trust affects customers' decisions/intentions regarding the adoption of Internet banking.

H3b: Security affects customers' decisions/intentions regarding the adoption of Internet banking.

H3c: Risk affects customers' decisions/intentions regarding the adoption of Internet banking.

H3d: Trust, security and perceived risk affect customers' decisions/intentions regarding the continued use of Internet banking.

H4a: The perceived risk of Internet banking will reduce trust.

H4b: The security of Internet banking will enhance trust.

H4c: The security of Internet banking will reduce perceived risk.

H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services. The next section will discuss the methodology of this research.

4.3 RESEARCH METHODOLOGY

4.3.1 RESEARCH PURPOSE

All studies are based in a research design, planned to study the problem in question. This is guided by a research methodology based on the research objectives. Literature on the subject of research methodology provides us with several approaches which are appropriate for research studies, namely exploratory, descriptive, analytical and predictive approaches (Churchill and Iacobucci, 2002). These four approaches will be described below.

Exploratory research is the discovery of ideas and insights, as well as the exploration of new phenomena, thereby supporting the researcher's need for a better understanding. This kind of study aims for ideas or hypotheses, instead of testing or confirming. In short, the primary aims of exploratory study are to gain insights into phenomena and to have a better understanding of them. This type of research is appropriate when the subject of the study cannot be measured in a quantitative manner, or where the problem must be defined more precisely prior to confirming the findings (Malhotra et al., 2012).

Analytical or explanatory research is a branch of research, which looks at the nature and reasoning of certain relationships and utilises critical thinking to find out facts on a given topic. Others see it as a continuation of descriptive research that goes beyond merely describing characteristics in order to analyse and explain the rationale for events. The underlining emphasis is on studying a situation or an issue, thereby explaining the relationship between factors.

Predictive research establishes the current state of events and allows the generalisations about phenomena to be predicted using a hypothesised basis. This broadens the research

and supplements the valid, robust and clear understandings of predictive study (Hamed, 2009). Descriptive research has been defined as the act of obtaining information on particular problem characteristics of the research phenomena. Others argue that this type of study is a forerunner or an extension of exploratory research. This type of research is typically linked by determining the frequency of events or two variables connected by a hypothesis (Churchill and Iacobucci, 2002).

The goal of the study, therefore, is to create a profile describing the phenomena from the perspective of an individual, an organisation or that of another interested party (Sekaran and Bougie, 2010). Commonly, prior formulation is characterised by specific research questions and hypotheses. It is typically based on large representative samples.

In summary, (Robson, 1993, cited in Yousafzai, 2005) exploratory research seeks to rationalise aims, while descriptive research creates a precise portrait of the situation. In turn, explanatory research aims to construct causal relationships between phenomena

With this in mind, Sekaran and Bougie (2010) mentioned, descriptive studies thus become important in many states. While qualitative information obtained by interview helps the understanding of an issue at the investigative stages of a study, quantitative data in terms of frequencies, or mean and standard deviations becomes essential for descriptive research. However, Malhotra et al. (2012, p.77) mentioned, "Descriptive research is characterised by the prior formulation of specific research questions and hypotheses and is typically based on large representative samples". In light of the above, a descriptive study appears appropriate to this research. The research design will discuss in next section.

4.3.2 THE RESEARCH DESIGN

Research design is defined as a frame or strategy for conducting a research project, a set of details and procedures for obtaining data and solving any problems which might occur during the research project. Thus, a good research design is crucial for the efficient execution of a research project (Malhotra et al., 2012).

Research designs can fall into two categories, namely deductive and inductive theories. Deductive research shifts from general ideas or theories to specific situations, which are deduced from general principles (Bryman and Bell, 2015). Thus, the researcher will develop a theory or hypotheses and design a research strategy to test, and confirm or reject, the theory or hypotheses (see Figure 18). According to Bryman (2012, pp.24-25) this theory is formulated in four stages. The first stage is to conclude a theory and hypotheses. The second stage is to test the hypotheses. The next stage is to confirm the theory or indicate if any amendments are required. Finally, if any hypotheses are rejected, the last stage is the modification of the theory in the light of the results.

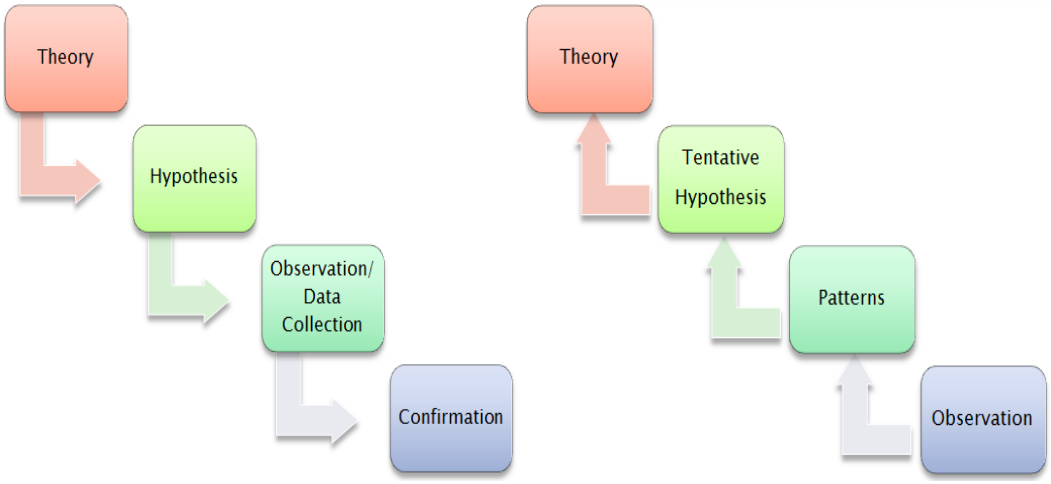


Figure (18) Deductive and Inductive approaches
The source: (Bryman, 2012, p.24).

In contrast, inductive research shifts from particular situations to broader ideas or theories. This is sometimes termed a “bottom up” approach. When using this this approach, researchers will collect data and develop tentative hypotheses, and then develop a theory based on the findings which result from the researcher's data analysis. The researcher begins with specific observations and measurements and then begins to detect patterns and regularities. This leads to the formulation of tentative hypotheses, and finally, the development of general conclusions or models. The primary difference between the two theories is that deductive design moves from theorem to data, whilst inductive design takes the inverse approach (Bryman and Bell, 2015).

Overall, an inductive method aims to use facts to generate new theories, and it uses survey questions to narrow the field of study. Moreover, the objective of this approach is commonly focused on searching for new phenomena or investigating a phenomenon from past studies from various perspectives. Furthermore, the nature of this method is somewhat open and exploratory, especially in the early stages.

This study adopts inductive research methods, because at the beginning of this process, the researcher started by reviewing previous studies on the research subject and identifying a gap in the literature. He then formulated temporary hypotheses for the purpose of exploring and studying the phenomenon. This was followed by the data-collection stage, which was conducted using surveys, and then by an analysis of the data in order to draw conclusions.

4.3.3 RESEARCH STRATEGIES

There are two research strategies, namely quantitative research, which seems to be more common in economics, and qualitative research, which is widely used in the field of anthropology. It should be emphasised that the researcher cannot underpin the virtues of qualitative or quantitative studies for this study, despite the existence of plenty of qualitative studies in the field of economics and good qualitative studies in the field of anthropology. Furthermore, although rules of thumb exist for both types of research, the choice of method should only be made by considering the following questions: What problem is being studied? Is the researcher attempting to conduct an explorative, descriptive, causal or predicative study? What kind of outcomes is he looking for? What information is being sought and how accessible is it? Nevertheless, it is often an impossible feat to examine the suitability of qualitative or quantitative research for a particular study (Blumberg et al., 2008).

Qualitative study is a research strategy that has a qualitative rather than quantitative focus during the data collection and analysis stages. It is an investigation that provides meaningful insight by delving more deeply into social phenomena.

By contrast, quantitative research is constructed as a research strategy which focuses on the collection and analysis of data quantification. When using this method, researchers plan to collect data in order to describe or predict a social phenomenon as a guide to action or to analyse the relationship between the variables; this method also focuses on the analysis of causal or correlational relationships between variable measurements (Sekaran and Bougie, 2010). There are some differences between quantitative and qualitative research strategies: qualitative research is interactively open and observation

precedes theory, whereas structuring and theory precedes observation in quantitative research. Quantitative research involves a large sample, while qualitative research involves a small sample.

As regards the principal orientations of each type of study, it can be said that quantitative research is a predominantly deductive method, as it places emphasis on the relationship between theory and research. On the other hand, qualitative research uses inductive approaches in order to generate theory.

Qualitative research often uses an exploratory approach, whereas descriptive or explanatory approaches are a common feature of quantitative research. A researcher using the quantitative approach uses tools such as surveys to collect numerical data, whereas in the qualitative approach, researchers use data-gathering instruments. The output of quantitative studies is numbers and statistics, whilst qualitative research tends to produce words, pictures or impressions of objects. For these reasons, quantitative methods will underpin the methodology of this study in order to achieve its aims and objectives (Bryman, 2012).

4.3.4 RESEARCH METHOD

Bryman (2012, p.46) defines research method as "simply a technique for collecting data, it can involve a specific instrument, such as a self-completion questionnaire or a structure interview schedule, or participant observation whereby the researcher listens to and watches others". Research methods are employed to collect samples and data, and to resolve problems. Various methods of data collection are available, namely surveys, case studies, experiments, action research, and ethnography.

Questionnaires and semi-structured interviews are the common methods employed in survey research; as well as observations and documents with data associated in surveys (Harrell and Bradley, 2009). This will be detailed more precisely in the forthcoming section.

4.3.4.1 RESEARCH INSTRUMENT

Malhotra et al. (2012, p.452) define questionnaires as "a schedule, interview, form or measuring instrument with a formalised set of questions for obtaining information from participants". For the reasons listed below, questionnaires were used within the context of this research study as an instrument for data collection:

- Given the research subject (Internet banking), a questionnaire survey would aid data collection.
- The cost-efficiency of administering this method.
- Questionnaires can be used to test and explain relationships between factors and the effect of those relationships.

A large sample of customers across Leicester (UK) was required for this study, as the questionnaire included three sections (users, non-users and abandoners of Internet banking). Consequently, the questionnaire was deemed to be a more reliable technique than alternative techniques such as case study or interview.

4.3.4.1.1 QUESIONNAIRE DESIGN PROCESS

The following section will present guidelines and rules to aid the development of questionnaire design for research efficiency. In order to develop additional

understanding of questionnaire design, the operation will be presented as a series of steps, as advocated by Malhotra et al. (2012). These steps are shown in Figure 19.

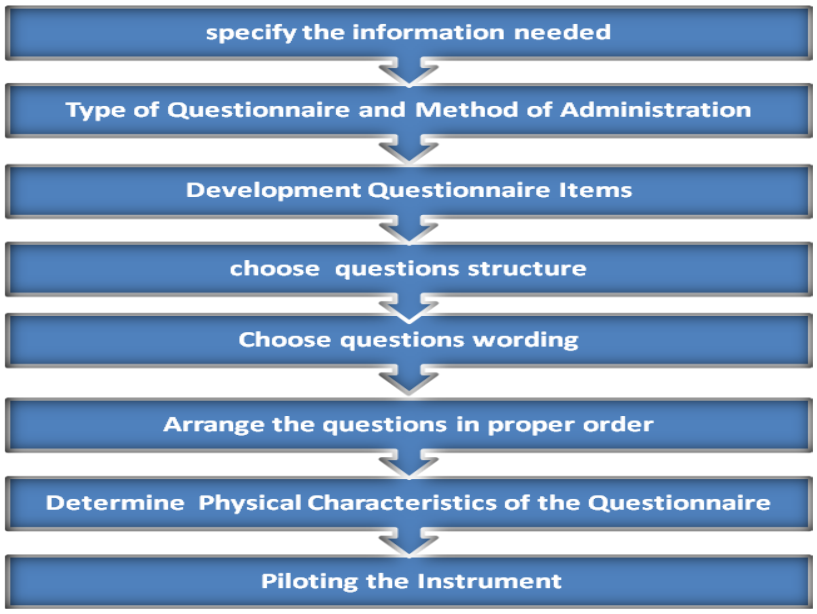


Figure (19) Questionnaire design processes.
The source: based on (Malhotra et al., 2012, p.456).

4.3.4.1.1.1 SPECIFY THE INFORMATION NEEDED

Specifying the information needed is a crucial step in questionnaire design. We should not that as the research project progresses, the data needed can become more clearly defined (Malhotra et al., 2012). In the present study, information was gathered on the variables specified in the conceptual model, which includes demographic questions to examine their effect on this model, and to enhance the researcher's understanding of the respondents. In summary, the questionnaire was designed to examine the hypotheses that were formed in this study.

4.3.4.1.1.2 TYPE OF QUESTIONNAIRE AND METHOD OF ADMINISTRATION

Having identified information gaps, the researcher outlined the process of locating, gathering and structuring data that the questionnaire will use, and the process of administering the questionnaire (by mail, phone or interview). Thus, the type of information gathered will have an effect on the method of data collection (Churchill and Iacobucci, 2002). This study made use of structured questionnaires, consisting of some closed-ended and some open-ended questions. The open-ended questions were included as they gave respondents an opportunity for expression, and this aided the diversity of the research. The questionnaire was intended to be distributed and administered inside and outside bank branches, including High Cross shopping centre, libraries and universities. The method of administration was adopted for the following reasons:

- Banks were unwilling to post the questionnaire to their customers or place it on their website.
- Banks refused to provide the researcher with any information regarding customers contact details which might have enabled direct contact.
- Limited bank support in the distribution of questionnaires.
- Compared with hard copies, online questionnaires produced fewer respondents, as demonstrated by the samples of various corporate entities.

4.3.4.1.1.3 DEVELOPMENT QUESTIONNARE ITEMS

The study instrument consists of three sections: the first relates to non-users of Internet banking, the second part examines respondents who have ceased using Internet banking, and the final part is concerned with current users of Internet banking. It is worth

mentioning that the order of these three parts of the questionnaire does not reflect their relative importance, since each part examines the phenomena of a specific and independent category. On the second page of the questionnaire, a guide was provided to direct respondents to the correct section. Moreover, each section contained both open-ended and closed-ended questions, with a third type of question also being included in section three. This third type of question was a mixed-response option, in which respondents choose an answer but also have an opportunity to express their opinions, thereby advancing the research subject. Several studies in the literature on Internet banking indicate that the open-ended and closed-ended approaches of quantitative studies are favourable. Therefore, this survey will use the quantitative method of research.

A five-point Likert scale was employed in relation to closed-format questions, ranging from strongly disagree to strongly agree; this scale has been used by many researchers in the literature on Internet banking (Nasri and Charfeddine, 2012; AI Somali and Ghinea, 2012; Yoon and Steege, 2013). The questionnaire includes several items which have been developed to satisfy the research aims shown in Table 1. It is important to note that this study did not adopt any questionnaire in full from previous studies, but rather established the items according to the needs of the study and fully checked the validity and reliability of each question as a research instrument. Consequently, the questionnaire was more suitable for achieving the objectives of the study.

Table (1) development of questionnaire items

Section of Non-Users Internet Banking		
Factors	**Hypotheses**	**Questions(Items)**
Trust	H1a: Trust affects customers' decisions/ Intentions regarding the non-adoption of Internet banking.	1. After hearing about fake websites and frauds regarding Internet banking activity, my distrust has been increased.
		2. I do not trust the internet as a channel for banking as it is not safe.
		3. I do not trust the ability of an internet bank to protect my privacy.
		4. I do not depend on internet banking as a trusted instrument of financial transactions.
		5. If an error occurred or my account has been hacked, I am not confident that the bank will repay my money and rectify the error.
		6. Trust concerns of the internet is a major influence on my decision in non- adoption of internet banking.
Security	H1b: Security affects customers' decisions/ Intentions regarding the non-adoption of Internet banking.	7. I worry about the security (phishing/fraud/identity theft) of Internet banking.
		8. I believe the "current security measures taken by banks to protect Internet banking are insufficient".
		9. I do not have confidence in internet banking security.
		10. Branch banking is more reliable and safer than e-banking.
		11. I feel that security concerning internet banking is questionable, because there is an increase in identity theft and fraud.
		12. A security issue on the internet has a major influence on my decision in not adopting internet banking. **(Continue...)**

Section of Non-Users Internet Banking (Continue...)		
Factors	**Hypotheses**	**Questions(Items)**
Risk	H1c: Risk affects customers' decisions/ Intentions regarding the non-adoption of Internet banking.	13. I feel that using Internet banking is too risky for me.
		14. I fear making mistakes while using an Internet banking system.
		15. I do not know the benefits and risks of using Internet banking.
		16. Internet Banking system might be at risk of viruses attack or hackers.
		17. I feel the use of e-banking facilities will make it easier for banks to reduce staff numbers and this could lead to increase unemployment.
		18. A risk issue on the internet has a major influence on my decision in not adopting Internet banking.
Other Questions		19. I am happy with cash machines (ATM).
		20. I am happy with branch banking.
		21. How often do you use the Internet? (Frequently to never).
		QB. Other reasons for not using Internet banking?
		QC. In order to encourage you to use Internet banking, what do you think the bank should do?

(Continue...)

Section of Abandoned The Use of Internet Banking		
Factors	**Hypotheses**	**Questions (Items)**
Trust	H2a: Trust affects customers' decisions/ Intentions regarding the abandoning of Internet banking.	22. I do not trust the ability of internet banking to protect my privacy and personal information.
		23. It is not difficult to hack the internet banking site via the Internet.
		24. I believe that Internet banking is insecure.
		25. I am not confident that the bank will help me to recover my money and rectify the error, if an error occurred or my account has been hacked.
		26. Trust issue in the internet banking have had a major influence on my decision to abandon this service.
Security	H2b: Security affects customers' decisions/ Intentions regarding the abandoning of Internet banking.	27. I am worried about the security (phishing/ fraud/identity theft) of Internet banking.
		28. I did not feel totally safe providing personal and sensitive private information over Internet Banking.
		29. The current security measures taken by banks to protect Internet banking are insufficient.
		30. I feel that security concerning internet banking is questionable, because there is an increase in identity theft and fraud.
		31. Security issues on the Internet have had a major influence on my decision to abandon this service.

(Continue...)

Section of Abandoned The Use of Internet Banking (Continue...)		
Factors	**Hypotheses**	**Questions (Items)**
Risk	H2c: Risk affects customers' decisions/ Intentions regarding the abandoning of Internet banking.	32. Whilst carrying out transactions, Internet banking takes longer than before due to security measures.
		33. While accessing internet banking, there is a risk that banks may not authenticate my username and my password in an accurate manner.
		34. Internet banking system might be at risk of virus attacks or hackers.
		35. I felt that using internet banking is too risky for me.
		36. When transferring money on the internet, I am afraid that I will lose money due to careless or mistakes in transactions.
		37. Risk issues on the internet banking have had a major influence on my decision to abandon this service.
Other Questions		38. I am happy with cash machines.
		39. I am happy with branch banking.
		QB. Are there other reasons behind your abandoning of Internet banking?
		QC. In order to encourage you to reuse internet banking, what do you think the bank should do?

(Continue...)

Section of Users Internet Banking Currently		
Factors	**Hypotheses**	**Questions (Items)**
Trust	H3a: Trust affects customers' decisions/ Intentions regarding the adoption of Internet banking.	40. I trust Internet banking to accomplish banking services satisfactorily.
		41. It is difficult to hack the Internet banking site via the internet.
		42. If an error occurred or my account has been hacked, I am confident that the bank will compensate my money and rectify the error.
		43. I prefer to use Internet banking rather than conventional banking, even if the transaction involves a large amount of money.
		44. I trust Internet banking systems not to disclose my private information and it is able to protect my privacy.
		45. I believe that Internet banking provides accurate records that all transactions have taken place.
Security	H3b: Security affects customers' decisions/ Intentions regarding the adoption of Internet banking.	48. I am not concerned about the security (phishing/fraud/identity theft) of Internet banking.
		49. The current security measures taken by banks to protect Internet banking are efficient
		50. I believe that Internet banking is able to conduct banking transactions securely.
		51. I feel that security concerning Internet banking is unquestionable, because there is a reduction in identity theft and fraud.

(Continue...)

Section of Users Internet Banking Currently (Continue...)		
Factors	**Hypotheses**	**Questions (Items)**
Risk	H3c: Risk affects customers' decisions/ Intentions regarding the adoption of Internet banking.	54. Internet banking system might not be at risk of virus attacks or hackers.
		55. While accessing internet banking, there is not a risk that banks may not authenticate my username and my password in an accurate manner.
		56. I am not afraid that I will lose money due to careless mistakes in transactions, because my bank will help me to recover any lost money.
		57. I do not feel that use of internet banking facilities will make it easier for banks to reduce staff numbers and this could lead to increased unemployment.
		58. Internet banking does not take longer than before due to security measures to ensure safety of data and confirm transactions.
		61. What degree of risk do you feel when you conduct transactions in online banking? (Very insignificant to Very significant risk).
Continuity Factor	H3d: Trust, security and risk affect customers' decisions/ Intentions regarding the continued use of Internet banking.	46. Trust in internet banking may have an impact on my decision to continue using it in the future.
		52. Security issues within Internet banking may have an impact on my decision to continue using it in the future.
		59. Risk issues within Internet banking may have an impact on my decision to continue using it in the future.
		62. In general, I predict I would continue using Internet banking service regularly the future.
		QB. If there are other reasons excluding (trust, risk and security) of adoption / continuous use of Internet banking decisions, please mention?

(Continue...)

Section of Users Internet Banking Currently (Continue...)		
Factors	**Hypotheses**	**Questions (Items)**
Relation between trust and risk	H4a: The perceived risk of Internet banking will reduce trust.	41. It is difficult to hack the Internet banking site via the internet.
		42. If an error occurred or my account has been hacked, I am confident that the bank will compensate my money and rectify the error.
		44. I trust Internet banking systems not to disclose my private information and it is able to protect my privacy.
		45. I believe that Internet banking provides accurate records that all transactions have taken place.
Relation between Security and Trust	H4b: The security of Internet banking will enhance trust.	42. If an error occurred or my account has been hacked, I am confident that the bank will compensate my money and rectify the error.
		49. The current security measures taken by banks to protect Internet banking are efficient.
Relation between Security, and Risk	H4c: The security of Internet banking will reduce perceived risk.	50. I believe that Internet banking is able to conduct banking transactions securely.
		51. I feel that security concerning internet banking is unquestionable, because there is a reduction in identity theft and fraud.
		54. Internet banking system might not be at risk of virus attacks or hackers.
Safety area of Internet banking	H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.	47. When I conduct transactions in Internet banking, I have..? (No confidence to very highly confidence).
		53. How concerned are you about the security of internet banking? (Not at all concerned to very concerned).
		60. When you conduct transaction in Internet banking what is your view of risk? (Very insignificant risk to very significant risk)

(Continue...)

QC- In order to increase your trust, what do you think the Bank should do? [Please select the five most important from the following options]		
Safety area of Internet banking	(Continue...) H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.	1. Give enough safeguards to make user feel comfortable when making Internet banking transactions.
		2. Direct contact with bank staff on the Internet if there is an inquiry/problem.
		3. Show due diligence and responsibility when problems occur.
		4. Offer assistance to guide users, if they get stuck or make a mistake as well providing useful tips.
		5. Website should provide information that helps decrease uncertainty related to Internet banking.
		6. Take necessary modern security measures, which would lead to reduced risks and increase users trust in Internet banking.
		7. Have a good navigability and visibility within the Internet banking website (e.g. easy to locate the services and professional design).
		8. Work as a group with banks to activate existing international and local rules and make it more efficient to protect banks and clients.
		9. Offer clear and reassuring responses about adverse news (identity theft and internet fraud).
		10. Maintaining and promoting a good reputation.
		11. Other (please specify). (Continue...)

QD- In order to enhance security, what do you think the Bank should do? [Please select the five most important from the following options]		
Safety area of Internet banking	(Continue...) H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.	1.Use multi-factor authentication (combination of factor) which uses two or more factors to assert identity are (password – PIN) and biometric technologies such as (Retinal Scan, Voice Pattern, Facial recognition and Fingerprints), rather than two-factor authentication methods to access to internet banking.
		2. Using personal electronic devices (e.g. Secure Key) to be highly secure for Internet banking transactions.
		3. Send warning messages when the communication is insecure.
		4. Make additional methods of verifying my identity before imputing account information and processing transactions.
		5. Enhance security measures even if there is limited time a day to access website.
		6. Promote security measures even if Internet banking transaction takes longer than before.
		7. Make clients change their PIN / Password every so often to make Internet banking more secure.
		8. Outline the risks and promote user's confidence of the effective security measures.
		9. Banks could send confirmation codes to customer's mobile phone for transactions under process, this will enable greater security.
		10. Banks increase the awareness about security of Internet banking.
		11. Other (please specify). (Continue...)

QE- In order to reduce risk, what do you think the Bank should do? [Please select the three most important from the following options]		
Safety area of Internet banking	(Continue...) H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.	1. Compensate any money taken from user account through unauthorized transactions.
		2. When problems occur or user gets stuck, the Internet banking system should guide him to solve them.
		3. Enhance security measures to protect Internet banking from risks of virus attacks, hackers or fraud.
		4. Running awareness campaigns against risks (e.g. identity theft, cyber-crimes and fraud).
		5. Give enough safeguards to make user feel comfortable toward risks when making Internet banking transactions.
		6. Should have clear laws and rules to protect users from risks using Internet banking.
		7. Other (please specify). (Continue...)

QF- Have you ever visited your bank branch since the time you started using Internet banking? [Yes, No] If yes, please select the most important reasons for the visit
1. To make a deposit.
2. To discuss other banking services which not available online.
3. When I get stuck or some mistakes had happened.
4. To make large cash withdrawal.
5. Other important (please specify).
QG -My Internet banking experience is.....Years. (Please fill the blank)

4.3.4.1.1.3.1 SECTION ONE OF QUESSIONNAIRE: NON-USERS OF INTERNET BANKING

The main purpose of this questionnaire was to identify the actual motives that inhibit consumers' Internet banking transactions, as well as non-users' preferences for other service channels in the British context. Specifically, this study investigates the role of trust, security and perceived risk on this phenomenon. Section one of the questionnaire consists of 21 closed-ended questions with two open-ended questions. The wording of questions 1-6 displays similarities with questions used in the existing literature related to the non-adoption and adoption of Internet banking (Omar et al., 2011; Nasri, 2011). The reported Cronbach's alpha coefficient values in these studies were between 0.6 and 0.8 and the constructs were acceptable and are valid.

In this study, items 1 to 6 will measure and explore the influence of trust on the non-adoption of Internet banking services. The Cronbach's alpha coefficient values reported in the pilot study were acceptable, which indicates that the items have adequate internal consistency and reliability. Consequently, these questions will test hypothesis number [H1a].

Questions 7 to 12 aimed to measure the influence of security on the non-adoption of Internet banking. These questions sought to find out whether customers believe that current security measures administered by banks to protect Internet banking are insufficient. In addition, respondents were asked if they were concerned about Internet banking security, given the increase in identity theft and fraud. Factor analysis was performed to validate the scale items and the reported Cronbach's alpha coefficient of both values was acceptable, so these questions will test hypothesis number [H1b]. In

literature on the Internet banking industry (Yeow et al., 2008; Sanchez and Jean-Baptiste, 2010), items similar to questions 7-12 in this questionnaire have been established and validated; the reported alpha values were good and demonstrated the reliability of these items.

Existing literature has identified the relationships between risks and the non-adoption of Internet banking (Nasri, 2011; Omar et al., 2011; Faroughian et al., 2012; AI-Somali and Ghinea, 2012); these studies have used questions which are similar to items 13-18 in this questionnaire, and the Cronbach's alpha coefficient values reported were acceptable. In this study, the validity and reliability values of questions 13 to 18 have shown that the items have adequate internal consistency and reliability. Therefore, questions 13 to 18 sought to examine the relationships between perceived risk factor and customers' decisions/ Intentions regarding the non-adoption of Internet banking; these questions allowed the testing of hypothesis number [H1c].

Questions 19 and 20 are closed-ended questions, which aim to measure the influence of cash machines and branch banking on customers' non-adoption of Internet banking. Of particular interest is the fact that ATMs now offer a wider range of services. In the pilot study, the validity and reliability values of these items were acceptable. In addition, this section also contained open-ended questions, which examined factors other than trust, risk and security, which may also have an influence on customers' non-adoption of Internet banking. Question 21 uses a five-point Likert scale, ranging from 'frequently' to 'never', to determine the frequency of Internet use; this data was collected in order to investigate customers' perceptions toward the Internet in general, as there may be a correlation between their attitudes towards the Internet in general and their non-adoption of Internet banking. Question C was developed by the research author in an

attempt to explore factors, which might induce customers who have not using Internet banking to reactive in the near future.

4.3.4.1.1.3.2 SECTION TWO OF QUESTIONNAIRE: ABANDONED INTERNET BANKING USERS

This section was designed to investigate ceased Internet banking users; this section contains 18 closed-ended questions and two open-ended questions. For this section, trust was measured on a five-point Likert scale as described above. Questions 22 to 26 discussed the effects of trust on the abandonment of Internet banking services. Trust is a key issue in service abandonment. All of the above mentioned items were used to examine the hypothesis [H2a]. In other studies Internet banking services, questions which are comparable to questions 22 to 26 in this study have been used (Mansumitrchai and AL-Malkawi, 2011). In previous studies, the reliability and validity values for these questions were acceptable.

In contrast, items 27 to 31 were developed to test [H2b], which posits that security issues are fundamental to ceased Internet banking users. These issues include: security concerns, feeling unsafe, and security measures due to increased e-fraud. Reliability and validity tests were conducted and the items were deemed to be acceptable. Moreover, several researchers have already used similar items (Sanchez and Jean-Baptiste, 2010; Masinge, 2011; Mansumitrchai and AL-Malkawi, 2011).

A further 6 questions (32 to 37) were included to investigate the issues related to risk which led to the cessation of Internet banking. These issues were the login authentication timeout, virus attacks, hackers, and loss of money. These questions all aimed to test hypothesis [H2c] and their reliability was assessed. Items included in the

risk were established in several studies in the existing literature (Omar et al., 2011; Abbad et al., 2012). Questions 38 and 39 are closed-ended questions which aim to measure the influence of cash machines and branch banking on customers' abandonment of Internet banking services., especially ATMs because they have been developed to offer numerous services. The Cronbach's alpha values obtained were adequate and acceptable for these items. In addition, QB will help to explore if there are other factors affecting Internet banking abandonment behaviour. Question C aims to investigate abandoners' viewpoints and what procedures or policies from their bank would encourage them to resume using Internet banking services.

4.3.4.1.1.3.3 SECTION THREE OF QUESTIONNAIRE: USERS OF INTERNET BANKING

This section consisted of twenty-three closed-ended questions and five open-ended questions. This study found that all the items included in this section exhibited satisfactory internal-consistency reliability, with a Cronbach's alpha value of 0.6 and above. The following discussion will consider these items in more detail.

Questions 40 to 45 of the questionnaire asked the respondents about their trust in the safety of Internet banking services, the accuracy of transactions, and their satisfaction with banking services and technical support. The above mentioned factors will test the validity of hypothesis [H3a] which assumes that trust is pivotal in users' adoption of Internet banking. The items included in this section which measures the trust of customers (Questions 40 to 45) were examined in previous studies (Sanchez and Jean-Baptiste, 2010; Adapa, 2011; Widjana and Rachmat, 2011; Foon and Fah, 2011; Clemes

et al., 2012). Cronbach's alpha coefficient values were computed to test for construct reliability and were identified as adequate (0.6 and above).

Questions 48 to 51 of the questionnaire investigate respondents' satisfaction with Internet banking security, and seek to verify hypothesis [H3b]. Security is an important underlying issue in users' adoption of Internet banking, and these questions measure security concerns, security protocols, and the bank's awareness of criminal activity. In the literature on Internet banking, several studies (Widjana and Rachmat, 2011; Adapa, 2011) were consistent with this research when examining the reliability and validity of these item, and they found that all of the items in the questionnaire relating to security exhibited satisfactory internal consistency reliability, with a Cronbach's alpha value of 0.6 and above.

Questions 54, 55, 56, 57 and 58 – 60 aim to research how users of Internet banking services access the Internet in order to perform their transactions and to find out the values for the degree to which they perceive that they are at risk. This will allow the researcher to validate hypothesis [H3c]. These questions consider a range of risks, including the risk of virus attacks or hackers, the accurate authentication of usernames and passwords, aversion to financial risks in transactions, and the belief that Internet banking improves efficiency, for example by reducing staff numbers and saving time. In studies related to perceived risk in the literature (Masinge, 2011; Omar et al., 2011; Faroughian et al., 2012) the Cronbach's alpha value was greater than 0.60.

In this study, questions 46, 52, 59 and 62 measured continuity factors of current Internet banking users on a five-point scale. Additionally, questions 46, 52 and59, queried users' trust, security and risk scales with prolonged use of Internet banking. Question 62

reviews the future behaviour of Internet banking users. In addition, open-ended questions were posed (QB) to users to determine the effect of factors other than trust, risk and security in governing the adoption and continued use of Internet banking amongst users. All of the above questions aim to validate hypothesis [H3d]. Previous surveys in the literature touched upon the continuity of use factor (El-kasheir et al., 2009; Adapa, 2011; Hoehle et al., 2012). Cronbach's alpha values obtained in this research and in previous studies in the literature were adequate (> 0.6).

Questions 41, 42, 44 and 45, investigate the causal relationships between consumer trust and the risks represented in hypothesis [H4a]. Trust in Internet banking will reduce perceived risk, and the findings will illustrate the extent of the impact that increased customer trust has on reducing perceived risk. The items included to investigate this hypothesis were examined in a number of previous studies in the literature (Sanchez and Jean-Baptiste, 2010; Foon and Fah, 2011; Clemes et al., 2012) and the Cronbach's alpha coefficient values stated were greater than 0.60, which indicates that the items had adequate internal reliability.

Hypothesis [H4b] investigates the relationship between security in Internet banking and customers' trust, thereby reducing perceived risk. In order to test this hypothesis, items 42 and 49 investigate the relationship between security and trust. The Cronbach's alpha coefficient values for these items were greater than 0.60. Moreover, these questions have been examined by several studies in the literature (Widjana and Rachmat, 2011). Since [H4c] studies the relationship between security and perceived risk, this research has used three questions to investigate this relationship (50, 51 and 54). In studies of this relationship in the existing literature on Internet banking services (Sattabusaya, 2008; Adapa, 2011) the Cronbach's alpha value of these items was greater than 0.60.

One of the important aims of the study is the identification of the safety area of Internet banking services in hypothesis [H5]. For the purpose of broadening understanding, items 47, 53 and 61 were created to collect data from active Internet banking users along a five-point Likert scale of users' transaction confidence ranging from 'not at all confident' to 'very highly confident'. In addition, security concerns were assessed along a scale ranging from 'not at all concerned' to 'very concerned'. Furthermore, Question 61 places users' transactions risks along the scale from 'very insignificant' to 'very significant' risk.

In order to validate this hypothesis [H5] the study has also developed three items for inclusion in the questionnaire: QC 'In order to increase your trust, what do you think the bank should do?'; QD 'In order to enhance security, what do you think the bank should do?'; QE 'In order to reduce risk, what do you think the bank should do?'. In this study Cronbach's alpha coefficient value reported was more than 0.60 for these items. In addition, previous studies have examined these questions and have also revealed that the Cronbach's alpha value was greater than 0.60 (Ho and Lin, 2009; Yousafzai et al., 2009). As noted above, the purpose of these questions is to validate hypothesis [H5], which suggests that there is safety combination of trust, risk and security that will ensure a favourable level of usage and degree of satisfaction with Internet banking services.

Whereas question F examines the behaviour and rationale of Internet banking users who have visited bank branches since adoption, question G investigates the Internet banking user behaviour of recent users versus old users; this may aid in studying the relationship between factors and this situation.

As for demographic characteristics, several previous surveys indicated that demographic factors are influential in the adoption of Internet banking services. For example, Patsiotis et al. (2012) explore customers' resistance behaviour towards Internet banking; they demonstrated that income is associated with non-adoption.

In several studies, age, education level, marital status, gender, income and occupation were found to have an influence on the acceptance and adoption of Internet banking (Clemes et al., 2012; Izogo et al., 2012; Munusamy et al., 2012). Therefore, the current study included six items (A to F) which are concerned with collecting data about demographic characteristics from the respondents.

- Gender: consisted of two groups (1) Male and (2) Female.
- Age: represented in four groups (1) 18–25 (2) 26–45 (3) 46–60 (4) Above 60 years.
- Education level: (1) Primary school, (2) Secondary school, (3) College, (4) Bachelor's degree, (5) Master's degree, (6) Doctorate (PhD), (7) other.
- Monthly income: (1) £1500 and under, (2) £1501- £2000, (3) £2001-£2500, (4) £2501-£3000, (5) £3001-£3500, (6) £3501-£4000, (7) £4001-£4500, (8) £4501 and above .
- Nationality of respondent.
- Occupation: (1) Student, (2) Housewife /Homemaker, (3) Self-employed, (4) Unemployed, (5) Employee/official in the government sector, (6) Employee/officer in the private sector, (7) Retired/pensioner, (8) other.

4.3.4.1.1.4 QUESTION STRUCTURE

This study has employed close-ended questions due to their simplicity of administration and ease of tabulation and analysis (Churchill and Iacobucci, 2002). In addition, a five-point Likert scale was used in order to have a greater uniformity of response type. This style of question was employed in three sections of the questionnaire. Similarly, open-ended questions were embedded in the questionnaire so that participants' opinions could extend the research topic. The third section of the questionnaire about Internet banking encouraged respondents to tick the answer that most closely corresponded to their position.

4.3.4.1.1.5 CHOOSING THE WORDING OF THE QUESTIONS

This stage of questionnaire development is perhaps the most critical and difficult, because if a question is worded poorly and is unclear, the participants may answer it incorrectly. When choosing the wording of questions, the aim should be simplicity and unambiguous words, as well as avoiding generalisations, estimates and advocating positive and negative statements (Malhotra et al., 2012). These issues have been averted in this study by piloting the questionnaire to allow any misleading questions, inappropriate abbreviations and ambiguous wording to be detected before the delivery of the final survey In addition, the questionnaire was reviewed for veracity by an English language expert before the main survey took place.

4.3.4.1.1.6 ORDER OF QUESTIONS

As noted by Malhotra et al. (2012), the sequence of questions is vitally important. Churchill and Iacobucci (2002) mention that the sequence in which the questions are

presented is essential to the success of the research effort. In the literature, researchers suggest that questions should be simple, interesting and non-threatening, to encourage respondents and motivate them to complete the questionnaire (Churchill and Iacobucci, 2002). The questionnaire in this study consists of three parts.

The first part measures the respondents' trust, risk and security related to the non-use of Internet banking. The second part deals with the respondents' trust, risk and security regarding the abandonment of Internet banking. The third part in the questionnaire investigated these three factors in relation to the use of Internet banking.

The demographic variables of respondents were placed in the final section of the questionnaire with open-ended questions attached at the end of each of the three parts of the questionnaire.

4.3.4.1.1.7 CHARACTERISTICS OF THE QUESIONNAIRE

The physical characteristics of the questionnaire influence the accuracy of response rates, as well as how respondents react to it. Thus, to drive respondent acceptance, efficiency and productivity of the questionnaire, a sound structure was founded, which included an explanation of the research objectives, and a cover letter to provide details and give guidance for responses (Churchill and Iacobucci, 2002).

4.3.4.1.1.8 PILOTING THE INSTRUMENT

Pilot testing refers to "testing the questionnaire on a small sample of participants to identify and eliminate potential problems" (Malhotra et al., 2012, p.476). This test is deemed to be best practice within research to explore and iron out potential weaknesses, and also allows researchers to make modifications to the questionnaire design in terms

of validity, reliability and practicality before the actual questionnaire run takes place. In order to maximise positive outcomes, pilot studies typically mirror the samples to be used in the real study (Phellas et al., 2011). Moreover, the pilot study for this survey was conducted in the UK, which supports a population study; therefore this will strengthen the research conclusions.

This study did not adopt any full instrument from previous studies; however, the study has selected items according to the needs of the study from the previous studies, alongside the creation of new items. The questionnaire was built step-by-step with the supervision team, and also made use of advice from academic experts. Linguistic experts checked the linguistic output of the questionnaire. After the building of the questionnaire, tests were conducted to check its reliability and validity. The pilot study showed that the questionnaire was acceptable and there was no need to reconstruct or delete any items, thus rendering it reliable for the main study. It is worth noting that linguistic experts have made some simple linguistic amendments in order to facilitate the respondents' understanding of the questions.

The pilot study was conducted amongst staff and postgraduate students at De Montfort University, Leicester, and also among people within the Leicester city centre radius, for example in shops, in front of banks, cafés, libraries and universities. The pilot study was conducted on a sample of 105 consenting respondents who met the criteria of being over 18 years and above and having a bank account.

Questionnaires were printed and handed to respondents and survey completion typically took between 10 and 15 minutes. The results of the pilot study revealed that 50 respondents were active Internet banking users, 20 respondents were abandoned Internet

banking users and 35 respondents were non-users of Internet banking. These numbers refer to the pilot questionnaires, which were not used for the main data collection phase. The collected samples were entered into SPSS software for reliability and validity verifications as a pre-cursor to the main questionnaire study, which will be detailed in the following section.

4.3.4.1.1.8.1 RELIABILITY AND VALIDITY

The next sections illustrate the concepts and procedures used to test the reliability and validity of the questionnaire during the pilot study.

4.3.4.1.1.8.1.1 RELIABILITY

According to Swesi (2011, p.216) reliability is "the technique used to measure the accuracy of the construct and to assess if the items in the construct are homogenous". The branches of measurement include: stability, internal reliability and inter-observer consistency reliability. The internal consistency reliability tests commonly employed within the field of research are known as Cronbach's Alpha (α). This assesses the mean correlation of all items in a construct (Bryman and Bell, 2011). Alpha was developed by Lee Cronbach in 1951 with Cronbach's Alpha's (α) values ranging being between 0 and 1 (Tavakol and Dennick, 2011).

A Cronbach's Alpha value of 0.7 or more is considered to be acceptable (Pallant, 2010). According to Bryman (2012, p.170) a minimum level of 0.6 is equally acceptable. In this study, Cronbach's Alpha was conducted to measure the reliability of questionnaire items as tabulated below in Table 2.

Table (2) Cronbach's Alpha for pilot study results Reliability

Factors Measured	Cronbach's Alpha Values	Number of items
Factors of Non-users of IB:		
Trust	0.791	6
Security	0.719	6
Risk	0.70	6
Factors of abandoned users of IB:		
Trust	0.788	5
Security	0.830	5
Risk	0.70	6
Factors of current users of IB:		
Trust	0.797	8
Security	0.70	6
Risk	0.70	8
Continuity	0.50	4
QC	0.50	10
QD	0.60	10
QE	0.60	6
QF	0.60	4

The above results show that the continuity factor of Internet banking users is slightly less than the required value of 0.6; this may be due to the small sample size or the fact that fewer than ten items were included (Pallant, 2010).

However, this is acceptable for a pilot study, therefore there is no need reconstruct or delete any items, and the questionnaire can be considered to be reliable for the purpose of the study.

4.3.4.1.1.8.1.2 VALIDITY

Chang (2009, p.81) states that quantitative research "determines whether the study truly measures that which it was intended to measure or how truthful the research results are". There are several ways of establishing validity in quantitative research: face validity, concurrent validity, constructs validity and convergent validity. Face validity and construct validity have been measured in the present study.

- **FACE VALIDTY**

Face validity was used in the pilot study as a test to assess the questionnaire's competence. It was piloted amongst three research experts and an English language specialist so that they could give recommendations which would make the questionnaire more efficient. In addition, a linguistic expert has made some simple linguistic amendments to improve the respondents' understanding of the questions (Bryman, 2012).

- **CONSTRUCT VALIDITY**

Research circles advocate construct validity estimations. This involves investigating the relationship between related (convergent validity) and unrelated constructs. Construct validity is considered from one the most important instruments of a measured dependent variable. To justify the requirements of construct validity several empirical experiments

have been implemented to amend the functions of factor analysis (Bryman and Bell, 2011).

- **FACTOR ANALYSIS**

Factor analysis is a multivariate statistical approach commonly used in research, and other fields. However, before proceeding to do the analysis, it is necessary to check outliers and assess the normality of the pilot study sample.

- Checking Outliers and Assessing Normality For Pilot Study Sample:

Factor analysis can be sensitive to outliers, so it is important to check them before conducting the factor analysis test. This study checked outliers before the pilot study test was conducted. This has been covered extensively in the chapter on data analysis. The outliers test confirmed that non-outlier cases among study data were within the suggested range. Furthermore, the two mean values are very similar and there were no outlier cases among the data. As for normality, the skewness and kurtosis values fall inside the range (the skewness absolute value <= 30.0 and the kurtosis absolute value <=10.0). The findings of both the skewness and kurtosis tests for the pilot study show that the distributions of all variables are normal and satisfied the Kolmorogov-Smirnov (K-S) test; the test is significant and normal.

Returning to the subject of factor analysis, Williams et al. (2012) claim that sample size is an integral facet in factor analysis; this opinion is not shared by all researchers in the literature on this subject. Some suggest that at least 300 cases are needed for factor analysis, while others suggest that sample sizes should be 100 or greater.

Table (3) Validity Factor analysis for constructs as pilot study results

Construct Measured	Number of items	Kaiser-Meyer-Olkin Measure of Sampling Adequacy[KMO]	Bartlett's Test of Sphericity
Items of Non-users of Internet banking			
Trust	6	0.641	P=.000
Security	6	0.669	P=.000
Risk	6	0.612	P=.036
Items of abandoned users of Internet banking			
Trust	5	0.692	P=.000
Security	5	0.702	P=.000
Risk	6	0.620	P=.000
Items of current users of Internet banking			
Trust	8	0.814	P=.000
Security	6	0.633	P=.001
Risk	8	0.702	P=.000
Continuity	4	0.550	P=.05
QC	10	0.60	P=.003
QD	10	0.550	P=.000
QE	6	0.60	P=.030
QF	4	0.70	P=.002

In spite of the limited sample size of 105, the factor analysis (as exemplified in Table 3 above) was conducted to ensure validity and accessibility, as advocated by Chau and Hu (2001).

For the verification of factor analysis, the (KMO) (Kaiser-Meyer-Olkin Measure of Sampling Adequacy) value should be 0.6; this was the case in the currents study with the exception of two items, namely continuity factor and QD. This may be due to the limited number of items. Additionally, the Bartlett's Test of Sphericity value should be significant ($P<0.05$), as was the case for all items in the current study.

In summary, KMO values and Bartlett's test of Sphericity are significant. Therefore, factor analysis in this study would deem it to be viable for data collection in actual study, without the need for any items to be deleted or removed. The next section will discuss the sampling design process.

4.3.4.2 THE SAMPLING DESIGN PROCESS

Research methodology involves selecting data collection tools and then determining the sample size to be used in the study. Sampling can be defined as the part of the population that is chosen for study (Bryman and Bell, 2011). There are two techniques for selecting the sample, as documented by namely the probability approach and the non-probability approach (Dillman, 2007). Bryman and Bell (2011) argue that determining sample size is source of concern within research. Thus, the procedure of determining sample becomes fundamental in the critical path of scientific research as outlined by Malhotra et al. (2012) in Figure 20.

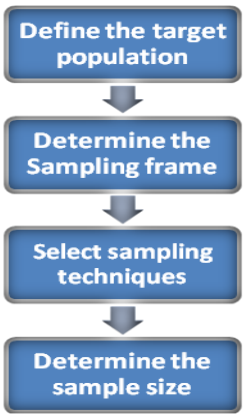


Figure (20): the sampling design process
The source: (Malhotra et al., 2012, p.496)

4.3.4.2.1 TARGET POPULATION DEFINITION

Defining the target population initiates sampling design before the investigation takes place (Bryman and Bell, 2011). The target population is defined as the totality about whom the researcher needs to obtain information that conforms to some designated specifications, be it a group of people that constitutes a community, a society or an organisation. Researchers should be mindful of strict of inclusion and exclusion factors of population definitions, as inaccurate definitions of target populations will result in doubts about the research, as noted by Churchill and Iacobucci (2002).

In the current study, the population was defined as all individuals who live in Leicester, whether British or non-British, who fulfil the following criteria:

Geography: People who live in the radius of Leicester city and have bank accounts. The rationale for this is the size of Leicester city, which has a population of 329,839 according to the Office for National Statistics (2011; 2013). Additionally, implications for resource efficiency, time and cost were taken into consideration.

Age of individuals: in this study, the minimum age for participants is 18 years. At this age humans are typically of sound mind and able to make rational judgments with a degree of basic education. According to the website of Leicester City Council (2013) the total adult population of the city is 217,536.

Individual variables: as mentioned above, the population of this survey includes both male and female bank customers who fall into the target categories: Internet banking users, Internet banking non-users and abandoned Internet banking users.

4.3.4.2.2 DETERMINATION OF THE SAMPLING FRAME

A sampling frame should be representative of the elements of the target population. It is a list, which contains directions for identifying the target population. Churchill and Iacobucci (2002) highlight that the second step in determining the sample study is stipulating the sampling frame (Bryman and Bell, 2011). Due to data sensitivity, there is no available data regarding the total of number bank customers in Leicester who fall into the categories of users, non-users or abandoners of Internet banking services. Nevertheless, the sampling frame only includes banks customers in Leicester city to shed light on users, non-users and abandoners of the Internet banking service for the purpose of this study.

4.3.4.2.3 SAMPLING TECHNIQUE SELECTION

Figure 21 illustrates selecting whether to use probability or non-probability sampling. Non-probabilistic sampling hinges on the researcher's personal judgement rather than on the selection of chance sample elements. Sometimes the researcher's judgement can

affect the sample as he can make arbitrary or conscious decisions about inclusions. In other situations the selection of population elements is made by individual field workers

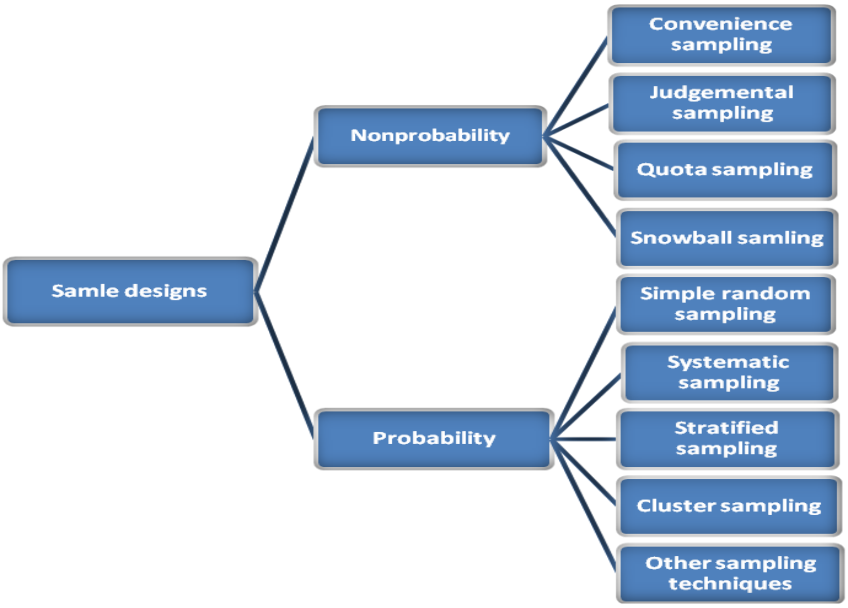


Figure (21): A classification of sampling techniques.
The source: (Churchill and Iacobucci, 2002, p.454;
Malhotra et al., 2012, p.501)

In non-probabilistic samples, population characteristics are often estimated. However, objective evaluation of sample results for precision are less forthcoming with random sampling. The estimates obtained in this method cannot be statistically projected to the overall population. Non-probability sampling techniques (pictured in Figure 21,) as noted by Malhotra et al. (2012, p.501), include convenience sampling, judgmental sampling, quota sampling and snowball sampling.

In probability samples, units are selected by chance; any selection method presents a specific probability of being chosen. As such, they are all equal. Furthermore, this requires not only a precise target population definition, but also a general sampling frame specification. Sample elements are selected by chance, thus increasing the

precision of the sample. Figure 21 demonstrates that probability sampling methods are simple random sampling, systematic sampling, stratified sampling, cluster sampling and sampling techniques (Malhotra et al., 2012, p.501; Churchill and Iacobucci, 2002, p.454).

The use of probability sampling procedures offsets the bias association, which is evident in non-probability sampling. Additionally, the sophisticated use of statistical tests makes it possible to search for group differences. The most appropriate sampling technique is probability sampling, which has been adopted by this study alongside simple random sample technique for data collection. The rationale is detailed in the forthcoming section.

4.3.4.2.3.1 SIMPLE RANDOM SAMPLING

In this type of sampling, each population has an equal probability of being selected as subjects. Simple random sampling has many desirable features. Equally, sample results collected using this approach may be projected onto the target population using typical statistical inference methods. However, simple random sampling of participants has significant limitations. Firstly, it is usually impractical to target the entire the population. Secondly, simple random sampling can be a difficult task when the population is spread over a large geographical area, requiring increased resources to collect the data (Malhotra et al., 2012).

In the context of this study, the most appropriate sampling technique is probability sampling. This is because of its ability to obtain unbiased and reliable estimates of the mean value of the parameters used in the research. Furthermore, it is based on the capability of a given chance for each member of the sample population to participate by

covering a broad area and a large number of customers. On the other hand, the non-probability method is a common feature in small-sample populations and when specifying the probability of each unit in the sample is difficult (Churchill and Iacobucci, 2002). Thus, this sampling method is inconsistent with the objective of this research, as the study seeks to involve a large sample of the population. Hence, simple random sampling was adopted to collect the target data.

4.3.4.2.4 SAMPLE SIZE DETERMINATION

Perhaps the most frequently asked questions regarding sampling are ‘what sample size do I need?’ and ‘How large should my sample be?’ The answer to these questions is affected by a number of matters, namely the aims of the study, the population size, risk attributed of selecting sample, and the acceptability of sampling error. Consequently, the determination of the proper sample size is a very significant stage for any survey, as inadequate or excessive volumes affect the research veracity and precision (Kotrlik and Higgins, 2001).

Cohen et al. (2011) and Bryman and Bell (2011) argue that there is no clear–cut answer for a correct sample. They argue that there is no guaranteed precision with a large sample or small sample. Hence, it is probably better to say that increasing the size of sample to enhance sample precision may lead to sampling error reduction.

There are various approaches to determining the sample size. The first approach is to use the entire population as the sample. Although cost and time considerations make this impossible for a large population, it is more effective with small populations because it eliminates sampling error. The second approach is to use the same sample size as a similar study. In this approach, the researcher can define his study simply by

benchmarking sample sizes of previous similar studies. A third approach to utilizing published tables, which are available in literature reviews or research centres (see Table 4). The fourth approach is using formulae (equations) to calculate a sample size: in this regard, several equations can be adopted by the researcher to calculate the sample sizes (Israel, 2012).

In the present study, the researcher determined the appropriate sample size using a simplified formula provided by Israel (2012), which compares the result with the results of previous studies and published tables. It should be noted here that there is no unified rule for sample size that can be used for all surveys (Scheuren, 2004).

$$\mathbf{N} = \frac{N}{1 + N(e)^2} = \frac{217536}{1 + (217536)(0.03)^2} = 1105$$

- N: is the population size.
- E: is the level of precision (Confidence level 3%).
- Population of Leicester (Aged 18 to 75+) in 2011 is 217536 (Leicester city council website, Accessed in 27/06/2013).

Observe, that sample size for the population shown in the below table from >100,000 to 1000,000 is almost equal. Thus, these correspond with sample size as presented in current studies.

Table (4): Samples Size for ±3%, ±4%, and ±5%, Precision Levels where Confidence Level is 95% and P=.5.

Adopted from	Population size	Sample Size (n) for Precision (e) of:		
		±5%	±4%	±3%
Cohen et al (2011,p. 147)	200,000	383	598	1061
Israel (2012,p.2)	>100,000	204	400	1,111
Saunders et al, (2012,p. 266)	1000,000	384	390	1066
Glasow (2005)	>100,000	-	-	1067
Dillman (2007, p. 207)	1000,000	384	400	1,066

Similar surveys by Adapa (2011) identify potential factors influencing consumers continued frequency of usage in Australian Internet banking. Selected sample sizes depend on the judgment of the researcher who used the previous study to make his decision; Adapa's survey involved the distribution of about 1308 questionnaires to both users and non-users of Internet banking in the foyers of shopping malls, and resulted in just 698 completed surveys.

In this study, the final questionnaire was distributed across Leicester city to 1400 customers who were present in Leicester at time of conducting the study, and were both users and non-users of Internet banking services. The questionnaire was distributed at various locations, including High Cross shopping centre in Leicester, universities, public libraries and in front of banks. Just 890 respondents completed the survey questionnaires, of which 838 were valid. The results showed that 503 respondents were users, 291 were non-users and 44 were abandoned users.

4.3 ETHICAL APPROVAL ISSUE

De Montfort University's (DMU) Human Research Ethics Committee granted approval for the project to be conducted by the researcher on 5 April 2013. The project approval was underlined by submission of questionnaire draft with ethical aspects considered and applied to protect respondent's confidentiality. This consent was agreed with participants bearing in mind the following points: It will not include personal information, such as, names, numbers or contact address, the information will be kept in strict confidence and Information will not be used for any non-research purpose.

4.4 CHAPTER SUMMARY

After the research scope was determined, and the gap in the literature regarding Internet banking in the UK was identified, the researcher determined the aims and questions of the study and then formulated hypotheses. Theoretical frameworks were built in order to achieve the objectives of the study; these are the non-adoption model, the abandonment model, the adoption model and the safety area model of Internet banking services. After the methodology of the study was determined and data collected through the use of the study questionnaire, these models were ready for evaluation. The study instrument was built on scientific foundations. It has been validated and checked for reliability, in order to be suitable for use in the main study. In addition, the study sample size also has been identified according to the steps involved in scientific research. Hence, after following these scientific steps, we can now proceed to the main study, and the implementation of frameworks will be discussed in next chapter.

CHAPTER 5: IMPLEMENTATION OF FRAMEWORK

5.1 INRODUCTION

This chapter focuses on the implementation of frameworks. Firstly, there is an outline of the data collection procedures; secondly, there is a discussion of construct abbreviations; thirdly there is a discussion of the descriptive statistics of the sample, along with a demographic profile analysis, and the relationship between trust, security, risk and the demographic characteristics of Internet banking services; fourthly, there is a discussion of general Internet usage trends (e.g. the nationality of samples studied and non-users and abandoners' perceptions of ATM and branch banking); fifthly, there is a description of normality and outlier testing, reinforced by instrument reliability and the validity of the instrument of study. Finally, there is an outline of the expected research results and a summary of the chapter.

5.2 DATA COLLECTION PROCEDURES

Once the survey instrument had been refined, approval was sought from the De Montfort University Human Research Ethics Committee. An information sheet related to the study was attached, along with guidance (which included an estimated 10-15 minutes for the completion of the survey) with the questionnaire to support survey responses (Appendix: C).

The respondent’s right to participate voluntarily, with total confidentiality and anonymity, was reinforced, along with their right to withdraw at any time. The contact details of the researcher and his supervisor (i.e. telephone numbers and email addresses) were provided on the information sheet. Once the sample had been selected, the final

field survey was undertaken over a period of 7 weeks, in order to obtain a valid sample, commencing on the fifth day of April, 2013 until the first day of June, 2013,

As noted previously, the final questionnaire was distributed among 1400 existing customers within the city of Leicester. These included both users and non-users of Internet banking services from Leicester's High Cross shopping centre, universities, public libraries and across diverse banks. At completion of the data collection stage, 890 completed questionnaires had been returned. 838 of which were valid (this does not include the questionnaires of the pilot study). The results were as follows: 503 users; 291 non-users; and 44 abandoners.

In relation to the low rate of response for abandoners, the study objective was to verify and explore the existence of any abandonment of the service. This phenomenon has not been previously identified, and nor has it been subjected to research. The study did not aim to achieve a specific rate of response from abandoners, due to the fact that the researcher was unsure of the existence of the phenomenon. The aim was rather to explore the percentage abandoners represented in relation to the complete study sample, along with any underlying factors. Moreover, the identification of this issue will lead to further research. The final survey was made up of seventy-seven (77) items for all questionnaire parts. The first segment related to non-users of IB, and was made up of a twenty-one (21) Likert-scale and two open-ended items. The second related to abandoners, and contained eighteen (18) Likert-scale items and two open-ended items. The final survey related to users of IB, and was made up of nineteen (19) Likert-scale items, one open-ended item, four rating scale items, three multiple-choice items, one dichotomous item and six demographic items (see Appendix C).

5.3 DATA ANALYSIS

The following section discusses construct abbreviations, sample descriptive statistics, demographics and the relationships between trust, security and perceived risk in relation to the demographic characteristic of customers. In addition, it discusses general Internet usage trends, normality and outlier testing descriptions, reinforced by instrument reliability and validity.

5.3.1 CONSTRUCTS ABBREVIATIONS

The SPSS 20.0 package is the foundation of this analysis. Respective abbreviations for each construct (variable) are identified in Table 5, in order to ensure the construct names are appropriate for the purpose of the analysis.

Table (5): Abbreviations of variables used in the analysis

Construct Name	Abbreviation Used for Analysis
Internet Banking (IB)	IB
Non-users of Internet Banking (NU)	NU
Given up of Internet Banking (GU)	GU
Users of Internet Banking (U)	U
Gender	Gender
Age	Age
Education	Education
Income	Income
Occupation	Occupation

5.3.2 DESCRIPTIVE STATISTICS OF THE SAMPLE

Validated frequencies percentiles of Internet banking users, non-users and ceased users from the total respondents are presented in Table 6. To summarise: the overall response rate obtained from the survey was 59.8 %, excluding any missing responses. Completed surveys accounted for 838 respondents, made up of, 503 Internet banking users (60 %); 291 non-users of Internet banking (34.7 %); and 44 abandoned users of Internet banking (5.3%).

Table (6): Frequencies of the Internet banking Users, Non-users and Abandoned

Item	Characteristic	Frequency	Percentage
Internet Banking	Non-users	291	34.7%
	Users	503	60%
	Abandoned	44	5.3%
	Total	838	100%

5.4 DEMOGRAPHIC PROFILE ANALYSIS

Instrument demographic variables include gender, age, education, income and occupation, with statistical demographics as supported in Table 7. The results imply that 57.5% of females favour Internet banking, as opposed to 42.5% of their male peers. This trend is mirrored among non-users of service, with 57% females versus 43% males. When it comes to customers who abandoned these services, males (52.3%) outweigh females (47.7%) (see Figure 22). The largest age group of those using Internet banking were those aged 18 to 45 (92%), with non-users and abandoners being 72.5% and 97.8%, respectively (see Figure 23). Education: Fifty-seven percent of those using service had a bachelor's degree, and 19.3% had some college level qualification. The majority of non-users were as follows, 32.3% had some degree of college education and 14.4% had completed secondary school. It should be noted that among those who had

abandoned service, 54.5% had a bachelor's level of education, followed by college (20.5%) and a master's degree level (18.2%) (see Figure 24). Economic levels: the majority of users (83.7%), non-users (80%), and those who had abandoned Internet banking (79.5%) were within the income range of £1500 to £2500 monthly (see Figure 25). The distribution of jobs amongst those using Internet banking were dominated by the governmental and private sector level (48.6%), with the self-employed equating to 23.1%, and students as 21.1%. When it came to non-users, the governmental and private sector formed 37.4%, with students 28.2%, and the self-employed 15.8%. Those who had ceased to use service comprised of: 43.2% at governmental and private sector and both students and the self-employed at 22.7% (see Figure 26). Overall, females dominated Internet banking use and non-use in comparison to male counterparts. Comparatively, percentage of abandoners was equally between male and female.

Interestingly, adults aged 26 - 45 years represented majorities across Internet banking patterns. Accordingly, weighty education levels amongst aforesaid noted college to master degrees. These education groupings were the highest in education groups. It is appearing the phenomenon does not have relationship with customers' education levels. With respect to sample study incomes, the majority of salaries within £1500-2500 per month, for all service patterns. With that noted minorities displayed of £2500 above per month, Evidencing non relations of income level with Internet banking service behaviours. The majority of respondents were employed in governmental and private sectors, followed by those who were self-employed, thus revealing that gender, age, education, income levels and occupation bore no relation to clients' Internet banking service behaviours, either in relation to adoption or ceasing. Next section will discuss relationships between three factors with demographic characteristics of customers.

Table (7-1): Demographic Characteristics of the Users, Non-users and Abandonment of Internet Banking.							
Item		Internet Banking Users		Non-users of Internet Banking		Abandoned of Internet Banking	
		Frequency	%	Frequency	%	Frequency	%
Gender	Male	214	42.5%	125	43%	23	52.3%
	Female	289	57.5%	166	57%	21	47.7%
Age	18 -25	229	45.5%	116	39.9%	16	36.4%
	26-45	234	46.5%	92	31.6%	27	61.4%
	46 -60	37	7.4%	55	18.9%	1	2.3%
	Over 60	3	0.6%	28	9.6%	0	0.0%
Education	Primary School	1	0.2%	22	7.6%	0	0.0%
	Secondary School	21	4.2%	42	14.4%	0	0.0%
	College	97	19.3%	94	32.3%	9	20.5%
	Bachelor	288	57.3%	94	32.3%	24	54.5%
	Master	65	12.9%	25	8.6%	8	18.2%
	PhD	12	2.4%	2	0.7%	2	4.5%
	Other	19	3.8%	12	4.1%	1	2.3%
Income	Under1500	185	36.8%	151	51.9%	17	38.6%
	1501-2000	142	28.2%	62	21.3%	6	13.6%
	2001-2500	94	18.7%	46	15.8%	12	27.3%
	2501-3000	56	11.1%	19	6.5%	3	6.8%
	3001-3500	6	1.2%	6	2.1%	3	6.8%
	3501-4000	7	1.4%	2	0.7%	2	4.5%
	4001-4500	3	0.6%	0	0.0%	0	0.0%
	Over4500	10	2.0%	5	1.7%	1	2.3%

Table (7-2): Demographic Characteristics of the Users, Non-users and Abandoned of Internet Banking							
Item		Internet Banking Users		Non-users of Internet Banking		Abandoned of Internet Banking	
		Frequency	%	Frequency	%	Frequency	%
Occupation	Student	106	21.1%	82	28.2%	10	22.7%
	Housewife	5	1%	10	3.4%	2	4.5%
	Self-employer	116	23.1%	46	15.8%	10	22.7%
	Unemployed	17	3.4%	12	4.1%	2	4.5%
	Employed in Government sector	123	24.5%	60	20.6%	11	25%
	Employed in private sector	121	24.1%	49	16.8%	8	18.2%
	Retired	1	0.2%	27	9.3%	0	0.0%
	Other	14	2.8%	5	1.7%	1	2.3%

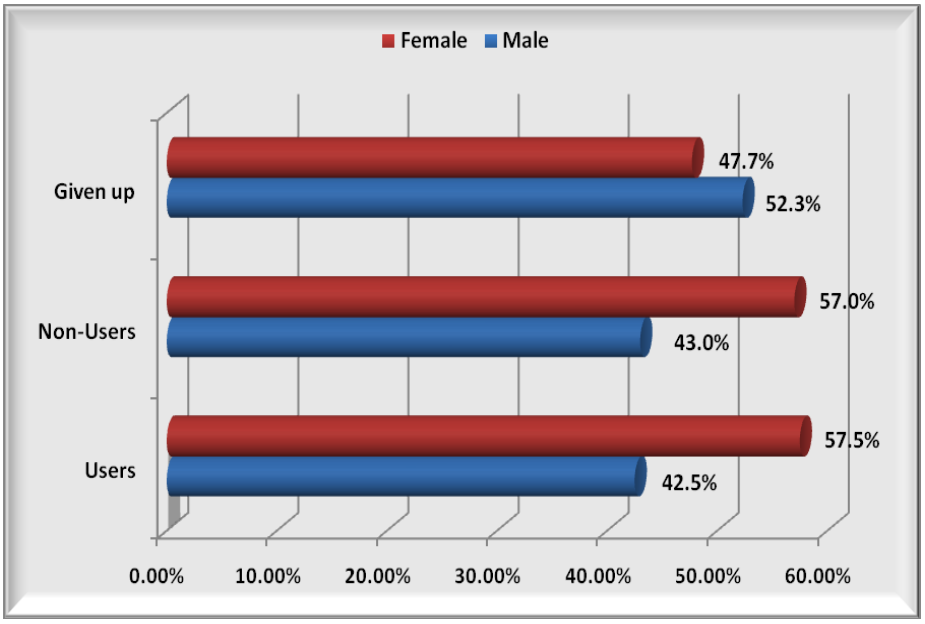


Figure (22): Gender Percentage Distribution of Users, Non-Users and Abandoned of Internet Banking

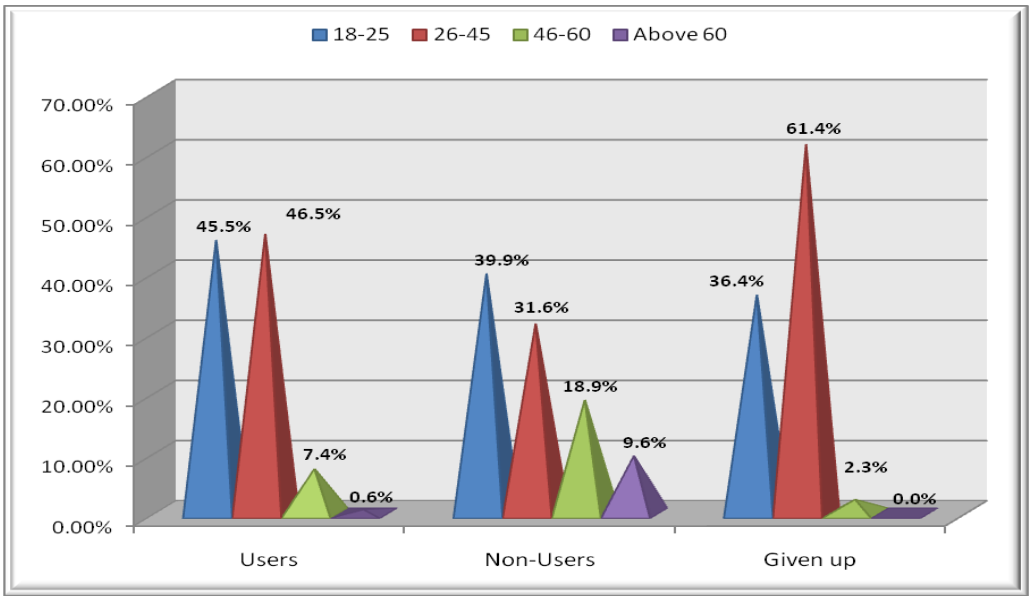


Figure (23): Age Percentage Distribution of Users, Non-Users and Abandoned of Internet Banking

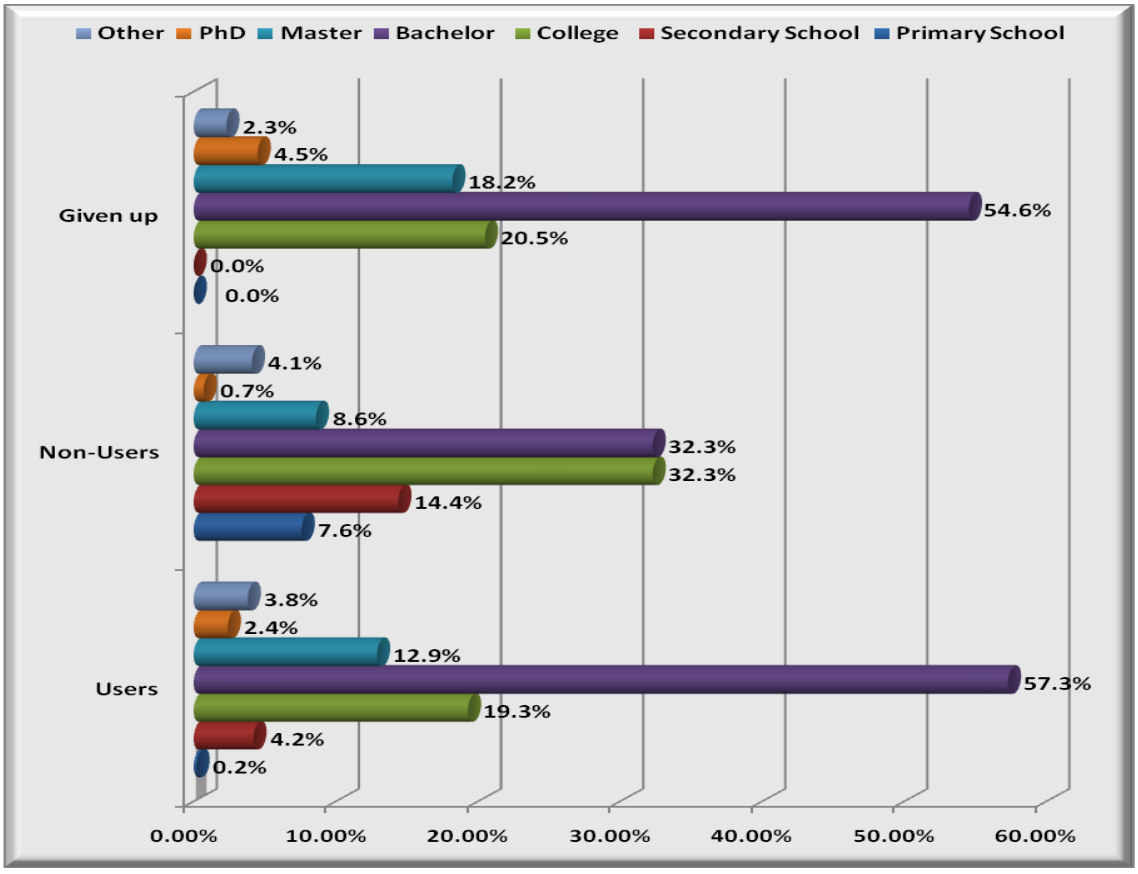


Figure (24): Education Percentage Distribution of Users, Non-Users and Abandoned of Internet banking

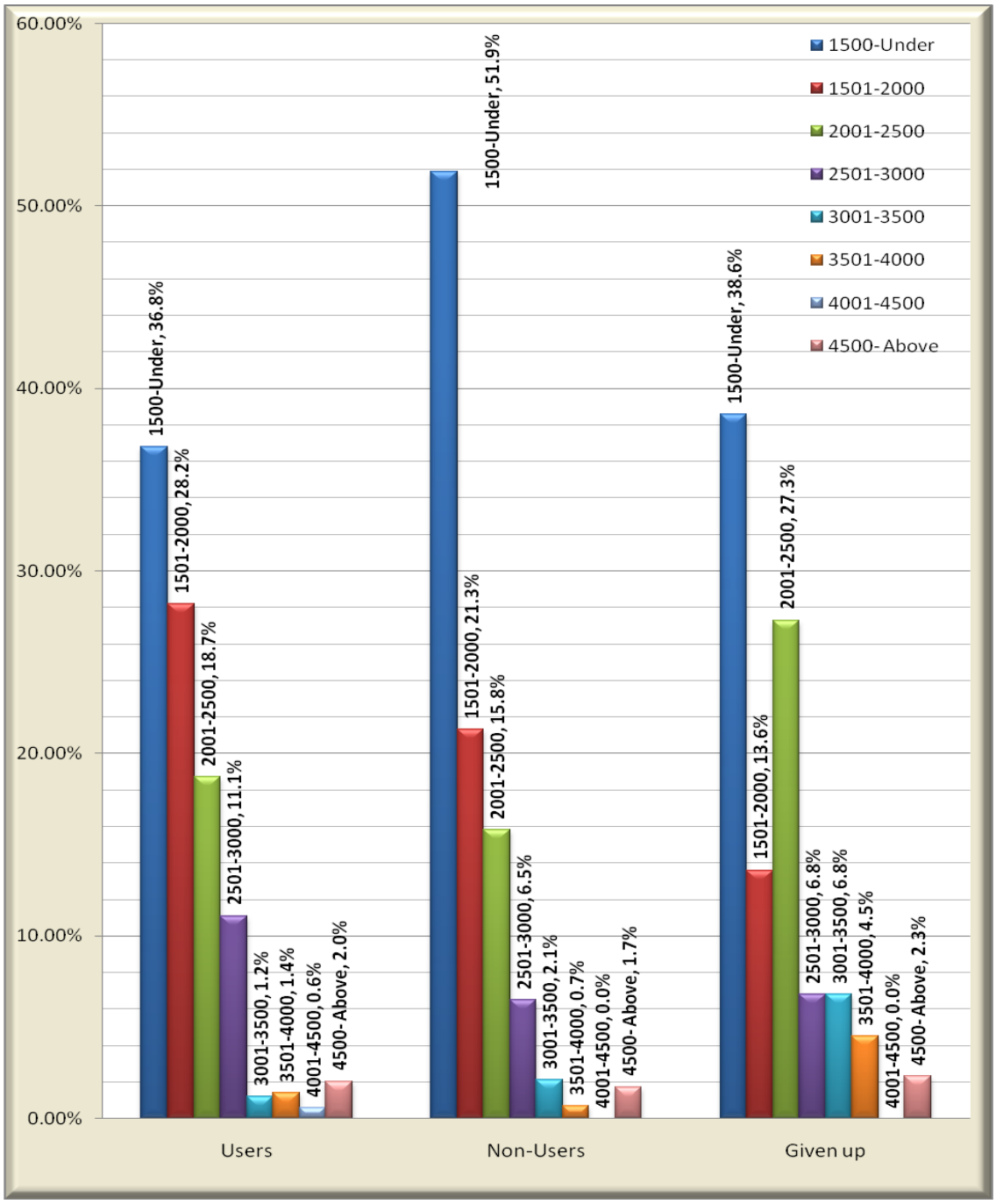


Figure (25): Income Percentage Distribution of Users, Non-Users and Abandoned of Internet Banking

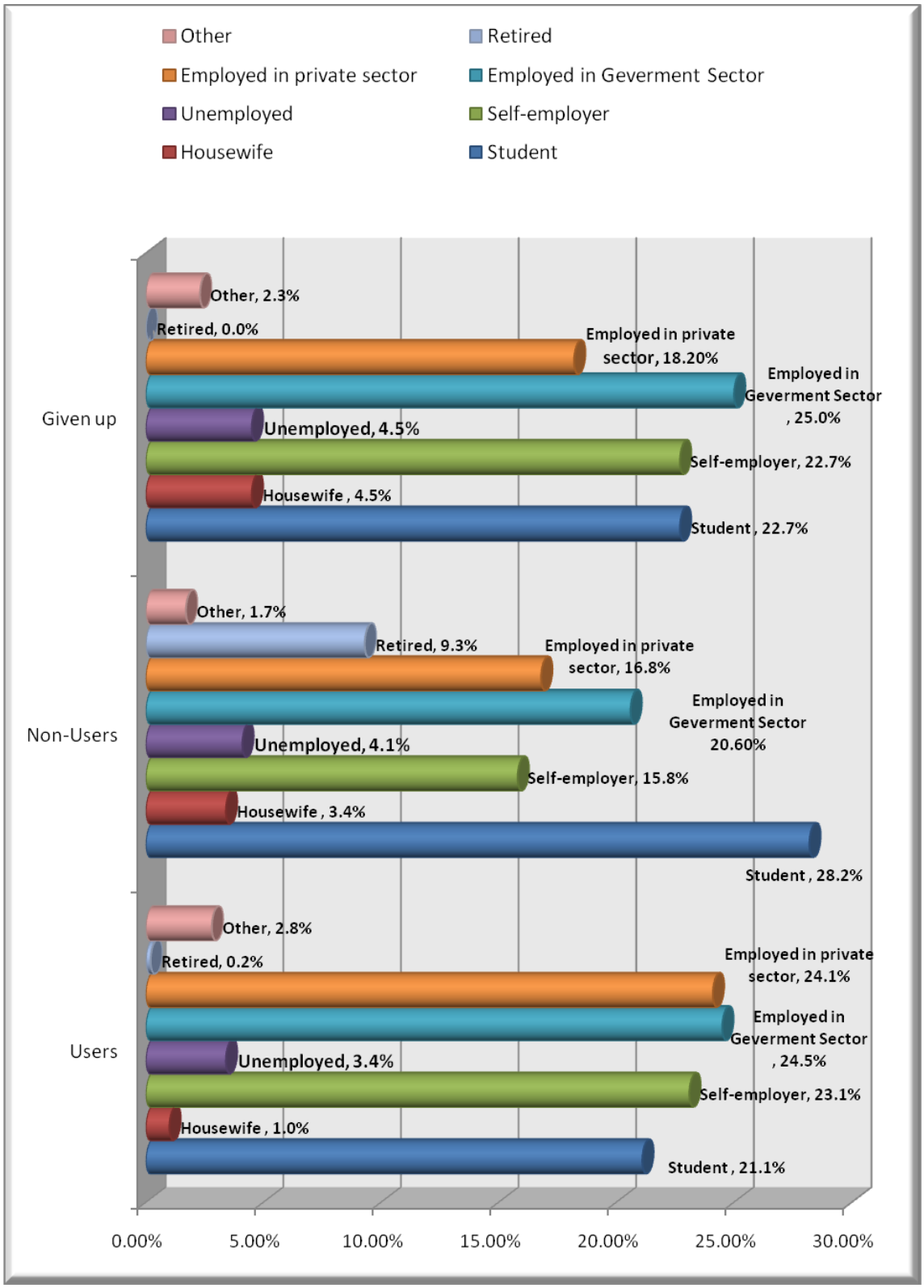


Figure (26): Occupation Percentage Distribution of Users, Non-Users and Abandoned of Internet Banking

5.5 RELATIONSHIPS BETWEEN TRUST, SECURITY AND RISK WITH DEMOGRAPHIC CHARACTERISTICS OF CUSTOMERS.

5.5.1 THE RELATIONSHIP BETWEEN TRUST, SECURITY, RISK AND THE DEMOGRAPHIC CHARACTERISTICS OF INTERNET BANKING SERVICES NON-USERS

The output of the study implied a weak correlation between the separate demographic characteristics of non-user customers' trust, security, and perceived risk. Trust in gender performed as (R= 0.126), with weak relationships to both genders. It is notable that the evidence established trust as being higher amongst users who were female as opposed to male. Along the same lines, the following were found to be equal: Age (R= 0.244); Education (R= - 0.112); Income (R= 0.089); Occupation (R= 0.160).

However, issues of security indicated the following: Gender (R= 0.056); Age (R= 0.220); Education (R=- 0.106); Income (R= -0.010); Occupation (R= 0.099). Likewise, issues of risk were represented as follows: Gender (R= 0.080); Age (R= 0.219); Education (R= - 0.107); Income (R= -0.015); and Occupation (R= 0.126). On the other hand, there was a relationship between these factors and their combined demographic characteristics, with the output of the correlations being (R=0.286) (R= 0.243) (R=0.249).

In addition, the sig values cross referencing of ANOVA tables offered values less than 0.05. Thus figures of (ANOVA p= 0.000), (ANOVA p= 0.004), (ANOVA p= 0.003) revealed the variables being statistically significant. Furthermore, the values of (R2) are (R2 = 0.082), (R2 = 0.059), (R2 = 0.062), implying that the model (which includes demographic characteristics) explains 8.2%, 5.9%, 6.2% of the variance in three factors, respectively (i.e. trust, security and perceived risk) (see appendix B1). Henceforth, weak

values forge unacceptable results. Thus, in brief, the research found weak relationships between the demographic characteristics of Internet Banking non-users, and trust, security and perceived risk.

5.5.2 RELATIONSHIP BETWEEN TRUST, SECURITY, RISK AND THE DEMOGRAPHIC CHARACTERISTICS OF INTERNET BANKING SERVICES ABANDONERS.

This section discusses the correlation between the demographic characteristics of abandoners of Internet banking services and the three factors of trust, security and perceived risk, with the trust relationship with gender being (R=- 0.199). Thus a weak negative relationship was established, although there were higher levels of trust in the use of Internet banking services among male, in comparison to female, users. In addition, the findings were recorded as: Age (R= 0.128); Education (R= 0.088); Income (R= 0.019); Occupation (R= 0.082).

Moreover, the relationship with security was demonstrated as follows: Gender (R=- 0.072); Age (R= 0.074); Education (R= -0.018); Income (R= - 0.016); Occupation (R= 0.081). The perceived risk was represented as follows: Gender (R=- 0.031); Age (R= - 0.198); Education (R= 0.173); Income (R= -0.065); and Occupation (R= 0.192). In addition, the summary of the model confirmed a weak relationship to Trust (R= 0.296); Security (R= 0.149); Risk (R= 0.354), with the demographic characteristics combined.

Furthermore, the ANOVA value was greater than 0.05, indicating the non-contribution of the demographic characteristics to the prediction of dependent variables (i.e. trust, security and perceived risk), giving a remarking of (ANOVA p=0.607), (ANOVA p=0.972) and (ANOVA p=0.384) (see appendix B2).

The value of the coefficient of determination (R2) is as follows: (R2 = 0.087), (R2 = 0.022), (R2 = 0.125), referring to 8.7%, 2.2% and 12.5%. This implies that the demographic characteristics of the users of Internet Banking services can establish the following variance: trust (8.7%), security (2.2%) and perceived risk (12.5%). Thus, a weak relationship is established between the demographic characteristics of abandoners of Internet banking services, and trust, security and perceived risk.

5.5.3 RELATIONSHIP BETWEEN TRUST, SECURITY, RISK AND THE DEMOGRAPHIC CHARACTERISTICS OF INTERNET BANKING SERVICES USERS.

The correlation of demographic characteristics with trust reveals gender as R= - 0.112, despite, the relationship being weak between the genders. However, trust in Internet banking was higher among male users than females, as well as when tracked in relation to the following: Age (R=0.025); Education (R= 0.023); Income (R= -0.020); Occupation (R= 0.000). Security was expressed as; Gender (R= - 0.095); Age (R= - 0.031); Education (R= - 0.22); Income (R= - 0.007); and Occupation (R= -0.001). However, risk was expressed in terms of: Gender (R=-.050), Age (R=0.083), Education (R= - 0.106), Income (R= 0.078), Occupation (R=0.019).

In general, the summary of the models reveals combined demographic characteristics of very weak correlations with trust, security and perceived risk, which are (R= 0.124), (R= 0.109), (R= 0.156), respectively. Additionally, R Square gives weak and unacceptable values to that of (R2 = 0.015), (R2 = 0.012), and (R2 = 0.024). This indicates that the demographic characteristics of Internet Banking service users explains

1.5% of the variance in trust, 1.2% of the variance in the security, and 2.4% of the variance in perceived risk (see appendix B3).

Furthermore, in order to assess the statistical significance of the findings, it is important to establish ANOVA values for these factors. These are highlighted as (ANOVA p=0.174), (ANOVA p=0.307), (ANOVA p=0.032) being statistically insignificant. Thus the demographic characteristics do not contribute significantly to the prediction of the variables relating to trust, security and perceived risk, exhibiting a very weak relationship between the demographic characteristics of Internet banking users' trust, security and perceived risk. The next section will discuss general Internet usage trends.

5.6 GENERAL INTERNET USAGE TRENDS

5.6.1 NATIONALITY OF SAMPLE STUDY

Further evidence in relation to all respondents is demonstrated in Figure 27. The sample of Internet banking users consists of 83.1% British citizens, with 16.9% being Non-British. The sample of non-users consists of 82.5% British citizens and 17.5% non-British citizens. The sample of service abandoners was consists of 86.4% British citizens and 13.6% non-British citizens. Thus, the average of all respondents consists of: 84% British citizens and 16% non-British citizens (i.e. individuals who, at the time of the study being conducted in Leicester City, were living in Britain but did not possess British nationality).

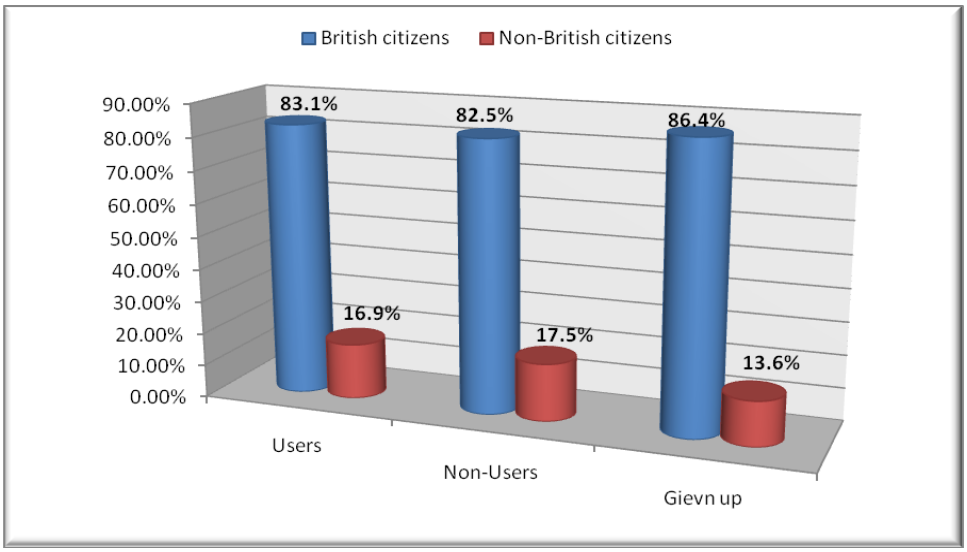


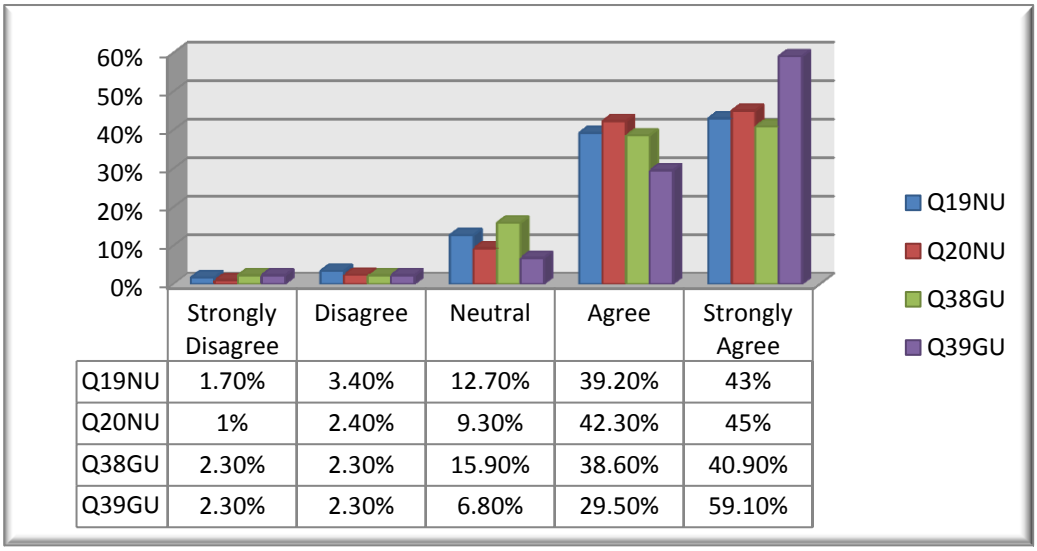
Figure (27): Nationality of sample study

5.6.2 NON-USERS AND ABANDONERS' PERCEPTIONS OF ATM AND BRANCH BANKING

Figure 28 illustrates 291 Internet banking non-users, evidencing a strong positive impression of cash machines (ATMs) and branch banking. 82.2% (strongly agree) and 87.3% (agree) were satisfied, and had confidence in both cash machines and branch banking. 17.27% and 12.7% were between strongly disagree, disagree and neutral. Abandoners in the sample totalled 44, with 80% and 89% highlighting satisfaction and confidence in cash machines and branch banking, respectively. However, 20% and 11% also had results within strongly disagree, disagree and neutral in relation to the usage of ATMs and branch banking.

The above respondents appear that there are satisfaction and confidence for non-users and abandoners toward cash machines and branches banking. However, Figure 28 reveals moderate dissatisfaction and non-conviction with cash machines and branches banking usage amongst some non-users. Thus an opportunity has arisen to attract these

customers to use Internet banking, due to their lack of satisfaction with ATM and branch banking. In order for this to take place, there is a need to establish solutions to the issues preventing them from using Internet banking, enabling them to improve their confidence towards an Internet Banking service.



	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q19NU	1.70%	3.40%	12.70%	39.20%	43%
Q20NU	1%	2.40%	9.30%	42.30%	45%
Q38GU	2.30%	2.30%	15.90%	38.60%	40.90%
Q39GU	2.30%	2.30%	6.80%	29.50%	59.10%

Figure (28) Non-users and Abandoners' Perceptions of ATM and Branch Banking

5.6.3 NON- INTERNET BANKING USERS BEHAVIOUR

The statistics of non-users of Internet banking in Figure 29 offer the following considerations:

- 43.6% of the sample use the Internet frequently.
- 17.9% of the sample use it sometimes.
- 16.5% of the sample use it often.
- 12.7% of the sample never use the Internet.
- 9.3% of the sample use the Internet infrequently.

Considering the previously noted total percentages of never and rarely, it is clear that: 22% of the sample do not use the Internet; 17.9% use it sometimes (thus inferring non-use of Internet banking). 60.1% of those who use the Internet frequently have yet to adapt to Internet banking. This indicates that the Internet is available, independent of financial capacity or any physical disability.

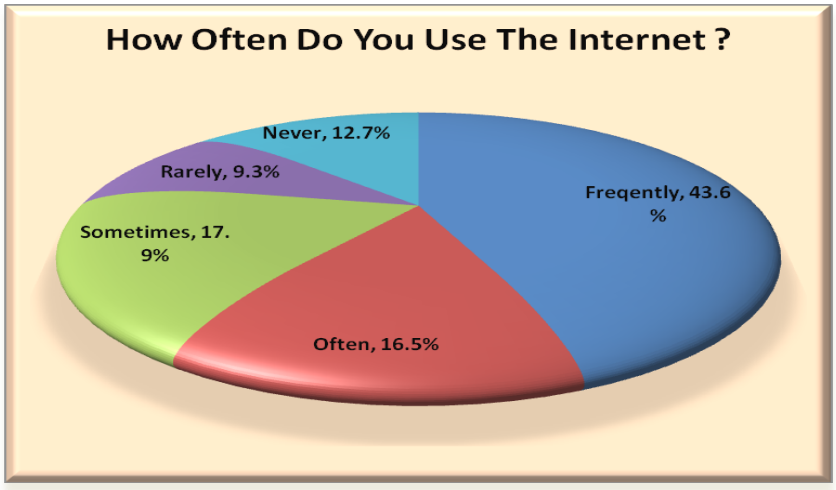


Figure (29): Internet banking Non-Users usage Percentage Distributions

5.6.4 EXPERIENCE OF USING INTERNET BANKING

Figure 30 illustrates the length of experience of active users of Internet banking, as follows: 18.3% were between 1-2 years; 72% between 1-6 years; 34% between 3-4 years; 19.7% between 5-6 years; 6.4% between 7-8 years; 10% between 9-10 years; and 11.7% 11 years and above. These appear to be relatively rational against age sample percentiles of 18-25 (45.5%) and 26-45 (46.5%).

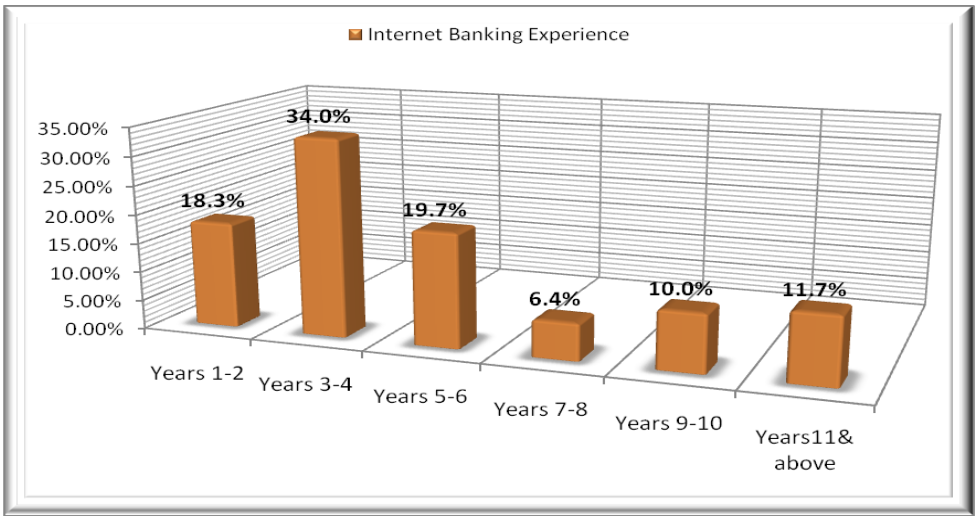


Figure (30): Internet banking experience of the respondents

5.6.5 CONTINUED BANK BRANCH USAGE BY INTERNET BANKING USERS

Table 8 reveals that 91.7% of Internet banking users still use a branch of their bank, with only 8.3% solely relying on online services.

Further questions were posed to rationalise branch behaviour, as described below. 64.4% visited the branch in order to make deposits; 41.7% to discuss banking services unavailable online; 22.9% for banking support and queries; 41.4% to make large cash withdrawals; 2% for card related issues and resolutions (e.g. lost card, new card application, blocked card and pin change); 0.9% for payments; 0.9% for transfers of money; 0.70% to pay a cheque; 0.43% to discuss applications and queries for mortgages and other loans. The next section will discuss the normality test.

Table (8): Percentage Distribution of Sample study (Users Internet banking) If they have visited their bank branch since adopted the services

Have you ever visited your bank Branch since the time you started using Internet Banking?		
Yes	461	91.7%
No	42	8.3%
Total	503	100%

5.7 TESTING THE ASSUMPTION OF NORMALITY

Based on the measurement scale of the variables involved, hypothesis testing procedures can be divided into two tests: (1) parametric; (2) non-parametric. Parametric tests assume the variables concerned are interval scale measured, while non-parametric tests assume that the variables are measured in relation to nominal or ordinal scaling (Malhotra et al., 2012).

Prior to the performance of any statistical analysis, it is important establish that the collection of the data does not violate any of the assumptions upon which a particular statistical test is based. This is due to the fact that an important violation of normality can give considerable misrepresentation of the values of correlations and the results of statistical inference tests (Adapa, 2011). Normality is the primary assumption to be assessed before performing any analysis. This assessment can range from using two statistical tests, to inferential tests of normality, i.e. Skewness (which indicates distribution symmetries) and Kurtosis (which indicates distribution peak insights) (Pallant, 2010).

Park (2008) states that Skewness and Kurtosis values indicate normal distribution if they fall within the range of -3 to +3. Likewise, a study in North Carolina State University by Garson (2012), established that Skewness and Kurtosis should be within the +2 to -2 range in normally distributed data, adding that some studies that are more lenient to the above rule, noting +3 to -3. Hair et al. (2006) also note that Skewness and Kurtosis should be within these ranges:

The Skewness absolute value <= 30.0

The Kurtosis absolute value <=10.0

The results of both the Skewness and Kurtosis tests for this study reveal that the distributions of all variables are normal and satisfied. Tables (9.1) (9.2) (9.3) (9.4) demonstrate the results and the value of each test as the average of each construct.

The Kolmorogov-Smirnov (K-S) test was normal. A value above 0.05 indicates normality, while if the test is significant (i.e. less than 0.05) then data is non-normal (Malhotra et al., 2012). In the current case, the test indicates the data as being non-normal, with the significant value being .000, suggesting a violation of a normality assumption. However, Garson (2012) and Pallant (2010) note this is a common occurrence in large samples. The checking for outliers also has been discussed in next section.

Table (9-1): Assessment of Normality

Items		Skewness		Kurtosis		K-S value	
		Statistics	Std. Error	Statistics	Std. Error	Statistics	Sig
Internet Banking non –users:							
Trust	Q1	- 0.843	0.143	0.440	0.285	0.254	.000
	Q2	-0.608	0.143	-0.411	0.285	0.270	.000
	Q3	-0.436	0.143	-0.774	0.285	0.249	.000
	Q4	-0.554	0.143	-0.499	0.285	0.256	.000
	Q5	-0.495	0.143	-0.634	0.285	0.239	.000
	Q6	-0.464	0.143	-0.290	0.285	0.250	.000
Security	Q7	-0.818	0.143	0.443	0.285	0.265	.000
	Q8	-0.172	0.143	-0.495	0.285	0.211	.000
	Q9	-0.410	0.143	-0.586	0.285	0.247	.000
	Q10	-0.680	0.143	-0.150	0.285	0.241	.000
	Q11	-0.401	0.143	-0.375	0.285	0.252	.000
	Q12	-0.475	0.143	-0.366	0.285	0.264	.000
Risk	Q13	-0.529	0.143	-0.425	0.285	0.258	.000
	Q14	-0.645	0.143	-0.020	0.285	0.258	.000
	Q15	-0.25	0.143	-0.795	0.285	0.180	.000
	Q16	-0.504	0.143	0.017	0.285	0.286	.000
	Q17	-0.371	0.143	-0.577	0.285	0.233	.000
	Q18	-0.104	0.143	1.095	0.285	0.272	.000

Table (9-2): Assessment of Normality

Items		Skewness		Kurtosis		K-S value	
		Statistics	Std. error	Statistics	Std. error	Statistics	Sig
Abandoning of Internet Banking:							
Trust	Q22	-0.214	0.357	-0.789	0.702	0.238	.000
	Q23	-0.520	0.357	-0.340	0.702	0.261	.000
	Q24	-0.137	0.357	-0.762	0.702	0.211	.000
	Q25	-0.354	0.357	-0.600	0.702	0.262	.000
	Q26	-0.175	0.357	-0.978	0.702	0.265	.000
Security	Q27	-0.646	0.357	0.058	0.702	0.297	.000
	Q28	-0.108	0.357	1.207	0.702	0.345	.000
	Q29	0.282	0.357	-0.068	0.702	0.287	.000
	Q30	-1.042	0.357	1.57	0.702	0.331	.000
	Q31	-0.263	0.357	-1.06	0.702	0.269	.000
Risk	Q32	0.102	0.357	-0.470	0.702	0.240	.000
	Q33	-0.243	0.357	-0.955	0.702	0.247	.000
	Q34	-0.827	0.357	1.56	0.702	0.382	.000
	Q35	-0.448	0.357	-0.419	0.702	0.274	.000
	Q36	-0.193	0.357	-1.47	0.702	0.290	.000
	Q37	0.434	0.357	-0.738	0.702	0.250	.000

Table (9-3): Assessment of Normality

Items		Skewness		Kurtosis		K-S value	
		Statistics	Std. error	Statistics	Std. error	Statistics	Sig
Users Internet Banking :							
Trust	Q40	-0.813	0.109	1.95	0.217	0.317	.000
	Q41	0.063	0.109	-0.716	0.217	0.187	.000
	Q42	-0.452	0.109	-0.247	0.217	0.280	.000
	Q43	-0.407	0.109	-0.722	0.217	0.239	.000
	Q44	-0.704	0.217	0.774	0.217	0.323	.000
	Q45	-0.967	0.109	2.24	0.217	0.314	.000
	Q46	-1.052	0.109	1.22	0.217	0.267	.000
	Q47	0.175	0.109	-0.597	0.217	0.247	.000
Security	Q48	0.326	0.109	-0.843	0.217	0.232	.000
	Q49	-0.442	0.109	0.316	0.218	0.309	.000
	Q50	-0.640	0.109	1.72	0.217	0.349	.000
	Q51	0.023	0.109	-0.322	0.217	0.218	.000
	Q52	-0.690	0.109	0.323	0.217	0.296	.000
	Q53	-0.233	0.109	-0.800	0.217	0.185	.000
Risk	Q54	0.535	0.109	-0.065	0.217	0.267	.000
	Q55	-0.074	0.109	-0.572	0.217	0.210	.000
	Q56	-0.011	0.109	-0.866	0.217	0.194	.000
	Q57	0.091	0.109	-0.922	0.217	0.221	.000
	Q58	-0.488	0.109	-0.367	0.217	0.275	.000
	Q59	-0.541	0.109	-0.093	0.217	0.282	.000
	Q60	-0.111	0.109	-0.442	0.217	0.223	.000
	Q61	-0.019	0.109	-0.619	0.217	0.207	.000
Continuity	Q62	-1,24	0.109	1.70	0.217	0.292	.000
Question C	QC1	1.065	0.109	-0.80	0.217	0.363	.000
	QC2	0.650	0.109	-1.58	0.217	0.320	.000
	QC3	0.398	0.109	1.44	0.217	0.387	.000
	QC4	-0.25	0.109	-1.94	0.217	0.373	.000
	QC5	-0.41	0.109	-1.83	0.217	0.393	.000

Table (9-4): Assessment of Normality

Items		Skewness		Kurtosis		K-S value	
		Statistics	Std. Error	Statistics	Std. Error	Statistics	Sig
Users Internet Banking: (Continue...)							
Question C	QC6	0.892	0.109	-1.020	0.217	0.354	.000
	QC7	-0.319	0.109	-1.600	0.217	0.382	.000
	QC8	-0.568	0.109	-1.654	0.217	0.411	.000
	QC9	-0.156	0.109	-1.784	0.217	0.361	.000
	QC10	-0.664	0.109	-1.422	0.217	0.332	.000
Question D	QD1	0.754	0.109	-1.111	0.218	0.322	.000
	QD2	0.713	0.109	-1.151	0.218	0.332	.000
	QD3	1.034	0.109	-0.735	0.218	0.332	.000
	QD4	0.233	0.109	-1.003	0.218	0.350	.000
	QD5	-0.720	0.109	-1.132	0.218	0.323	.000
	QD6	-0.399	0.109	-1.323	0.218	0.391	.000
	QD7	-0.416	0.109	-1.342	0.218	0.393	.000
	QD8	-0.574	0.109	-1.234	0.218	0.275	.000
	QD9	0.201	0.109	-1.033	0.218	0.365	.000
	QD1	-0.372	0.109	-1.303	0.218	0.376	.000
Question E	QE1	1.233	0.109	-0.456	0.217	0.374	.000
	QE2	-0.361	0.109	-1.332	0.217	0.387	.000
	QE3	1.322	0.109	-0.098	0.217	0.384	.000
	QE4	-0.938	0.109	-1,125	0.217	0.349	.000
	QE5	0.278	0.109	-1.432	0.217	0.376	.000
	QE6	-0.221	0.109	-1.122	0.217	0.369	.000
Question F	QF1	0.504	0.109	-1.642	0.217	0.315	.000
	QF2	-0.336	0.109	-1.062	0.217	0.384	.000
	QF3	-1.203	0.109	-0.321	0.217	0.378	.000
	QF4	-0.352	0.109	-1.383	0.217	0.386	.000

5.8 CHECKING FOR OUTLIERS

Outliers consist of statistical data distinctly dissimilar from other observations within the dataset (Kline, 2011). Outliers are minority measures observations that do not parallel the rule of thumb. A small number of outliers will have a limited impact on this statistic. Statistical inferences are frequently based on tests of means in which the standard deviation is used as a measure of the normal fluctuation of the examined processes (Cousineau and Chartier, 2010). Furthermore, Kline (2011) indicates that the presence of a small number of outliers within a large sample size should be of only minor concern. Therefore, this decision is in line with Hair et al. (2006), who suggest the deletion of outliers for multivariate analysis optimisation, despite the fact that limiting generalisation manifests risk. Outliers consist of values noticeably distinguishable among the response values during data collection. Thus the importance of their detection prior to any advanced analysis (Kline, 2011).

Field (2009) and Hair et al. (2006) note that the most common detection techniques concern an examination of the scores of standard deviations, i.e. inspecting the value around the mean. Therefore, cases greater than three standard deviations are regarded as outliers, as supported by the outliers tested as above, as supported by the results in Table 10. The confirmation of non-outlier cases among studies of data suggest the range is satisfied. Furthermore, outliers can be explored by comparing the trimmed mean to the mean, in order to establish any variation between the trimmed mean and mean rates. The study may need to further examine these data points, with the presence of mean signifying outliers, while if the values are similar, the data lacks outliers (Pallant, 2010). In this current study, the two mean values are very similar, thus establishing that there are no outlier cases among the data.

Table (10-A): Outlier descriptive assessment

Variable			Mean	Std. D	Trimmed Mean
Non-users Internet banking	Trust	Q1	3.90	1.003	3.94
		Q2	3.74	1.034	3.78
		Q3	3.75	1.005	3.78
		Q4	3.85	0.964	3.89
		Q5	3.84	0.978	3.88
		Q6	3.88	0.878	3.92
	Security	Q7	4.08	0.843	4.15
		Q8	3.65	0.906	3.67
		Q9	3.85	0.901	3.89
		Q10	3.13	0.856	4.18
		Q11	4.03	0.779	4.06
		Q12	3.79	0.862	3.94
	Risk	Q13	3.79	0.964	3.83
		Q14	3.74	0.996	3.80
		Q15	3.24	1.039	3.24
		Q16	3.96	0.780	4.01
		Q17	3.80	0.927	3.83
		Q18	3.87	0.878	3.90
		Q19	4.18	0.905	4.18
		Q20	4.32	0.810	4.36
Abandoning of Internet Banking	Trust	Q22	3.34	1.033	3.35
		Q23	3.25	0.866	3.28
		Q24	3.18	1.063	3.20
		Q25	3.36	0.990	3.37
		Q26	3.39	0.945	3.37
	Security	Q27	3.55	0.951	3.57
		Q28	3.64	0.865	3.68
		Q29	3.20	0.765	3.18
		Q30	3.55	0.791	3.58
		Q31	3.25	0.839	3.25

Variable			Mean	Std. D	Trimmed Mean
Abandoning of IB	Risk	Q32	3.32	0.829	3.30
		Q33	3.16	0.713	3.18
		Q34	3.82	0.657	3.85
		Q35	3.41	0.972	3.42
		Q36	3.18	0.922	3.18
		Q37	3.23	0.985	3.20
		Q38	4.14	0.930	4.23
		Q39	4.41	0.897	4.53
Users of Internet Banking	Trust	Q40	4.09	0.688	4.13
		Q41	3.09	0.954	3.07
		Q42	3.53	0.898	3.55
		Q43	3.52	1.107	3.57
		Q44	3.94	0.763	3.99
		Q45	4.10	0.718	4.16
		Q46	4.15	0.842	4.23
		Q47	3.12	0.788	3.10
	Security	Q48	2.53	1.118	2.50
		Q49	3.61	0.725	3.62
		Q50	3.91	0.653	3.93
		Q51	3.03	0.890	3.02
		Q52	3.88	0.856	3.93
		Q53	3.56	1.097	3.60
	Risk	Q54	2.43	0.952	2.39
		Q55	2.97	0.861	2.98
		Q56	2.89	1.059	2.89
		Q57	2.93	1.019	2.93
		Q58	3.36	0.938	3.36
		Q59	3.74	0.898	3.78
		Q60	3.06	0.821	3.07
		Q61	3.01	0.841	3.01
	Continuity	Q62	4.15	0.792	4.23

Table (10-B): Outlier descriptive assessment

Variable		Mean	Std. D	Trimmed Mean		Variable		Mean	Std. D	Trimmed Mean
Users of Internet banking: (Continue)										
Question C	QC1	1.26	1.24	0.439		Question D	QD1	1.29	1.27	0.453
	QC2	1.35	1.34	0.476			QD2	1.29	1.27	0.456
	QC3	1.33	1.32	0.633			QD3	1.27	1.26	0.445
	QC4	1.56	1.57	0.497			QD4	1.48	1.48	0.500
	QC5	1.60	1.61	0.490			QD5	1.69	1.70	0.463
	QC6	1.28	1.27	0.449			QD6	1.60	1.61	0.491
	QC7	1.58	1.59	0.494			QD7	1.60	1.61	0.490
	QC8	1.64	1.65	0.482			QD8	1.64	1.65	0.481
	QC9	1.54	1.54	0.499			QD9	1.45	1.44	0.498
	QC10	1.68	1.69	0.468			QD10	1.59	1.60	0.492
Question E	QE1	1.24	1.23	0.426						
	QE2	1.59	1.60	0.493						
	QE3	1.22	1.20	0.412		Question F	QF1	1.36	1.35	0.470
	QE4	1.71	1.73	0.453			QF2	1.58	1.59	0.480
	QE5	1.43	1.42	0.487			QF3	1.70	1.72	0.420
	QE6	1.55	1.56	0.490			QF4	1.59	1.60	0.490

5.9 RELIABILITY AND VALIDITY OF THE INSTRUMENT

Prior to a further discussion of the statistical analysis, the reliability and validity of the constructs must first be examined, in order to ensure the validity of the instrument. Thus the avocation to incorporate Cronbach's alpha (α) as research best practice, employing internal consistency indicators with the underpinning of SPSS software techniques.

The method measures reliability coefficients between consistency items. Similarly, Cronbach's 0.6 Alphas (or significant) would be valuable and its veracity considered (Bryman, 2012; Pallant, 2010). Additionally, item values of Inter-Item correlation matrix should be regarded as positive.

Moreover, factor analysis commonly complements research in establishing data validity, verification and suitability. As affirmed by (KMO), values below 0.6, or above in accordance with Bartlett's test of Sphericity, are significant in the range of .05 or .000 (Pallant, 2010). This point has been previously discussed at length in the section focussing on the pilot study. Thus the construct reliability and validity for the main data of the study will be appropriately detailed in the following section.

5.9.1 CONSTRUCT RELIABILITY

As revealed in Table 11, the factor reliability of part of this research scored from 0.600 to 0.73, apart for QD, which highlighted slightly low reliability. However, these values are deemed acceptable, as ranging from moderate to good, in accordance with the recommendations of researchers.

When it comes to the QD from factors of current users of Internet banking, the table reveals that the scale is slightly less than the required range >0.6. This could, however, be due to the small number of items.

Thus, Cronbach's Alpha values (as shown in the table) are above 0.6, suggesting good internal consistency reliability. Furthermore, Inter-Item Correlation Matrix tables show that all values are positive, thus indicating measurement items have the same underlying characteristic. In summary: from all of above factors, it is deemed that Cronbach's Alpha Values are acceptable.

Table (11) Reliability (Cronbach's Alpha) of the present study (N = 838)

Factors Measured	Cronbach's Alpha Values	Number of items
Factors of Non-users of Internet banking:		
Trust	0.841	6
Security	0.806	6
Risk	0.722	6
Factors of abandoned users of Internet banking:		
Trust	0.737	5
Security	0.811	5
Risk	0.622	6
Factors of current users of Internet banking:		
Trust	0.700	8
Security	0.658	6
Risk	0.600	8
Continuity	0.600	4
QC	0.700	10
QD	0.500	10
QE	0.780	6
QF	0.600	4

5.9.2 VALIDITY

Pallant (2010) states that KMO 0 to 1 with 0.6 index ranges good minimum factor analysis propositions. In addition, Hair et al. (2006) identify that an item with a loading of >0.5 should be accepted. In this current research, the findings of the factor analysis in accordance with KMO and Bartlett's Test indicate that the data is suitable for factor analysis and construct loadings, located between 0.6 and 0.05, and Bartlett's Test of sphericity value cements the aforementioned notion (see Table 12).

Table (12) Validity (Factor analysis) of the present study (N =838)

Construct Measured	No. of items	Kaiser-Meyer-Olkin Measure of Sampling Adequacy[KMO]	Bartlett's Test of Sphericity
Items of Non-users of Internet banking:			
Trust	6	0.839	P=.000
Security	6	0.814	P=.000
Risk	6	0.750	P=.000
Items of abandoned users of Internet banking:			
Trust	5	0.705	P=.000
Security	5	0.718	P=.000
Risk	6	0.620	P=.000
Items of current users of Internet banking:			
Trust	8	0.800	P=.000
Security	6	0.700	P=.000
Risk	8	0.700	P=.000
Continuity	4	0.636	P=.000
QC	10	0.632	P=.000
QD	10	0.600	P=.000
QE	6	0.600	P=.000
QF	4	0.630	P=.000

5.10 THE EXPECTED RESEARCH RESULTS

In general, it is expected that the research results will contribute to an enhanced understanding of the behaviour patterns of existing bank customers towards Internet banking services in the UK; in the post-adoption phase (continued use and abandonment of use) and in the pre-adoption stage (non-adoption of use). Furthermore,

the study will be adding to the growing technology acceptance literature, through developing theoretical models of Internet banking services. First of all, with regard to the conceptual framework for the non-adoption of Internet banking, this study expects to find that numerous customers are still non-adopters of the services. It is expected also that customers' trust, security and perceived risk from important factors are behind these attitudes and there is a strong correlation between customers' behaviour for non-adoption of Internet banking services and these factors. In addition, this study believes that there are other factors behind the non-adoption of services, but these are less important than factors already mentioned.

In respect to the abandonment of the Internet banking model, this study predicts it will be difficult to find, those who abandon Internet banking among the study sample members. Or it may there will be too few non-adopters. This expectation is because, after reviewing the literature related to Internet banking in the UK, no study could be found specifically related to the abandonment of services, to the best of the researcher's knowledge; however there are indications which refer to this phenomenon. Thus, this model aims to research this issue, even if the proportion of users who abandoned Internet banking in this study is relatively small, this matter needs to be studied, because as this service becomes more widespread it is likely that the numbers of abandoners will increase. It is therefore important to understand this phenomenon. Another expected outcome in this model is that there are strong correlations between the three factors (trust, security and perceived risk) and the abandonment of internet banking.

Furthermore, a framework for adoption and continued usage of Internet banking services will be developed. In this model the study expects that the relationship between the adoption of Internet banking and trust, security and perceived risk is weak. On the

other hand, it is expected that there will be a correlation between the continued usage of Internet banking in the future with trust, security and perceived risk.

The study will also develop a safety area model, and the expected benefits of this model will be to provide a safety region, which maximizes the productivity of Internet banking services in order to achieve a favourable financial climate that takes into account security, customer's trust and reduced perceived risks. This theoretical model aims to translate customers' and users' views and aspirations into percentages that will help to determine the safety zone. This model which is relatively new, will contribute to the body of literature (at least to the researcher's knowledge), by producing procedures that will be implemented by banks which will be recommend by customers, therefore enhancing the way Internet banking services work (as shown in figure 17). One the other hand, this model might face limitations in being implemented and validated due to its novelty. This model can therefore serve as a basis and a preliminary step to future studies in determining a safety area to utilise Internet banking services.

In short, the expected outcomes of this research are to provide a comprehensive assessment of the Internet banking system in the UK, through designing some models to highlight customers' behaviour in terms of adoption, non-adoption and abandonment of Internet banking services, and to attempt to develop a framework to provide a security region in which to exercise Internet banking services safely.

5.11 CHAPTER SUMMARY

This chapter has discussed the implementation of the framework. Firstly, there has been a discussion of the data collection procedures in the current research. It is clear that, as a fundamental data collection method, the questionnaire is the most suitable for gathering

the data. This data collection method is able to provide the researcher with a deep understanding of the phenomenon under investigation. This chapter has also clarified the construction abbreviations employed.

The descriptive statistics of the samples has established that the majority of respondents were users (60%), followed by non-users (34.7 %), followed by users who had abandoned Internet banking (5.3%). The descriptive analysis of the respondents' demographic profile found that the majority were women. The descriptive analysis also found that the majority of the respondents were educated, with most having an income located in category 'under 1500 to 2000,' and were employees in government and private sectors. Furthermore, this chapter has revealed the extent of the relationship between the demographic characteristics of customers of Internet banking with trust, security, and perceived risk.

When it comes to the use of Internet banking, the result of the descriptive analysis established that approximately 72% of the respondents had been using Internet banking services for 6 years, followed by 34% who had been using the service for 3-4 years. In addition, a test of the assumption of normality has been undertaken. The Skewness and Kurtosis values reveal that all variables fall within an acceptable range for normality. This study has also checked for outliers, finding no such cases amongst the data. Furthermore, in order to ensure content validity in this instrument research, all items have been subjected to the requirements of validity and reliability. From all of the above, it can be summarised that Cronbach's Alpha values are deemed acceptable, and have met the requirements of validity and reliability. Finally, there has been a discussion of the expected research results. The following chapter will discuss the research results and their implications.

CHAPTER 6: DISCUSSION

6.1 INTRODUCTION

This chapter presents a discussion of the variety of techniques, including the simple regression model, correlation model and descriptive statistics used in this study to carry out the statistical analysis, arrive at the research results, validate the study models and test the research hypotheses. The chapter will use the results of the quantitative analysis to support the discussion and it is therefore expected that this investigation will offer a better understanding of the reality of Internet banking in the UK, specifically in Leicester. This chapter also provides an explanation of the results achieved through all the study models used, namely the non-adoption model of Internet banking; the abandoning model of Internet banking and the adopting and predicting the continued use of Internet banking and safety area model for usage of internet banking.

Finally, this chapter also discusses the significant findings related to customers' non-adoption and abandoning; acceptance and continuing usage of Internet banking and the safety area model for Internet banking services. This chapter will also provide a summary of the research hypotheses.

6.2 DATA ANALYSIS TECHNIQUES HYPOTHESES

In this study, the initial vetting of data was done by subjecting the data to descriptive statistical analysis using SPSS software. Descriptive statistics bridge the measurement and understanding, incorporated in the initial phase of statistical analysis, to identify relationships and determine directions for further analysis. Furthermore, descriptive

statistics often use pictorial representation of the data to summarise a particular characteristic of a data sample (Adapa, 2011).

Several methods were used during this analysis. Specific methods were applied to particular phases in the analysis to establish validation and to ensure a precise instrument exists to collect the data. These methods comprise statistical tests developed on the basis of research questions selected to satisfy the formulated study hypotheses. Similarly, descriptive analysis suggests data for most of the variables are parametric, and the distribution of all variables is demonstrated by skewness and normality of Kurtosis tests.

The research study aimed to assess the realities of Internet banking service through an investigation of current customer behaviour, focusing on the impact of trust, risk and security on non-adoption, adoption and ceased Internet banking behaviours. The study also sought to identify the relationships between selected variables and proposed modelled impacts. The sections below are divided for analysis convenience into regression, correlation and descriptive statistics.

PART ONE: REGRESSION MODELS

The regression model is a method used to estimate the value of one of two variables by knowing the value of another variable underpinning the regression equation. There are three types of regression models namely, simple regression; multiple regression which is used to analyse relationships between single dependent variables and several independent variables and, last but not least, nonlinear regression which is a form of regression analysis with model combinations of parameters and founded on one or multiple independent variables (Hair et al., 2006).

The study used simple linear regressions which are defined as a way of predicting an outcome variable from one predictor variable (Field, 2009). Simply, put , dependent variable Y depends on one independent variable X, with the two variables (Y, X) being in a linear relationship. It should be noted that simple linear regressions are widely used statistical techniques for line regression of Y to X estimate as depicted below (Liu and Chen, 1998):

$$\mathbf{Y = A + BX}$$

Where Y: is dependent variable.
A: is a constant.
B: is slope.
X: is independent (predicator).

The regression model technique used incorporated five levels. Level one examined the relationship between non-adoption of internet banking and trust, risk and security individually.

Levels two, three and four investigated the relationship between abandon on, adoption and continued use of Internet banking with three variables and, lastly, level five, examined the relationship between the factors and their impact on one another. The regression analysis model comprises the model table supporting of R Square values. This value show how much variance in the dependent variable is explained by the independent variables (Pallant, 2010).

Statistical significance assessing results are referenced in ANOVA as sig marked values which define whether an equation is statistically significant and has a unique contribution. Thus, if the significant value is less than 0.05, the variable is making a significant unique contribution to the dependent variable predictions. If the significant

value is greater than 0.05, the variable is not making a significant unique contribution to the prediction of the dependent variable (Field, 2009).

PART TWO: CORRLATION MODEL

Correlation analysis exhibited variables mean value constructs and factors measures of values. The one-tailed Pearson's correlation coefficient (R2) is used for variables variance calculations. Correlation coefficients of digital scales measure relationships between two variables using the values -1 and +1. A positive relationship idealism indicating non relationships by 0 and -1. As such perfect negative idealism relationship by 1 indication (Hair et al., 2006).

The Pearson linear correlation coefficient is a commonly used statistical technique to determine whether two variables values are linearly related and extended. Consequently, the correlation coefficient (R) represents the linear relationship between two variables. A point to note is that a Pearson coefficient equated value of 0 does not necessarily mean that there is no correlation between two variables but rather that there is no non-linear correlation (Erdeljic et al., 2011).

Furthermore, there is no difference between a negative and a positive correlation. The minus refers to the relationship direction not to its strength. The strength of correlation of r = 0.5 and r = -0.5 is the same but in opposing directions (Cohen, 1988; Vaus, 2002; Pallant, 2010). The value guidelines are listed in Table 13 below.

Table (13) Interpretation of correlation values
The sources: (Cohen, 1988; Vaus, 2002; Pallant, 2010)

Coefficient, *r*		
Strength of Association	Positive	Negative
Small	0.1 to 0.29	-0.1 to -0.29
Medium	0.30 to 0.49	-0.30 to -0.49
Large	0.50 to 0.99	-0.5 to -0.99
A perfect Correlation	1	-1
No correlation	Zero	Zero

PART THREE: DESCRIPTIVE STATISTICS

Descriptive statistics are the numerical and graphical methods used to organise, display and analyse information (Fisher and Marshall, 2009). The descriptive statistics forms used to describe a variable in a sample are dependent on the level of measurement that has been used. They provide a quick summary of the characteristics of variables and measures using simple graphics. Descriptive analyses are the basis of virtually every quantitative data analysis. They allow the visualisation of the results.

- **Categorical Variables**

Categorical variables are descriptive statistics based on frequencies, highlighting respondent population numbers such as how many males and how many females were in the sample. "It does not make any sense asking for means, standard deviation etc. for categorical variables, such as sex or marital status" (Pallant, 2010, p.55). Descriptive statistics frequencies were used to test Hypothesis H5 regarding safety area establishment of Internet banking service performance. The next section will discuss the explanation of results.

6.3 EXPLANATION OF RESULTS

This section explains the research hypotheses used in the four models, namely: non-adoption model of Internet banking; abandoning model of Internet banking, adopting and predicting the continued use of service and safety area model for usage of Internet banking. Each part will present the hypotheses and the technique adopted to test it.

6.3.1 EXPLANATION OF THE MODEL NON-ADOPTION OF INTERNET BANKING

A simple regression analysis was employed to test the effects of independent variable sets on non-adoption of Internet banking as the dependent variable. Regression analysis was performed between non-adoption and the three factors individually, namely trust, security and risk. Table 14 displays the hypotheses testing outcomes of the simple regression analyses and ANOVA performed with non-adoption of Internet banking as a dependent variable.

Table (14): Simple Regression Analysis and ANOVA on dependent variable (Non-adoption of Internet banking)

Hypotheses	R	Type of Correlation	R Square	Sig. Value	Result
H1a: Trust affects customers' decisions/intentions regarding the non-adoption of Internet banking.	-0.673	Negative Strong	0.453	0.000	Supported
H1a: Security affects customers' decisions/ intentions regarding the non-adoption of Internet banking.	-0.689	Negative Strong	0.475	0.000	Supported
H1c: Risk affects customers' decisions/intentions regarding the non-adoption of Internet banking.	0.525	Positive Strong	0.276	0.000	Supported

DISCUSSION:

The R Square (R2) results in the model summary shows how much of the variance in the dependent variable is explained by independent variables. The value of the independent variables were Trust (R2 = 0.453), (ANOVA p=0.000), Security (R2 = 0.475), ANOVA (p=0.000) and Risk (R2 = 0.276); ANOVA (p=0.000). This means that trust, security and risk were respectively 45.3%, 47.5% and 27.65% of the variance in non-adoption Internet banking. Furthermore, all the ANOVA values are less than 0.05, making the variables statistically significant, meaning that these factors have contributed to Internet banking non-adoption.

Moreover, the correlation between Internet banking non-adoption and trust (its value = -0.673) and security (its value = -0.689) is negative. This means that an increase in these factors is linked to a decrease in the number of customers who did not adopt Internet banking, while a decrease in these factors is linked to an increase in the non-adoption Internet banking services. The correlation between risk and Internet banking non-adoptions (value = 0.525) is positive implying that increase in risk is linked to an increase in the number of customers who do not rely on Internet banking (see appendix A1). In sum, in light of the above, there is a significant relationship between non-adoption of Internet banking as a dependent variable and trust, security and risk as independent variables (see Figure 31). Thus, H1a, H1b and H1c hypotheses are fully accepted.

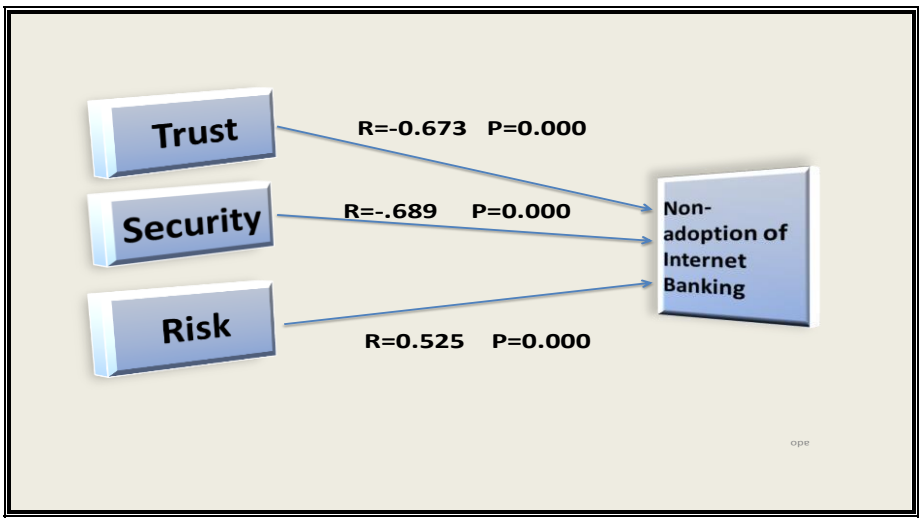


Figure (31): Research framework of customers' non-adoption of Internet banking with correlation coefficient (R) and P value.

6.3.2 EXPLANATION OF INTERNET BANKING MODEL ABANDONING

A simple regression and ANOVA were performed to predict the relationship between trust, security, risk and ceased behaviours. The test results of the relationships between abandoning of Internet banking as a dependent variable and the three factors (Trust, Security and Risk) as independent variables are given in Table 15. This is a relatively new area of investigation. The aim of this study is to find out whether there are any abandoners of Internet banking services in the UK. The proportion of users who abandoned Internet banking in this study is relatively small, but as Internet banking becomes more widespread it is likely that the numbers of abandoners will increase. It is therefore important to understand why users abandon Internet banking and specifically what role trust, security and perceived risk have in controlling or minimising abandonment.

Table (15) Simple Regression Analysis and ANOVA on dependent variable (Abandoning of Internet banking)

Hypotheses	R	Type of Correlation	R Square	Sig. Value	Result
H2a: Trust affects customers' decisions/intentions regarding the abandoning of Internet banking.	-0.696	Negative Strong	0.484	0.000	Supported
H2b: Security affects customers' decisions/intentions regarding the abandoning of Internet banking.	-0.710	Negative Strong	0.504	0.000	Supported
H2c: Risk affects customers' decisions/intentions regarding the abandoning of Internet banking.	0.466	Positive Moderate	0.217	0.001	Supported

DISCUSSION:

The R Square (R2) results of the Internet banking abandoning model show independent variables values of trust (R2 = 0.484; ANOVA p=0.000), security (R2 = 0.504; ANOVA p=0.000) and risk (R2 = 0.217; ANOVA p=0.001); that is trust, security and risk respectively have 48.4%, 50.4% and 28% of variance in the abandoning of Internet banking. Moreover, the ANOVA values being less than 0.05 indicates that the variables are statistically significant. This is quite an important finding. The values related to these factors have contributed to the explanation of the variance in the abandoning of Internet banking.

There is a strong and statistically significant negative correlation between Internet banking abandoning and trust (its value = -0.696) and security (its value = -0.710). The results show an increase in trust and security in connection with a decrease in the

number of customers who give up Internet banking and a decrease in these factors in connection with an increase in the avoidance of Internet banking services.

Furthermore, Internet banking risks and abandoning correlated positively (its value = 0.466). Meaning that an increase in the risk is linked to an increase in the number of customers who abandon Internet banking, while a decrease in risk is linked to a decrease in the number of customers who abandon Internet banking (see appendix A2). Hence, based on the results given above, it could be concluded that there is a significant relationship between the abandoning of Internet banking as a dependent variable and trust, security and risk as independent variables (see Figure 32). Thus, the H2a, H2b and H2c hypotheses are supported.

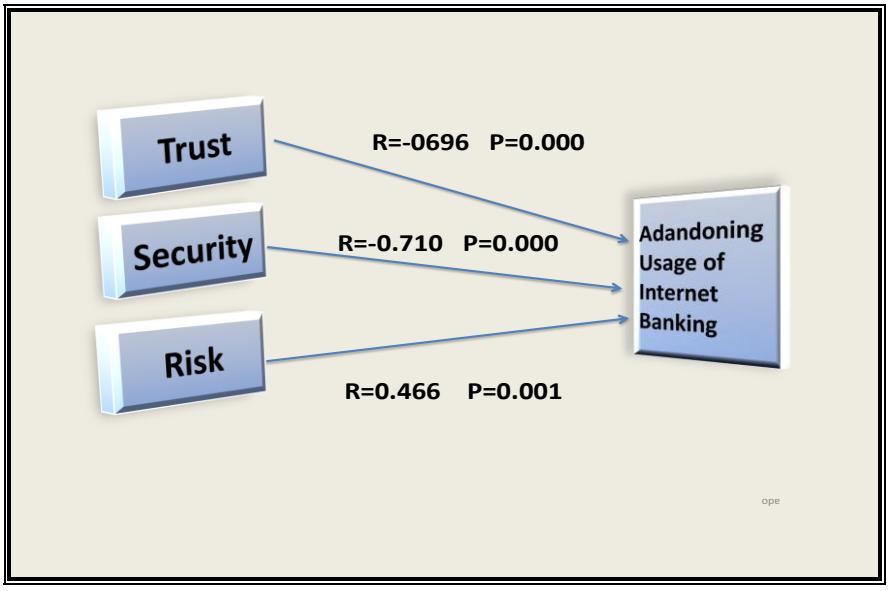


Figure (32): Research framework of customers' abandoning of Internet banking with correlation coefficient (R) and P value

6.3.3 EXPLANATION OF THE MODEL ADOPTING AND PREDCTING THE CONTINUED USE OF INTERNET BANKING

In this model, trust, security and risk are taken to be independent variables, while Internet banking adoption and predicting continuity are taken to be dependent variables. In this case a simple regression and ANOVA analysis were employed. The results are given in Table 16.

Table (16) Simple Regression Analysis and ANOVA on dependent variable (Adoption and continued usage of Internet banking)

Hypotheses	R	Type of Correlation	R Square	Sig. Value	Result
H3a: Trust affects customers' decisions/intentions regarding the adoption of Internet banking.	0.238	Positive Low	0.056	0.000	Supported
H3b: Security affects customers' decisions/intentions regarding the adoption of Internet banking.	0.067	Positive Low	0.005	0.131	Partly Reject
H3c: Risk affects customers' decisions/intentions regarding the adoption of Internet banking.	-0.005	Negative Low	0.000	0.905	Partly Reject
H3d: Trust, security and risk affect customers' decisions/intentions regarding the continued use of Internet banking.	0.220	Positive Low	0.048	0.000	Supported
H4a: The perceived risk of Internet banking will reduce trust.	-0.225	Negative Low	0.065	0.000	Supported
H4b: The security of Internet banking will enhance trust.	0.509	Positive Strong	0.259	0.000	Supported
H4c: The security of Internet banking will reduce its perceived risk.	-0.395	Negative Moderate	0.156	0.000	Supported

DISCUSSION:

The results of this model show that there is a positive low correlation between trust and the adoption of Internet banking (R= 0.238). This means that an increase in this factor is linked to an increase in Internet banking adoption, while a decrease in this factor is linked to a decrease in the adoption of Internet banking services. The R Square (R2) results in this model show a trust variable value (R2 = 0.056) which means that there is only 5.6% of variance in the adoption of Internet banking. Moreover, the ANOVA value (p=0.000) was less than 0.05, which means that it is statistically significant.

Despite the low correlation, it is an acceptable finding meaning that for the respondents trust influences their Internet banking adoption behaviour. Thus, hypothesis H3a was supported. The correlation of the security factor with Internet banking adoption was positive and low (R= 0.067). The R Square value (R2 = 0.005) indicates that security explains just 0.5% of the variance of the adoption of Internet banking while the ANOVA value (p=0.131), being greater than 0.05, means that it is statistically insignificant.

It can be concluded from the results above that the issue of security is not significant to the adoption of the Internet banking service. Hence, hypothesis H3b was partly rejected. In contrast, H3c is not supported because the sig value is greater than 0.05, p= 0.905 and R2 = 0.000. However, the correlation between perceived risk and adoption of Internet banking is low (-0.005). In short, risk did not influence Internet banking adoption. In hypothesis H3d, the relationship between trust, security and perceived risk jointly as independent variable and the users' perceived intention to continue Internet banking use as a dependent variable showed a small positive correlation (R= 0.220). The model in this case yielded a statistical significance (sig. =0.000). The value of R

Square (R2 = 0.048) means that the three factors jointly give just 4.8% of the variance in the continuity of the Internet banking service (see appendix A3).

It appears from this data that trust, security and risk influence the intention of users to continue using the Internet banking service in the future. The H4a, H4b and H4c hypotheses investigated the relationship among trust, security and risk factors.

A model summary of the H4a hypothesis shows a value of (R2 = 0.065). This signifies 6.5% of the variance in customers' trust; an acceptable result despite the low value, because there was a small negative correlation between risk and trust (R= -0.225). In addition, the sig. value is less than 0.05 (p= 0.000). This variable is making a significant unique contribution to the prediction of the dependent variable. In sum, respondents agree that risk significantly influences trust in Internet banking; therefore H4a was accepted.

The positive correlation between security and trust in H4b = 0.509. In addition (R2 = 0.259). This means that security accounts for 25.9% of the variance in customers' trust in Internet banking. This is quite a respectable result. Furthermore, the significant value is less than 0.05 (p= 0.000) meaning that the variable is making a significant unique contribution to the prediction of the dependent variable.

In total, respondents agreed that security significantly influenced their trust in Internet banking. Therefore, the H4b hypothesis was accepted. Also, the H4C hypothesis model summary showed (R2 = 0.156). This means that security accounts for 15.6% of the variance in perceived risk. This is an acceptable result, especially given that the significant value is less than 0.05 (p= 0.000) and there is a moderate negative correlation between security and risk (R= -0.395). In sum, security significantly influences perceived risk in Internet banking. Hypothesis H4c was therefore accepted.

The outcomes of this model found that perceived risk and security did not have an effect on customers' decision to adopt use of service, while trust has an acceptable effect on the intention to adopt the use of Internet banking. On the other hand, despite the tests showing that these factors having a low impact on customers' adoption, customers believed that trust, risk and security have an effect on them continuing to use service. The three factors mentioned here that influence one other can be seen in Figure 33.

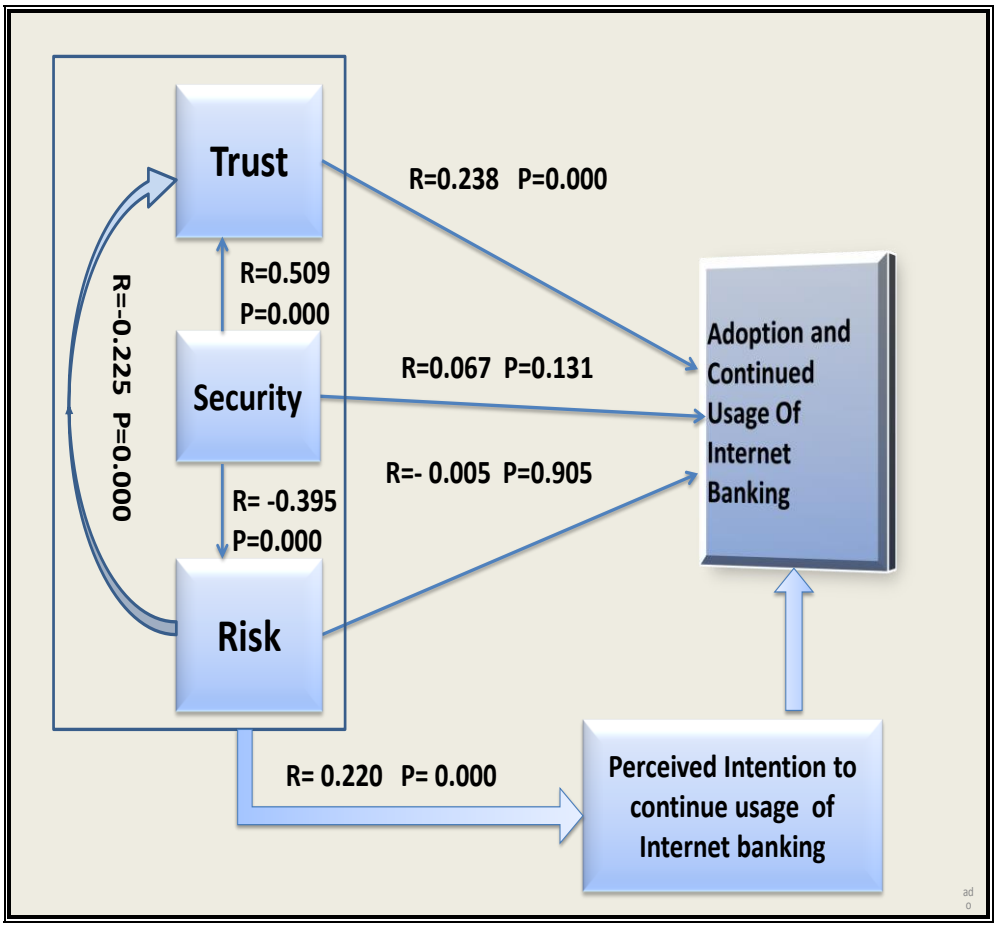


Figure (33): Model Adopting and Predicting the Continued Use of Internet banking with correlation coefficient (R) and P value

6.3.4 EXPLANATION OF SAFETY AREA MODEL FOR USAGE OF INTERNET BANKING

This section presents the aims of obtaining a safety region to practice Internet banking services efficiently in order to increase customers' trust. The chapter thus discusses the work stages of the safety area model and offers an analysis of the findings. There are two stages in this model namely:

First stage: Current /pre-review

The paradigm in this stage aims to discover the current area to work Internet banking services. The model is three dimensional comprising three factors: trust, security and risk and uses a metric scaling model of percentiles measures from 0% to 100%. The result is the identification of the current area regionally located as illustrated below in Figure 34.

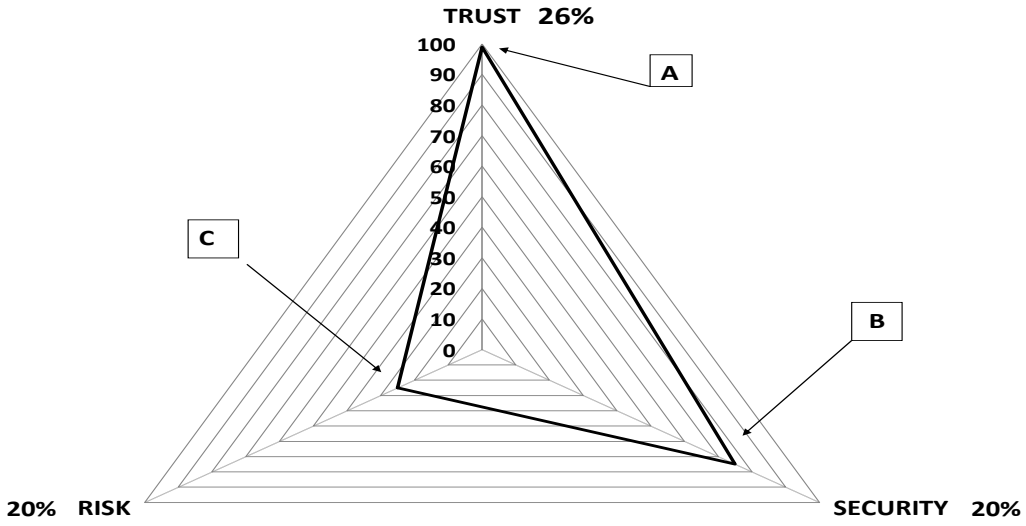


Figure (34) Illustration form of the current area for usage of Internet banking

Moreover, current area obtained of three questioning of trust, security and risk as namely:

Q47U - My confidence in Internet banking when I conduct transactions is…?

- No confidence (0%).
- Low confidence (1-25%).
- Moderately confidence (26-50%).
- Highly confidence (51-75%).
- Very highly confidence (76-100%).

Q53U- How concerned are you about the security of Internet banking?

- Not at all concerned (0%).
- A little concerned (1-25%).
- Concerned (26-50%).
- Moderately concerned (51-75%).
- Very concerned (76-100%).

Q61U- What degree of risk do you feel when you conduct transactions using Internet banking?

- Very insignificant risk (0%).
- Insignificant risk (1-25%).
- Neutral (26-50%).
- Significant risk, (51-75%).
- Very significant risk (76-100%).

The results (Frequencies and Percentages) are shown in next tables (17, 18, and 19) and Figures (35, 36, and 37) below.

Table (17) Q47U: My confidence in Internet banking when I conduct transactions is:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all confident	0	0	0	0
	Low confident	113	22.5	22.5	22.5
	Moderately confident	232	46.1	46.1	68.6
	Highly confident	142	28.2	28.2	96.8
	very highly confident	16	3.2	3.2	100.0
	Total	503	100.0	100.0	

Table (18) Q53U: How concerned are you about the security of Internet banking?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not at all concerned	14	2.8	2.8	2.8
	A little concerned	72	14.3	14.3	17.1
	concerned	160	31.8	31.8	48.9
	moderately concerned	131	26.0	26.0	75.0
	very concerned	126	25.0	25.0	100.0
	Total	503	100.0	100.0	

Table (19) Q61U: what degree of risk do you feel when you conduct transaction in Internet banking?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Very insignificant risk	10	2.0	2.0	2.0
	insignificant risk	135	26.8	26.8	28.8
	Neutral	208	41.4	41.4	70.2
	Significant risk	140	27.8	27.8	98.0
	Very significant risk	10	2.0	2.0	100.0
	Total	503	100.0	100.0	

Figure (35) Q 53U Security Levels

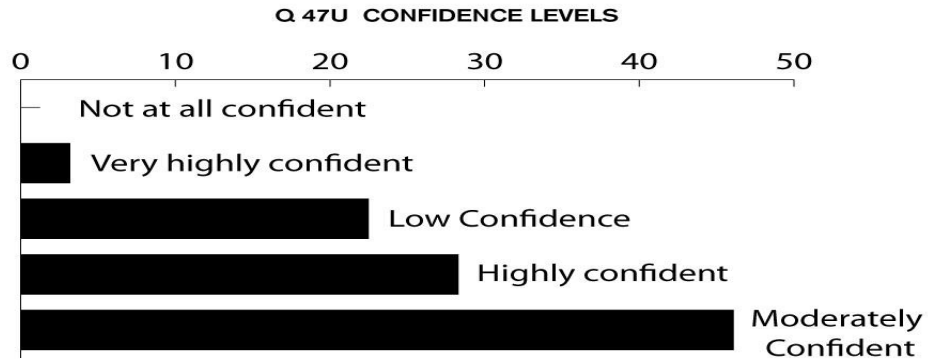


Figure (36) Q 47U Confidence Level

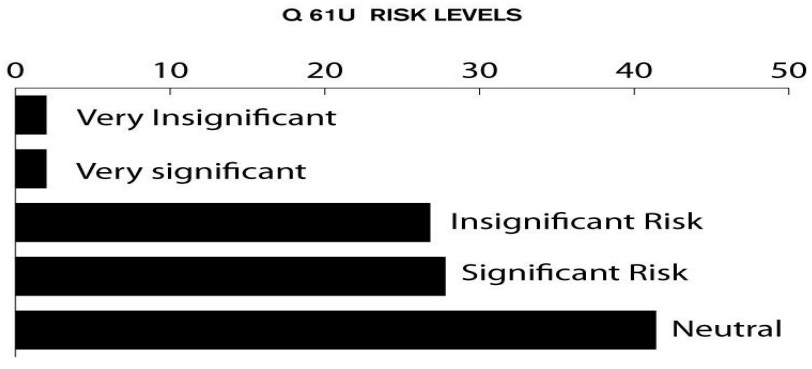


Figure (37) Q 61U Risk Levels

The results were plotted in the model to determine the current area located within 26% trust, 20% security and 20% risk. Basically, this region is the result of statistics generated from the opinions and replies given by 503 Internet banking users regarding their current feelings about service security, confidence and risk perceptions.

Second stage: Safety/Post-review

The second and last step determined the current area according to Internet banking users. The second stage of this diagram determines the safety area. This study has structured three questions (C, D, E) dealing with the HOW and WHAT customers want banks to do to enhance trust and security, as well to reduce risk. The questions contain some options to chosen by respondents to achieve the safety area from the point of view of Internet banking users.

- **Service quality indicators**

The area between current and safety pillars captures respondents' perceived positioning in the factoring enhancements cycle development loop. The results are articulated in Tables 20, 21, and 22 below.

Table (20) Question (C) with answer options and the percentages

QC- In order to increase your trust, what do you think the bank should do?			
NQ	The options	Keywords	The percentages Of answers
1	Give enough safeguards to make user feel comfortable when making Internet banking transactions.	Safeguards	75%
2	Direct contact with bank staff on the Internet if there is an inquiry/problem.	Customer Service	65%
3	Show due diligence and responsibility when problems occur.	Due diligence Monitoring	69%
4	Offer assistance to guide users, if they get stuck or make a mistake as well providing useful tips.	Online tips	44%
5	Website should provide information that helps decrease uncertainty related to Internet banking.	Information-FAQS	40%
6	Take necessary modern security measures, which would lead to reduced risks and increase users trust in Internet banking.	Security Measures	72%
7	Have a good navigability and visibility within the Internet banking website (e.g. easy to locate the services and professional design).	Website design	43%
8	Work as a group with banks to activate existing international and local rules and make it more efficient to protect banks and clients.	Banking Optimised Community	37%
9	Offer clear and reassuring responses about adverse news (identity theft and Internet fraud).	Timely Communications	47%
10	Maintaining and promoting a good reputation.	Building Brand Values and PR	33%

Table (21) Question (D) with answer options and the percentages

QD- In order to enhance security, what do you think the bank should do?			
NQ	The options	Keywords	The percentages Of answers
1	Use multi-factor authentication (combination of factor) which uses two or more factors to assert identity are (password – PIN) and biometric technologies such as (Retinal Scan, Voice Pattern, Facial recognition and Fingerprints), rather than two-factor authentication methods to access to internet banking.	Multi-factor authenticity schemes	72%
2	Using personal electronic devices (e.g. Secure Key) to be highly secure for internet banking transactions.	Personal ID keys	71%
3	Send warning messages when the communication is insecure.	Warning messages	73%
4	Make additional methods of verifying my identity before imputing account information and processing transactions.	Alternative password inputs	52%
5	Enhance security measures even if there is limited time a day to access website.	Security Measures	32%
6	Promote security measures even if Internet banking transaction takes longer than before.	Timely Security communications	41%
7	Make clients change their PIN / Password every so often to make Internet banking more secure.	Promote regular user password changes	40%
8	Outline the risks and promote user's confidence of the effective security measures.	Build customer confidence via schemas	37%
9	Banks could send confirmation codes to customer's mobile phone for transactions under process, this will enable greater security.	Generate security codes for Mobile phone devices	55%
10	Banks increase the awareness about security of Internet banking**.**	Grow and build safeguard awareness	41%

Table (22) Question (E) with answer options and the percentages

QE- In order to reduce risk, what do you think the Bank should do?			
NQ	The options	Keywords	The percentages Of answers
1	Compensate any money taken from user account through unauthorized transactions.	Timely Compensation	77%
2	When problems occur or user gets stuck, the Internet banking system should guide him to solve them.	Resolution support system	42%
3	Enhance security measures to protect Internet banking from risks of virus attacks, hackers or fraud.	Pro-active security software	79%
4	Running awareness campaigns against risks (e.g. identity theft, cyber-crimes and fraud).	Awareness campaigns	29%
5	Give enough safeguards to make user feel comfortable toward risks when making Internet banking transactions.	User confidence training guides	57%
6	Should have clear laws and rules to protect users from risks using Internet banking.	Stringent security policies and practices	46%

The average scores of each question (QC, QD, and QE) were calculated separately to determine the safety area. This was done by taking the average of the results of the three questions which worked out as 53% enhanced trust, 51% enhanced security and 55% minimise risk.

The methods below show the percentages relating to the factors:

- Trust first step (current area) 26%. Second step (the safety area) 53%. To determine the ratio for enhanced trust, subtract 53% - 26% = 27%. As shown above, the elevation rating on users' recommendations in QC rose from 26% to 53% by 27%.
- Security first step (current area) 20%. Second step (the safety area) risen to 51% (by 31%). Percentiles were obtained by subtracting 51%-20%= 31%.

- Risk first step (current area) 20%. Second step (the safety area) risen to 55%. Risk percentage was 20% in current area.

However, when the recommendations have been chosen by customers of question (E), the risk is reduced by 55%. Mathematically, the current risk 20% reduced by 55% means that the risk is cut to 9%. The result demonstrated that the risk was reduced from 20% to 9%, a fall of 11%.

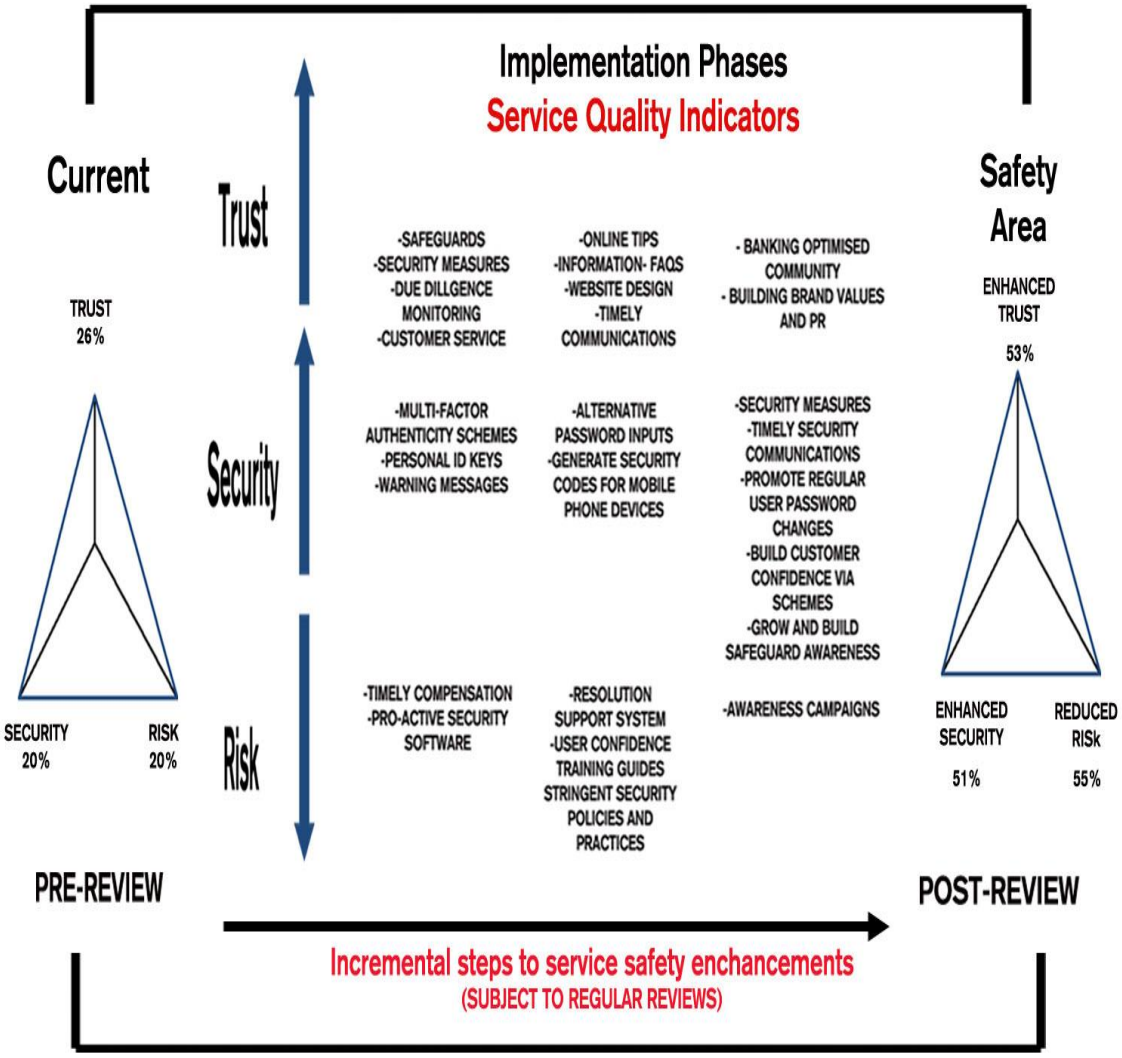


Figure (38): Safety model for Internet banking usage.

- **Service Safety Cycle**

As mentioned above this model aimed to identify the safety region which maximises the productivity of Internet banking services to achieve the best and most favourable position obtainable in terms of client's confidence, enhanced protection systems and reduced risks. In this model the safety area is located between the perceived trust of customers (53%), perceived security of system (51%) and reduced perceived risk (by 55%) i.e. the perceived risk in the safety area stage is 9%.

The model does not stop at this result because it is a cyclic model which can run once more than once to get other outcome as the human variable and circumstances can affect customers' behaviour and their orientation. Thus it will be useful to re-run the model to get suggestions and recommendations to help banks to amend and improve services to satisfy clients' aspirations and provide effective and safe services.

With regard to the second stage of this model, there are clear improvements in customers' trust (53%) and security (51%) while the perceived risk was decreased by 55%, i.e. it was reduced to 9% instead of 20%. This enhances customers ' trust in the service (see Figure 38 above).

The contribution of the model proposed in this research is a new method of ensuring a safe and optimal way to use Internet banking services, by providing an acceptable degree of security that is reflected in customers' confidence in and satisfaction with services.

The model first identifies customers' current levels of confidence in regards to security and risk. The second phase, based on inclusion of a set of questions in the questionnaire that describe the mechanisms and steps required by the user, are to increase the level of

security, trust and reduce risk. Thus, after taking these mechanisms and steps into consideration and applying them, the model must re-test levels of trust, security and perceived risk, and then determine the degree of safety according to customers' perceptions, and identify whether any further proposals and mechanisms are applicable, in order to establish a safe area within which to use Internet banking services.

In sum, respondents agree that there is a combination of trust, risk and security that can guarantee a favourable degree of usage and satisfaction with Internet banking. Thus, hypothesis H5 - there is a safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services was accepted. The next section will discuss the significant findings.

6.4 SIGNIFICANT FINDINGS

This section will discuss the significant findings of the research, and will be split into four parts. The first part will discuss the non-adoption of the Internet banking model; the second describes the abandoning of Internet banking model; the third further extends the adoption and continuing usage of Internet banking model; the last part will discuss the findings of the safety area model for Internet banking.

6.4.1 DISCUSSION OF THE FINDINGS OF THE NON-ADOPTION OF INTERNET BANKING MODEL

This sub-section will address the significant findings of the empirical work through an analysis of the research hypotheses. As previously mentioned the study by (Yousafzai and Yani-de-Soriano, 2012, p.60) conducted in the UK, aimed "to deepen understanding of customers' actual Internet banking behaviour by combining the construct of

technology readiness with the technology acceptance model and demographics". About 435 (valid) questionnaires were completed, by UK based Internet banking users. The study surveyed only existing Internet banking customers.

Thus, observed recommended for future studies might also include existing non-users of Internet banking services. Furthermore, Yousafzai and Yani-de-Soriano's (2012) research concentrated on particular factors, such as technology readiness, age and gender, over others, but acknowledged that there are other relevant behavioural factors, e.g. perceived risk, trust, service quality and security, which could also provide insight into the process of adoption or non-adoption of Internet banking services. This study has been focused on trust, security and perceived risk.

Adapa (2011) provides additional research, having conducted a study in Australia, specifically aimed at Internet banking users and non-users in a particular banking sector; as a result, the researcher commented that, the outcomes could differ if the application of the research conducted in other countries. Therefore, part of this study was focused on an investigation of pre-adoption of Internet banking and the influence of trust, security and perceived risk on potential customers' feelings toward this service.

Out of the overall study, which consists of 838 samples, the total for 'non-adoption of Internet banking' was 291 (34.70%). This means that there were 291 customers (34.70%) out of 838 (100%) who did not use Internet banking.

The research study therefore supports the assertion of a negative relationship between trust and security and customers' tendencies towards non-adoption of Internet banking. The study, based on simple regression and correlation analysis, found that trust and security have a significant influence on customers' decision not to use the service, and

so these factors have a strong negative correlation (R = - 0.673, P = 0.000; R = -0.689, P = 0.000 respectively).

Few previous studies have examined the pre-adoption behaviour of customers, particularly in the UK. The study further found that trust has a greater effect than concerns about security on the behavioural intention not to use Internet banking, as demonstrated by the coefficient.

Substantially, the above findings show that the relationship between trust, security and non-adoption of Internet banking services has a strong negative relationship, meaning that an increase in trust and security is offset by a decrease in the number of customers who do not rely on Internet banking, and a decrease in these factors is offset by an increase in customers who do not rely on an Internet banking service.

Additionally, the results demonstrate a strong positive relationship (R = 0.525, P = 0.000) between risk and non-adoption of Internet banking, which means that an increase in perceived risks is offset by an increase in the number of customers who do not rely on Internet banking, and a decrease is similarly offset by a decrease in customers who do not adopt Internet banking services.

Therefore, the study's finding that trust, security and perceived risk are significant factors influencing customers' intentions in the non-adoption of Internet banking services is considered to be the result of relatively new research, as it has not been a dominant feature of previous research.

On the other hand, when non-users of Internet banking (291 people) were asked if they were happy with cash machines and branch banking (Q19-Q20), the responses showed that between 82.2% and 87.3% strongly agreed that they were satisfied and comfortable with the use of both cash machines and branch banking respectively.

In addition, the first section of the study questionnaire, relating to non-users of Internet banking, asked participants an open question (QB), to establish whether there were any other reasons behind their non-use of Internet banking to perform banking transactions. No more than 27 (9.28%) open questioning from the total study sample were non-users of Internet banking services, from a sample of 291.

Responses breakdown are as follows: 13 respondents (5%) stated that they preferred to deal with staff face to face when carrying out banking transactions; 7 respondents (2.49%) said that they did not use Internet banking because the procedures were long and difficult to access; 4 respondents (1.5%) thought that the process was too complicated; three respondents (1.10%) said that they did not use Internet banking because they had forgotten their password.

In order to expand on the data acquired from this poll, the study also asked the participants a further open question (QC): What do you think the bank should do in order to encourage you to use Internet banking? Just 57(20%) respondents of 291 non-users of Internet banking services have been answered this question.

In question C the majority of these respondents (80%) stated that in order to encourage them, banks should enhance security, reduce risk and provide guarantees against fraud. They also wanted banks to make the service easier to use, with advice and training on how to use it provided. Furthermore, the study found weak relationships between Internet banking non-users demographic characteristics and three factors (trust, security and perceived risk).

To summarise, this part of the study established that out of 838 (100%) banking customers, 291 of these did not use an Internet banking service, about (34.70%). It further found that all participants emphasised trust, security and perceived risk as

having a significant influence on customers' intentions in non-adoption of Internet banking in the UK, specifically in Leicester.

6.4.2 DISCUSSION OF THE FINDINGS FOR THE ABANDONING OF INTERNET BANKING MODEL

Yousafzai and Yani-de-Soriano (2012) state that it is important to examine if there are any customers leave Internet banking; they also claimed that about two million people have given up the customers in the UK. This position is echoed by Forrester's research (Forrester research, 2008).

These observations stimulated the opening up of the field and prompted the idea of research that would delve deeper and investigate whether there are any Internet banking users who decide to abandon the service post-adoption and, furthermore, to explore the role and influence of trust, security and perceived risk on these decisions.

Thus, this section was discussed the impact of these three variables on the abandonment (giving up) of the use of Internet banking. A review of the literature related to Internet banking in the UK did not reveal any study specifically related to the abandonment of services, most previous studies discussed customers' intentions related only to the adoption of Internet banking.

In this study, from a total sample size of 838, the number of those who fell into the category of 'abandoning Internet banking' was 44 participants (5.30%). These were participants who had adopted Internet banking services, but later left the service. Evidently, this is a small percentage compared to users, and non-users who had never used the service at all, but this category of customer still exists.

These results demonstrate that trust and security have an important effect on the decision to abandon Internet banking (R = -0.696, P = 0.000; R = -0.710, P = 0.000 respectively). These findings further show that the relationship between trust, security and the abandoning of Internet banking is a strong negative relationship, where an increase in trust and security is offset by a decrease in the number of customers who have abandoned Internet banking, while a decrease in these factors is offset by an increase in customers who abandon these services.

The results additionally show that the relationship between perceived risk and customers abandoning Internet banking is a moderately positive one (R = 0.466, P = 0.001). This means that an increase in perceived risks is offset by an increase in the number of customers who abandon Internet banking. On the other hand, when the 44 'abandoners' were asked if they were happy using cash machines and in branch banking(Q38-Q39), Eighty-nine per cent answered that they 'strongly agreed' that they were satisfied with the use of cash machines and in branch banking. This satisfaction indicates to ATMs may have influence especially today many of them became provides deposit service.

As mentioned earlier, the study also asked participants an open question (QB) that aimed to establish if there were any other factors behind customers' decisions to abandon the use of Internet banking for banking transactions (see the second section of the questionnaire, QB). Just 44 participants (5.30%) from the total study sample of 838 acknowledged as abandoned. Among them, 15 (34%) of open question (QB) respondents of which can be broken down as follows: 8 respondents (53.4%) stated that security measures made it too difficult to access the service; 4 (26.6%) said that they

were worried about electronic fraud; and, 3 respondents (20%) said that they had forgotten their password.

In order to gain a deeper understanding, this study asked the sample members a further open question (QC): What do you think the bank should do, in order to encourage you to re-use Internet banking? No more than 15 (QC) respondents of abandoned 44 samples (34%) totals. The respondents majorities accounting 98%, said that to encourage them to begin using Internet banking again, security needed to be enhanced, in order to reduce risk, and that both log in and general access to services should be made easier and simpler. What is more, there are weak relationships between demographic characteristics of abandoners of Internet banking and three factors.

To sum up, the findings show that the number of quitters, those who had abandoned Internet banking, from the total sample of Internet banking users across the study was 44 customers (5.30%). Whilst this is a minority relative, studies demonstrates that although there is a clear uptake of Internet banking, there are customers who abandon Internet banking services after their initial adoption. Therefore, this phenomenon does exist, albeit a minority one.

The finding is therefore that: there are some customers abandoning Internet banking after adoption. Further, trust, security and perceived risk were significant factors behind customers' intentions in giving up Internet banking. This is, furthermore, a relatively new conclusion, considering the notable lack of previous research.

6.4.3 DISCUSSION OF THE FINDINGS OF THE ADOPTION AND CONTINUED USAGE OF INTERNET BANKING MODEL

This part of the study aims to propose a framework based on the three aforementioned influencing factors (trust, security and perceived risk) and their impact on customers' adoption and continued usage of Internet banking services in the UK.

Many of the earlier studies on use of Internet banking services focused on customers' initial adoption of the service, rather than continued use (Riffai et al., 2012; Yousafzai and Yani-de-Soriano, 2012; Al-Smadi, 2012; Muzividzi et al., 2013; Al-Ajam and Nor, 2013; Goudarzi et al., 2013; Alsheyyab and Singh, 2013; Farzianpour et al., 2014).

Whilst the literature review found that, historically, little research had been carried out in identifying factors that influence the post-adoption phase of Internet banking, in more recent times, studies have begun to focus on investigating the continued use of Internet banking, due to its perceived importance after earlier studies recommended an examination of this area as the possible focus for future research.

This newfound interest may help to overcome many of the limitations of previous studies and contribute new findings in this field. A study by Tat (2008) in Malaysia investigated current Internet banking users, looking for predictors of intentions for continued usage. Their findings indicated that trust was the strongest factor that impacted customers' intentions to keep using services. The researchers recommended that the questionnaire be translated into other languages so that participants from other countries could also respond to the survey questions.

Advocate further mores, should concentrate on particular factors, and for example perceived risk, in order to gain an in-depth understanding of the influences on decisions regarding whether to continue using Internet banking. Further recommendation for

future research is offered by Hoehle et al. (2012) who state that future work should aim to develop a new conceptual model through which to examine the factors that impact on continued usage or not of Internet banking services.

Choudhry et al. (2013) similarly recommended, when concluding their study, that future research should examine the relationship between the variables that influence continued usage of Internet banking services.

A survey conducted by Adapa (2011) aimed to examine the factors that impact how customers continue to use Internet banking services in Australia, finding that, continued use and frequency of use of Internet banking have been neglected, majority of the existing studies emphasis on clients' adoption of Internet banking service.

Adapa's study was conducted in Australia, and included both users and non-users of Internet banking services, though the researcher suggested that the results might differ if the study was repeated in a different banking environment. Furthermore, similar studies reaffirm as abovementioned relating to the continuing use of Internet banking, such as (Pi et al., 2012; Kartiwi et al., 2013).

This section in current study has discussed the effect of three influencing factors on customers' intention to accept and continue to use Internet banking services, namely: trust, security and perceived risk. This study uses a sample of Internet banking users, and the following discussion will be divided into three parts: First, the impact of each of the three aforementioned factors will be addressed separately, regarding the adoption of services. Second will be a discussion of the combined influence of the three factors on the continued usage of Internet banking. The third and final part will focus on the association between trust, security and risk.

Part one: influence of trust, security and perceived risk, separately, on the adoption of Internet banking services.

The findings of the study demonstrate that trust has influence on the intention to adopt the use of Internet banking services, although it has a low positive correlation (R = 0.238, P = 0.00), it provides support for the H3a hypothesis. Trust was followed by security, which was shown to have the second largest influence; however, the variable had a low positive correlation (R = 0.067, P = 0.131), with a P value of more than 0.05, constituting a non-significant result, which therefore demands the partial rejection of the H3b hypothesis.

Finally, perceived risk was shown to have a very small influence on the decision to use Internet banking, due to its low negative correlation and a P value of more than 0.05 (R = -0.005, P = 0.905), indicating a non-significant result that thus provides no support for the H3c hypothesis. In conclusion, the results establish that trust does affect customers' decisions regarding the adoption of Internet banking. However, concerns about security had only a weak impact on customers' decisions, whilst risk had no effect at all on customers' decision to adopt Internet banking.

Part two: combined influence of trust, security and perceived risk on the continued usage of Internet banking.

The study findings demonstrate that the three predictors (trust, security and perceived risk) have an effect on customers' intentions to continue to use Internet banking services (R = 0.220, P = 0.000). It should be noted here that whilst trust did affect customers' decisions and intentions in the initial adoption of services, security had a very low effect, and perceived risk had no effect on customers' decisions or intentions in the

adoption of Internet banking. However, with regard to predictions of continued usage of Internet banking, customers felt that the combination of the three factors did affect their decisions and intentions. This finding therefore provides support for the H3d hypothesis that trust, security and perceived risk, combined, affect customers' decisions and intentions relating to continued use of Internet banking.

Part three: The relationship between trust, security and perceived risk.

After establishing that they have a combined influence on customers' behaviour, this section will discuss the relationship among the three factors: trust, security and perceived risk. The findings demonstrate that trust in Internet banking is influenced by perceived risk. The survey results reveal a low negative correlation ($R = -0.225$, $P = 0.000$), meaning that when perceived risk increases, trust will decrease and conversely. This finding thus supports the H4a hypothesis, and it is therefore apparent that perceived risk has a clear influence on customers' trust in Internet banking and that this will consequently effect rates of adoption and usage of Internet banking services.

Regarding the relationship between security and trust, a strong positive correlation ($R = 0.509$, $P = 0.000$) was observed, which means that if there is an increase in security, this will lead to an enhancement in customer trust, and a decrease in security levels, this will cause customers' trust to also deteriorate. This finding therefore also provides support for the H4b hypothesis. Finally, there was a moderate negative correlation between security and perceived risk ($R = -0.395$, $P = 0.000$). This result shows that strong security procedures will reduce the perceived risk of Internet banking services, and thus provides support for the H4c hypothesis.

As mentioned earlier, there was another important element to the questionnaire, the open question (QB) that asked participants whether there were any other reasons, excluding trust, security and perceived risk, behind their decisions regarding the adoption and continued use of Internet banking services to perform banking transactions.

Active users represented 503 samples (60%) from the total study sample of 838. In this fashion a mere 167 (QB) respondent (33.20%) with break down as follows: 49 respondents (29.34%) felt that Internet banking services were convenient; a further 49 respondents (29.34%) cited ease of use; 16 respondents (9.58%) thought that Internet banking saved them time; 30 respondents (18%) said that the service was quick to perform transactions; 16 respondents (9.58%) liked the ease of access, available 24/7, anywhere and anytime.

Lastly, 7 respondents (4.19%) felt that Internet banking provided them with good monitoring, control and management of their account. Additionally, the study exhibited that there are a very weak relationships between demographic characteristics of Internet banking users amongst trust, security and perceived risk.

In short, it is clear from the above results that trust is the strongest influencing factor on customers' intentions to adopt the use of Internet banking services as, despite the fact that it had a low positive correlation; it had a significant (P) value result. With regard to security, this had a simple effect on the adoption and usage of Internet banking services, leading to a partial rejection of hypothesis H3b, as the study demonstrated that security had very weak influence on the adoption of Internet banking for current users. Perceived risk was shown not have an effect on current users' intentions when they adopted the service, and so hypothesis H3c was rejected.

However, the findings show that the combination of trust, security and perceived risk had a clear effect on customers' decisions and intentions relating to continued use of Internet banking services. Therefore, the H3d hypothesis is accepted and supported. Regarding the H4a, H4b and H4c hypotheses, concerning the relationships between trust, security and perceived risk, the findings show that these three factors do affect each other, thus providing support for the three above hypotheses.

6.4.4 DISCUSSION OF THE FINDINGS OF THE SAFETY AREA FOR INTERNET BANKING MODEL

This section will discuss the findings outlined in the data analysis and results chapter; particularly part four, which will explain the model of safety area for the use of Internet banking. This paradigm is developed in the current research, and thus makes a significant contribution to emerging literature relating to customers' behaviour in relation to Internet banking services.

This model concerns the provision of a safe area in which to utilise Internet banking services efficiently, so as to achieve a desired degree of customer trust, an appropriate level of security and a low level of perceived risk of environmental safety.

The study considers the analysis of descriptive statistics and utilises these results in the main examination of the research model. To obtain descriptive statistics for categorical variables, in this model the study has used frequencies; the model is based on the perceptions and recommendations of Internet banking users only, it does not include non-users or those who have abandoned Internet banking services.

As already noted in chapters theoretical models, this model will consist of two stages. The first stage concerns the current feelings of users towards Internet banking services

regarding their trust in the service, the level security when they use it and the risks they face in using it. In this phase, the levels of trust, security and risks for users were determined to be 26%, 20% and 20% respectively.

Although these are only estimates, average trust was 26%, and so this level was considered to be the medium. It was noticed that the highest level of confidence reported by users was moderately confident, at 46.1%, and 22.5% of respondents answered that their confidence was low.

One possible reason for these levels may be related to security, despite the fact that the average level for concerns about security was 20% of total findings current. This level is considered relatively low, despite the individual percentages for the response options (slightly concerned, moderately concerned and very concerned) being 31%, 26% and 25% respectively, across 503 users. In relation to risk, customers' feelings were neutral, ranging between fear and satisfaction; the average level here was 20%, and the highest percentage of answers was neutral, at 41.4%.

The second stage of the model considers safety area, representing a development of the current area through the implementation of customer recommendations in order to provide access to a safety zone with low-risk, which would enable effective use of the service and enjoy the confidence of customers. The next figure (39) shows the identified Safety Area, which is located between 53%, 51% and 9% for trust, security and risk respectively.

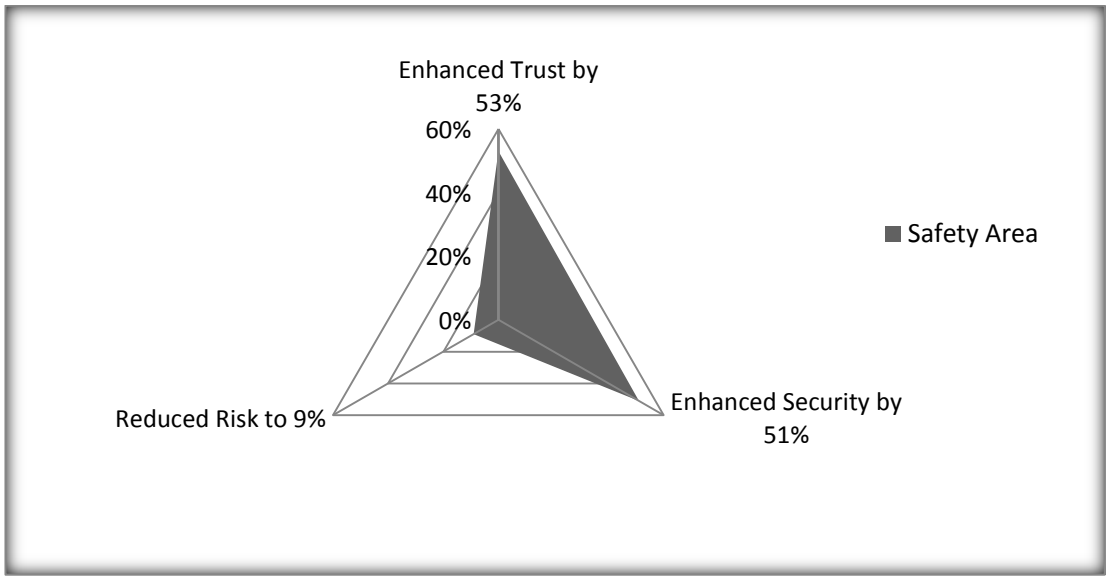


Figure (39) the Safety Area

Table (23) Improvement from current area stage to safety area stage

Current Area		***Safety Area***
Trust was 26%	→	Trust Enhanced To 53%
Security was 20%		Security Enhanced To 51%
Risk was 20%		Risk Reduced To 9%

Regarding risk, in the current area showed a level of 20%, while in the Safety Area it is 55%. This was the average of responses to question "E", which was: In order to reduce risk, what do you think the bank should do?

The above shows that the current area carries a risk level of 20%, and that if the bank carries out the recommendations of customers, risk would be reduced. Expressed mathematically:

$$R = \frac{55 \text{ x } 20}{100} = 11\%$$

Utilization of above noted recommendation findings accounting 55% multiplied by risk present (20 %) over 100 expresses 11%. This means that risks are reduced by 11%, [20% - 11% = 9%], and so, at this stage, the risk level is reduced to 9%. Arguably, if the model were re-tested on the study sample, or another sample, the risks would be reduced even further (see Table 23).

In this theoretical model, the bank will reduce the risks to 9%, by acknowledging and incorporating the views and proposals obtained by the survey, where these are practical and useful. This model has translated these views and proposals into percentages, as mentioned above. In addition, the periodic operation of this model provides an opportunity for banks to stay close to customers, understand their feelings towards their service, eliminate any problems immediately and reduce risks.

Economically, known that the fundamental of success of any project is to gain customers and satisfy them. As well as banks concerning to Internet banking service, should satisfy customers and maintaining them after the adoption to continue use service. Thus, the views and suggestions of the customer have surveyed and solving the problems that they face and it is placed into effect in the bank policies. This will lead to enhance customer confidence in the service and bank, therefore motivate customers to continue in the service.

The safety area concept could be used by a bank to improve its performance with customers, by build and enhance their trust in the service. That is through periodic survey and put useful opinions and suggestions within the bank plans for future development. This is not only requires the factors that are researching now (Trust, Security, Risk), it could be in future research investigate other factors be the subject of customers attention and affect their continuity in service.

6.5 CHAPTER SUMMARY

The objective of this section was to discuss the results of the data that had been analysed in the earlier analysis chapters. The study used the analysis of simple regression results and the correlation model as the main examination of the simultaneous effects three identified variables (trust, security and risk) on the research models.

This chapter presented these variables as the key determinants influencing customers' intention to adopt, not accept or abandon the use of Internet banking. The study examined the effect of the independent variables (trust, security and risk) on the dependent variables, which were: non-adoption of Internet banking, abandonment of Internet banking and adoption and continuous use of Internet banking, in order to stimulate further discussion examining the predictive ability of the independent variables and the explanatory power of the study models, so as to assess the reality of the usage of Internet banking services in the United Kingdom.

The study confirmed that the dependent variables non-adoption of Internet banking and abandonment of Internet banking were both affected by the independent variables of trust, security and risk, and so that there was indeed a relationship between the dependent and independent variables. The study also found that one dependent variable, the adoption of Internet banking, was affected by the independent variable trust, yet while security had only a weak impact, and risk was not an influence at all. However, the study did find that trust, security and risk all affect customers' decisions and intentions relating to continued use of Internet banking services. The study further found that there is a relationship between the independent variables of trust, security and risk.

Finally, one of the main contributions of this study was the development of a model of safety area for the use of Internet banking, an important contribution to the emerging literature on internet banking services.

This model outlines the provision of a safe area in which to utilise Internet banking efficiently, so as to achieve the most favourable degree of customer trust, appropriate levels of security and a low level of risk in the environmental safety. The Safety Area identified by this study is located at 53% for trust, 51% for security and 9% for risk.

It is worth noting, this study has reinforced the importance of integrated theory testing, by developing a conceptual frameworks Inspired by from technology acceptance models in order to obtain a comprehensive understanding of Internet banking services reality in the UK. Through, examine of the factors influencing consumers' adoption, non-adoption, abandonment and continued use of Internet banking.

The comprehensive studies of all patterns of services are still parsimonious, developed in the present study, thus, makes an important contribution to the emerging literature on online customer behaviour. The results also suggest that the proposed internet banking models possesses substantial explanatory ability, through the integration of trust and perceived risk and security in all patterns of customers towards Internet banking services (user, non-user, abandoner and continuity of usage).

To conclude, user acceptance and adoption of technology especially Internet banking services remains a complex, yet extremely important phenomenon. Research on the TAM starting from Davis in 1989 has made significant contributions toward unravelling some of its mysteries. More than that abandoned the service after the adoption. The internet banking acceptance model, non-adoption model, abandonment model and safety area model proposed and validated in this thesis.

Having discussed the important findings of the data analysis, taking into account the impact of all the variables involved in the research models and the relationships between them, Table (24) summarises the impact of the findings on the research hypotheses, as formulated prior to the introductory chapter.

The aforementioned discussion enables the study to respond to the research questions presented in the introductory chapter. Thus, the following chapter will provide responses to the survey questions, followed by the research contributions, along with their implications and limitations. Finally, recommendations for future research directions will be given.

Table (24) Findings Summary of Research Hypotheses

Hypothesis	*Result*
H1a: Trust affects customers' decisions/ intentions regarding the non-adoption of Internet banking.	Accepted
H1b: Security affects customers' decisions/ intentions regarding the non-adoption of Internet banking.	Accepted
H1c: Risk affects customers' decisions/ intentions regarding the non-adoption of Internet banking.	Accepted
H2a: Trust affects customers' decisions/ intentions regarding the abandoning of Internet banking.	Accepted
H2b: Security affects customers' decisions/ intentions regarding the abandoning of Internet banking.	Accepted
H2c: Risk affects customers' decisions/ intentions regarding the abandoning of Internet banking.	Accepted
H3a: Trust affects customers' decisions/ intentions regarding the adoption of Internet banking.	Accepted
H3b: Security affects customers' decisions/ intentions regarding the adoption of Internet banking.	Partly Rejected
H3c: Risk affects customers' decisions/ intentions regarding the adoption of Internet banking.	Rejected
H3d: Trust, security and risk affect customers' decisions/intentions regarding the continued use of Internet banking.	Accepted
H4a: The perceived risk of Internet banking will reduce trust.	Accepted
H4b: The security of Internet banking will enhance trust.	Accepted
H4c: The security of Internet banking will reduce its perceived risk.	Accepted
H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.	Accepted

CHAPTER 7: CONCLUSION AND FUTURE RESERCH

7.1 INTRODUCTION

The overall objective of the study was to contribute to the current body of knowledge in the field of technology adoption and to extend existing knowledge of the factors that impact on intentions towards the use, non-use and abandonment of Internet banking services specifically.

This chapter will summarise the results of the research questions and conclude the outcomes of the study. In order to achieve the study's objectives the following research questions were formulated:

Do trust, security and risk have an effect on customers' decisions and intentions regarding the non-adoption of Internet banking? Do trust, security and risk have an effect on customers' decisions and intentions regarding the abandonment (giving up) of Internet banking? Do trust, security and risk have an effect on customers' decision and intentions regarding the adoption of Internet banking? What constitutes 'significant' degrees of trust, risk and security when considering customers' decision-making process in relation to Internet banking engagement sustainability (continuity of use)? Does a perceived risk related to Internet banking affect customers' levels of trust? Does the security of Internet banking affect customers' levels of trust? Does the security of Internet banking affect the perceived risk? What is the safety combination of trust, security and perceived risk, which would determine desired levels of usage and degrees of Internet banking services satisfactions?

These overall research questions aimed to investigate trust, security and risk as factors influencing customer patterns of Internet banking in the UK, across users (in terms of adoption and continuity of use), non-users and abandoners of the service. These questions were examined through research models that were put forward through theoretical frameworks, and the following research hypotheses:

H1a: Trust affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H1b: Security affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H1c: Risk affects customers' decisions/intentions regarding the non-adoption of Internet banking.

H2a: Trust affects customers' decisions/intentions regarding the abandoning of Internet banking.

H2b: Security affects customers' decisions/intentions regarding the abandoning of Internet banking.

H2c: Risk affects customers' decisions/intentions regarding the abandoning of Internet banking.

H3a: Trust affects customers' decisions/intentions regarding the adoption of Internet banking.

H3b: Security affects customers' decisions/intentions regarding the adoption of Internet banking.

H3c: Risk affects customers' decisions/intentions regarding the adoption of Internet banking.

H3d: Trust, security and risk affect customers' decisions/intentions regarding the continued use of Internet banking.

H4a: The perceived risk of Internet banking will reduce trust.

H4b: The security of Internet banking will enhance trust.

H4c: The security of Internet banking will reduce perceived risk.

H5: There is safety combination of trust, risk and security that will ensure favourable level of usage and degree of satisfaction with Internet banking services.

This chapter will also present the implications of the research. The chapter will conclude by describing the contributions of this research, as well as its limitations and scope for future research.

7.2 THE KEY FINDINGS OF THIS RESEARCH

This section will discuss the empirical results of the study according to the eight research questions set out earlier. The results for each research question are summarised below:

1) Do trust, security and risk affect customers' decisions and intentions regarding the non-adoption of Internet banking?

The results showed that trust, security and perceived risk have a strong influence on customers' decisions and intentions regarding the non-adoption Internet banking services in the UK. Furthermore, 27 respondents (9.28%) out of the total sample of non-users, 291 participants, mentioned other reasons in response to the open question. Thirteen of these (5%) commented that they preferred to deal face to face with staff when performing banking transactions. Additionally, 7 respondents (2.49%) stated that the procedures were too lengthy and that it was difficult to access the service, 4

respondents (1.5%) claimed that the service was too complicated and 3 respondents (1.10%) said that they did not use the service because they had forgotten their passwords.

2) Do trust, security and risk have an effect on customers' decisions and intentions regarding the abandonment (giving up) of Internet banking?

There were a small number of customers, abandoners, who had given up using Internet banking post-adoption; they represented 5.30% of the overall study sample, so just 44 of 838 respondents, a small percentage compared to users (60%) and 'non-users' (34.70%) of Internet banking services. Amongst these 44 respondents, the survey found that trust, security and perceived risk had a strong effect on these customers' decisions or intentions regarding the abandoning of Internet banking services, in the UK.

In addition, the results of the open question also found that as well as trust, security and perceived risk, 15 respondents (34%) of the total abandoners cited further reasons; 8 respondents (53.4%) added that security measures made it too difficult to access the service; 4 (26.6%) said that they were worried about electronic fraud; and, 3 respondents (20%) stopped using the service because they had forgotten their password.

3) Do trust, security and risk have an effect on customers' decisions and intentions regarding the adoption of Internet banking?

The results showed that trust has a low amount of influence on customers' decisions and intentions towards the adoption of Internet banking services, while security and perceived risk have a weak effect on customers' decisions and intentions to adopt Internet banking services, in the UK. The findings also exhibited a very weak relationship between demographic characteristic of users and trust security and perceived risk.

4) What constitutes ‘significant’ degrees of trust, risk and security when considering customers’ decision-making process in relation to Internet banking engagement sustainability (continuity of use)?

The results found that the combination of trust, security and perceived risk have a positive and low an influence on customers' decisions and intentions regarding continued usage.

The findings also showed that those who adopt Internet banking services expected to continue using Internet banking regularly in the future; out of the total sample of service users (503), the percentages regarding expectations for continued usage were as follows: 9.3% (47 respondents) were neutral; 53.3 % (268 respondents) agreed; and, 33.6 % (169 respondents) strongly agreed that they intended to continue their usage. Therefore, the results show that approximately 87% either agree or strongly agree that they intend to continue to use the service in the future.

Furthermore, the outcomes of the open questions showed that, in addition to low impact for trust, security and perceived risk, 167 respondents of the total sample of services users (503; 60% of the total study sample) mentioned there were other reasons behind their intentions for continued use.

Out of these, 49 respondents (29.34 %) felt that the service was convenient; 49 respondents (29.34%) also felt it was easy to use; 16 respondents (9.58%) thought that the service saved them time; 30 respondents (18%) found it was quick to perform transactions; 16 respondents (9.58%) cited ease of access, and the ability to log in 24/7, anywhere and anytime; finally, 7 respondents (4.19%) felt that Internet banking services provided them with good monitoring, control and management of their account.

5) Does a perceived risk related to Internet banking affect customers' levels of trust?

The survey results found a relationship between perceived risk and trust, specifically, which is a perceived risk related to Internet banking that will reduce customer trust.

6) Does the security of Internet banking affect customers' levels of trust?

The study findings showed that there is a relationship between security and trust, which is that greater security of Internet banking will enhance customers' levels of trust.

7) Does the security of Internet banking affect the perceived risk?

The survey results showed that there is a relationship between security and perceived risk, which is that greater security of Internet banking reduces the perceived risk.

8) What is the safety combination of trust, security and perceived risk, which would determine desired levels of usage and degrees of Internet banking services satisfactions?

As the literature review (section 2.4) in this study showed that majority of studies building models related to either adoption or non-adoption such as (Adapa, 2011; Yousafzai and Yani-de-Soriano, 2012; Al-Fahim, 2013; Alihosseini, 2014; Farzianpour et al., 2014; Kaur and Kiran, 2015).

Therefore, study puts forward a model, aimed at the provision of a safe area in which to utilise Internet banking services efficiently. This region is identified as the point of safety combination (safety area) of trust, security and perceived risk, and so guarantees the appropriate levels of satisfaction and usage of Internet banking services. It should be noted that this model is based on the perceptions and recommendations of Internet banking users. This study identified that the safety area was located at the point where customers' level of trust was at 53%, security at 51% and level of perceived risk at 9%. The research implications will discuss in next section.

7.3 RESEARCH IMPLICATIONS

This section will outline three implications, namely: theoretical, methodological and practical. Theoretical implications include the development of a paradigm, and an explanation of how the relevant factors of trust, security and risk affect customers' perceptions towards use, non-use and the possibility of abandoning Internet banking services. Additionally, this section will discuss issues related to the theoretical model of an 'Safety Area' that provides a safe space in which to utilise Internet banking, in order to increase its effectiveness, and is centred around trust, security and risk levels.

The methodological implications include stimulating a debate regarding the potentials of using a mixed method in order to explain variations in the findings. Regarding practical implications, the outcomes of the study add value to research in the field of business, particularly relating to the British financial sector and, more specifically, to the banking industry. Accordingly, the implication for practitioners, such as bank managers, is the provision of a beneficial study model.

7.3.1 THEORETICAL IMPLICATIONS

The theoretical implication of this study is that it contributes a modest addition to the current literature relating to the banking industry and an understanding of the relevant issues, as well as providing recommendations for future research. The study relates to understanding of customers' pre-adoption and post-adoption behaviour, in other words a realistic assessment of Internet banking, in contrast to earlier studies that have focused predominantly only on either customers' pre-adoption or post-adoption behaviour.

This research investigates and develops conceptual paradigms to assess customers' non-adoption of Internet banking; abandonment of use; and, adoption and continued use of Internet banking services, particularly exploring the influence of trust, security and risk.

In the existing literature on banking, customers' non-adoption or uptake followed by abandonment of Internet banking is a neglected area. This is highlighted in recommendations in literature for further research, such as Yousafzai and Yani-de-Soriano (2012).

However, regarding the initial adoption of Internet banking, several studies have investigated this area, including: (Hong et al., 2013; Kesharwani and Radhakrishna, 2013; Ofori-Dwumfuo and Dankwah, 2013; Al-Smadi, 2012; Namamian et al., 2013). Customers' continued use of Internet banking is again an often ignored area, as a study by Adapa (2011) and Choudhry et al. (2013) revealed. Adapa and Choudhry's study examined the factors impacting on whether customers continued to use Internet banking, and recommended the application of the research model in other countries.

Therefore, this study aimed to bridge this gap in the existing literature on Internet banking in the UK, through investigate these phenomenons which are customers' non-adoption, abandonment of Internet banking and customers' continued use of Internet banking. The importance of investigating the motivations behind customers' non-adoption, abandonment or continued use of Internet banking relates to the plans and business strategies of banks, enabling them to encourage their customers to adopt and to continue using their Internet banking services. This consequently helps to inform cost-effective business strategies and increase profitability. Thus, the factors of trust, security and risk factors were considered helpful in elucidating the motivations behind

customers' non-adoption, abandonment, or adoption and continued use of Internet banking, in order to begin to account for the diverse patterns of customer behaviour.

The study findings have highlighted the importance of trust, security and risk in influencing customers' decisions regarding the use of Internet banking, particularly in relation to non-adoption and abandonment. The study identified security and risk as having a very small influence on the initial adoption of Internet banking services, whilst trust also had a low impact.

However, the study found that all three factors were an influence on customers' continued usage of Internet banking. Furthermore, the findings demonstrated the combined influence of the three variables (trust, security and risk), and their effect on each other. The study set out to develop a new framework based on a theoretical model inspired by the acceptance of technological theory that encompasses trust, security and perceived risk factors as predictors in the identification of safe and effective area for the use of Internet banking services.

Regarding the study's findings related to continued usage, the results aligned with the existing literature, particularly those of Adapa's study (2011) which aimed to research the factors impacting on customers' continued use of Internet banking in Australia. Adapa's (2011) study illuminated customers' perceptions concerning Internet banking services as a safe way to carry out their banking transactions.

Yousafzai and Yani-de-Soriano (2012) study aimed to deepen the understanding of customers' actual behaviour towards Internet banking services, and used UK Internet banking users to validate their framework. Their study recommended that future research should investigate other variables, such as perceived risk, trust and security, in order to provide further information on the acceptance process.

The study took into account the recommendations contained in the report, and examined the influence of trust, security and risk on the adoption of Internet banking services. Yousafzai and Yani-de-Soriano's (2012) study further recommended surveying non-users as well as existing Internet banking customers.

Additionally, Yousafzai and Yani-de-Soriano's (2012) study enquired as to why customers might visit a branch after adopting Internet banking services. Current study therefore asked 503 Internet banking users if they had visited a branch of their bank since they started using the online service. The results were that 91.7% of Internet banking users still visited bank branches, despite adopting online services. Clarifying the reasons for this, 64.4% of respondents said that their branch visits entailed making deposits, 41.7% of respondents visited in order to carry out other banking services not available online, and 41.4% made large cash withdrawals. Yousafzai and Yani-de-Soriano's (2012) study also argued that it is important to investigate whether there are any customers who leave the service post-adoption.

Present study concluded that there were indeed customers who abandoned Internet banking services post-adoption, although this portion of customers represented just 5.25% (44 respondents) of the total study sample of 838.

7.3.2 METHODOLOGCAL IMPLICATIONS

Most of the methods used in this study were taken from the existing literature relating to studies of customers' intentions and behaviours towards Internet banking services, although further methods were also used. In order to address the methodological limitations of the existing literature and research on Internet banking, questionnaires for this study have undergone to several examinations.

The study used a quantitative strategy to collect data, assess the reliability of the results and validate the research models. The quantitative technique was chosen first of all because the study needs to gather data from a large sample of customers through a questionnaire which included three sections (non-adoption, abandonment, adoption and continuity of use). Qualitative, non-numerical methods would not have provided the numerical data that the study needs. Secondly, because so little, if any, research has been done into non-adoption and abandonment of internet banking in the UK, the researcher wanted to find out how widespread this phenomenon was. How many people have actually left this service and why? Quantitative research is good at providing broad information from a large number of units.

Thirdly, it is also possible that, although factors such as trust, security and risk are more pronounced in the category of people who have not adopted or have abandoned the service, it is possible that they could also influence the rate of adoption or some form of behaviour of internet bank users. The study wanted to establish how widespread the problem is and give the researcher some idea of what puts people off internet banking and how trust, security and perceived risk are influencing the patterns of usage of internet banking. Fourth, quantitative methods are best for looking at cause and effect (causality) as well as for the testing of theories and hypotheses. Thus, this study chose quantitative research methods as these were deemed to be the best suited method for the purposes of this study.

The number of abandoners of internet banking in this study is relatively small, but as internet banking becomes more widespread it is likely that the number of abandoners and the people not adopting services will increase. It is therefore important to understand these phenomena, in particular what role trust, security and perceived risk

play. Thus future studies will need to opt for qualitative or mixed methods such as interviews and in-depth case studies. Quantitative analysis is more useful when supported by qualitative data. Additionally, this will help designers and developers gain a comprehensive understanding of the need to generate suitable features that will increase the rate of service acceptance and continued use.

7.3.3 IMPLICATIONS FOR PRACTICE

The overall findings and results of this study contribute considerable value to research and practice in electronic business, from a wide perspective to the UK financial sector and, more specifically, to the British banking industry.

Very few previous studies have investigated, comprehensively, the reality of Internet banking in the UK. This study therefore contributes additional knowledge to the body of literature already existing on understanding the relationship between influencing factors (trust, security and risk) and patterns (non-adoption; abandonment; adoption and continued use) of Internet banking usage.

There is, therefore, a clear need for an understanding of the factors associated with customers' perceptions of Internet banking services that can direct the strategic plans of relevant decision-makers in order that they can enable effective use of these services. The findings of this research identify some important knowledge that can make these suggestions for managers and developers of banks and help them to formulate a strategy that maximise the level of their clients' acceptance.

The findings of this study have a number of important implications for future practice. The most significant implication for the banking industry is the need to create a beneficial service and to build a trusting relationship with customers, in order to

encourage adoption of their service, and a stabilisation of users. It is clear that the relationship between customers and banks will benefit from an effective Internet banking service, and customers' trust is a fundamental and valuable part of this relationship.

The evidence examined by this study suggests that trust has a clear influence on customers across all of the three study models. Therefore, banks should focus on putting trust-building mechanisms in place, as well as ensuring effective performance by building useful and easy to use websites.

Additionally, the findings also indicate that the relationship between customers and Internet banking services influenced all of the research hypotheses, except for those related to the effects of security on customers' intentions towards Internet banking, where the relationship was weak, thus leading to a partial rejection of the hypothesis.

In order to decrease customers' security concerns, banks should enhance their security procedures and reduce complexity, and this point was discussed in the literature review (section 3.2.2.3). In addition, the safety area model results (section 6.3.4) show that most of the users in the sample study (503) stated that banks should use multi-factor authentication, which uses two or more factors to establish identity (password – PIN), and biometric technologies such as retinal scan, facial recognition and fingerprints, rather than two-factor authentication methods to access Internet banking with enhanced security.

With respect to trust, banks should build systems, which should include providing warranties to reassure users who experience fraudulent transactions, as customers may be more willing to accept the perceived risk if they trust that their bank will support

them (as discussed in section 3.2.1.4). In addition, users (503) of the safety area model (section 6.3.4) stated that banks should provide sufficient safeguards, direct contact with bank staff in case of an emergency and show due diligence and responsibility when problems occur, all of which make users feel comfortable when making Internet banking transactions, and enhance customers' trust.

Furthermore, with regard to the perceived risk of Internet banking-based transactions, banks could reduce this by increasing customer awareness of safe Internet banking, and build an effective risk management strategy to identify risks and try to reduce them. It is worth mentioning here that in this study risk was shown to have an effect on customers' intentions across all models. In addition, the safety area model of this study in section 6.3.4 shows that, in regards to perceived risk, the majority of users in the sample study, which amounts to 503 samples, mentioned that banks should compensate for any money taken from user accounts via unauthorised transactions, in order to reduce the feeling of risk. Therefore, it is advised that banks in Leicester - the UK focus on the issues this study identifies, in order to develop their strategies, build desirable Internet banking services, and so increase their Internet banking customer base and retain their existing customers. To recap, these issues are:

- In the non-adoption and abandonment of Internet banking models, this study proposes and describes three factors that influence the development of online trust, as well as the necessary measures to enhance security and reduce risks, which will help to transform a customer from being an observer (non-user) to an adopter (user) of Internet banking services, and engender greater acceptance and adoption of Internet banking. The three factors this study identifies are trust,

security and perceived risk, which have been shown to influence the intentions of non-users and abandoners towards Internet banking services in the UK. Banks should identify these user groups and try to reach them through an effective, continuous promotional strategy, in order to gain an understanding of their behaviours so that a suitable strategy can be formulated that will change their convictions towards Internet banking.

- Regarding the initial adoption of Internet banking, trust has been shown to be an influencing factor for customers, whilst the effect of security and perceived risk on customers' intentions was shown to be negligible. Thus, the study used open questions to ask users about any other factors influencing their adoption of Internet banking service.

  Just 167 respondents (33.20 %) of the total sample of users (503), provided further reasons, which were as follows, in order of importance: convenience; ease of use; speed of performing transactions; time saving; ease of access - 24/7 anywhere and anytime; good monitoring, control and management of their account.

- However, what the research is interested in, in relation to this usage model, is how to maintain the number of customers who will continue to use the service. On this point, the findings showed that there was a clear influence of trust, security and perceived risk on customers' decisions and intentions towards continued use of Internet banking services.

  Thus, it is important that bank managers and decision-makers are more oriented towards imparting further benefits and providing the necessary support and guarantees to users, and encourage them to use Internet banking on a continuing

basis. To this end, they must build mechanisms that will enhance trust, security and reduce risk, as described above.

- Finally, the study findings have an important implication for future practice, regarding the identification of the safety area in which to utilise Internet banking services. The research identified this area using the information provided by current users, relating to the three dimensions of trust, security and perceived risk. It is recommended that bank administrators and decision-makers take advantage of this model and implement the recommendations of customers in order to retain them. The research contributions will discuss in next section.

7.4 RESEARCH CONTRIBUTIONS

The findings of this study make several contributions to the current research literature on online customer behaviour. The majority of previous research within the UK has studied only the initial adoption of Internet banking; just a very few studies have examined the behaviour of non-users (Gerrard et al., 2006: White and Nteli, 2004), or that of continuing users of Internet banking. The researcher believes that this study is the first to examine the behaviour of customers who have abandoned Internet banking services in the UK.

The findings of this study therefore make a significant contribution to the existing body of literature, as it is the first to comprehensively study the patterns of customers' behaviour in relation Internet banking in the UK. It does this by proposing separate models for non-users, abandoners of the service and current, continuing users, and finally, a paradigm aimed at determining safety area in which to utilise Internet banking

services. Through testing the hypotheses, addressing the research questions and validating the research models this study has made significant contributions to knowledge in this area, as described below:

1- As discussed in the literature review, some studies mentioned that, there is a reduction in the rate of uptake of Internet banking services in UK and it is lagging behind the US, Germany and France. Furthermore, it appear that these studies suggest there is an increase in the number of Internet users, but the level of Internet banking usage has not increased at the same rate (Jayawardhena and Foley, 2000; White and Nteli, 2004; Yousafzai and Yani-de-Soriano, 2012; Office for National Statistics, 2013). According to these perceptions this study has developed a model of non-adoption, which specifically examines and validates the impact of trust, security and perceived risk on the non-adoption of Internet banking in the UK. This model will provide valuable information for decision makers in banks, and may also be of benefit for future researchers in this country. Prior to this study, this model had not been applied or validated in a UK context, as research is almost non-existent in this field.

   Therefore, the validation of this model is the first contribution made by this study. This model makes a further significant contribution to the current literature by elucidating the fact that more than one-third of the study sample were non-users of Internet banking, and that for them, trust, security and perceived risk are significant influences on their behaviour and decision-making. In short, there is dearth of evidence, which had been carried out on this area in the UK. This study has investigated this phenomenon and discovered the

significant factors of relevance to non-adoption of Internet banking in Leicester in the UK. This adds value to the body of knowledge to develop services and to motivate customers to use Internet banking.

2- In Internet banking studies, Yousafzai and Yani-de-Soriano (2012) recommended that it is important to examine if customers leave Internet banking services; they also claimed that there are indicators about abandonment of Internet banking in the UK. This position is echoed by Forrester's research (Forrester research, 2008).

Based on this reasoning, the present study asserts that there were few customers who abandoned Internet banking services post-adoption; they represented just 5.30%, or 44 customers out of an overall study sample of 838. The study was able to achieve this finding by developing an 'abandonment' model, which was implemented and thereby validated as a model for abandoners of Internet banking. This model specifically examines the impact of trust, security and perceived risk on the abandonment of Internet banking in the UK. Despite that the proportion of users who abandoned Internet banking in this study is relatively small, but as Internet banking services becomes more widespread it is likely that the numbers of abandoners will increase. It is therefore important to understand users abandon Internet banking and in particular what role trust, security and perceived risk have in controlling or minimising abandonment. Scientific analysis of pattern of abandonment can therefore provide the basis for prevention of widespread abandonment of Internet banking as discussed in section 6.4.2.

This is an important contribution of the present study, as it constitutes the first investigation of the behaviour of customers who give up on Internet banking services in Leicester. This research discovered a significant phenomenon of the relevance in abandonment of Internet banking services in UK. This represents a unique contribution to the body of knowledge in main area. This new contribution will help future researchers in considering this phenomenon from a consumers needs' perspective

3- As discussed in section 6.4.3 there is a lack of research that has been carried out in the UK to investigate the continued use of Internet banking and identifying factors that influence the post-adoption phase of Internet banking. Due to the importance of this stage, earlier studies recommended an examination of post-adoption stage in future research (Adapa, 2011; Choudhry et al., 2013). Moreover, future research should examine the relationship between the variables that influence continued usage of Internet banking services. Therefore, the third model developed by this study is the adoption and continuity model, which specifically examines the influence of trust, security and perceived risk on the adoption and continued usage of Internet banking in Leicester- the UK. The study implemented and validated this as a model for users of Internet banking. The findings of this model contribute to literature in the industrial banking field; for example, the outcomes show that trust has a direct effect on customers' intentions towards the adoption of Internet banking, whilst security and perceived risk were shown to have a weak influence.

Furthermore, the study has revealed that one-third of the users sampled cited further reasons other than trust, namely: convenience; ease of use; speed of performing transactions; time saving; ease of access 24/7 anywhere and anytime; good monitoring, control and management of accounts. However, the findings of this model, with regard to continued use of Internet banking services, show that current users expect that a combination of trust, security and perceived risk factors will have influence their decisions and intentions regarding continued use of Internet banking services in the future.

In addition, the present model is that it has enabled an understanding of the influence that the identified factors have on each other toward adoption and continuity of usage of Internet banking. The findings demonstrate that there is a relationship between the three factors; the results indicated that the perceived risk of Internet banking had an impact on trust, showing a low negative correlation, whilst the relationship between security and trust had a strong positive correlation. These outcomes indicate that increased security of Internet banking will enhance trust, and reduce perceived risk, showing a moderate negative correlation between security and perceived risk.

This model has investigated the post-adoption stage and discovered the significant factors that mention the relevance of adoption and continuity of usage in Internet banking in Leicester. This represents an important contribution to the body of knowledge, especially as it relates to the stage of continuity or abandonment of use.

4- The study provides a further significant contribution to the current literature in this field in the development of a model of safety area for Internet banking services, because most of the studies in literatures of Internet banking industry have focused on building models related to either adoption and non-adoption such as (Adapa, 2011; Yousafzai and Yani-de-Soriano, 2012; Al-Fahim, 2013; Alihosseini, 2014; Farzianpour et al., 2014; Kaur and Kiran, 2015). Based on this reasoning, the present study has built a safety area model that provides new ideas to reach safe areas to use this service securely, with three factors combined, so as to achieve the desired degree of customer trust, an appropriate level of security and a low-risk environment. This research identified the safety area as being located between 53%, 51% and 9% for trust, security and risk respectively, as this research has discussed in section 6.4.4. These three factors in this model may not necessary be used in future research but the framework provides an opportunity for others factors to be added in the future. Thus, this model can therefore serve as a basis for future studies and illustrate safety areas in which to utilise Internet banking, as this may vary between environments, time periods, and circumstances. In short, this research has built a significant model (safety area model) regarding Internet banking services in Leicester. The next section will discuss limitations of the research.

7.5 LIMITATIONS OF THE RESEARCH

As already stated, this study attempts to provide a simple contribution to the body of knowledge surrounding Internet banking. The study developed conceptual models and

validated these by using a sample of Internet banking customers in the United Kingdom. The study succeeded, to some extent, in answering the research questions; however, as with any research associated with customer behaviour, there were a number of limitations, detailed as follows:

1- The range of the study was limited to one city in the UK, Leicester. The study targeted both users and non-users of Internet banking services, as well as customers who had abandoned the service. Thus, the results could have limited generalisability, and so findings may vary if the study is applied to other cities.

2- The study employed a quantitative research method only. This may have limited the freedom of the participants in their answers, as they were only able to respond to questions of what? Rather than rationale and reasoning which may have limited research engulfed understanding of the reasons underlying the perceptions of the participants and their behaviour.

3- The study was restricted by time, but the possibility of change over time and experience in using the technology indicate that a longitudinal study may be useful, particularly regarding the safety area model. Therefore, after the implementation of the recommendations by banks and a possible re-definition of the safety area, this model should be studied again. Time also provides the opportunity to gain a broader coverage, a study that is more comprehensive in terms of the number of individuals, and also geographically, including other cities. This would provide the opportunity to explore whether there are others

non-users and abandoners of Internet banking services, and the reasons underlying their intentions.

In spite of the limitations encountered by this study, the research has succeeded, to some extent, in illuminating the reality of Internet banking in the UK. It has also succeeded, again to some extent, in highlighting new findings in the field of acceptance and non-acceptance of Internet banking services. Additionally, the study has somewhat succeeded in answering the research questions.

7.6 FUTURE WORK

Aside from interesting research findings, clear responses to the study questions and the validation of hypotheses, several related areas were encountered, which would benefit from additional investigation. The following are proposals for future research:

1- As mentioned previously, this research was conducted in as single city; i.e. Leicester city, in the UK. Therefore, the outcomes could have limited generalisability. Hence, future research should aim to replicate similar research and sampling to include consumers' from other cities in the UK, including non-users, users, abandoners and re-application as safety area model. This would enhance knowledge and provide a larger body of information. This would also generate findings to assist in developing strategies to contribute to the development of these services in the UK.

2- Conducting additional research to provide a greater insight into the usage continuity model proposed in the present study would be useful, in order to discover whether or not customers' behaviour in regard to the use of Internet

banking is subject to over time. Moreover, the study could examine other possible factors that may impact on consumers' continued usage in the UK.

3- Studies related to consumer behaviour, business services and marketing areas generally focus on quantitative findings neglecting the qualitative data. As the present study describes in the methodological implications section, further research could usefully examine the relevance of using additional mixed methodological approaches. A mixed method would be useful to replicate the study in the UK or in other countries. This would enable researchers to gain greater insights and information into the underlying factors pertaining to customers' perceptions.

4- Future research could also improve the safety area model developed in the present study by investigating the role of study factors, or by examining other factors across different time periods and in different locations. This could then exert an influence in this area, facilitating comparisons between findings.

5- It is dangerous and often inaccurate to generalise the results of studies that relate to consumer behaviour, and current research is no exception. The survey was performed in the UK and it targeted all consumer patterns.

Future studies could be conducted to further investigate the conceptual models developed in the present study in different countries for comparative purposes, consequently providing greater insight into these phenomena, as well as providing further insight into factors such as exploitation, accessibility services quality, word of mouth, the media, changes in banking laws and the role of alternative banking services influencing customers to adopt, non-adopt or abandon internet banking services. Also further studies on how the factors of

trust, security and risk affect customer behaviour should be studied more deeply. The findings may provide alternate results, which would increase the scope of the literature in this field. Also this study recommends investigating the effect of other factors on trust, security and risk and their influence on customers' behaviour towards internet banking service in the UK.

7.7 CHAPTER SUMMARY

The primary objective of this study was to assess the reality of behaviour patterns towards Internet banking in Britain among existing bank customers. Thus, the research attempted to explore the influence of trust, risk and security on non-adoption, adoption and cessation of Internet banking behaviours. Accordingly, it uncovered behavioural insights by post-adoption users, in terms of Internet adoption, migration, engagement, sustainability and abandonment behaviours.

In summary, the study developed three theoretical models for studying customers' behavioural models, namely: non-adoption, adoption and abandonment of Internet banking. One of the most important aims was also to design a model (theoretical model) of trust, risk and security to reach safety area for the exercise of Internet banking. In addition, to unearth the relationship between trust, security and risk as it influences Internet banking adoption in Leicester-the UK.

The empirical results were related to eight research questions: (1) Do trust, security and risk have an effect on customers' decisions or intentions regarding the non-adoption of Internet banking? (2) Do trust, security and risk have an effect on customers' decisions and intentions regarding the abandonment (giving up) of Internet banking? (3) Do trust, security and risk have an effect on customers' decision and intentions regarding the

adoption of Internet banking? (4) What constitutes 'significant' degrees of trust, risk and security when considering customers' decision-making process in relation to Internet banking engagement sustainability (continuity of use)? (5) Does a perceived risk related to Internet banking affect customers' levels of trust? (6) Does the security of Internet banking affect customers' levels of trust? (7) Does the security of Internet banking affect the perceived risk? (8) What is the safety combination of trust, security and perceived risk, which would determine desired levels of usage and degrees of Internet banking services satisfactions?

The main results of this study suggest the following: that safety area can be identified, according to customers' recommendations, and made ready for application by the banks. Also, regarding the non-adoption model, one-third of the study sample were non-users of the service, and three factors influenced customers' intentions in the non-adoption of internet banking services. The investigation has also shown that in the abandonment model, few customers abandoned Internet banking services.

Also, trust, security and perceived risk exert an influence on customers' intentions to stop using the service. The results also reveal that current users expect that trust, security and perceived risk will have an effect on their intentions and decisions to continue using Internet banking in the future.

It was also shown that there was a relationship between trust, security and perceived risk and that these aspects all influence each other. The present study was based on the findings of research questions, and validating the research models has contributed to knowledge by providing an understanding of customers' behaviour toward Internet banking services, as well determining the role of trust, security and perceived risk in influencing customers' intentions.

As discussed earlier in this study, a safety area model has been designed and developed to engage in Internet banking safely, through building a comprehensive model of a safety area. When applied to a particular case study, the model will help to determine the safety area for that particular case study. In addition, as customer service is important, this knowledge can have a practical application that will improve service provision and be satisfactory for customers. In addition, the problem the model addresses is based on a real life problem; therefore, throughout this work, improving customer service is the underlying motivation.

The subject of trust in this study has been adequately dealt with by examining the concept from several perspectives, and its influence on three categories of customers: non-users, users and abandoners, in regards to continuing usage of Internet banking. The outcomes show that trust has a direct and significant influence on customers' intentions towards Internet banking services, for all categories (non-users, abandoners, users and continuous usage). In addition, there is a relationship between trust, security and perceived risk in regards to Internet banking in Leicester.

The study has also adequately addressed the subject of security by investigating its influence on non-users, users, abandoners and continuous usage of Internet banking in Leicester, UK. The research shows that security has a considerable effect on customers' attitudes towards Internet banking services, across non-users, abandoners and continuous usage categories, whereas its impact on the adoption of Internet banking is weak.

Lastly, the subject of risk has been adequately addressed, through considering the relationship between perceived risk, all of the aforementioned categories and Internet

banking services in Leicester. It is found that there is a direct and a significant relationship between perceived risk and customers' behaviour towards Internet banking services, across the non-use, abandoners and continuous usage groups. At the same time, the relationship shows that weak security influences the adoption of services (as discussed in sections 6.3 and 6.4).

However, there are other areas of future work beyond the scope of this research, in regards to trust, security and perceived risk, although this study has investigated the relationship between these factors and use of Internet banking services in Leicester. This is because trust is not a single monolithic structure, but rather has a multi-dimensional relationship with different factors that influence the service. Therefore, an interesting future study might investigate the relationship between these factors and other affective factors widely in the UK. This may help to explain customers' behavioural patterns, whether in the pre or post adoption stages of internet banking, in order to reach definite conclusions.

From the above, it is apparent that there has been an abandonment of services; although a small problem now, as use of Internet banking increases and more users begin to adopt it, abandonment could become a barrier to further development. Certainly, it is essential to consider that perceived risk, security and trust are important factors in rates of abandonment. As for the non-adoption of services, in spite of Internet usage growing rapidly in the UK, there is still significant number of non-users of Internet banking services, as shown in this study. As mentioned earlier in this study, to the best of the researcher’s knowledge, this is the first study to develop a comprehensive model for Internet banking to explain usage, non-usage, abandonment and continuity of Internet banking services usage. Hence, the unique contribution of this research is the

identification of abandonment as a potential barrier to future progress. For this reason, defining a safe area is used to define and analyse new cases as they arise.

The findings of this research can be used by banks to improve the image of Internet banking services, and give banks knowledge of how problems can be solved. This research used an analytical process, based on models and outcomes. The banks can use this to inform customers when problems are identified and how the bank will solve these; this helps to build the reputation of the bank and enhance customer trust, in both the bank and internet banking services. In short, study models can be used to improve internet banking services through addressing the issues that are likely to affect the future of internet banking services.

This study makes just a modest contribution to the abundance of science and knowledge in this field; the hope is that it has contributed something useful to the advancement of this service.

REFERENCES

- Abbad, M., Abed, H., and Abbad, M. (2012) the development of e-banking in developing countries in the Middle East. *Journal of Finance, Accounting and Management*, 3 (2), pp.107-123.

- Abbass, S. and Ibrahim, O. (2011) A Model for Trust-building in E-commerce from Consumer to Consumer Perspective in KSA. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 1 (3), pp. 223-227.

- Abdellaoui, R. and Pasquet, M. (2010) Secure Communication for Internet Payment in Heterogeneous Networks. *International Conference on Advanced Information Networking and Applications*, pp.1085-1092.

- Abukhzam, M. and Lee, A. (2010) Factors Affecting Bank Staff Attitude Towards E-banking Adoption In Libya. *The Electronic Journal on Information Systems in Developing Countries*, 42(2), 1-15.

- Adapa, S. (2011) Continued and Frequent Use of Internet Banking by Australian Consumers: Identification of The Factor Components. *Journal of Internet Banking and Commerce*, 16(2) .pp.1-22.

- Adepoju, A. and Alhassan, M. (2010) Challenges of Automated Teller Machine (ATM) Usage and Fraud Occurrences in Nigeria- A Case Study of Selected Banks in Minna Metropolis. *Journal of Internet Banking and Commerce*, 15(2), pp.1-10.

- Aderonke, A. and Charles, A. (2010) an Empirical Investigation of the Level of Users' Acceptance of E-Banking in Nigeria. *Journal of Internet Banking and Commerce,* 15 (1), pp.1-13.

- Ahmad, A. and Al-Zubi, H. (2011) E-banking Functionality and Outcomes of Customer Satisfaction: An Empirical Investigation. *International Journal of Marketing Studies,* 3 (1), pp. 50 -65.

- AI Somali, Z. and Ghinea, G. (2012) Investigation of factors affecting growth of e-banking services in Saudi Arabia. *International Conference for Internet Technology and Secured Transactions,* pp.583-588.

- Akbari, P., Najafi, Y., and Arfaei, A. (2013) Comparison and Ranking Factors of Effect on Customer's Satisfaction of Electronic Banking Service Quality in Public and Private Banks of West Iran. *International Journal of Management and Humanity Sciences,* 2 (1), pp. 44-52.

- Akhlaq, A. and Ahmed, E. (2013) the effect of motivation on trust in the acceptance of internet banking in a low income country. *International Journal of Bank Marketing,* 31 (2), pp.115-125.

- Akhlaq, M. and Shah, A. (2011) Internet Banking in Pakistan: Finding Complexities. *Journal of Internet Banking and Commerce,* 16 (1), pp.1-14.

- Aktan, B., Teker, E., and Ersoy, P. (2009) Changing face of banks and the evaluation of internet banking in Turkey. *Journal of Internet Banking and Commerce,* 14 (1), pp.1-11.

- Al-Ajam, A. and Nor, K. (2013) Internet Banking Adoption: Integrating Technology Acceptance Model and Trust. *European Journal of Business and Management,* 5 (3), pp.207-215.

- Aldas-Manzano, J., Lassala-Navarre, C., Mafe, C., and Sanz-Blas, S. (2009) Key drivers of internet banking services use. *Online Information Review,* 33 (4), pp. 672-695.

- AL-Fahim, N. (2012) Factors Affecting the Adoption of Internet Banking Amongst IIUM' students: A Structural Equation Modelling Approach (SEM). *Journal of Internet Banking and Commerce,* 17 (3), pp.1-14.

- Alihosseini, O. (2014) an Overview of Electronic Services and Electronic Banking Quality. *Universal Journal of Management and Social Sciences*, 4 (4), pp. 55-59.

- Aliyu, A., Younus, M., and Tasmin, R. (2012) an Exploratory Study on Adoption of Electronic Banking: Underlying Consumer Behaviour and Critical Success Factors, Case of Nigeria. *Business and Management Review*, 2 (1), pp. 1-6.

- Aljazzaf, M., Perry, M., and Capretz, A. (2010) Online trust: Definition and principles. *IEEE*, pp. 163-168.

- Ally, M. and Toleman, M. (2005) A Framework for Assessing Payment Security Mechanisms and Security: Information on e-Commerce Web Sites. *Proceedings of the 9th Pacific Asia Conference on Information Systems*, pp.1216-1231.

- AL-Majali, M. (2011) The Use of Theory Reasoned of Action to Study Information Technology in Jordan. *Journal of Internet Banking and Commerce*, 16 (2). pp, 1-11.

- Almohaimmeed, B. (2012) *Customer behaviour towards internet banking: A study of dormant users of Saudi Arabia*. Unpublished thesis (PhD), The University of Birmingham.

- Alnsour, M. and Alhyari, K. (2011) Internet Banking and Jordanian Corporate Customers: Issues of Security and Trust. *Journal of Internet Banking and Commerce,* 16 (1), pp.1-14.

- Al-Rfou, A. (2013) the usage of internet banking evidence from Jordan. *Asian Economic and Financial Review*, 3 (5), pp. 614-623.

- Alsaffar, E. and Sun, L. (2009) A design of e-procurement infrastructure model for public service sector. *In Computer Science and Information Technology*, pp. 192-196.

- Alsajjan, B. and Dennis, C. (2006) the Impact of Trust on Acceptance of Online Banking. *European Association of Education and Research in Commercial Distribution*, pp.1-19.

- Alsajjan, B. and Dennis, C. (2010) Internet banking acceptance model: a cross-market examination. *Journal of Business Research*, 63 (1), pp.1-19.

- Al-Shawabkeh, M., Saudi, M., and Alwi, M. (2015) Computer security factors effects towards online usage of internet banking system. *Journal of Engineering and Applied Sciences*, 10(2), pp. 532-539

- Alsheyyab, M. and Singh, D. (2013) Effect of Trust on E-Banking User's Satisfaction: A Review. *Research Journal of Applied Sciences, Engineering and Technology*, 5(4), pp. 1397-1406.

- Al-Smadi, M. (2012) Factors Affecting Adoption of Electronic Banking: An Analysis of the Perspectives of Banks' Customers. *International Journal of Business and Social Science*, 3 (17), pp. 294-309.

- Al-Somali, A., Gholami, R., and Clegg, B. (2009) an investigation into the acceptance of online banking in Saudi Arabia. *Technovation*, 29 (2), pp.130-141.

- Altintas, M. and Gursakal, N. (2007) Phishing Attacks and Perceptions of Service Quality: A Content Analysis of Internet Banking in Turkey. *Journal of Internet Banking and Commerce*, 12 (2), pp.1-1.

- Amin, H. (2007) Internet Banking Adoption among Young Intellectuals. *Journal of Internet Banking and Commerce*, 12 (3), pp.1-13.

- Anguelov, E., Hilgert, A., and Hogarth, M. (2004) US consumers and electronic banking, 1995-2003. *Fed. Res. Bull*, 90(1), pp.1-18.

- Ankit, S. (2011) Factors Influencing Online Banking Customer Satisfaction and Their Importance in Improving Overall Retention Levels: An Indian Banking Perspective. *Information and Knowledge Management*, 1 (1), pp.45-54.

- Aristeidis, C. and Ioannis, M. (2010) A study on user behavior and acceptance of electronic banking services. *14th Panhellenic Conference on Informatics*, pp.180- 183.

- Ashtiani, P. and Iranmanesh, A. (2012) new approach to study of factors affecting adoption of electronic banking services with emphasis on the role of positive word of mouth. *African Journal of Business Management*, 6 (11), pp. 4328-4335.

- Auta, E. (2010) E-banking in developing economy: Empirical evidence from Nigeria. *Journal of applied quantitative methods*, 5 (2), pp.212-222.

- Ayo, K., Adewoye, O., and Oni, A. (2010) the State of e-Banking Implementation in Nigeria: A Post-Consolidation Review. *Journal of Emerging Trends in Economics and Management Sciences*, 1 (1), pp.37-45.

- Azim, M., Ahmed, E., and D'Netto, B. (2011) Corporate Social Disclosure in Bangladesh: A study of the Financial Sector. *International Review of Business Research Papers*, 7 (2), pp.37-55.

- Azouzi, D. (2009) the adoption of electronic banking in Tunisia: An Exploratory Study. *Journal of Internet Banking and Commerce*, 14 (3), pp.1-11.

- Baabdullah, A., Dwivedi, K., and Williams, D. (2013) IS/IT Adoption Research in The Saudi Arabian Context: Analysing Past and Outlining Future Research Directions. *In European, Mediterranean and Middle Eastern Conference on Information Systems*, pp. 17-18.

- Bahtiyar, S. and Caglayan, M. (2013) Security similarity based trust in cyber space. *Knowledge-Based Systems*, 52(1), pp. 290-301.

- Bakar, M. (2011) Online and E-banking (Convenience and Risks of Security Breaches). *Journal of Business and Globalization*, 2(1), pp. 49-55.

- Banakdeh, R. and Ganginia, H. (2014) check out effective factors on customers trust in Internet banking services (Bank Mellat branches gullan province). *Indian Journal of Fundamental and Applied Life Sciences*, 4 (1), pp. 688-698.

- Bartlett, W. and Prica, I (2011) The Variable Impact of the Global Economic Crisis In South East Europe. *Economic annals*, pp.7-34.

- Baten, M. and Kamil, A. (2010) E-Banking of Economic Prospects in Bangladesh. *Journal of Internet Banking and Commerce*, 15 (2), pp.1-10.

- Bauer, K. and Hein, S. (2006) the effect of heterogeneous risk on the early adoption of Internet banking technologies. *Journal of Banking and Finance*, pp. 1713–1725.

- Belanger, F. and Carter, L. (2008) Trust and risk in e-government adoption. *Journal of Strategic Information Systems*, 17(1), pp. 165–176.

- Beldad, A., De Jong, M., and Steehouder, M. (2010) How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, 26(5), pp. 857-869.

- Biswas, S., Taleb, A., and Shinwary, S. (2011) Electronic Banking in Bangladesh: Security Issues, Forms, Opportunities and Challenges. *Canadian Journal on Scientific and Industrial Research*, 2 (5), pp. 181-194.

- Blumberg, B., Cooper, D., and Schindler, P. (2008) *Business research Methods*. Second edition. Published by McGraw-Hill Education in the UK.

- Borland, H. and Nteli, F. (2005) do all UK online banking customers want the same kind of service. *The university of Birmingham*, pp.1-27.

- Boyacioglu, A., Hotamis, N., and Cetin, H. (2010) an evaluation of Internet banking in Turkey. *Journal of Internet Banking and Commerce,* 15 (2), pp.1-32.

- Bryman, A. (2008) *Social Research Methods*. 4th edition. New York: United State by Oxford University Press Inc.

- Bryman, A. (2012) *Social Research Methods*. 4th edition. New York: United State by Oxford University Press.

- Bryman, A. and Bell, E. (2011) *Business Research Methods*. 3rd Edition. Oxford University Press Inc., New York.

- Bryman, A., and Bell, E. (2015) *Business research methods*. Oxford university press.

- Capece, G. and Campisi, D. (2013) A Behavioural Model of E-Banking Usage in Italy. *International Journal of Engineering Business Management*, 5 (1), pp.1-9.

- Celik, H. (2008) what determines Turkish customers' acceptance of internet banking? *International Journal of Bank Marketing*, 26 (5), pp. 353-370.

- Centeno, C. (2002) Building Security and Consumer Trust in Internet Payments: The potential of "soft" measures. *Institute for Prospective Technological Studies*, pp.1-39.

- Centeno, C. (2004) Adoption of Internet services in the Acceding and Candidate Countries, lessons from the Internet banking case. *Telematics and Informatics*, pp. 293-315.

- Chakrabarti, A. and Manimaran, G. (2002) Internet Infrastructure Security: Taxonomy. *IEEE*, 16 (6), pp, 13-21.

- Chambers, C. and Turksen, U. (2010) E-banking and e-fraud: A comparison investigation in Jamaica and the UK. *IEEE*, pp, 345-352.

- Chan, C., Wong, W., Lee, M., and Chi, I. (2009) Modified automatic teller machine prototype for older adults: A case study of participative approach to inclusive design. *Applied Ergonomics*, 40 (2), pp.151-160.

- Chang, F. (2009) *How teacher questioning behaviours assist and affect language teaching and learning in EFL classrooms in Taiwan*. Unpublished thesis (PhD) University of Warwick.

- Chang, H. and Hamid, B. (2010) an empirical Investigation of Internet banking in Taiwan. *Global Journal of Business Research*, 4 (2), pp. 39-48.

- Chang, K., Cheung, W., and Tang, M. (2013) Building trust online: Interactions among trust building mechanisms. *Information and Management*, 50 (7), pp.439-445.

- Chang, Y. (2005) Dynamics of Internet Banking Adoption, ESRC Centre for Competition Policy, *University of East Anglia*, pp.1-63.

- Chau, P. and Hu, P. (2001) Information technology acceptance by individual professional: A model comparison Approach. *Information technology acceptance*, 32 (4), pp. 719-699.

- Chen, Y. and Barnes, S. (2007) Initial trust and online buyer behaviour. *Industrial Management and Data Systems*, 107 (1), pp. 21-36.

- Chen, Y. H. (2011). Mr. Risk! Please trust me: Trust antecedents that increase online consumer purchase intention. *Journal of Internet Banking and Commerce*, 16 (3). pp, 1-23.

- Cheng, S., Lee, J., and Lee, R. (2014) User Resistance of Mobile Banking in China: Focus on Perceived Risk. *International Journal of Security and Its Applications*, 8 (2), pp. 167-172.

- Cho, V. (2006) A study of the roles of trusts and risks in information-oriented online legal services using an integrated model. *Information and Management*, pp. 502–520.

- Chong, A., Ooi, B., Lin, B., and Tan, I. (2010) online banking adoption: an empirical analysis. *International Journal of Bank Marketing*. 28 (4), pp. 267-287.

- Choudhry, G., Gupta, R., and Gupta, P. (2013) Dimensions Affecting Consumers' Continued Usage and Frequency of Usage of Internet Banking: Empirical Evidence from India. *International Journal of Engineering and Innovative Technology*, 2 (12), pp.21-32.

- Chuang, C. and Hu, F (2011) An Empirical Study of Customers' Perception of E-Banking Service Based on Time Usage. *Journal of Internet Banking and Commerce*, 1(2), pp.1-11.

- Churchill, G. and Iacobucci, D. (2002) *Marketing research: methodological foundations*. Eighth edition. Michael P. Roche.

- Chuttur, M. (2009) Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *Indiana University, USA. Sprouts: Working Papers on Information Systems*, 9 (37), pp. 1-23.

- Clemes, M. D., Gan, C., and Du, J. (2012) the factors impacting on customers' decisions to adopt Internet banking. *Banks and Bank Systems*, 7(3), pp. 33-50.

- Cohen, J. (1988) *Statistical power analysis for the behavioural sciences*. Second Edition. Lawrence Erlbaum Associates, Inc. New Jersey.

- Cohen, L., Manion, L., and Keith, M. (2011) *Research Methods in Education*.7th ed. Routledge in the USA and Canada.

- Coles, G. and Smart, W. (2011) Building Trust in Online Customers. *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp.93-98.

- Colesca, S. (2009) Increasing e-trust: A solution to minimize risk in e-government adoption. *Journal of applied quantitative methods*, 4 (1). pp, 31-44.

- Cousineau, D., and Chartier, S. (2010) Outliers detection and treatment: a review. *International Journal of Psychological Research*, 3 (1), pp. 58-67.

- D'Alessandro, S., Girardi, A., and Tiangsoongnern, L. (2012) perceived risk and trust as antecedents of online purchasing behavior in the USA gemstone industry. *Asia pacific journal of marketing and logistics*, 24 (3), pp. 433-460.

- Dalhatu, U., Abdullah, B., Ibrahim, Y., and Abideen, A. (2014) Nigerian Retail Customers' Adoption of Online Banking in an Islamic Bank. *Global Business and Management Research: An International Journal*, 6 (3), pp. 237-245.

- Daneshgadeha, S and Yildirima, S. (2014) Empirical investigation of internet banking usage: The case of Turkey. *Procedia Technology*, 16 (1), pp. 322-331.

- Daniel, E. (1999) Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of Bank Marketing*, 17 (2), pp.72-82.

- Dapp, T. (2013) Silver surfers: The importance of older generations for the internet. *Banking and Technology Snapshot Demography*, pp.1-7.

- Dauda, Y., Santhapparaj, S., Asirvatham, D., and Raman, M. (2007) The Impact of E-Commerce Security and National Environment on Consumer adoption of Internet Banking in Malaysia and Singapore. *Journal of Internet Banking and Commerce,* 12 (2), pp.1-20.

- Davis, F. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, pp.319- 340.

- Delafrooz, N., Taleghani, M., Karami, R. and Moradi, A. (2013) Factors Affecting the Adoption of Internet Banking. *International Journal of Business and Behavioural Sciences*, 3 (2), pp.82-100.

- Delgado, O., Sabater, A., and Sierra, M. (2008) Analysis of new threats to online banking authentication schemes. *ACTAS DE LA X RECSI, Salamanca*, pp.337-344.
- Delong, G. and De Young, R. (2007) Learning by Observing: Information Spill overs in the Execution and Valuation of Commercial Bank M&As. *The Journal of Finance,* 1(1), pp.181-216.

- Demirdogen, O., Yaprakli, S., Yilmaz, K., and Husain, J. (2010) Customer Risk Perceptıons of Internet Bankıng - A Study In Turkey. *Journal of Applied Business Research*, 26(6), pp. 57-68.
- Dillman, D. (2007) *Mail and internet surveys*. 2th edition. Published by John Wiley and Sons, Inc., Hoboken, New Jersey.

- Dimitriadis, S and Kyrezis, N (2008) Does trust in the bank build trust in its technology-based channels? *Journal of Financial Services Marketing*, 13 (1), pp. 28-38.

- Dolatabadi, H. and Ebrahimi, H. (2010) Factors Influencing Iranian Consumers' Trust in Internet Shopping. *European Journal of Social Sciences*, 16 (2), pp.307-318.

- Donner, J. and Tellez, C. (2008) Mobile banking and economic development: Linking adoption, impact, and use. *Asian Media and Information Centre* .pp.1-24.

- Doost, H. and Ashrafi, A. (2014) Relationship of Online Service Quality with Customer Satisfaction in Internet Banking Case Study: Pasargad Bank. *International Journal of Economy, Management and Social Sciences*, 3 (1), pp. 130-135.

- Downs, D. and Hausenblas, H. (2005) The Theories of Reasoned Action and Planned Behavior Applied to Exercise: A Meta-analytic Update. *Journal of Physical Activity and Health*, 2 (1) pp.76-97.

- Dulcic, Z., Pavlic, D., and Silic, I. (2012) Evaluating the intended use of Decision Support System (DSS) by applying Technology Acceptance Model (TAM) in business organizations in Croatia. *Procedia-Social and Behavioural Sciences*, 58 (1), pp.1565 -1575.

- Eanas, A. and Sun, L. (2009) E-governments' Role Activation in Arab Countries. *In Information Management and Engineering*, pp. 617-623.

- Echchabi, A. (2011) Online Banking Prospects in Morocco: An Extension of Technology Acceptance Model. *Journal of Internet Banking and Commerce*, 16 (3), pp.1-13.

- El-Kasheir, D., Ashour, A., and Yacout, O. (2009) Factors affecting continued usage of internet banking among Egyptian customers. *Communications of the IBIMA*, 9 (29), pp. 252-263.

- Esmaili, E., Desa, M., Moradi, H., and Hemmati, A. (2011) the role of trust and other behavioural intention determinants on intention toward using internet banking. *International Journal of Innovation, Management and Technology*, 2 (1), pp. 95-100.

- Eze, C., Manyeki, K., Yaw, H., and Har, C. (2011) Factors Affecting Internet Banking Adoption among Young Adults: Evidence from Malaysia. *International Conference on Social Science and Humanity*, 5 (1), pp.377-381.

- Faroughian, F., Kalafatis, P., Ledden, L., Samouel, P., and Tsogas, H. (2012) Value and risk in business-to-business e-banking. *Industrial Marketing Management,* 41(1), pp.68-81.

- Farzianpour, F., Pishdar, M., Shakib, D., and Toloun, H. (2014) Consumers' Perceived Risk and its Effect on adoption of online banking services. *American Journal of Applied Sciences,* 11 (1), pp. 47-56.

- Fatima, A. (2011) E-Banking Security Issues -Is There A Solution in Biometrics. *Journal of Internet Banking and Commerce*, 16 (2), pp.1-9.

- Featherman, M. and Pavlou, P. (2003) Predicting e-services adoption: a perceived risk facets perspective. *International journal of Human-Computer Studies*, pp. 451–474.

- Featherman, S., Miyazaki, D., and Sprott, E. (2010) Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, 24 (3), pp. 219-229.

- Field, A. (2009) *Discovering statistics using SPSS*. Third edition. Sage publications Ltd, London.

- Financial Fraud Action UK (2011) *Deception crimes drive small increase in card fraud and online banking fraud losses*, pp.1-4.

- Financial Fraud Action UK (2013) Fraud the Facts 2013. *The UK Payments Administration*, pp.1-101.

- Financial Fraud Action UK (2014) Fraud the Facts 2014. *The UK Payments Administration*, pp.1-100.

- Finextra Research (2011) *Brits happy with online banking; mobile uptake slow, social media a no-no* [www] Finextra website. Available from: http://www.finextra.com [Accessed: 9/5/2012].

- Finextra Research (2011) *UK banking fraud losses at their lowest for a decade* [WWW] Finextra website. Available from: http://www.finextra.com [Accessed in 09/05/2012].

- Finextra Research (2012) *Young Brits still visit bank branches-they're usually closed though* [www] Finextra website. Available from: http://www.finextra.Com [Accessed 21/8/2012].

- Finextra, (2006) *Security fears scare off US customers from online banking, shopping* [www] Finextra website. Available from: http://www.finextra.com [Accessed 23/11/2011].

- Fisher, M. and Marshall, A. (2009) Understanding descriptive statistics. *Australian Critical Care*, 22 (2), pp.93-97.

- Flavian .C and Guinaliu .M (2006) Consumer trust, perceived security and privacy: policy three basic elements of loyalty to a web site. *Industrial Management and Data Systems,* 106 (5), pp. 601-620.

- Floros, C. (2008) Internet Banking Websites Performance in Greece. *Journal of Internet Banking and Commerce,* 13 (3), pp. 1-9.

- Foon, Y. and Fah, B. (2011) Internet Banking Adoption in Kuala Lumpur: An Application of UTAUT Model. *International Journal of Business and Management,* 6 (4), pp. 161-167.

- Forrester Research (2008) *Internet banking goes mainstream in US and UK* [www] Available From: www.finextra.com [Accessed May 2010].

- Fox, S. (2013) 51% of U.S. Adults Bank Online. *Pew Research Centre's Internet and American Life Project*, 7 (1), pp.1-11.

- Francois, J. (2013) Reducing transatlantic barriers to trade and investment: An economic assessment. *Institute for International and Development Economics*, pp.1-124.

- Fratila, A., Zota, D., and Constantinescu, R. (2013) an Analysis of the Romanian Internet Banking Market from the Perspective of Cloud Computing Services. *Procedia Economics and Finance*, 6 (1), pp. 770-775.

- French, A. (2012) a Case Study on E-Banking Security- When Security Becomes Too Sophisticated for the User to Access Their Information. *Journal of Internet Banking and Commerce*, 17 (2), pp. 1-14.

- Gan, C., Clemes, M., Limsombunchai, V., and Weng, A. (2006) A logit analysis of electronic banking in New Zealand. *International Journal of Bank Marketing*, 24 (6), pp. 360-383.

- Garson, G. (2012) Testing statistical assumptions. *Statistical Publishing Associates*, pp. 1-51.

- Gefen, D., Rao, S., and Tractinsky, N. (2003) the conceptualization of trust, risk, and their relationships in e-commerce. *In Proc. 36th Hawaii Int. Conf. on System science*, pp.1-10.

- Gerrard, P., Cunningham, J., and Devlin, F. (2006) why consumers are not using internet banking: a qualitative study. *Journal of Services Marketing*, 20 (3), pp.160-168.

- Ghane, A., Fathian, M., and Gholamian, R. (2011) Full relationship among e-satisfaction, e-trust, e-service quality, and e-loyalty: The case of Iran e-banking. *Journal of Theoretical and Applied Information technology*, 33 (1), pp. 1-6.

- Gilaninia, S., Fattahi, A., and Mousavian, J. (2011) Behavioural factors tend to use the internet banking services case study: system (SABA), the Melli Bank, Iran, Ardabil. *International Journal of Business Administration*, 2 (3), p173-179.

- Giovannini, E. and Ensor, E. (2006) Why Half of Europe's Net Users Don't Bank Online. *Forrester Research*, pp.1-10.

- Goudarzi, S., Ahmad, M., Soleymani, S., and Mohammadhosseini, N. (2013) Impact of Trust on Internet Banking Adoption: A Literature Review. *Australian Journal of Basic and Applied Sciences*, 7 (7), pp. 334-347.

- Grabner-Krauter, S. and Faullant, R. (2008) Consumer acceptance of internet banking: the influence of internet trust. *International Journal of Bank Marketing*, 26 (7), pp.483-504.

- Gurung, A. (2006) *Empirical Investigation of the relationship of privacy , security and trust with behavioural intention to transact in e-commerce.* Unpublished thesis (PhD). The University of Texas at Arlington.

- Hair, F., Black, C., Babin, J., Anderson, E., and Tatham, L. (2006) *Multivariate data analysis*. 6th Ed. Upper Saddle River, New.

- Hale, J. et al (2002) *the theory of reasoned action* (TRA). By sage publications, Inc.

- Hamed, A. (2009) *E-commerce and Economic Development in Libya*. Unpublished thesis (PhD), the University of Wales Institute.

- Hanzaee, K. and Alinejad, S. (2012) An Investigation about Customers Perceptions of Security and Trust in E-Payment Systems among Iranian Online

Consumers. *Journal of Basic and Applied Scientific Research*, 2 (2), pp.1575-1581.

- Harrell, M. and Bradley, M. (2009) Data Collection Methods: Semi-Structured Interviews and Focus Groups. *The RAND National Defense Research Institute*, pp.1-140.

- Harrison, S. (2013) Annual Fraud Indicator. *The National Fraud Authority*, pp.1-58.

- Hasan, S., Baten, A., Kamil, A., and Parveen, S. (2010) Adoption of e-banking in Bangladesh: An exploratory study. *African journal of business management*, 4 (13), pp. 2718-2727.

- Hassanuddin, N., Zalinawati Abdullah, Z., Mansor, N., and Hassan, N. (2012) Acceptance towards the Use of Internet Banking Services of Cooperative Bank. *International Journal of Academic Research in Business and Social Sciences*, 2 (2), pp. 135-147.

- Hayashi, F., Sullivan, R. J., and Weiner, S. E. (2003) A guide to the ATM and debit card industry. *Payments System Research Department, Federal Reserve Bank of Kansas City.*

- Heijden, H., Verhagen, T., and Creemers, M. (2003) Understanding online purchase intentions: contributions from technology and trust perspectives. *European journal of information systems*, 12 (1), pp. 41-48.

- Ho, C. and Lin, W. (2010) Measuring the service quality of internet banking: scale development and validation. *European Business Review*, 22 (1), pp. 5-24.

- Hoehle, H., Huff, S., and Goode, S. (2012) the role of continuous trust in information systems continuance. *Journal of Computer Information Systems*, 52 (4), pp.1-9.

- Hogarth, J. and Anguelov, C. (2004) Are Families Who Use E-Banking Better Financial Managers. *Association for financial Counselling and Planning Education*, pp. 61-77.

- Hong, H., Teh, H., Vinayan, G., Soh, H., Khan, N., and San Ong, T. (2013) Investigating the Factors Influence Adoption of Internet Banking in Malaysia: Adopters Perspective. *International Journal of Business and Management*, 8 (19), pp. 24-31.

- Hong, Z. and Yi, L. (2012) Research on the Influence of Perceived Risk in Consumer Online Purchasing Decision. *International Conference on Applied Physics and Industrial Engineering Physics Procedia*, pp. 1304-1310.

- Hosein, N (2009) Internet Banking: An Empirical Study of Adoption Rates Among Midwest Community Banks. *Journal of Business and Economics Research*, 7 (11), pp. 51-72.

- Howcroft, B., Hamilton, R., and Hewer, P. (2002) consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *International journal of bank marketing*, 20 (3), pp. 111-121.

- Hua, G. (2009) an Experimental Investigation of Online Banking Adoption in China. *Journal of Internet Banking and Commerce*, 14 (1), pp.1-12.

- Huang, L., Rau, P., Salvendy, G., Gao, F., and Zhou, J. (2011) Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 69 (12), 870-883.

- Hunaiti, Z., Masadeh, R., Mansour, M., and Al-Nawafleh, A. (2009) Electronic commerce adoption barriers in small and medium-sized enterprises (SMEs) in developing countries: the case of Libya. *IBIMA Business Review*, 2 (5), pp. 37-45.

- Hussain, K., Chang, E., and Dillon, S. (2006) Comparative Analysis of Trust and Security. *IEEE*, pp.1019-1023.

- Hussien, M and Abd Elaziz, R (2013) Investigating e-banking service quality in one of Egypt's banks: a stakeholder analysis. *The TQM Journal*, 25 (5), pp. 557-576.

- Ilyas, A., Danish, Q., Nasir, H., Malik, R., and Munir, S. (2013) Factors affecting the Customer Acceptance of E-Banking in Pakistan. *Journal of Basic and Applied Scientific Research,* 3 (6), pp.474-480.

- Ismail, M. and Osman, M. (2012) Factors Influencing the Adoption of E-banking in Sudan: Perceptions of Retail Banking Clients. *Journal of Internet Banking and Commerce*, 17 (3), pp. 1-16.

- Israel, G. (2012) *Determining Sample Size*. The Institute of Food and Agricultural Sciences, University of Florida, pp.1-5.

- Izogo, E., Nnaemeka, C., Onuoha, A., and Ezema, S. (2012) Impact of Demographic Variables on Consumers' Adoption of E-banking in Nigeria: An Empirical Investigation. *European Journal of Business and Management*, 4(17), pp. 27-39.

- Jahangir, N. and Begum, N. (2008) the role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking. *African Journal of Business Management,* 2 (1), pp.32-40.

- Janahi, Y., Mellor, J. and Toqeer, R. (2013) Trust and other factors influencing the take up of internet banking in the Kingdom of Bahrain. *The Business and Management Review*, 3 (4), pp. 7-16.

- Jaruwachirathanakul, B. and Fink, D. (2005) Internet banking adoption strategies for a developing country: the case of Thailand. *Emerald*, 15(3), pp. 295-311.

- Jayawardhena, C. and Foley, P. (2000) Changes in the banking sector-the case of Internet banking in the UK. *Internet Research: Electronic Networking Applications and Policy,* 10 (1), pp. 19-30.

- Jham, V. and Van Genderen, E. (2012) Strategic Adoption of Multi-channel Banking by Customers in UAE Banks. *International Conference on Technology and Business Management,* pp.771-778.

- Jin, S. and Kim, Y. (2010) An Empirical Investigation into the Factors Influencing the Use of E-Banking Services. *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pp.1-10.

- Johnson, R., Anthony, J. Onwuegbuzie, A., and Turner, L. (2007) Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research*, 1 (2), pp.112-133.

- Joseph, M., and Stone, G. (2003). An empirical evaluation of US bank customer perceptions of the impact of technology on service delivery in the banking sector. *International Journal of Retail and Distribution Management*, 31 (4), 190-202.

- Joseph, M., Sekhon, Y., Stone, G., and Tinson, J. (2005) an exploratory study on the use of banking technology in the UK: A ranking of importance of selected technology on consumer perception of service delivery performance. *International Journal of Bank Marketing*, 23 (5), pp. 397-413.

- Joshua, A J. and Koshy, M. (2011) Usage Patterns of Electronic Banking Services by Urban Educated Customers: Glimpses from India. *Journal of Internet Banking and Commerce,* 16 (1), pp.1-12.

- Joubert, J. and Belle, J. (2013) the Role of Trust and Risk in Mobile Commerce Adoption within South Africa. *International Journal of Business, Humanities and Technology*, 3 (2), pp. 27-38.

- Kaleem, A. and Ahmad, S. (2008) Bankers' Perceptions of Electronic Banking in Pakistan. *Journal of Internet Banking and Commerce*, 13(1), pp.1-16.

- Kamarulzaman, Y. (2007) Adoption of travel e-shopping in the UK. *International Journal of Retail & Distribution Management*, 35 (9) .pp. 703-719.

- Karimzadeh, M. and Alam, D. (2012) Electronic banking challenges in India: An empirical investigation. *Interdisciplinary Journal of contemporary Research in Business*, 4 (2), pp.31-45.

- Kartiwi, M., Rfieda, A., and Gunawan, S. (2013) a conceptual framework for assessing electronic banking continued use. *8th International Conference on Information Technology in Asia (CITA)*, pp. 1-7.

- Kasemsan, L. and Hunngam, N. (2011) Internet banking security guideline model for banking in Thailand. *Communications of the IBIMA*, pp.1-13.

- Kaur, N. and Kiran, R. (2015) E-Banking Service Quality and Customer Loyalty: Changing Dynamics of Public, Private and Foreign Bank Consumers in India.

- Kaur, N., and Kiran, R. (2015) E-Banking Service Quality and Customer Loyalty: Changing Dynamics of Public, Private and Foreign Bank Consumers in India. *Global Business and Management Research: An International Journal*, 7 (1), pp.74-92.

- Keivani, S., Jouzbarkand, M., Khodadadi, M., and Sourkouhi, Z. (2012) A General View on the E-banking. *Department accounting, Islamic Azad University, Roudsar and Amlash Branch, Iran*, pp. 62-65.

- Kesharwani, A. and Bisht, S. (2012) the Impact of Trust and Perceived Risk on Internet Banking Adoption in India: An Extension of Technology Acceptance Model. *International Journal of Bank Marketing*, 30 (4), pp. 303-322.

- Kesharwani, A. and Radhakrishna, G. (2013) Drivers and Inhibitors of Internet Banking Adoption in India. *Journal of Internet Banking and Commerce*, 18 (3), pp.1-18.

- Kim, C., Tao, W., Shin, N., and Kim, S. (2010) an empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications,* 9 (1), 84-95.

- Kim, H., Xub, Y. and Guptac, S. (2011) which are more important in Internet shopping, perceived price or trust? *Electronic Commerce Research and Applications*, pp1-12.

- Kim, K., Prabhakar, B., and Park, K. (2009) Trust, perceived risk, and trusting behavior in Internet banking. *Asia Pacific Journal of Information Systems*, 19 (3), pp.1-23.

- Kini, A. and Choobineh, J. (2000) An Empirical Evaluation of the Factors Affecting Trust in Web Banking Systems. *Conference on Information System*, pp.185-191.

- Kissel, R. (2011) Glossary of Key Information Security Terms. *U.S. Department of Commerce,* pp.1-211.

- Kline, R. (2011) Principles and Practice of Structural Equation Modelling. *Third Edition the Guilford Press, division of Guilford publications, Inc. London*.

- Kolodinsky, M., Hogarth, M., and Hilgert, A. (2004) the adoption of electronic banking technologies by US consumers. *The International Journal of Bank Marketing,* 22 (4), pp. 238-259.

- Koskosas, I. (2011) E-banking security: A communication perspective. *Macmillan Publishers Ltd*, 13 (2), pp. 81-99.

- Kotrlik, J. W., and Higgins, C. C. (2001) Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information technology, learning, and performance journal*, 19 (1), pp. 43-50.

- Kurnia, S., Peng, F., and Liu, R. (2010, January) Understanding the adoption of electronic banking in China. *IEEE*, pp. 1-10.

- Lallmahamood, M. (2007) An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce*, 12 (3), pp.1-26.

- Lamberti, H. and Kawamura, T. (2003) Building Consumer Trust Internet Payments. *Global Business Dialogue on electronic commerce*, pp.34-43.

- Laroche, M., McDougall, H., Bergeron, J., and Yang, Z. (2004) Exploring how intangibility affects perceived risk. *Journal of Service Research*, 6 (4), p. 373-389.

- Lasheng, Y. and Placide, M. (2009) Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services. *Proceedings of the Second Symposium International Computer Science and Computational Technology*, pp.114-119.

- Laukkanen, T., Sinkkonen, S., and Laukkanen, P. (2009) Communication strategies to overcome functional and psychological resistance to Internet banking. *International journal of information management*, 29 (2), pp.111-118.

- Lee, H., Lim, G., and Lim, I. (2013) a study of the security of Internet banking and financial private information in South Korea. *Mathematical and Computer Modelling*, 58(1), pp. 117-131.

- Lee, M. (2009) Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8 (3), pp.130-141.

- Lee, S., Lee, S., and Kim, Y. (2007) Factors Influencing the Adoption Behavior of Mobile Banking: A South Korean perspective. *Journal of Internet Banking and Commerce*, 12 (2), pp. 1-9.

- Lee, W., Tsai, T., and Lanting, L. (2011) from marketplace to marketspace: Investigating the consumer switch to online banking. *Electronic Commerce Research and Applications*, 10 (1), 115-125.

- Leicester City Council website (2013*) Facts and figures* [www] Leicester City Council. Available from: http://www.leicester.gov.uk [Accessed 27/06/2013].

- Liao, C., Liu, C., and Chen, K. (2011) Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, 10 (6), pp. 702-715.

- Lichtenstein, S. and Williamson, K (2006) Understanding Consumer Adoption of Internet Banking: An interpretive study in the Australian banking context. *Journal of Electronic Commerce Research*, 7 (2), pp.50-66.

- Liebana-Cabanillas, F., Munoz-Leiva, F., and Sanchez-Fernandez, J. (2013) the impact of risk on the technological acceptance of mobile payment services. *Global Business Perspectives*, 1 (4), pp.309-328.

- Lim, N. (2003) Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications*, pp.216-228.

- Lin, F., Fofanah, S., and Liang, D. (2011) Assessing citizen adoption of e-Government initiatives in Gambia: A validation of the technology acceptance model in information systems success. *Government Information Quarterly*, 28 (2), pp. 271-279.

- Ling, C., bin Daud, D., Piew, H., Keoy, H., and Hassan, P. (2011) Perceived risk, perceived technology, online trust for the online purchase intention in Malaysia. *International Journal of Business and Management*, 6 (6), p167-182.

- Littler, D. and Melanthiou, D. (2006) Consumer perceptions of risk and uncertainty and the implications for behaviour towards innovative retail services: The case of Internet Banking. *Journal of Retailing and Consumer Services*, pp. 431–443.

- Liu, G., Song, F., and Qian, C. (2008) User Acceptance of Internet Banking: An Empirical Study in China. *IEEE*, pp.1-4.

- Liu, S. and Chen, R. (1998) Sequential Monte Carlo methods for dynamic systems. *Journal of the American statistical association*, 93(443), pp.1032-1044.

- Lu, P., Hsu, L., and Hsu, Y. (2005) an empirical study of the effect of perceived risk upon intention to use online applications. *Information Management and Computer Security*, 13(2), pp. 106-120.

- Luo, X., Li, H., Zhang, J., and Shim, 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), pp. 222-234.

- Maditinos, D. (2007) Predicting e-commerce purchasing intention in Greece: An extended TAM approach. *International Conference on Accounting and Finance in Transition*, pp.1-21.

- Mahdi, M. (2011) Trust and security of electronic banking services in Saudi commercial banks: Saudis versus Non Saudis opinions. *African Journal of Business Management,* 5(14), pp. 5524-5535.

- Mahdi, M., Rezaul, K., and Rahman, M. (2010) Credit Fraud Detection in the Banking Sector in UK: A Focus on E-Business. *IEEE,* pp. 232-237.

- Mahmood, Z. (2009) Attitudes towards the use of E-banking: Result of a Pilot Survey. *Communications of the IBIMA*, pp.170-174.

- Malhotra, N., Baalbaki, I., and Bechwati, N. (2012) *Marketing research, an applied approach*. Fourth edition. Pearson education Limited.

- Mangin, P., Bourgault, N., Guerrero, M., and Egea, M. (2011) Modelling perceived usefulness on adopting online banking through the TAM model in a Canadian banking environment. *Journal of Internet Banking and Commerce,* 16 (1), pp.1-23.

- Mansumitrchai, S. and Al-Malkawi, H. (2011) Factors Underlying the Adoption of Online Banking by Mexican Consumers. *International Journal of Business and Management,* (6) 9, pp.155-169.

- Martins, C., Oliveira, T., and Popovic, A. (2014) Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management,* 34 (1), pp.1-13.

- Masinge, K. (2011) Factors influencing the adoption of mobile banking services at the Bottom of the Pyramid in South Africa. *Gordon institute of business science, University of Pretoria,* pp.1-135.

- McCole, P., Ramsey, E., and Williams, J. (2010) Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, 63 (9), pp.1018-1024.

- Mermod, A. (2011) Customer's Perspectives and Risk Issues on E-Banking in Turkey; Should We Still be Online. *Journal of Internet Banking and Commerce*, 16 (1), pp.1-15.

- Migdadi, Y. (2008) the Quality of Internet Banking Service Encounter in Jordan. *Journal of Internet Banking and Commerce*, 13 (3), pp.1-7.

- Moga, L., Nor, K., Neculita, M., and Khani, N. (2012) Trust and Security in E-banking Adoption in Romania. *Communications of the IBIMA*, pp.1-10.

- Moghadam, A., Behboudi, I., and Jafari, F. (2012) does Internet Advertising Affect the Internet Banking Effectiveness? A three Dimensional Model for Iran. *Journal of Internet Banking and Commerce*, 17 (3), pp. 1-16.

- Mohammadian, M. and Ghanbar. M (2014) A study of Factors Influencing Online Brand Trust in Online Service Retailing. *Switzerland research park journal*, (103) 2, pp. 956-976.

- Mohammed, N. (2011) *Future of Interactive Technologies: The Forecasting of Interactive Technologies and their overall acceptance*. Unpublished thesis (PhD), University of Edinburgh.

- Mondal, C., and Saha, K. (2013) Client Satisfaction of Internet Banking Service in Bangladesh: An Exploratory Study. *ASA University Review*, 7 (1), pp.131-141.

- Montazemi, R., and Saremi, Q. (2013) Factors affecting Internet banking pre-usage expectation formation. *IEEE*, pp. 4666-4675.

- Mughal, M., Farhan, M., Ali, K., and Khan, J. (2012) Accepting of E-banking among Banking Customers of Pakistan. *Information Management and Business Review*, 4 (6), pp. 332-339.

- Munusamy, J., De Run, C., Chelliah, S., and Annamalah, S. (2012) Adoption of Retail Internet Banking: A Study of Demographic Factors. *Journal of Internet Banking and Commerce,* 17 (3), pp. 1-14.

- Muzividzi, D. Mbizi, R. and Mukwazhe, T. (2013) an analysis of factors that influence internet banking adoption among intellectuals: Case of Chinhoyi of University of Technology. *Interdisciplinary journal of contemporary Research in Business,* 4 (11), pp. 350 - 369.

- Namamian, F., Hassani, S., Mohammadi, M., Arabi, S., and Almasitabar, H. (2013) Design a New Model in Adoption of Internet Banking (B2c). *Journal of Basic and Applied Scientific Research,* 3(6), pp.374-379.

- Namin, T., Rangriz, H., and Akbariyeh, H. (2012) Evaluating Electronic Trust in Payment Internet Banking (Case Study: Bank Melli of Iran). *Journal of Basic and Applied Scientific Research,* 2(4), pp. 3339-3348.

- Nasir, A., Wu, J., Yago, M., and Li, H. (2015) Influence of Psychographics and Risk Perception on Internet Banking Adoption: Current State of Affairs in Britain. *International Journal of Economics and Financial Issues*, 5 (2), pp. 461-468.

- Nasri, W. (2011) Factors Influencing the Adoption of Internet Banking in Tunisia. *International Journal of Business and Management*, 6 (8), pp.143-160.

- Nasri, W. and Charfeddine, L. (2012) Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behaviour. *Journal of High Technology Management Research*, pp.1-14.

- Nasri, W., and Zarai, M. (2014) Empirical Analysis of Internet Banking Adoption in Tunisia. *Asian Economic and Financial Review*, 4 (12), pp.1812-1825.

- Naumann, I. (2009) Privacy and Security Risks when authenticating on the Internet with European eID Cards. *European Network and Information Security Agency*, pp. 1-41.

- Nchise, A. (2012) an Empirical Analysis of the Theory of Planned Behavior. *JeDEM*, 4(2), pp. 171-182.

- Ndlovu, I. and Sigola, M. (2013) Benefits and Risks of E-Banking: Case of Commercial Banking in Zimbabwe. *The International Journal of Engineering and Science (IJES)*, 2 (4), pp. 34-40.

- Nepomuceno, V., Laroche, M., and Richard, O. (2014) How to reduce perceived risk when buying online: The interactions between intangibility, product knowledge, brand familiarity, privacy and security concerns. *Journal of Retailing and Consumer Services*, 21(4), pp. 619-629.

- Nochai, R., and Nochai, T. (2013) the Impact of Internet Banking Service on Customer Satisfaction in Thailand: A Case Study in Bangkok. *International Journal of Humanities and Management Sciences*, 1 (1), pp. 2320–4044

- Nor, K. and Pearson, J. (2007) the Influence of Trust on Internet Banking Acceptance. *Journal of Internet Banking and Commerce*, 12 (2), pp.1-10.

- Nwogu, E. and Odoh, M. (2015) Security Issues Analysis on Online Banking Implementations in Nigeria. *International Journal of Computer Science and Telecommunications*, 6 (1), pp. 20-27.

- Ochuko, E., Cullen, J., and Neagu, D. (2009) Overview of Factors for Internet Banking Adoption. *IEEE*, pp. 163-170.

- O'Donnell, A., Durkin, G., and McCartan-Quinn, D. (2002) corporate banking in the UK: personal vs remote interaction. *International Journal of Bank Marketing*, 20 (6), pp. 273-284.

- Office for National Statistics (2011) *Internet Access Households and Individuals 2011, August 2011*.The United Kingdom.

- Office for National Statistics (2012) *Internet Access Quarterly Update, 2012 Q2, August 2012*.The United Kingdom.

- Office for National Statistics (2012) *Internet Access Quarterly Update, Q4 2011, February 2012*.The United Kingdom.

- Office for National Statistics (2013) *Internet Access - Households and Individuals, August 2013*.The United Kingdom.

- Office for National Statistics (2014) *Internet Access Households and Individuals 2014, August 2014*. The United Kingdom.

- Ofori-Dwumfuo, G. and Dankwah, B. (2013) Adopting Internet Banking in Ghana. *Current Research Journal of Social Sciences,* 5 (4), pp. 143-151.

- Omar, B., Sultan, N., Zaman, K., Bibi, N., Wajid, A., and Khan, K. (2011) Customer Perception towards Online Banking Services: Empirical Evidence from Pakistan. *Journal of Internet Banking and Commerce,* 16 (2), pp. 1-24.

- Osei, M., Seth, A., and John, A. (2015) Customers' preference in service delivery, an assessment of TAH and IDT on the means-end theory in the banking industry: A case of Ghana commercial bank Ltd in Ghana. *European Journal of Business and Social Sciences*, 3(11), pp.79-100.

- Pallant, J. (2010) *SPSS: Survival Manual*. 4th edition. Allen and Unwin book publishers, Australia.

- Park, H. (2008) Univariate analysis and normality test using SAS, Stata, and SPSS. *The University Information Technology Services (UITS), Centre for Statistical and Mathematical Computing, Indiana University*, pp. 1-41.

- Park, S. (2009) An Analysis of the Technology Acceptance Model in Understanding University Students' behavioural Intention to Use e-Learning. *Educational Technology and Society*, 12 (3), pp.150-162.

- Patsiotis, G., Hughes, T., and Webber, J. (2012) Adopters and non-adopters of internet banking: a segmentation study. *International Journal of Bank Marketing*, 30 (1), pp. 20-42.

- Pennanen, K., Kaapu, T., and Paakki, M. (2006) Trust, Risk, Privacy, and Security in e-Commerce. *Frontiers of e-business research*, pp. 1-10.

- Phellas, N., Bloch, A., and Seale, C. (2011) Structured methods: Interviews, Questionnaires and Observation. *Researching Society and Culture. London: SAGE Publications Ltd*, pp.181-205.

- Pi, M., Liao, L., and Chen, M. (2012) Factors that affect consumers' trust and continuous adoption of online financial services. *International Journal of Business and Management,* 7 (9), pp.108-119.

- Polasik, M. and Wisniewski, T. (2009) Empirical analysis of internet banking adoption in Poland. *International Journal of Bank Marketing*, 27 (1) pp. 32-52.

- Poon, W. (2008) Users' adoption of e-banking services: the Malaysian perspective. *Journal of Business and Industrial Marketing*, 23 (1), pp.59 - 69.

- Popola, N. F. (2013) The Effect of Trust in Adoption of Internet Banking: A case study of Nigeria. *International Journal of Economic and Business Management,* 1 (2), pp.19-24.

- Popola, N. F. (2013) The Effect of Trust in Adoption of Internet Banking: A case study of Nigeria. *International Journal of Economic and Business Management*, 1 (2), pp.19-24.

- Prapavessis, H., Gaston, A., and DeJesus, S. (2015) The Theory of Planned Behavior as a model for understanding sedentary behavior. *Psychology of Sport and Exercise,* 19, 23-32.

- Qzguven, N. (2011) Analysis of the relationship between perceived security and customer trust and loyalty in online shopping. *Chinese Business Review*, 10 (11), pp. 990-997.

- Radojevic, T and Radovanovic, D. (2010) the impact of electronic banking on offer of financial services. *MIPRO*, pp.1131-1136.

- Radulescu, M. and Serbanescu, L (2009) Development of the electronic banking services in Romania. *Communications of the IBIMA*, 8 (1), pp. 42-51.

- Rahmati, F., Navid, J., and AliShiri, G. (2013) Factors Effective on the Adoption of Internet Banking (A Case Study OfIlam Province Banks). *International Research Journal of Applied and Basic Sciences,* 4 (8), pp.2159-2164.

- Raman, M., Stephenaus, R., Alam, N., and Kuppusamy, M. (2008) Information Technology in Malaysia: E-service quality and Uptake of Internet banking. *Journal of Internet Banking and Commerce,* 13 (2), pp.1-18.

- Ramya, S., Rajam, K., and Sivasubramania, D. (2013) Effectiveness of electronic banking systems. *International Journal of Research in Management, Economics and Commerce*, 3 (9), pp. 12-23.

- Randall, C. (2010) e-Society, *office for national statistics*, pp. 1-32.

- Ratnasingham, P. (1999) Risks in Low trust among trading partners in electronic commerce. *Computers and Security*, 18 (1), pp. 587-592.

- Ravoet, G. (2010) EU Banking Sector: Facts and Figures. *European Banking Federation,* pp. 1-28.

- Reddy, A. (2012) A study on consumer perceptions on security, privacy and trust on E-commerce portals. *EXCEL International Journal of Multidisciplinary Management Studies*, 2 (3), pp.1-15.

- Reid, M. and Levy, Y. (2008) Integrating Trust and Computer Self-Efficacy with TAM: An Empirical Assessment of Customers' Acceptance of Banking Information Systems (BIS) in Jamaica. *Journal of Internet Banking and Commerce*, 12 (3), pp.1-18.

- Reis, A., Gülseçen, S., and Bayrakdar, B. (2011) to develop an education system for secure internet banking: GIBES. *Procedia Computer Science*, 3(1), pp.1333-1340.

- Riffai, M., Grant, K., and Edgar, D. (2012) Big TAM in Oman: Exploring the promise of on-line banking, its adoption by customers and the challenges of banking in Oman. *International Journal of Information Management*, pp. 239-250.

- Riyadh, M., Akter, S., and Islam, N. (2009) The Adoption of E-banking in Developing Countries: A Theoretical Model for SMEs. *International Review of Business Research Papers*, 5 (6), pp.212-230.

- Rotchanakitumnuai, S., and Speece, M. (2003) Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand. *International Journal of Bank Marketing*, 21(7), pp.312-323.

- Ruyter, K., Wetzels, M., and Kleijnen, M. (2001) Customer adoption of e-service: an experimental study. *International Journal of Service Industry Management*, 12 (2), pp.184-207.

- Sadeghi, T. and Farokhian, S. (2010) Electronic Banking Acceptance Model (EBAM) in Iran. *World Applied Sciences Journal*, 11 (5), pp.513-525.

- Saeed, S., Azim, M., Choudhary, I., and Humyon, A. (2015) service quality factors affecting adoption of Internet banking in Pakistan. *International Journal of Economics, Commerce and Management*, 2 (1), pp1-10.

- Safeena, R., Date, H., and Kammani, A. (2011) Internet Banking Adoption in an Emerging Economy: Indian Consumer's Perspective. I*nternational Arab Journal of e-Technology*, 2 (1), pp.56 -64.

- Sakhaei, F., Afshari, J., and Esmaili, E. (2013) the Impact of Service Quality on Customer Satisfaction in Internet Banking. *Journal of mathematics and computer*, 9 (1), pp. 33-40.

- Salari, S. and Salajegheh, M. (2011) Analysis of Factors Affecting the Adoption of Internet Banking. Case Study: Customers of Mellat Bank in Isfahan City. *International Conference Risk in Contemporary Economy*, pp. 304-310.

- Salehi, M. and Alipour, M. (2010) E-Banking in Emerging Economy: Empirical Evidence of Iran. *Journal of Economics and Finance*, 2 (1), pp.201-209.

- Salih, M. (2009) *E-banking, trust and security*. Published thesis (MSc), Swedish School of Economics and Business Administration.

- Sanayei, A. and Jafari, N. (2011) Appraisal of Influencing Factor on Accepting Electronic Banking (A Case Study: Customers of Industry and Mine Bank). *Interdisciplinary Journal of Contemporary Research in Business*, 3(8), pp.814-821.

- Sanayei, A. and Noroozi, A. (2009) Security of Internet Banking Services and its linkage with Users' Trust. *International Conference on Information Management and Engineering*, pp.3-7.

- Sanchez, C. and Jean-Baptiste, G. (2010) Adoption on internet banking: Evidence from France. *International Journal of Management and Marketing Research*, 3 (3), pp.107-117.

- Sankari, A., Ghazzawi, K., El-danawi, S., El-nemar, S., and Arnaout, B. (2015) factors affecting the adoption of Internet banking in Lebanon. *International Journal of Management,* 6 (3), pp. 75-86.

- Sarma, G. and Singh, P. (2010) Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. *International Journal of Pure and Applied Sciences and Technology,* 1 (2), pp. 67-78.

- Sattabusaya .D (2008) *Key factors that determine acceptance and adoption of Internet banking: The case of Thailand*. Unpublished, PhD thesis, Cardiff University.

- Scheuren, F. (2004) what is a Survey? *American Statistical Association*, pp.1-68.

- Sekaran, U. and Bougie, R. (2010) *Research Methods for Bushiness: A skill Building an approach*. John Wiley and Sons Ltd.

- Shafei, R. and Mirani, V. (2011) Designing a model for analysing the effect of risks on e-banking adoption by customers: A focus on developing countries. *African Journal of Business Management*, 5(16), pp. 6684-6697.

- Shafiee, M., Sangi, M., and Ghaderi, M. (2013) Bank performance evaluation using dynamic DEA: A slacks-based measure approach. *Journal of Data Envelopment Analysis and Decision Science*, pp. 1-12.

- Shah, M. and Siddiqui, F. (2006) Organisational critical success factors in adoption of e-banking at the Woolwich bank. *International Journal of Information Management*, 26 (1), pp. 442-456.

- Shahibi, M. and Fakeh, S. (2011) Security Factor and Trust in E-Commerce Transactions. *Australian Journal of Basic and Applied Sciences*, 5(12), pp. 2028-2033.

- Shannak, R. (2013) Key Issues in E-banking Strengths and Weaknesses: the case of two Jordanian banks. *European Scientific Journal*, 9 (7), pp. 239-263.

- Sharma, G. and Malviya, S. (2014) Internet banking services quality and its impact on customer satisfaction in Indore District of madhya pradesh. *International Journal of Business and Management Invention*, 3(3), pp. 2319-8028.

- Shin, D. (2010) the effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, pp.428-438.

- Simpson, J. (2002) the impact of the Internet in banking: observations and evidence from developed and emerging markets. *Telematics and Informatics*, pp, 315-330.

- Singh, A. (2004) Trends in South African Internet banking. Aslib Proceedings: New Information Perspectives. *By Emerald Group Publishing Limited*, 56 (3), pp. 187-196.

- Siu-cheung, C. and Lu, M. (2004) Understanding internet banking adoption and use behavior: a Hong Kong perspective. *Journal of Global Information Management*, 12(3), pp. 21-43.

- Srinivasan, S. (2004) Role of trust in e-business success. *Information Management and Computer Security*, 12 (1), pp. 66-72.

- Subsorn, P. and Limwiriyakul, S. (2012) An Analysis of Internet Banking Security of Foreign Subsidiary Banks in Australia: A Customer Perspective. *International Journal of Computer Science Issues*, (9) 2, pp. 8-16.

- Suki, N. (2010) An Empirical Study of Factors Affecting the Internet Banking Adoption among Malaysian Consumers'. *Journal of Internet Banking and Commerce,* 15 (2), pp.1-11.

- Sun, D., Chang, G., Sun, L., and Wang, X. (2011) Surveying and analysing security, privacy and trust issues in cloud computing environments. *Procedia Engineering*, 15(1), pp. 2852-2856.

- Swesi, K. (2011) *An Investigation into the Influence of Learning Styles and other Factors Affecting Students' Perception of Virtual Learning Environments*. Unpublished thesis (PhD), De Montfort University Leicester UK.

- Taddei, S. and Contena, B, (2013) Privacy, trust and control: Which relationships with online self-disclosure*? Computers in Human Behavior*, 29 (1), pp. 821–826.

- Takele, Y. and Sira, Z. (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. *European Scientific Journal,* 9 (13), pp.402-417.

- Taleghani, M. and Taban, H. (2012) Investigation and Analysis Organizational Behaviour Factors in Performance Improvement of Internet Banking Services (Case Study: Northern of Iran). *Journal of Basic and Applied Scientific Research*, 2 (1), pp.172-178.

- Tandrayen-Ragoobur, V. and Ayrga, A. (2011) Is Mauritius Ready to E-Bank? From A Customer and Banking Perspective. *Journal of Internet Banking and Commerce*, 16(1), pp. 1-17.

- Tat, H. (2008) Predictors of intention to continue using the internet banking services: an empirical study of current users. *International Journal of Business and Information*, 3 (2), pp. 233-244.

- Tavakol, M. and Dennick, R. (2011) Making sense of Cronbach's alpha. *International Journal of Medical Education*, pp.53-55.

- Thirunarayan, K., Anantharam, P., Henson, C., and Sheth, A. (2014) Comparative trust management with applications: Bayesian approaches emphasis. *Future Generation Computer Systems*, 31 (1), pp. 182-199.

- Thulani, D., Tofara, C., and Langton, R. (2009) Adoption and Use of Internet Banking in Zimbabwe: An Exploratory Study. *Journal of Internet Banking and Commerce,* 14 (1), pp1-13.

- Trivedi, P. (2010) E-Banking: an Overview. *E-track Dhamendra Tewari Swastik Printing Press*, 2 (3), pp.1-32.

- Tsai, H., Zhu, S., and Jang, M. (2013) A Study on the Consumer Adoption Behaviors of Internet Bank. *IEEE*, 8 (12), pp.2956-2963.

- Tsai, Y. and Yeh, J. (2010) Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products. *African Journal of Business Management*, 4 (18), pp. 4057-4066.

- Tsiakis, T. (2012) Consumers' issues and concerns of perceived risk of information security in online framework, the marketing strategies. *Procedia - Social and Behavioural Sciences*, 62 (1) pp.1265-1270.

- Twati, J. (2008) the Influence of Societal Culture on the Adoption of Information Systems: The Case of Libya. *Communications of the IIMA*, 8 (1), pp1-12.

- Twum, F. and Ahenkora, K. (2012) Internet Banking Security Strategy: Securing Customer Trust. *Journal of Management and Strategy*, 3 (4), pp.78-83.

- Tyagi, N. and Srinivasan, S. (2011) Ten-Stage Security Management Strategy Model for the Impacts of Security Threats on e-Business. *International Journal of Computer Applications*, 21(5), pp. 1-4.

- Urban, L., Amyx, C., and Lorenzon, A. (2009) online trust: state of the art, new frontiers, and research potential. *Journal of Interactive Marketing*, 23(2), pp.179-190.

- Vaus, D. (2002) *Analysing social science data: 50 Key Problems in Data Analysis*. First edition. Saga Publications Ltd, London.

- Venkatesh, V. and Bala, H. (2008) Technology Acceptance Model 3 and a Research Agenda on Interventions. *Journal compilation, Decision Sciences Institute*, 39 (2), pp. 273- 314.

- Venkatesh, V. and Davis, F. (2000) a Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, 46 (2), pp.186-204.

- Venkatesh, V., Thong, Y., and Xu, X. (2012) Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 36 (1), pp.157-178.

- Verhagen, T., Meents, S., and Tan, H. (2006). Perceived risk and trust associated with purchasing at electronic marketplaces. *European Journal of Information Systems*, 15 (6), pp.542-555.

- Vijesh, R. (2011) Technology Management in Bank-Risk on Alternate Channels: A Global Study. *International Conference on Technology and Business Management*, pp. 1433-1439.

- Waheed, M., Qaisar, K., and Noor-Ul-Ain (2013) Role of satisfaction, security and risk towards customer's turnover intention from traditional to internet banking. *International Arab Journal of e-Technology*, 3 (2), pp.83-89.

- Wang, S., Wang, M., Lin, H., and Tang, I. (2003) Determinants of user acceptance of Internet banking: an empirical study. *International Journal of service industry management*, 14 (5), pp. 501-519.

- Weerakkody, V. and Choudrie, J. (2005) Exploring E-Government in the UK: Challenges, Issues and Complexities. *Journal of Information Science and Technology*, 2 (2), pp. 25-45.

- White, H. and Nteli, F. (2004) Internet banking in the UK: Why are there not more customers. *Journal of Financial Services Marketing*, 9 (1), pp. 49-56.

- Widjana, M. and Rachmat, B. (2011) Factors Determining Acceptance Level of internet banking Implementation. *Journal of Economics, Business and Accountancy Ventura*, 14 (2), pp. 161-174.

- Williams, B., Brown, T., and Onsman, A. (2012) Exploratory factor analysis: A five-step guide for novices. *Australasian Journal of Paramedicine*, 8 (3), pp.1-14.

- Wong, D., Loh, C., Turner, B., Bak, R., and Yap, K. (2009) Risky business: perceived risk, trust and the use of e-banking. *ANZMAC*, pp, 1-8.

- Worku, G. (2010) Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges. *Journal of Internet Banking and Commerce*, 15 (2), pp1-8.

- Wu, W., Huang, Y., Yen, C., and Popova, I. (2012) the effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, 28 (3), pp. 889-897.

- Yaghubi.N and Seyedin. S, (2015) Ranking the technical dimensions of e-banking service quality evaluation models using Analytical Hierarchy Process.

- Yang, J., Cheng, L., and Luo, X. (2009) a comparative study on e-banking services between China and USA. *International Journal of Electronic Finance*, 3 (3), 235-252.

- Yap, B., Wong, H., Loh, C., and Bak, R. (2010) Offline and online banking-where to draw the line when building trust in e-banking? *International Journal of Bank Marketing*, 28 (1), pp. 27-46.

- Yazdanifard, R., AbuTabik, A., and Seyedi, P. (2011) Security and Trust in Electronic Commerce-Finding the Safe Side. *Information Communication and Management-International Proceedings of Computer Science and Information Technology*, 16 (1), pp.141-146.

- Yeow, H., Yuen, Y., Tong, K., and Lim, N. (2008) User acceptance of online banking service in Australia. *Communications of the IBIMA,* 1 (22), pp.191-197

- Yiu, S., Grant, K., and Edgar, D. (2007) Factors affecting the adoption of Internet Banking in Hong Kong-implications for the banking sector. *International Journal of Information Management*, 27 (5), pp. 336-351.

- Yoon, H. and Steege, L. (2013) Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. *Computers in Human Behavior*, pp.1133-1141.

- Yousafzai Y., Pallister, J., and Foxall, R. (2005) Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology and Marketing*, 22 (2), pp.181-201.

- Yousafzai, S. (2005) *Internet Banking in the UK: A Customer Behaviour Perspective*. Unpublished thesis (PhD), Cardiff University UK.

- Yousafzai, S. and Yani-de-Soriano, M. (2012) Understanding customer-specific factors underpinning internet banking adoption. *International Journal of Bank Marketing*, 30 (1), pp. 60-81.

- Yousafzai, S. Pallister, J. and Foxall, G. (2009) Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29 (5), pp. 591–605.

- Yousafzai, Y., Foxall, R., and Pallister, G. (2010) Explaining Internet Banking Behavior: Theory of Reasoned Action, Theory of Planned Behavior, or Technology Acceptance Model? *Journal of Applied Social Psychology*, 40 (5), pp. 1172-1202.

- Yousafzai, Y., Pallister, G., and Foxall, R. (2003) a proposed model of e-trust for electronic banking. *Technovation,* 23 (11), pp. 847-860.

- Yu, L., Balaji, S., and Khong, W. (2015) Building trust in internet banking: a trustworthiness perspective. *Industrial Management and Data Systems*, 115 (2), pp. 235-252.

- Yuan, X., Lee, S., and Kim, Y. (2010) Present and future of internet banking in China. *Journal of Internet Banking and Commerce*, 15 (1), pp.1-16.

- Yulihasri, E., Islam, M., and Daud. K (2011) Factors that influence customers' buying intention on shopping online. *International Journal of marketing studies*, 3 (1), pp.128-139.

- Zaglago, L., Chapman, C., and Shah, H. (2013) The Trust Factor: Design Team Knowledge Sharing Culture. *In Proceedings of the World Congress on Engineering,* 3 (5), pp.1-6.

- Zarei, S. (2011) Risk Management of Internet Banking. Recent Researches in Artificial Intelligence. *Knowledge Engineering and Data Bases*, pp.134-139.

- Zhao, A., Hanmer-Lloyd, S., Ward, P., and Goode, M. (2008) Perceived risk and Chinese consumers' internet banking services adoption. *International Journal of Bank Marketing,* 26 (7), pp. 505-525.

- Zhao, A., Koenig-Lewis, N., Hanmer-Lloyd, S., and Ward, P. (2010) Adoption of internet banking services in China: is it all about trust. *International Journal of Bank Marketing*, 28 (1), pp. 7-26.

- Zhou, T. (2013) Understanding continuance usage of mobile sites. *Industrial Management and Data Systems*, 113 (9), pp. 1286-1299.

- Zimmer, C., Arsal, E., Al-Marzouq, M., and Grover, V. (2010) Investigating online information disclosure: Effects of information relevance, trust and risk. *Information and management*, 47 (2), pp.115-123.

- Zissis, D. and Lekkas, D. (2012) Addressing cloud computing security issues. *Future Generation Computer Systems*, 28 (3), pp. 583-592.

APPENDICES

APPENDIX A

- **APPENDIX A1: ANALYSIS TABLES OF THE MODEL NON-ADOPTION.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.673[a]	.453	.451	.52530

a. Predictors: (Constant), A. Trust NU
b. Dependent Variable: A. Non Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	65.962	1	65.962	239.041	.000[b]
	Residual	79.748	289	.276		
	Total	145.710	290			

a. Dependent Variable: A. Non Adoption
b. Predictors: (Constant), A. Trust NU

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.689[a]	.475	.473	.51464

a. Predictors: (Constant), A. Sec NU
b. Dependent Variable: A. Non Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	69.166	1	69.166	261.142	.000[b]
	Residual	76.544	289	.265		
	Total	145.710	290			

a. Dependent Variable: A. Non Adoption
b. Predictors: (Constant), A. Sec NU

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.525[a]	.276	.273	.60421

a. Predictors: (Constant), A. Risk NU
b. Dependent Variable: A. Non Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	40.204	1	40.204	110.125	.000[b]
	Residual	105.506	289	.365		
	Total	145.710	290			

a. Dependent Variable: A. Non Adoption
b. Predictors: (Constant), A. Risk NU

- **APPENDIX A2: ANALYSIS TABLES OF THE MODEL ABANDONING.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.696[a]	.484	.472	.54676

a. Predictors: (Constant), A. Trust GU
b. Dependent Variable: A. Abandoning

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.798	1	11.798	39.466	.000[b]
	Residual	12.556	42	.299		
	Total	24.354	43			

a. Dependent Variable: A. Abandoning
b. Predictors: (Constant), A. Trust GU

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.710[a]	.504	.492	.53626

a. Predictors: (Constant), A. Sec GU
b. Dependent Variable: A. Abandoning

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.275	1	12.275	42.686	.000[b]
	Residual	12.078	42	.288		
	Total	24.354	43			

a. Dependent Variable: A. Abandoning
b. Predictors: (Constant), A. Sec GU

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.466[a]	.217	.199	.67371

a. Predictors: (Constant), A. Risk GU
b. Dependent Variable: A. Abandoning

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.290	1	5.290	11.655	.001[b]
	Residual	19.063	42	.454		
	Total	24.354	43			

a. Dependent Variable: A. Abandoning
b. Predictors: (Constant), A. Risk GU

- **APPENDIX A3: ANALYSIS TABLES OF THE MODEL ADOPTING AND THE CONTINUED USE.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.238[a]	.056	.055	.63758

a. Predictors: (Constant), A. Trust U
b. Dependent Variable: A. Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.194	1	12.194	29.997	.000[b]
	Residual	203.662	501	.407		
	Total	215.856	502			

a. Dependent Variable: A. Adoption
b. Predictors: (Constant), A. Trust U

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.067[a]	.005	.003	.65554

a. Predictors: (Constant), A. Sec U
b. Dependent Variable: A. Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.982	1	.982	2.285	.131[b]
	Residual	214.869	500	.430		
	Total	215.851	501			

a. Dependent Variable: A. Adoption
b. Predictors: (Constant), A. Sec U

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.005[a]	.000	-.002	.65638

a. Predictors: (Constant), A. Risk U
b. Dependent Variable: A. Adoption

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.006	1	.006	.014	.905[b]
	Residual	215.850	501	.431		
	Total	215.856	502			

a. Dependent Variable: A. Adoption
b. Predictors: (Constant), A. Risk U

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.220[a]	.048	.047	.77450

a. Predictors: (Constant), A. TSR
b. Dependent Variable: A. Per-Intention

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	15.267	1	15.267	25.452	.000[b]
	Residual	299.922	500	.600		
	Total	315.189	501			

a. Dependent Variable: A. Per-Intention
b. Predictors: (Constant), A.TSR

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.255[a]	.065	.063	.50985

a. Predictors: (Constant), A. Risk U
b. Dependent Variable: A. Trust U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.921	1	10.921	34.865	.000[b]
	Residual	156.926	501	.313		
	Total	167.846	502			

a. Dependent Variable: A. Risk U
b. Predictors: (Constant), A. Trust U

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.509[a]	.259	.0257	.45401

a. Predictors: (Constant), A. Sec U
b. Dependent Variable: A. Trust U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	35.961	1	35.961	174.463	.000[b]
	Residual	103.061	500	.206		
	Total	139.022	501			

a. Dependent Variable: A. Trust U
b. Predictors: (Constant), A. Sec U

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	-.395[a]	.156	.154	.53210

a. Predictors: (Constant), A. Sec U
b. Dependent Variable: A. Risk U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	26.202	1	26.202	92.544	.000[b]
	Residual	141.564	500	.283		
	Total	167.766	501			

a. Dependent Variable: A. Risk U
b. Predictors: (Constant), A. Sec U

APPENDIX B

- **APPENDIX B1: Relationship between Trust, Security, Perceived Risk and Demographic Characteristics of Internet Banking Services Non-Users.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.243[a]	.059	.043	.60331

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age
b. Dependent Variable: A. Sec NU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.529	5	1.306	3.588	.004[b]
	Residual	103.736	285	.364		
	Total	110.265	290			

a. Dependent Variable: A. Sec NU

b. Predictors: (Constant), Occupation, Gender, Income, Education, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.249[a]	.062	.045	.61519

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age

b. Dependent Variable: A. Risk NU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.116	5	1.423	3.760	.003[b]
	Residual	107.859	285	.378		
	Total	114.975	290			

a. Dependent Variable: A. Risk NU

c. Predictors: (Constant), Occupation, Gender, Income, Education, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.286[a]	.082	.066	.73377

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age

b. Dependent Variable: A. Trust NU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.695	5	2.739	5.087	.000[b]
	Residual	153.448	285	.538		
	Total	167.143	290			

a. Dependent Variable: A. Trust NU

b. Predictors: (Constant), Occupation, Gender, Income, Education, Age

- **APPENDIX B2: Relationship between Trust, Security, Perceived Risk and Demographic Characteristics of Internet Banking Services Abandoners.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.354[a]	.125	.010	.47643

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age
b. Dependent Variable: A. Risk GU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.232	5	.246	1.085	.384[b]
	Residual	8.625	38	.227		
	Total	9.857	43			

a. Dependent Variable: A. Risk GU
c. Predictors: (Constant), Occupation, Gender, Income, Education, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.149[a]	.022	-.107	.67813

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age
b. Dependent Variable: A. Sec GU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.394	5	.079	.172	.972[b]
	Residual	17.475	38	.460		
	Total	17.869	43			

a. Dependent Variable: A. Sec GU
c. Predictors: (Constant), Occupation, Gender, Income, Education, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.296[a]	.087	-.033	.69864

a. Predictors: (Constant), Occupation, Gender, Income, Education, Age
b. Dependent Variable: A. Trust GU

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.776	5	.355	.728	.607[b]
	Residual	18.548	38	.488		
	Total	20.324	43			

a. Dependent Variable: A. Trust GU
b. Predictors: (Constant), Occupation, Gender, Income, Education, Age

- **APPENDIX B3: Relationship between Trust, Security, Perceived Risk and Demographic Characteristics of Internet Banking Services Users.**

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.124[a]	.015	.005	.52534

a. Predictors: (Constant), Occupation, Education, Gender, Income, Age
b. Dependent Variable: A. Trust U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.135	5	.427	1.547	.174[b]
	Residual	137.164	497	.276		
	Total	139.299	502			

a. Dependent Variable: A. Trust U
b. Predictors: (Constant), Occupation, Education, Gender, Income, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.156[a]	.024	.014	.57405

a. Predictors: (Conant), Occupation, Education, Gender, Income, Age
b. Dependent Variable: A. Risk U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.066	5	.813	2.468	.032[b]
	Residual	163.780	497	.330		
	Total	167.846	502			

a. Dependent Variable: A. Risk U
b. Predictors: (Constant), Occupation, Education, Gender, Income, Age

Model Summary [b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.109[a]	.012	.002	.59366

a. Predictors: (Constant), Occupation, Education, Gender, Income, Age
b. b. Dependent Variable: A. Sec U

ANOVA [a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.120	5	.424	1.203	.307[b]
	Residual	174.806	496	.352		
	Total	176.926	501			

a. Dependent Variable: A. Sec U
b. Predictors: (Constant), Occupation, Education, Gender, Income, Age

APPENDIX C: SURVEY INSTRUMENT

Software Technology Research Laboratory

De Montfort University

Bede Island Building,

The Gateway

Leicester LE1 9BH, UK

Email: P09002053@myemail.dmu.ac.uk

Dear Sir/Madam

You are invited to participate in a survey that constitutes part of my PhD at De Montfort University, Leicester, United Kingdom. The survey is about investigation of some factors which influencing Internet banking in the UK. The information you provide will be published in aggregate form within my thesis and in any resulting academic publications or conferences. **This project has been approved by the De Montfort University Human Ethics Committee.**

Involvement in this research is completely voluntary in nature and treated with total confidence and anonymity at all times and you are free not to participate at any stage.

The survey will take approximately 10-15 minutes to complete and all participants are required to be a minimum of 18 years of age.

Your contribution to this project would be highly valued and beneficial to:

- You as customers.
- Banks.
- Academics in the electronic businesses area.

If you have any questions about this survey, please contact me via any of the following:

- Telephone: 07510337221 / Email: p09002053@myemail.dmu.ac.uk.
- Post: Ahmed Massoud, 46 Dale Street, LE2 0FX, LEICESTER.
- You can also contact my supervisor Professor Hussein Zedan by means of: Telephone, +44 (0) 116 250 6152; Email: zedan@dmu.ac.uk .

Thank you for your invaluable time & kind co-operation.
Yours Sincerely,
Ahmed Massoud - PhD Student at De Montfort University

Questionnaire Guide

- If you have never used Internet banking, please complete **section one on page 3**.

- If you have previously used but have now stopped using Internet banking, please complete **section two on page 5**.

- If you use Internet banking currently, please complete **section three on page 7**.

Involvement in this research is completely voluntary in nature and treated with total confidence and anonymity at all times and you are free to decide not to participate at any stage.

Section one: [People who have never used online banking]

QA- Why have you never used online banking?

Please place a X within the below scale which best describes you experience

Q	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
1	After hearing about fake websites and frauds regarding Internet banking activity, my distrust has been increased.					
2	I do not trust the internet as a channel for banking as it is not safe.					
3	I do not trust the ability of an internet bank to protect my privacy.					
4	I do not depend on internet banking as a trusted instrument of financial transactions.					
5	If an error occurred or my account has been hacked, I am not confident that the bank will repay my money and rectify the error.					
6	Trust concerns of the internet is a major influence on my decision in non- adoption of internet banking.					
7	I worry about the security (phishing/fraud/identity theft) of Internet banking.					
8	I believe the current security measures taken by banks to protect Internet banking are insufficient.					
9	I do not have confidence in internet banking security.					
10	Branch banking is more reliable and safer than e-banking.					
11	I feel that security concerning internet banking is questionable, because there is an increase in identity theft and fraud					
12	A security issue on the internet has a major influence on my decision in not adopting internet banking.					
13	I feel that using Internet banking is too risky for me.					
14	I fear making mistakes while using an internet banking system.					
15	I do not know the benefits and risks of using internet banking. *(Continue...)*					

Q	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
16	Internet Banking system might be at risk of viruses attack or hackers.					
17	I feel the use of e-banking facilities will make it easier for banks to reduce staff numbers and this could lead to increase unemployment.					
18	A risk issue on the internet has a major influence on my decision in not adopting internet banking.					
19	I am happy with cash machines (ATM).					
20	I am happy with branch banking.					
21	How often do you use the internet?	**Frequently** ☐	**Often** ☐	**Sometimes** ☐	**Rarely** ☐	**Never** ☐
QB	Other reasons for not using internet banking to perform banking transactions?					
QC	In order to encourage you to use internet banking, what do you think the Bank should do?					

Now: please go to the demographic question on page number (11).

Thank you very much for your valuable time and information

Section two: [People who have previously used but have now stopped using internet banking]

QA- Why have you stopped using online banking?

Please place a X within the below scale which best describes you experience

Q	Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
22	I do not trust the ability of internet banking to protect my privacy and personal information.					
23	It is not difficult to hack the internet banking site via the internet.					
24	I believe that internet banking is insecure					
25	I am not confident that the bank will help me to recover my money and rectify the error, if an error occurred or my account has been hacked.					
26	Trust issue in the internet banking have had a major influence on my decision to abandon this service.					
27	I am worried about the security (phishing/fraud/identity theft) of Internet banking.					
28	I did not feel totally safe providing personal and sensitive private information over Internet Banking.					
29	The current security measures taken by banks to protect Internet banking are insufficient.					
30	I feel that security concerning internet banking is questionable, because there is an increase in identity theft and fraud.					
31	Security issues on the internet have had a major influence on my decision to abandon this service.					
32	Whilst carrying out transactions, internet banking takes longer than before due to security measures.					
33	While accessing internet banking, there is a risk that banks may not authenticate my username and my password in an accurate manner.					
34	Internet banking system might be at risk of virus attacks or hackers.					
35	I felt that using internet banking is too risky for me. ***(Continue please...)***					

Q	Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
36	When transferring money on the internet, I am afraid that I will lose money due to careless or mistakes in transactions.					
37	Risk issues on the internet banking have had a major influence on my decision to abandon this service.					
38	I am happy with cash machines.					
39	I am happy with branch banking.					
QB	*Are there other reasons behind your abandoning of internet banking?*					
QC	*In order to encourage you to reuse internet banking, what do you think the Bank should do?*					

<u>Now</u>: please go to the demographic question in page number (11).

<u>Thank you very much for your valuable time and information</u>

Section three: [People who are using online banking currently]

QA- What factors of internet Banking contributes to a positive experience?

Please place a X within the below scale which best describes you experience

Q	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
40	I trust internet banking to accomplish banking services satisfactorily.					
41	It is difficult to hack the internet banking site via the internet.					
42	If an error occurred or my account has been hacked, I am confident that the bank will compensate my money and rectify the error.					
43	I prefer to use internet banking rather than conventional banking, even if the transaction involves a large amount of money.					
44	I trust internet banking systems not to disclose my private information and it is able to protect my privacy.					
45	I believe that Internet banking provides accurate records that all transactions have taken place.					
46	Trust in internet banking may have an impact on my decision to continue using it in the future.					
47	When I conduct transactions in Internet banking, I have…?	Not confidence ☐	Low Confidence ☐	moderately Confidence ☐	highly Confidence ☐	Very-highly confidence ☐
48	I am not concerned about the security (phishing/fraud/identity theft) of Internet banking.					
49	The current security measures taken by banks to protect Internet banking are efficient.					
50	I believe that Internet banking is able to conduct banking transactions securely.					
51	I feel that security concerning internet banking is unquestionable, because there is a reduction in identity theft and fraud *(Continue please ...)*					

Q	Statements	Strongly Disagree	Disagree	Neutral	Agree	Strongly agree
52	Security issues within internet banking may have an impact on my decision to continue using it in the future**.**					
53	How concerned are you about the security of internet banking?	Not at all concerned ☐	A little concerned ☐	Concerned ☐	Moderately concerned ☐	Very concerned ☐
54	Internet banking system might not be at risk of virus attacks or hackers.					
55	While accessing internet banking, there is not a risk that banks may not authenticate my username and my password in an accurate manner.					
56	I am not afraid that I will lose money due to careless mistakes in transactions, because my bank will help me to recover any lost money.					
57	I do not feel that use of internet banking facilities will make it easier for banks to reduce staff numbers and this could lead to increased unemployment.					
58	Internet banking does not take longer than before due to security measures to ensure safety of data and confirm transactions.					
59	Risk issues within internet banking may have an impact on my decision to continue using it in the future.					
60	Whilst performing Internet banking transactions , I would rate the risk of financial loss and losing personal information as:	Very likely to Occur ☐	Likely to Occur ☐	Neutral ☐	Unlikely to Occur ☐	Very Unlikely to Occur ☐
61	When you conduct transactions in Internet banking what is your view of risk?	Very insignificant risk ☐	Insignificant risk ☐	Neutral ☐	Significant risk ☐	Very significant risk ☐
62	In general, I predict I would continue using Internet banking regularly the future.					
QB	If there are other reasons except (trust, risk and security) behind your decision of adoption / continuous use of internet banking, please mention? ..... (***Continue please...)***					

QC- In order to increase your trust, what do you think the Bank should do? **[**Please select ***the five most important*** from the following options**]**		
1	Give enough safeguards to make user feel comfortable when making internet banking transactions.	
2	Direct contact with bank staff on the Internet if there is an inquiry/problem.	
3	Show due diligence and responsibility when problems occur.	
4	Offer assistance to guide users, if they get stuck or make a mistake as well providing useful tips.	
5	Website should provide information that helps decrease uncertainty related to internet banking.	
6	Take necessary modern security measures, which would lead to reduced risks and increase users trust in internet banking.	
7	Have a good navigability and visibility within the internet banking website (e.g. easy to locate the services and professional design)	
8	Work as a group with banks to activate existing international and local rules and make it more efficient to protect banks and clients.	
9	Offer clear and reassuring responses about adverse news (identity theft and internet fraud).	
10	Maintaining and promoting a good reputation.	
11	Other *(please specify)*:	

QD- In order to enhance security, what do you think the Bank should do? **[**Please select ***the five most important*** from the following options**]**		
1	Use multi-factor authentication (combination of factor) which uses two or more factors to assert identity are (**password – PIN**) and **biometric technologies** such as (Retinal Scan, Voice Pattern, Facial recognition and Fingerprints), rather than two-factor authentication methods to access to internet banking.	
2	Using personal electronic devices (e.g. Secure Key) to be highly secure for internet banking transactions.	
3	Send warning messages when the communication is insecure.	
4	Make additional methods of verifying my identity before imputing account information and processing transactions.	
5	Enhance security measures even if there is limited time a day to access website.	
6	Promote security measures even if internet banking transaction takes longer than before.	
7	Make clients change their PIN / Password every so often to make internet banking more secure.	
8	Outline the risks and promote user's confidence of the effective security measures.	
9	Banks could send confirmation codes to customer's mobile phone for transactions under process, this will enable greater security.	
10	Banks increase the awareness about security of internet banking**.**	
11	Other *(please specify)*: ***(Continue please...)***	

QE- In order to reduce risk, what do you think the Bank should do? [Please select ***the three most important*** from the following options]		
1	Compensate any money taken from user account through unauthorized transactions.	
2	When problems occur or user gets stuck, the internet banking system should guide him to solve them.	
3	Enhance security measures to protect internet banking from risks of virus attacks, hackers or fraud.	
4	Running awareness campaigns against risks (e.g. identity theft, cyber-crimes and fraud).	
5	Give enough safeguards to make user feel comfortable toward risks when making internet banking transactions.	
6	Should have clear laws and rules to protect users from risks using internet banking.	
7	Other *(please specify)*: .... ***(Continue please...)***	

QF	**Have you ever visited your bank branch since the time you started using online banking?** **If yes,** please select the most important reasons for the visit	Yes	No
1	To make a deposit.		
2	To discuss other banking services which not available online.		
3	When I get stuck or some mistakes had happened.		
4	To make large cash withdrawal.		
5	**Other important *(please specify):***		

QG	**My Internet banking experience is.....Years. (Please fill the blank space)**

<u>Now</u>: please go to demographic question in page number (11)

<u>Thank you very much for your valuable time and information</u>

Demographic Question:

For research statistic purposes, please can you answer the following by placing a circle for your response for each question?

A. Gender:
   1. Male
   2. Female

B. Age group :
   1. 18-25
   2. 26-45
   3. 46-60
   4. Above 60 years

C. Education level (please indicate highest a achieved)
   1. Primary school
   2. Secondary school
   3. College
   4. Bachelor degree
   5. Master degree
   6. Doctorate (PhD)
   7. Other (please specify).....

D. Monthly income :
   1. £1500 and under
   2. £1501- £2000
   3. £2001-£2500
   4. £2501-£3000
   5. £3001-£3500
   6. £3501-£4000
   7. £4001-£4500
   8. £4501 and above

E. Please specify your Nationality.....

F. Occupation:
   1. Student
   2. Housewife /Homemaker
   3. Self-employed
   4. Unemployed
   5. Employee/officer in the government sector
   6. Employee/officer in the private sector
   7. Retired/pensioner
   8. Other (please specify).....

Thank you very much for your valuable time and information

APPENDIX D: CERTIFICATE OF ETHICAL APPROVAL

From: Amita Patel
Sent: 10 April 2013 14:38
To: P09002053@myemail.dmu.ac.uk
Subject: RE: Ahmed Massoud p09002053 - 1011/049

Hello

Your application to gain ethical approval for research degree activities has been considered and APPROVED by the Faculty Human Research Ethics Committee (FHREC). No further issues were raised by the committee.

Please be aware that changes to the project plan or unforeseen circumstances may raise ethical issues. If this is the case it is the researcher's duty to repeat the ethics approval process.

Kind regards

Amita Patel

Faculty Secretary/Administrator
Faculty of Technology

De Montfort University
T: +44(0) 116 257 7473
E: a.patel@dmu.ac.uk
W: dmu.ac.uk