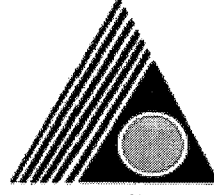


160806



**T.C
YEDİTEPE UNIVERSITY
GRADUATE INSTITUTE OF SOCIAL SCIENCES**

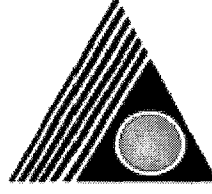
**A STUDY ON THE IMPACT OF SECURITY FRAMEWORK
ON THE DEVELOPMENT OF INTERNET BANKING**

by

Gökhan AFACAN

**Submitted to the Graduate Institute of Social Sciences
In partial fulfillment of the requirements for the degree of
Master of
Business Administration**

ISTANBUL, 2005



T.C
YEDİTEPE UNIVERSITY
GRADUATE INSTITUTE OF SOCIAL SCIENCES

**A STUDY ON THE IMPACT OF SECURITY FRAMEWORK
ON THE DEVELOPMENT OF INTERNET BANKING**

by

Gökhan AFACAN

Supervisor

Prof. Dr. Ahmet SERPİL

**Submitted to the Graduate Institute of Social Sciences
In partial fulfillment of the requirements for the degree of
Master of
Business Administration**

ISTANBUL, 2005

**A STUDY ON THE IMPACT OF SECURITY FRAMEWORK
ON THE DEVELOPMENT OF INTERNET BANKING**

by

GÖKHAN AFACAN

Approved by:

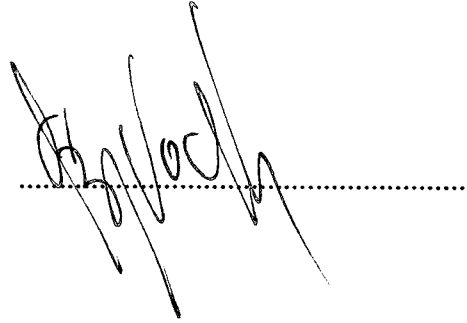
Prof. Dr. Ahmet SERPİL
(Supervisor)



Asst. Prof. Dr. M. Atilla ÖNER



Asst. Prof. Dr. Saso VRBOSKI



Date of Approval by the Administrative Council of the Institute 22/07/2005

TABLE OF CONTENTS

	Page
LIST OF ABBREVIATIONS	V
LIST OF FIGURES	VI
LIST OF TABLES	VII
ACKNOWLEDGEMENTS	VIII
ACKNOWLEDGEMENTS	VIII
ABSTRACT	IX
ÖZET	X
1. INTRODUCTION.....	1
1.1. RESEARCH OBJECTIVE	2
1.2. METHODOLOGY	2
2. ONLINE BANKING.....	3
2.1. DEFINITIONS	3
2.2. ADVANTAGES OF INTERNET BANKING	4
2.3. RISKS OF USING INTERNET BANKING.....	5
2.4. FRAUD ON ONLINE BANKING.....	6
A. PHISHING	6
B. DATASTREAMING FOR IDENTITY THEFT	7
C. SPYWARE AND SPAM.....	7
D. DEFAACEMENT.....	8
E. MALWARE AND VIRAL ATTACKS	9
F. DENIAL OF SERVICE (DOS)	9
2.5. CASES OF INTERNET BANKING FRAUDS	9
2.5.1. MIMAIL CASE.....	10
2.5.2. ABSA BANK CASE	10
2.5.3. PHISHING ATTACK ON CITIBANK.....	11
2.6. LIABILITIES OF PARTIES	13
2.6.1. GENERAL PRECAUTION STEPS TAKEN BY BANKS:	14
2.6.2. GENERAL PRECAUTION STEPS TAKEN BY CUSTOMERS:.....	15
2.6.3. BANKS' APPROACH ON SECURITY ISSUES IN TECHNICAL AND SOCIOLOGICAL VIEWS 18	
2.6.3.1. APPROACH ON SECURITY ISSUES	18
2.6.3.2. APPROACH ON LIABILITY ISSUES.....	19
3. EMPIRICAL STUDIES ON INTERNET BANKING	22
3.1. LITERATURE REVIEW	22
3.1.1. BANKS AND TRUST NOTION.....	22
3.1.2. STUDIES ON ADOPTION OF INTERNET BANKING	23

3.2.	STATISTICAL STUDIES.....	24
4.	RESEARCH QUESTION AND EMPIRICAL ANALYSIS.....	26
4.1.	RESEARCH PROBLEM	26
4.2.	HYPOTHESIS.....	27
4.3.	METHODOLOGY	27
4.4.	RESEARCH APPROACH	28
5.	EMPIRICAL RESULTS.....	30
5.1.	GENERAL FINDINGS	30
5.2.	DETAILED SURVEY RESULTS	31
5.2.1.	SECURITY CONSIDERATIONS	31
5.2.2.	USABILITY CONSIDERATIONS	34
5.2.3.	STANDARDIZATION CONSIDERATIONS.....	37
5.3.	DATA CONSISTENCY AND RELIABILITY	39
6.	DISCUSSION AND CONCLUSION	42
6.1.	RECOMMENDATIONS FOR FURTHER RESEARCH	44
6.1.1.	E-SIGNATURE.....	44
6.1.2.	INTERNET BROWSER CHANGES	44
6.1.3.	SMS ISSUES	45
6.1.4.	SINGLE SIGN-ON FEATURES	46
APPENDICES.....		48
APPENDIX A: QUESTIONNAIRE – TURKISH VERSION.....		48
APPENDIX B: QUESTIONNAIRE – ENGLISH VERSION		52
REFERENCES.....		56
CV OF THE AUTHOR.....		59

LIST OF ABBREVIATIONS

APACS	Association for Payment Clearing Services
ATM	Automated Teller Machine
DoS	Denial of Service
E-banking	Electronic Banking
EFT	Electronic Funds Transfer
E-Signature	Electronic Signature
I-banking	Internet Banking
ISP	Internet service provider
PC	Personal Computer
PDA	Personal Digital Assistant
SMS	Short Messaging Services
SSL	Secure Sockets Layer
TLS	Transport Layer Security



LIST OF FIGURES

Figure 2.1: Reported phishing sites by week of Oct 2005-Jan 2005	7
Figure 2.2: Fake e-mail sent to Citibank customers	12
Figure 2.3: Fake web site which Citibank customers are redirected.	13
Figure 5.1 Overall view on security of Internet banking services	31
Figure 5.2 Overall view on usability of Internet banking services	35
Figure 5.3 Bank login mechanism usability	35
Figure 5.4 Virtual keyboard usability	36
Figure 5.5 Transaction password usability	36
Figure 5.6 Session timeout usability	37
Figure 5.7 Using unstandard interfaces in scalar	39



LIST OF TABLES

Table 5.1 Respondents' willingness on using Internet banking	30
Table 5.2 Overall view of Internet banking services	30
Table 5.3 Security based Internet banking services variables.	31
Table 5.4 Bank login mechanism security	32
Table 5.5 Virtual keyboard	33
Table 5.6 Transaction password	33
Table 5.7 Session timeout	34
Table 5.8 Usability based Internet banking services variables.	34
Table 5.9 Standardization based Internet banking services variables.	37
Table 5.10 Respondents' willingness on facing advertising and inserts in an Internet banking environment.	38
Table 5.11 Respondents' opinion on using same interface for all the banks they are registered.	39
Table 5.12 Correlation table concerning security	40
Table 5.13 Correlation table concerning usability	41



ACKNOWLEDGEMENTS

The work presented in this thesis was carried out during the fall and spring of 2005 at Yeditepe University MBA Program. Therefore, I would like to show my sincere gratitude and appreciation to the people that have helped me during the process of writing and making this thesis possible.

First I would like to express my sincere gratitude to my advisor, Cemil Tarhan, at the MBA program in Yeditepe University, for his valuable supervision and encouragement to make this research to arise. This study would not ever be completed without his ideas and approaches.

Specially thanks to the survey participants who spent their valuable time for this study. Public view is always valuable for any project to begin and get success. I also would like to thank to my teacher Altan Coner who made it possible the public opinion flow to my research.

I would like to thank to my mother who encouraged me to begin this MBA program. Finally I would like to thank to my wife for her understanding, endless support and love.

Gökhan AFACAN

May 2005

İstanbul, Turkey

ABSTRACT

As the usage of Internet becomes wide spread, nearly all banking activities are now quickly performed online. It did not take a long time to adapt using Internet banking, with the help of both technological opportunities used by banks and due to the nature of human. With the increase in number of users in a short period, this system has introduced new definitions for trust matters in banking.

This research work mainly concentrates on the Internet Banking services in Turkey, with respect to security and ease of use. In what level does the current infrastructure of Internet banking encourages customers to perform banking operations through the Internet? In what levels do we have to suffer from usability difficulties against security fear? Would it cause paranoia that an endless patchwork of current Internet Banking tools exists aiming to block security gaps? How does it affect customers that every day a new precaution has to be faced with? In what level do bank customers satisfied from the security and usability infrastructure of Internet Banking? What is the adoption to the new and variant possibilities?

The results of the study shows that, as the level of hardening in security increased by the bankers and new, but transient, precautions are introduced; a meaningful level of trust seems to be accepted by the users. Findings tell us that; when general security precautions are considered, with a rate of 80 percent, current security implementations taken by banks are welcomed by customers. A large percent of respondents find using Internet Banking is easy to use. The rank above average is 92 percent which denotes the belief of their internet bank is easy to use. Regarding the answer of whether there exists a potential seek for using same interface for all the banks they are registered, it is found that approximately one third of the respondents think that it will be beneficial to have a standard interface interconnecting all the banks that respondents are currently registered.

It is the author's belief that; due to newly developed Internet fraud methods and as these methods become more wide spread in Turkey, all the personal banking operations will sometime be handled through a unified, single sign on, transaction based, secure, easy to use interfaces and possibly including hardware based solutions such as smart cards.

ÖZET

Günümüzde yaygın Internet kullanımını sayesinde ülkemizde de hemen hemen tüm bankacılık işlemleri online olarak hızlı bir şekilde gerçekleşmektedir. Gerek bankaların teknolojik olanakları sayesinde gerekse de insan doğası gereği Internet bankacılığına adaptasyon çok fazla zaman almadı. Kullanıcısı kısa sürede artan bu sistem, beraberinde yeni güven bunalım tanımlarını da bankacılığa kazandırdı.

Bu araştırmanın temel amacı Türkiye'deki Internet bankacılığı hizmetlerini güvenlik ve kullanım kolaylığı açılarından sorgulamaktır. Varolan Internet bankacılığı yapısı, insanları, bankacılık işlemlerini Internet üzerinden yapmaya ne oranda teşvik etmektedir? Internet bankacılığı sistemlerinin güvenlik açıklarını kapatmaya yönelik bitmek bilmeyen yamalanma çalışmaları bir paranoyaya mı yol açmaktadır? Güvenlik korkusuna karşı kullanım zorluğu çekmeye ne oranda mecburuz? Her geçen gün yeni bir önlemle karşılaşılıyor olmamız bizi nasıl etkiliyor? Banka müşterileri kendilerine sunulan şu anki güvenlik ve kullanılabilirlik altyapısından ne oranda tatmin sağlıyor? Yeni ve farklı olanaklara adaptasyonları nedir?

Bu sorulara yanıt arayan araştırmamızın sonuçları gösteriyor ki güvenliğin bankacılar tarafından sıkılaştırılması ve yeni güvenlik önlemleri, aynı zamanda güvenin de müşteri tarafından yüksek oranda sağlanmış olarak kabullenilmiş anlamına geliyor. Tez bulguları şunu anlatıyor ki, bankaların genel güvenlik önlemleri göz önünde bulundurulduğunda, yüzde 80 oranla müşteri memnuniyeti sağlanmış durumdadır. Ayrıca, online banka web siteleri genel kullanılabilirlik oranı da yüksek oranda gözlemlenmektedir. Ortalama üzeri genel kullanılabilirlik düzeyi yüzde 92 oranında olduğu görülmektedir. Müşterilerin farklı bankalardaki hesaplarını ortak bir arayüzde toplama ve böylelikle müşterilerin kayıtlı oldukları bankalardaki hesaplarını ortak bir ara birimde birleştirme amaçlı araştırma sonuçlarına göre ise, müşterilerin üçte biri bu tür bir özelliğe sıcak yaklaşmakta olduğunu görüyoruz.

Bize göre gelişen dolandırıcılık yöntemleri ve bu yöntemlerin ülkemizde daha yaygın bir hale gelişi, şu an kullanılan yöntemlerin yerini tek işlem bazlı, tüm bankacılık faaliyetlerinin ortak, tam güvenilir ve belki de akıllı kart gibi donanımsal altyapı içeren bir ortama bırakmasını sağlayabilecektir.

1. INTRODUCTION

One of the most important enabling infrastructures of the today's globalised economy is the Internet. Having revolutionized many industries in all corners of the world, with developing countries being no exception, this global network is now being used by banking sector wide spread. Most banks are now aware of online delivery and many banks now consider online delivery as an important strategic initiative. Today, in Turkey, only a few number of banks do not offer transactional online banking services for their retail or business customers.

An important factor driving change in personal banking has been the growth in use of the personal computers (PCs). During 1980's, personal finance programs were introduced by banks to provide convenient tracking of spending patterns, taxes and investments. Until 1995, customers still had to enter their own personal financial information, but in that year, some banks began offering on-line banking via interfaces with either industry standard software (e.g., Quicken) or using their own proprietary software (Clark and Lee, 1998). Earlier efforts to promote home banking failed to catch on because the appropriate technology was not in place, but this was no longer expected to be a barrier with more than one-third of all homes owning PCs by 1996 (Clark and Lee, 1998).

Some banking industry analysts and consultants view on-line banking as a continuation of the shift away from face-to-face transactions that began with the rapid expansion of ATM (automatic teller machine) networks. (Barth and Brumbaugh, 1995) Enormous advances in computer and related communications technology are enabling a revolution in personal banking, and new forms of on-line banking appear to be gaining momentum (Clark and Lee, 1998).

Companies have realized that the Internet has encompassed revolutionary changes in communications, entertainment, information and computing. The implications of these changes will be persuasive, transforming banking as we know it today. Banks not only initiate their own moves onto the Internet but are also pushed by other non-bank competitors (Yan and Paradi, 1998). Today banking sector, one of the primary driver of the economy, uses Internet technologies as one of the primary delivery channel.

1.1. Research Objective

This research work mainly concentrates on the following issues:

- Query the level of using the Internet banking as an alternative method for traditional brick-and-mortar banks.
- Research for security considerations of Internet banks and in what level of customer satisfaction is covered throughout these considerations.
- Research for usability considerations of Internet banks and test whether usability issue are in adequate level of customers' expectations.
- Research the potential demand for a real secure and easy-to-use standard interfaces for Internet banking environment.
- Finally, research the current technological framework used by banks and the way of Internet banking is adequate and encourage customers banking through the Internet?

In the light of current technological implementations, this research work will propose alternative solutions to be used in Internet banking.

1.2. Methodology

Following the objective, public opinion was researched through a survey. A questionnaire was designed on a public Internet site, to incorporate elements that allow customers of Internet Banking to rate the performance of their banks. It captures data about the banks' effectiveness and level of satisfaction with current online banking products. Customers were asked whether the currently taken steps of precautions are satisfactory with respect to security and ease of use.

2. ONLINE BANKING

2.1. Definitions

In this section we begin by defining some different types of terms in the literature such as E-banking, PC banking, Internet banking. The following terms all refer to one form or another of electronic banking: personal computer (PC) banking, Internet banking, virtual banking, online banking, home banking, and remote electronic banking. Internet or online banking and PC banking terms are the most frequently used designations. It should be noted, however, that the terms used to describe the various types of electronic banking are often used interchangeably. (Bankersonline.com, 2003)

E-banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution. E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. (ffiec.gov, 2004)

PC banking refers to computer hardware, software, and telecommunication systems that enable retail customers to access both specific account and general bank information on bank products and services through a personal computer. The bank's network design and telecommunication links may include the use of private networks (e.g., direct dial-in using leased or dedicated telephone lines) or public networks (e.g., the Internet).

In most PC banking ventures, the bank offers the customer a proprietary financial software program that allows the customer to perform financial transactions from his or her home computer. The customer then dials into the bank with his or her modem, downloads data, and runs the programs that are resident on the customer's computer. Currently, many banks

offer PC banking systems that allow customers to obtain account balances and credit card statements, pay bills, and transfer funds between accounts electronically.

Internet banking, sometimes called online banking, is an outgrowth of PC banking. Internet banking uses the Internet as the delivery channel by which to conduct banking activity, for example, transferring funds, paying bills, viewing checking and savings account balances, paying mortgages, and purchasing financial instruments and certificates of deposit. An Internet banking customer accesses his or her accounts from a browser— software that runs Internet banking programs resident on the bank’s World Wide Web server, not on the user’s PC. NetBanker defines a “true Internet bank” as one that provides account balances and some transactional capabilities to retail customers over the World Wide Web. Internet banks are also known as virtual, cyber, net, interactive, or web banks. (Bankersonline.com, 2003)

2.2. Advantages of Internet Banking

From both bankers’ and customers’ points of view, because Internet banks generally have lower operational and transactional costs than do traditional brick-and-mortar banks, they are often able to offer low-cost checking and high-yield Certificates of deposit. Internet banking is not limited to a physical site; some Internet banks exist without physical branches, for example, Telebank (Arlington, Virginia) and Banknet (UK). Further, in some cases, web banks are not restricted to conducting transactions within national borders and have the ability to make transactions involving large amounts of assets instantaneously.

According to industry analysts, electronic banking provides a variety of attractive possibilities for remote account access, including:

- Availability of inquiry and transaction services around the clock;
- worldwide connectivity;
- Easy access to transaction data, both recent and historical; and
- “Direct customer control of international movement of funds without intermediation of financial institutions in customer’s jurisdiction.”

(Bankersonline.com, 2003)

From customers' point of view more specifically, key benefits include;

- **Convenience:** Unlike brick-mortar banks, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a mouse click away.
- **Ubiquity:** If customer is out of state or even out of the country when a money problem arises, he can log on instantly to online bank and take care of business, 24/7.
- **Transaction speed:** Online bank sites generally execute and confirm transactions at or quicker than ATM processing speeds.
- **Efficiency:** All bank accounts are always available and manageable, including IRAs, CDs, even securities, from one secure site.
- **Effectiveness:** Many online banking sites now offer sophisticated tools, including account aggregation, stock quotes, rate alerts and portfolio managing programs to help manage all customer assets more effectively. Most are also compatible with money managing programs such as Quicken and Microsoft Money. (Bankrate.com, 2004)

2.3. Risks of Using Internet Banking

Apart from the obvious benefits of the system there are however collateral risks associated with the absence of personal contact. The most dangerous of these is the reduced risk and effort for the "would-be-thieves" for "passing off" as legitimate clients. Before Internet banking age, such a delinquent would have to forge not only the signature but also the whole identification document. Today, though much easier ways of defrauding are available to them (Granova and Eloff, 2004).

Other online banking risks and disadvantages include the topics below:

- **Start-up may take time:** In order to register for bank's online program, customer will probably have to provide ID and sign a form at a bank branch. As the customer or his spouse wishes to view and manage assets together online, he may have to sign a durable power of attorney before the bank will display all of holdings together.
- **Learning curve:** Banking sites can be difficult to navigate at first. Customers must plan to invest some time and/or read the tutorials in order to become comfortable with the interface.
- **Bank site changes:** Even the largest banks periodically upgrade their online programs, adding new features in unfamiliar places. In some cases, customer may have to re-enter account information.

- The trust thing: For many people, the biggest hurdle to online banking is learning to trust it. Did the transaction go through? Customer should always print the transaction receipt and keep it with his bank records until it shows up on his personal site and/or his bank statement. (Bankrate.com, 2004)

2.4. Fraud on Online Banking

In this section we will identify security threats upon online banks, hence upon customers. To begin with the definition of identity theft, it is the act of stealing or using an individual's personal information without their knowledge or consent, for example, to illegally apply for credit, make purchases, or gain access to funds. Since the statements or bills related to the fraudulent accounts are often sent to a different address, victims may not become aware of the increased debt until, for instance, they are tracked down by creditors or are turned down when they apply for credit. Identity theft can take months to detect and even longer to clear.

In the following part, the reader will find currently used methods of fraud to aim at identity theft and to prevent functioning of online services on one or both of the side, i.e. on customers' PC or banks' network. A brief discussion is presented about what that specific method is based on:

a. Phishing

Phishing, also called "carding," is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information such as T.R. Identity numbers, passwords, credit card numbers, bank account numbers, and other sensitive information that will be used for identity theft. The emails pretend to be from businesses the potential victims deal with - for instance, their online banks, Internet service provider (ISP), online payment services. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and direct them to a "look-alike" website of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request.

Unknowingly, consumers submit their financial information — not to the businesses — but the scammers, who use it to order goods and services and obtain credit (Granova and Eloff,

2004). Figure 2.1 below, depicts the number of most recently reported phishing sites week by week.

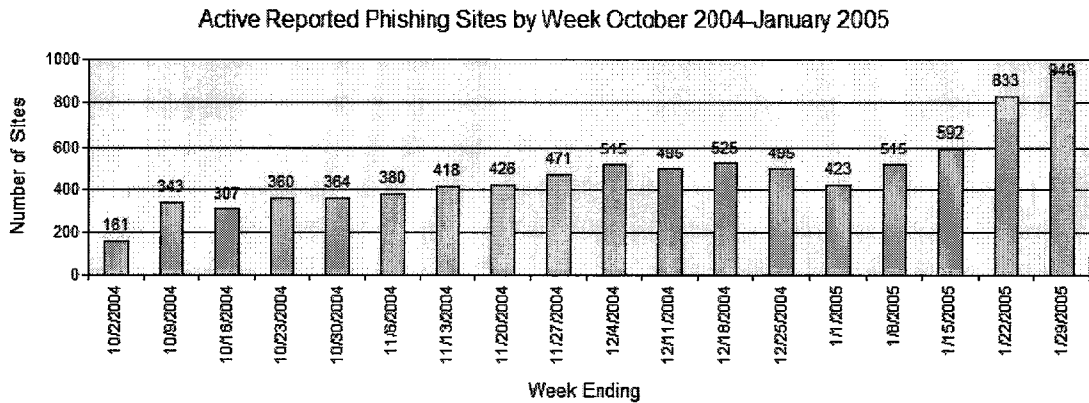


Figure 2.1: Reported phishing sites by week of Oct 2005-Jan 2005 (Antiphishing.org, 2005)

b. Datastreaming for identity theft

Datastreaming is one of the threats that is more likely to explicitly target the E-commerce domain, and involves the bulk theft of personal data such as card details by individuals or groups hacking into related systems. Although consumers may instinctively consider that their data requires protection against interception as it travels across the network, the evidence shows that it is far more likely to be vulnerable at the remote destination, where hackers may break in and steal it en masse (Furnell, 2004).

Hackers can dive into the mass data, i.e. banks' customer database, which is opened by means of Internet banking applications using public network as well as with the help of an insider working in the bank. Huge amount of fraud has been detected through the latter method especially inside global banks.

c. Spyware and spam

Spyware is the technology that assists in gathering information about a person or organization without their knowledge. On the Internet, "spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties." As such, spyware is cause for public concern about privacy on the Internet.

If a computer suffers from the following symptoms, spyware is on the computer:

- Browser home page keeps changing and new toolbars appear in browser.
- Excessive pop-up ads appear.
- The computer and Internet access speed is slow and frequent computer crashes occur.

Spam is an inappropriate attempt to use an e-mail address, mailing list, newsgroup or other networked communications facility as if it was a broadcast medium by sending the same message to a large number of people who didn't ask for it. Spam is e-mail sent indiscriminately to a large number of recipients, usually promoting a product or service. As e-mail costs close to nothing to send, many people have taken this as an invitation to send as much as they can to as many people as they can find. (Mxes.org. 2005)

Beginning with the new millennium, there is an increase of spam. According to third SpyAudit Report which has been released by EarthLink, a US Internet service provider, and, Webroot Software, there is a constant growth of spyware on consumer PCs for the first half of 2004. Since the SpyAudit report's inception on 1 January 2004, more than two million scans have been performed. The scans discovered approximately 54.8 million instances of spyware, giving an average of 26.5 traces per SpyAudit scan. Adware and Adware Cookies account for the bulk of these (26.1). Trojans, although account for only 0.2 per scan, this does mean that every fifth PC had a Trojan (Hinde, 2004).

d. Defacement

Defacement is simply alteration of the web site content of the e-bank or e-commerce site and publishing of hacker's own data on the public web site of the institution. Given that the website is often the shop window for the E-business, it is important to ensure that it conveys the correct information and the best impression. With this in mind, vandalism of the site and alteration of its content is clearly unwelcome. Defacement has become a significant problem, and sites running unpatched Web server software represent a relatively easy target, even for novice hackers. For example, encountering a defaced site has the potential to cause lasting damage to the customer's impression of the business, and in particular to the perception of its security (e.g. if the business cannot even protect its shop window, why should I trust it with my data?) (Furnell, 2004).

e. Malware and viral attacks

Worms, viruses and other forms of malicious software represent the biggest threat to networked systems in general, and thus are certainly issues that E-commerce operators cannot afford to ignore. An infection may affect the operation of services, and hence represents a cause of lost revenue if this results in impairment or unavailability. Malware is also an issue from the customer perspective, in the sense that it could compromise security during their use of E-commerce services (Furnell, 2004).

f. Denial of service (DoS)

DoS involves the intentional impairment or blocking of legitimate access by an unauthorized party (e.g. by flooding the victim site with spurious traffic). The 2004 version of the CSI/FBI's annual Computer Crime and Security Survey reveals that DoS attacks were the most costly reported, accounting for \$26M from the 269 respondents that were willing and able to quantify their losses (Furnell, 2004).

In addition to the facts mentioned above, there exist some more things to consider when being an online banking customer. Even though the customer is certain about a fully secure banking system, a new bug may be detected in the tools that the customer uses. To illustrate, The Microsoft phishing bug, is an easily exploited flaw in the way Internet Explorer displays URLs in the address bar because the browser is incapable of displaying the special character "%01," or anything following it, in a Web address.

Above simple vulnerability appears to be tailor-made for phishing attacks. The phishing link takes the victim to a fake website designed – with increasing sophistication - to look like the real deal, but where any personal or financial information entered is routed directly to the scammer (Hinde, 2004). This threat is also reasonable when considering the banks' Internet banking applications such as Microsoft SQL Server and Internet Information Server.

2.5. Cases of Internet Banking Frauds

Although nearly every week we hear about an Internet banking incident event, we do not sense that much of them. This maybe because of the fright of the banks, in part, because the major banks don't want to divulge the amount of losses they're seeing for fear that it will damage their online banking businesses.

In this section we will present some example scenarios about fraud on Internet banking which took place throughout the world. Sample scenarios are included here to emphasize the dimensions of this type of fraud and the new methods for stealing empowered by the information technology. We have to state that these are only the selected ones from thousands of experiences all of which vindicate the anxiety of both of the included parties, i.e. the bank and the customer. Based on the information supplied by an organization which keeps track of and publishes recently up to date phishing attacks, we will also mention about key losses.

2.5.1. Micemail case

The Micemail worm, one of the latest major phishing attacks, took a giant step forward in sophistication by blending its phishing attack with a mail worm application. The "link" in the Micemail email was actually an executable that asked the viewer for personal and credit card information in an official-looking interface, with the added capability of being able to spread itself through the usual worm-spreading techniques. The virus arrives via an email, which is thought to have been distributed through the usual spamming channels, that purports to come from eBay's online-payment service, with the subject "PAYPAL.COM NEW YEAR OFFER". The email text goes on to explain that users can get their hands on a few bob if they register with the site by handing over their financial details. If the recipient opens the email attachment and launches the file it contains, the Trojan will download and run a new variant of the Micemail virus. The virus goes on to harvest more email addresses from the user's hard drive and sends itself out every time the user opens Windows (Hinde, 2004).

2.5.2. ABSA bank case

ABSA bank, has provided an Internet banking service to its clients for several years. In this "identity theft" incident, 10 ABSA Internet banking clients cumulatively lost R530,000 due to unauthorized online Internet transactions performed on their accounts, all of which were carried out between May and July 2003.

Contrary to popular belief, the loss of money could not have been attributed to "hacking" since the spyware software in question, also known as a Trojan, was attached to an email, which unsuspecting clients were enticed to open on their computers. Thereafter, the Trojan

recorded all key strokes and secretly emailed this information to the perpetrator. The perpetrator then logged into his victim's online Internet banking accounts and transferred money to selected organizations as payment for goods purchased, or another bank account for the purposes of withdrawal (Granova and Eloff, 2004).

2.5.3. Phishing attack on Citibank

E-mail users throughout the world received an e-mail which claimed to have come from Citibank Credit Card Department asking for personal details including Internet banking user id and password of the customer. In reality, the server that will pick customer information was owned by the phisher and the server is up for only a few days. Even this time is enough for making money over uneducated and careless but real customers.

Figure 2.2 shows the mail request for information, arranged in a formal manner, from the customer.



Dear Customer:

Recently there have been a large number of cyber attacks pointing our database servers. In order to safeguard your account, we require you to sign on immediately.

This personal check is requested of you as a precautionary measure and to ensure yourselves that everything is normal with your balance and personal information.

This process is mandatory, and if you did not sign on within the nearest time your account may be subject to temporary suspension.

Please make sure you have your Citibank(R) debit card number and your User ID and Password at hand.

Please
Citibank(R) Card Department

(C)2004 Citibank. Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC. Citibank and Arc Design is a registered service mark of Citicorp. use our secure counter server to indicate that you have signed on, please click the link bellow:

<http://211.158.34.250/citifi/>

!! Note that we have no particular indications that your details have been compromised in any way.

Thank you for your prompt attention to this matter and thank you for using Citibank(R)

Regards,

Citibank(R) Card Department

(C)2004 Citibank. Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC. Citibank and Arc Design is a registered service mark of Citicorp.

Figure 2.2: Fake e-mail sent to Citibank customers
(Antiphishing.org, 2005)

E-mail redirects the customer to phisher's web site which has a clumsy design not likely to be found on a legitimate page. Web site is a very basic one which has no security setting. The web page is shown on Figure 2.3.

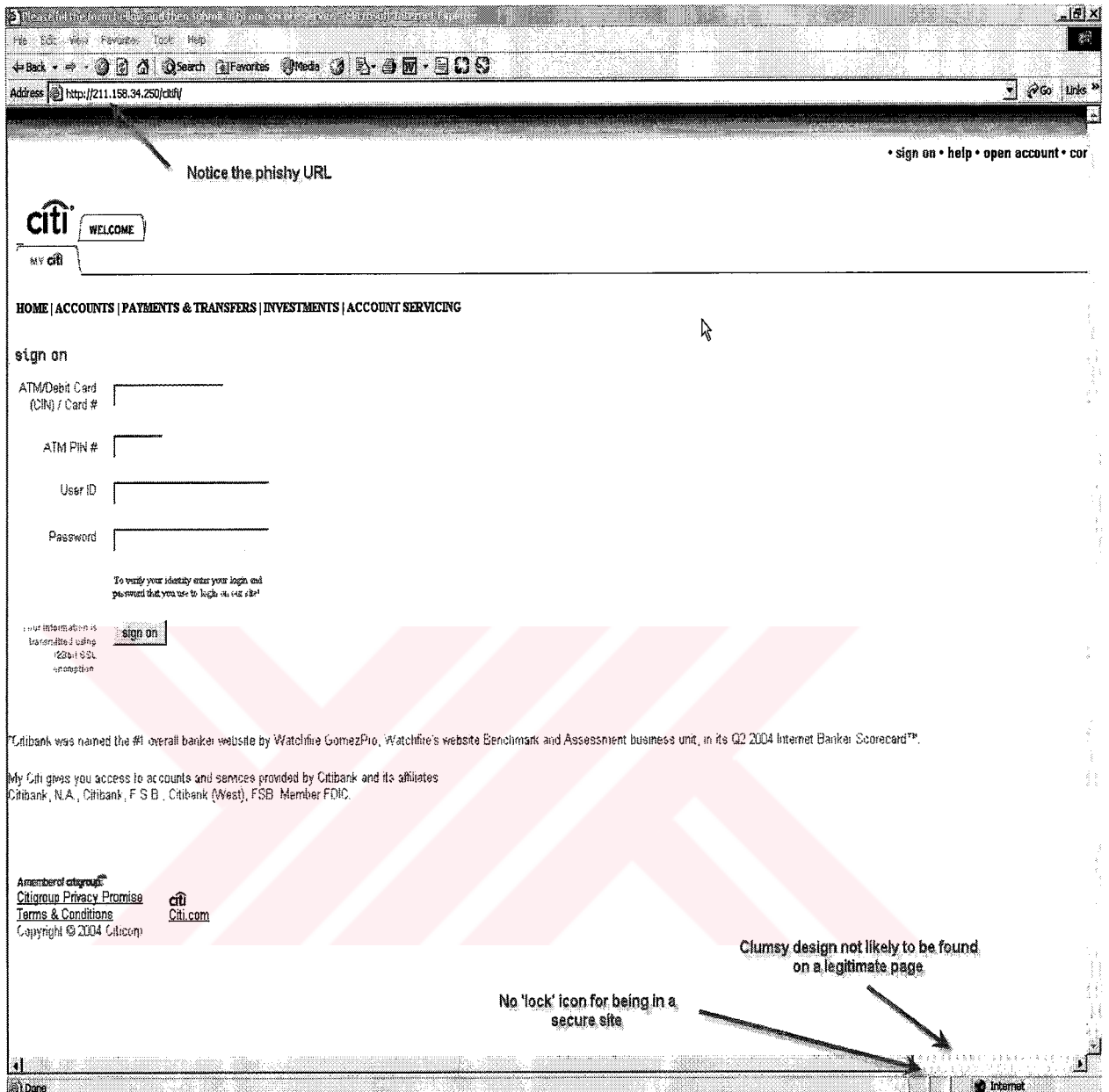


Figure 2.3: Fake web site which Citibank customers are redirected. (Antiphishing.org, 2005)

2.6. Liabilities of Parties

In this section we will identify the both of the parties' liabilities that involved in Internet banking transaction. We will divide the section into two listing the responsibilities of customers and banks. From one point of view; listed precautions make use of the Internet banking a very hard to use. On the other hand, it is well-accepted that the Internet is a

highly insecure public network. In order to protect the confidentiality of the personal data, banks multiplex the level of precautions from day to day.

It is important to emphasize that as authors of this study, we believe that a successful design involves addressing users' expectations and ensure the exact level of security is applied in order to protect customer's wealth. In the results and recommended systems division of this study, readers will be able to find some of the proposed solutions to address the security vs. usability issues.

2.6.1. General precaution steps taken by banks:

In general there are three key areas to safeguard customer account from any unauthorized access: (HSBC.com, 2005)

a. Privacy

Banks use industry standard encryption method within their Internet banking services such as secure sessions, encryption, and session time out.

a.1 Secure sessions

When user logs in to Internet Banking user is said to be in a secure session. User knows he is in a secure session if the URL address begins with https:// or a padlock symbol appears in the lower right hand corner of user's browser.

a.2 Encryption

Secure Sockets Layer (SSL) Encryption technology is used within user's Internet Banking session to encrypt personal information before it leaves the client computer in order to ensure no one else can read it. Encryption converts the data into an encoded form before it's sent over the Internet, thereby stopping unauthorised users from reading the information. Many of the banks make use of use 128-bit SSL Encryption , which is accepted as the industry standard level.

a.3 Session time-out

If users forget to log-off after banking online, or client computer remains inactive for a period of time during a session, then banking systems automatically log the user off and the connection between the customer computer and bank's system is terminated.

b. Technology

Banks updated their internal systems with the latest security patches, have their anti-virus software kept updated, and use firewalls to prevent unauthorized intrusion.

c. Identification privacy

c.1 Login id and dual password mechanisms

Online access to user account is only possible once the user has authenticated himself using the correct Internet banking ID and password. For this reason, it is vital that users do not share their password and do not use the same password for other services (e.g., Yahoo, Hotmail, etc.)

c.2 Automatic Lock-out

After a number of incorrect attempts to log in, online access is disabled to customer's account. To re-activate the account, customer himself should contact bank's usual helpdesk number.

2.6.2. General precaution steps taken by customers:

There is much that the customer should do to protect himself online. Some are simple, others may require a little time invested or serious help from someone else like an IT personnel.

In addition to precautions taken, banks direct their customers to follow these general "golden rules": (HSBC.com, 2005)

Customers should;

- Ensure the client operating system and Internet browser has the latest security updates and "patches".

- Use and regularly update anti-virus software
- Use a “personal firewall”
- Keep passwords private and not to use the same password for all their needs

Besides the general “golden rules”, banks warn their customers to keep their details and identity secure. Below is a list with a brief discussion on each item specifying what actions should be taken in order to prevent online banking incidents and to offer extra knowledge aiming raise on public education and awareness.

Customer should take care where to go online from

Customers should avoid using Internet Banking, or any other Internet services which require the use of critical passwords, at Internet Cafés, Libraries, and other public sites to avoid the risk of information being copied and abused after leaving.

Customer should get wise to online fraud

Customers should be aware that there are phoney web sites designed to trick him and collect all the personal information. Sometimes links to such web sites are contained in email messages purporting to come from financial institutions. Whenever possible, customer should try to use a known web address, or use a Favourite, to link to bank pages.

Customer should change passwords regularly

Customers should change passwords that may have been compromised.

Customer should disable the 'AutoComplete' function within the browser

On Internet Explorer, for example, the ‘AutoComplete’ function remembers data have been input, sometimes including passwords. Avoiding this functionality will help prevent others from seeing personal information.

Customer should keep his password secure

Users of online banks should try and create passwords that are unique, impersonal, not easy to guess, containing upper and lower case letters, numbers, and symbols.

When logging in

Customers should ensure to enter correct password(s) without the details being inadvertently disclosed to someone who may be looking over shoulder.

When logging off

Users of e-banks should always remember to log off from the Internet Banking session and close the browser when finished using online banking. This will clear all traces of visit to online bank from the PC's memory.

Customer should not use links to access bank's internet site

When using a browser, user must always enter the web address or use a Favourite. In order to avoid phishing, he should not use a link as this may take the customer to a phoney web site that may look exactly like online banking web site.

Avoiding phishing scams

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule customers should be careful about giving out personal financial information over the Internet. The Anti-Phishing Working Group has compiled a list of recommendations below to avoid becoming a victim of these scams: (antiphishing.org, 2005)

Online banking customers should;

- Be suspicious of any email with urgent requests for personal financial information
 - unless the email is digitally signed, one can't be sure it wasn't forged or 'spoofed'
 - phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
 - they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.
 - phisher emails are typically NOT personalized, while valid messages from real bank or e-commerce company generally are

- E-banking customer should not use the links in an email to get to any web page, if it is suspected that the message might not be authentic
 - instead, he should call the company on the telephone, or log onto the website directly by typing in the Web address in the browser
- Customer should avoid filling out forms in email messages that ask for personal financial information
 - customer should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Customer must always ensure that a secure website is being used when submitting credit card or other sensitive information via Web browser
 - to make sure using a secure Web server, customer might check the beginning of the Web address in the browsers address bar - it should be "https://" rather than just "http://"
- Customer should consider installing a Web browser tool bar to help protect from known phishing fraud websites
- Customer should regularly log into his online accounts
 - He should not leave it for as long as a month before checking each account
- Customer should regularly check the bank, credit and debit card statements to ensure that all transactions are legitimate
 - if anything is suspicious, customer should contact the bank and all card issuers
- Customer should ensure that the browser is up to date and security patches applied.

2.6.3. Banks' approach on security issues in technical and sociological views

2.6.3.1. Approach on security issues

In this section, we will try to identify the banks' technical and sociological attitudes on avoiding fraud and approach on the results regarding Internet Banking incidents.

Before we examine banks' commitment on fraud, we take a look at definition to the term "fraud": Fraud is defined as "the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another" (Granova and Eloff, 2004).

Many banks claim to provide secure online banking facilities but remain silent on the necessity and therefore obligation on the part of the client to ensure the security of his/her computer (whether it is in the form of updated antivirus or otherwise), and therefore they failed to fulfill their legal duty of care and as stated above (Granova and Eloff, 2004).

Despite some new innovative ideas, based on our research on Internet Banking services in our country and equivalent services throughout the world, we observe the same style of online banking behaviors. A long list of warnings and steps to be taken to be more secure are presented to customers' interest since warning users is mostly just a way for banks to avoid liability. In addition, depending upon the author of the site, basic technical security knowledge is presented to clients which may not be easily comprehended by many of the customers.

Educating customers on using online banking is not the only way of avoiding fraud. It is actually, a passive method for preventing fraud. Banks invest great amounts to improve the security culture about Internet banking. As human resources, there is, at most of them, an expert security staff, who decides and implements the improvements on online banking security. They follow the technology, innovate and present new ideas to management such as using hardware tokens, which are known as "one-time password generators".

Technology gives the ability to hackers to develop new methods for theft. When a new method of fraud threatens online customers, a new reaction is taken by the security staff. The security staff is forced to improve their methods, as the hackers' ways of stealing diversifies. So the result is the boundless precautions and dozens of pages to be read just to be able to bank on line. Unfortunately, the security staff, in general, is comprised of technical people who lack the sociological point of view. So as authors of this text, our opinion on banks' approach on security is that, it is out of balance.

2.6.3.2. Approach on liability issues

As banking through Internet became widespread, though a relatively new phenomenon, internet bank fraud affects millions of people every year. Criminal fraudsters are always looking for new ways to accrue financial gain at the expense of others, and the internet is often their chosen means of scams and deception.

As we have addressed, in part, the major banks don't want to divulge the amount of losses and incidents on online banking frauds, they're seeing for fear that it will damage their online banking businesses. Applying the definition of "fraud" to the facts at hand, it is clear that the bank may have misled the public in respect to the security of Internet banking, perhaps creating false sense of security pertaining to online banking transactions over the Internet. Lack of awareness campaigns warning clients of potential risks may further support the proposition that there was misrepresentation. The customer, at least, needs to be educated as to the nature of and risks associated with "passwords", "usernames" and "identity theft". Furthermore, clear default instructions as to what steps to take if either password or username are even suspected to have been stolen need to be issued (Granova and Eloff, 2004).

In our country, in response to Internet banking incidents, internet fraud lawsuits have been brought against the banks claiming the banks' disability on saving customers money. The main argument is that whether the responsibility of securing the client computer is only owned by the customer. Both in our country and around the world, we know that some of the banking fraud incidents have resulted by covering of the loss of the customer by the bank. Depending on the evidents and investigations, the suit may result in favour of defendant (bank) or the plaintiff (customer) or damage would partly be shared among the parties.

In the light of the above, regarding security context, it is clear that an organization will always carry the risk and be liable for damages or loss that result from an incident, unless it can prove that it has identified all potential risks and took "all reasonable steps to avoid the risk or at least limit the consequences."³² The client will only bear the risk if the organization can prove that he/she has disregarded explicit instructions it supplied to him/her for the purposes of reducing the risk (Granova and Eloff, 2004). In any case, it is clear that banking organizations are affected from the incident, since the loss of any customer means getting a bad reputation of the internet bank and possibly resulting shift of customers to its rivals.

The important lesson that should have been learnt here is that information security has to be given a high priority when providing online services to clients. Failing to do so could expose an organization to recurring, yet avoidable liabilities (Granova and Eloff, 2004).



3. EMPIRICAL STUDIES ON INTERNET BANKING

In parallel to rapid growth of Internet and digital revolution on Internet banking, there have been large amount of studies investigating online banking sector after Internet banking revolution. These studies have mainly focused on commercial banks' adoption of Internet banking as well as consumer adoption of using online banking, the role of the trust in the e-commerce environment, identifying the risks perceived by customers and banks along with many regional researches evaluating local Internet Banking services. The aim of this study is to explore the main arguments on the usage of Internet banking such as security and ease of use. These variables determine the level of consumer acceptance of the online bank, currently the major and future primary delivery channel for e-banking. In this section we supply the reader, literature information covering this framework.

3.1. Literature Review

One of the major points of research in this study is to identify primarily the trust expectations of the consumer and how banks behave towards these expectations. So we take a brief look at the "trust" notion in banking and how it is applied on Internet banking environment.

3.1.1. Banks and trust notion

A question we have in our mind is the people's necessity for banking. Why do people bank? One possible answer might be that; people bank, because of the convenience and security associated with holding money at financial institutions. The sense of security, in particular, was because of the assumed responsibility of the bank to verify the identity of the person who requested access to the account (Granova and Eloff, 2004). Thus we have a key point of focus: People feel in safe with their wealth when their wealth is saved by a "trustworthy" and legal association. People bank because these organizations, such as banks, fulfill their "trust needs".

So what actually is trust? Trust refers to the belief that the promise of another can be relied upon and that, in unforeseen circumstances, the other will act in a spirit of goodwill and in a benign fashion toward the trustor (Grazioli and Jarvenpaa, 2000). The customer's trust is, therefore, a confident belief in the supplier, the bank in this case (Crosby et al., 1990; Gefen, 2000). In many cases, the trust is based on previous interactions, although a

supplier's previous behavior cannot guarantee that he/ she will act as expected (Gefen, 2000). Customers' trust will increase if a supplier has behaved previously as expected.

The question of trust may be even more important in the Internet banking environment than it is in the offline banking environment (Ratnasingham, 1998). This is because the cultivation of trust is particularly important where uncertainty and risk are inherent and where contracts and warranties are often absent (Crosby et al., 1990; Grazioli and Jarvenpaa, 2000).

In the Internet environment, remote users in all corners of the world are allowed to access critical files on computers and information transferred via the Internet. Internet banking is, therefore, inherently risky from the viewpoint of security. Moreover, Internet banking is highly uncertain, because the parties involved in a transaction are not in the same place (Clarke, 1997). Customers cannot, therefore, observe a teller's behavior directly, and so cannot depend on things like physical proximity, handshakes, and body signals of the teller. Because of the importance of trust in Internet -banking, customer trust is a major factor influencing the growth of Internet banking.

In the following subsection, some studies on adoption of Internet banking around the world along with factors affecting customer preferences will be given.

3.1.2. Studies on adoption of Internet banking

According to reports published by the technology research firm, Gartner Inc., number of U.S. adults using online banking increased from about 6 million in early 1998 to about 27 million by early 2000, and this figure is expected to increase to about 75 million by 2005. According to a survey conducted by Jupiter Research Center, nearly one in every three online households used online banking in early 2001. The Internet revolution of the late 1990s has therefore greatly modified the ways in which consumers conduct business with their financial institutions (Khan, 2004).

Sathye, in 1999, proposed a model for Internet banking adoption, which argued that the intention of Internet banking in Australia is significantly influenced by variables of system in security, ease of use, awareness of service and its benefits, reasonable price, availability of infrastructure and resistance to change (Ramayah and Ling, 2003).

According to Polatoglu and Ekin, in 2001, as more and more banks in Turkey offer the Internet banking, the greater the awareness level among customers and therefore the higher will be Internet banking adoption (Ramayah and Ling, 2003).

Besides awareness, the services provided by the banks should be perceived to be innovative with high quality and user friendly to meet individual's expectation. Cooper, in 1997, reported that ease of use of innovative product or service as one of the three important characteristics for adoption from the customer's perspective. This is related to user friendliness and ease of navigation as well as simple instructions to use the service (Ramayah and Ling, 2003).

As for the perceived risk or security, O' Connell (1996) and Daniel, in 1999, discovered that security concern is an important affecting acceptance and adoption of new technology or innovation. Lockett and Littler, in 1997, reported that perceived risks of the innovation were inversely related to adoption in telephone based direct banking services (Ramayah and Ling, 2003).

According to Stewart, in 1999, the failure of Internet as a retail distribution channel has been attributed to the lack of trust customers have in the electronic channel and in the web merchants. Sathye, in 1999, confirmed security concern is a burning issue for financial transactions done over the Internet (Ramayah and Ling, 2003).

3.2. Statistical Studies

In order to emphasize customers' point of view to precautions taken for e-commerce environments, a research by the Association for Payment Clearing Services will be given as an example. One would expect that Internet Banking incidents, such as the phishing, datastreaming etc. would have adverse impacts from the perspective of potential online consumers. However, the statistics have provided an implicit indication that E-commerce is forging ahead in spite of these problems.

Indeed, survey data from the Association for Payment Clearing Services (APACS) in the latter half of 2003 indicated that 30 million UK adults used the Internet, with around 18 million having made online purchases during the 2003 (representing an increase of over

50% compared to 2002).¹⁰ With such a high proportion of users making online purchases, it would certainly appear that security is of little concern (Furnell, 2004).

In addition to APACS research, a 2003 survey by PaymentOne revealed security concerns to be far and away the prime reason preventing consumers from shopping online - accounting for 70% of responses (Furnell, 2004).

According to Steven Furnell, Network Research Group, School of Computing it would be naïve to assume that all of those using E-commerce services are doing so with complete confidence. For example, a survey conducted by Furnell's research group back in 2000 revealed that over 90% of users who shopped online were doing so in spite of having some form of security concern. There is little doubt that many consumers would give similar responses today, and the growth of E-commerce has had more to do with factors such as the cost and convenience than the perceived improvements in protection (Furnell, 2004).

There is evidence to suggest that the scale of the security problem is over-estimated. Although the latest findings suggest that fraud through E-commerce channels is increasing (estimated at £45m during 2003), the majority relates to the use of card details that have been fraudulently obtained in the real world – the proportion relating to data actually stolen from websites is described as “very low ” (Furnell, 2004).

In the following sections, examination of research problem, methodology, key findings and analysis of survey research that is subject to this study will be given.

4. RESEARCH QUESTION AND EMPIRICAL ANALYSIS

This chapter begins with discussion and formulations of the research problem that initiates this study. Subsequently the research methodology and hypothesis are discussed.

4.1. Research Problem

A bank needs to make its web site customercentric in order to attract people to I-banking (Williams, 2000). Performance measures enable banks to determine Internet customer satisfaction and identify the key drivers of customer retention so as to improve and maintain service level (Groenfeldt, 2000). According to Robinson (Robinson, 2000), banks must offer customers an "experience" – personalised and customised interactions that engage customers, capture their attention, and build an online relationship. In addition, customers express concern about the security of online transactions (Hamlet, 2000). Security practices should be established and enhanced, especially when banks offer transaction-oriented services.

While accumulating personal data, a bank should not underestimate privacy issues. Privacy and security are the most important issues that consumers have when dealing with I-banking (Stafford, 2001). These two concerns are the main barriers that constrain the uptake of I-banking. Consumers who have these concerns or less familiar with Internet technology need reassurance from their Internet banks. A secure and fully featured web site allows a bank to increase both revenue and customer loyalty (Chung and Paytner , 2002).

In the light of the above discussion, the research problem of this study may be formulated as follows:

Does internet's current security framework hinder the development of Internet Banking?

Aim of this study is to examine the Internet banking services in Turkey with respect to security considerations and ease of use. We probe for answers to the following questions:

- ✓ In what levels does the current framework of Internet Banking services encourage consumers?
- ✓ Is there a demand from the customers for a fundamental variation on these services?
- ✓ Having to continuously patchwork of currently available web browsers and custom Internet banking tools would cause paranoia?
- ✓ Does current security framework of Internet banking lead to an unnecessary anxiety over us, the online banking customers?
- ✓ How does it affect people that everyday a new precaution is introduced?

A part of this study is to research on the need for a single online identity that can be validated once, perhaps with a series of passwords and questions, or even some biometric measurement such as fingerprints.

4.2. Hypothesis

Specifically we hypothesized that:

1. Level of willingness of using Internet as a method for personal banking is high.
2. There is a potential seek and demand for using standard and serious interfaces for an environment which interconnects all of the banks that the customer actively using and registered.
3. Precautions applied by the Internet bank during the login period and the period which the user is logged on and making operations is excessive.

4.3. Methodology

After defining the problem and put the hypothesis, we explain the chosen method of collecting and analyzing the data. According to Miles and Hubberman (Miles and Hubberman, 1994) and with reference to Bernard, to describe is to make complicated things understandable by reducing them to their component parts. Descriptive study is therefore developing careful descriptions of different patterns that were expected during the exploratory stage. The purpose could be to develop generalizations and to explain these (Akhtar and Dong, 2004).

A questionnaire was designed to incorporate elements that allow customers of Internet Banking to rate the performance of their banks. It captures the evaluation of banks'

effectiveness and satisfaction with current online banking products. Customers were asked whether the currently taken steps of precautions are satisfactory with respect to security and ease of use.

4.4. Research Approach

More specifically, variables listed below were questioned which may be examined in the following three groups:

Under security considerations group we have four dependent variables:

1. Login into Banking website (supplying personal information such as place of birth and mother's maiden name)
2. Using virtual keyboard (supplying login information such as PIN and password through an optionally sliding interface which customer can use via mouse)
3. Transaction passwords (supplying extra password for authentication of customer to be used for certain operations such as EFT, payments...)
4. Session time-outs (if customer forgets to log-off after banking online, or customer's computer remains inactive for a period of time during a session, then the system automatically logs the customer off)

Under usability considerations group we have five dependent variables:

1. Login into Banking website (having to supply too many personal information in order to log in)
2. Using virtual keyboard (having to use a poorly designed login information entry interface)
3. Transaction passwords (a burdensome activity during operations and an extra data which the customer has to remember)
4. Session time-outs (hinders usability as it forces the customer to relogin the online bank after an auto logoff)

Under standardization group we have two dependent variables:

1. Using standard interfaces (if the customer has registered more than one online banking account through different banks, the willingness of using a standard input and output interface)

2. Willing to use a more formal, branding and advertise free, robust banking web interfaces.

Descriptive statistics are employed to gain insights the current level of security precautions and level of usability considerations impact the choice of using Internet banking as an alternative channel of personal banking.

We based our tests on the following:

1. Test whether current security considerations of internet banks are in adequate level of customer satisfaction.
2. Test whether current usability considerations of internet banks are in adequate level of customer satisfaction.
3. Test whether current standardization considerations of internet banks are in adequate level of customer satisfaction.
4. Test the level of correlation between security and usability variables vs. level of satisfaction of customers' security and usability perception.

A randomly chosen subset of advanced and graduate students at the Yeditepe University MBA program was thus selected to provide the information. Some of the Turkish electronic news group users consisting of internet users belonging to a dispersed set of sectors have been added to sampling frame as well. It has been paid attention that those actually answering the survey questions are not totally security professionals, nor the bankers, since evaluation of the performance of a web site which they have built would not actually make sense.

The survey respondents were reached via e-mail. First of all, the respondents were given information about the study and they were redirected to the web site which contains the questions. Survey data were collected into a database specifically designed for that purpose. The database was located in a web site on the Internet. Totally seventy eight of the respondents have filled the questionnaire; of those seventy five were usable data. The reader may find the full questionnaire (in Turkish) located at the web site <http://n.domainlx.com/afacang/default.html> . The reader could find those questions in the Appendix-A section as well (in both English and Turkish versions).

5. EMPIRICAL RESULTS

5.1. General Findings

Respondents were asked whether they hesitate using Internet banking as a service channel, given four different options to state their opinions. It was hypothesized that the level of willingness of using Internet as a method for personal banking is high. As shown in Table 5.1, 70.7 percent of respondents are comfortably using the Internet banking without a hesitation. On the other hand, this percent figure shows us; approximately one of every three customers is hesitating to do so.

Table 5.1 Respondents' willingness on using Internet banking

Hesitation Using Internet Banking	
	Percent checked
Using comfortably	70,7
Hesitate, using frequently.	17,3
Hesitate, rather not using.	8,0
Hesitate and not using	4,0
Total	100,0

In order to inquiry an overall view of customers on Internet Banking services that they are currently using, respondents were asked their thoughts on service satisfaction and especially security precautions. Table 5.2 shows the satisfaction and customers' point of view on general security precaution levels taken by their banks. According to these figures, currently used Internet Banking environments and implementation of security gives 46.7 percent of satisfactory to the respondents. One of every three respondents believes that there are hassling amount of precaution although they should not be left out.

Table 5.2 Overall view of Internet banking services

Overall View of Services	
	Percent checked
Feel secure and satisfied.	46,9
So much precaution, but must have	33,3
Generally dissatisfactory	16,0
Feel negative, must be changed	3,7
Total	100,0

5.2. Detailed Survey Results

5.2.1. Security considerations

Under security considerations section, survey includes the following topics and corresponding dependent variables to each of the inquiry which are shown in Table 5.3.

Table 5.3 Security based Internet banking services variables.

Security variables	
Overall Security	overalls
Security in login into bank mechanism	logins
Security in using virtual keyboard	keybs
Security in using a transaction password	txnpwds
Security in using a session timeout	logoffs

In order to investigate overall view on Internet Banking services questions below were asked to respondents. Figure 5.1 shows the rating by customers when general security is considered. This figure tells us a large percent in the sample, with a rate of 80 percent, believe the security implementations by banks are welcomed.

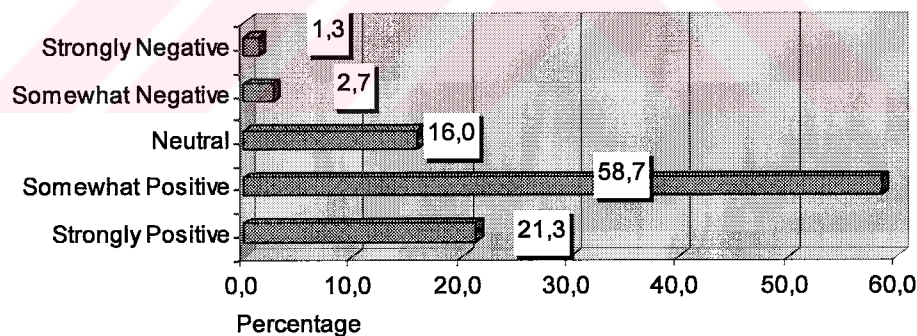


Figure 5.1 Overall view on security of Internet banking services

Results on other variables are listed below with a brief discussion about the outputs.

In order to learn customers' opinion on login mechanism security respondents were asked to choose from a range of options indicating their trust feeling about while entering an Internet bank. This data includes how the respondents react to the way their bank identify their customers in typical authentication session concerning security. The Internet banking

interface asks customer's private information such as Customer Id, a password, father's name, and phone number etc. to be able to let the customer get in. These multi-authentication steps were emphasized to the customer and let him/her to choose their feeling on the way they login to the bank.

The results are given in the Table 5.4. Results indicate a long portion of the respondents feel positive and in secure the way that they login to bank. It was hypothesized that, precautions applied by the Internet bank during the login period and the period which the user is logged on and making operations is excessive. The biggest portion (48.2 %) of the respondents, feel current authentication methods that the online banks apply are too much but must not be given up.

Table 5.4 Bank login mechanism security

Bank login mechanism	
	Percent checked
Feel secure, positive.	47,1
So much precaution, but must have	48,2
Uncomfortable or hinders usability.	2,4
Feel negative, must be changed.	2,4
Total	100,0

For further research on customers' adoption on security considerations, respondents were asked to choose from a range of options indicating their feeling about using a sliding or static virtual keyboard when login into an online bank. This data too, inquiries how respondents react to the way their bank identify their customers in typical authentication session concerning security. The results are given in the Table 5.5. Results indicate a long portion of the respondents feel secure when using a virtual keyboard through login to bank. Again a great portion (40.7 %), feel using a virtual keyboard is obstructive but also is a must.

Table 5.5 Virtual keyboard

Virtual Keyboard	
	Percent checked
Feel secure, positive.	44,4
So much precaution, but must have	40,7
Uncomfortable or hinders usability.	12,3
Feel negative, must be changed.	2,5
Total	100,0

Continuing to research on respondents' adoption on security considerations, they were asked to choose from a range of options indicating their feeling about having to type an extra transaction password in the middle of an operation. The Internet banking application asks the customer to type or enter their secondary password through a virtual keyboard, which is a common fashion, when the customer wants to perform an operation. This operation might be an outgoing EFT transaction as well as an order for a bill payment. Respondents are told about this situation and were asked their adoption on having to use transaction passwords through their operations concerning security.

The results are given in the Table 5.6. Results are similar to the previous variables. A long portion of the sample feels secure when using auxiliary transaction passwords. Again a great portion (39.5 %), feel this property is obstructive but also is a must. We should not underestimate 24.6 % of the respondents who feel negative and think that auxiliary transaction passwords results discomfort or hinders usability.

Table 5.6 Transaction password

Transaction Password	
	Percent checked
Feel secure, positive.	35,8
So much precaution, but must have	39,5
Uncomfortable or hinders usability.	16,0
Feel negative, must be changed.	8,6
Total	100,0

The last variable that targets research on respondents' adoption on security considerations, asks the respondents to choose from a range of options indicating their feeling about

session timeouts. If customer forgets to log-off after banking online, or computer remains inactive for a period of time during a session, then Internet Banking system automatically logs them off. Respondents are told about this situation and were asked their adoption on that issue concerning security. The results are given in the Table 5.7. With the 72.7 % rate, it is clear that this property gives the respondents an extra security feeling. We observe 16.9 % of the respondents who feel that auto logoff feature does not hinder their operations.

Table 5.7 Session timeout

Session Timeout	
	Percent checked
Feel secure, positive.	72,7
Does not hinder	16,9
Uncomfortable or hinders usability.	3,9
Feel negative, must be changed.	6,5
Total	100,0

5.2.2. Usability considerations

Under usability considerations section survey includes the following topics and corresponding dependent variables to each of the inquiry which are shown in Table 5.8.

Table 5.8 Usability based Internet banking services variables.

Usability variables	
Overall Usability	overallu
Usability in login into bank mechanism	loginu
Usability in using virtual keyboard	keybu
Usability in using a transaction password	txnpwdu
Usability in using a session timeout	logoffu

Respondents were asked to evaluate, in general, usability of Internet banking applications, given five different scales to state their opinions. Surprisingly, as shown in Figure 5.2, a large percent of respondents find using Internet Banking is easy to use. The rank above average is 92 percent which denotes the belief of their internet bank is easy to use.

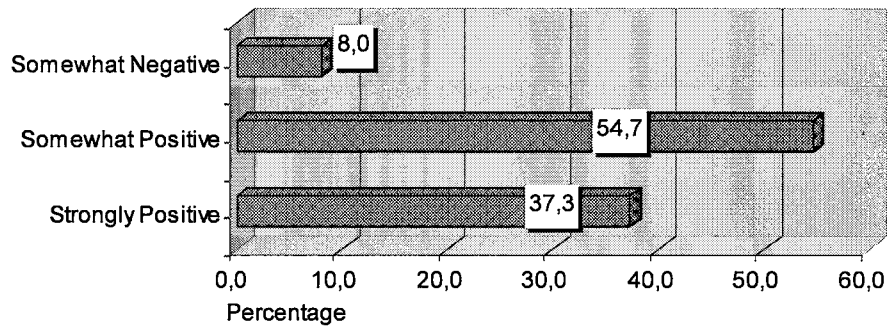


Figure 5.2 Overall view on usability of Internet banking services

Results on other variables are listed below with a brief discussion about the outputs:

In order to learn respondents' opinion on login mechanism usability they were asked to choose from a scale of options indicating their feeling about while entering an Internet bank. This data includes how the respondents react to the way their bank identify their customers in typical authentication session concerning usability. We try to learn how multi-authentication steps, such as supplying customer id, password, father's name, phone numbers, etc. affect the respondent on the way they login to the bank. The results are shown in Figure 5.3. Results show that a long portion of the respondents find the way that they login to bank is easy to use.

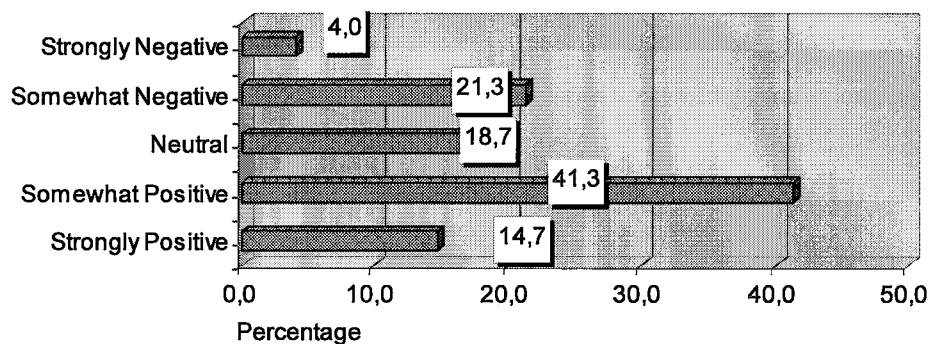


Figure 5.3 Bank login mechanism usability

For further research on respondents' adoption on usability considerations, they were asked to choose from a five-scale option list indicating their feeling about using a sliding or static virtual keyboard when login into an online bank concerning usability. The results are given

in the Figure 5.4. We observe a more homogenous distribution among customers who feel positive about using a virtual keyboard and who do not.

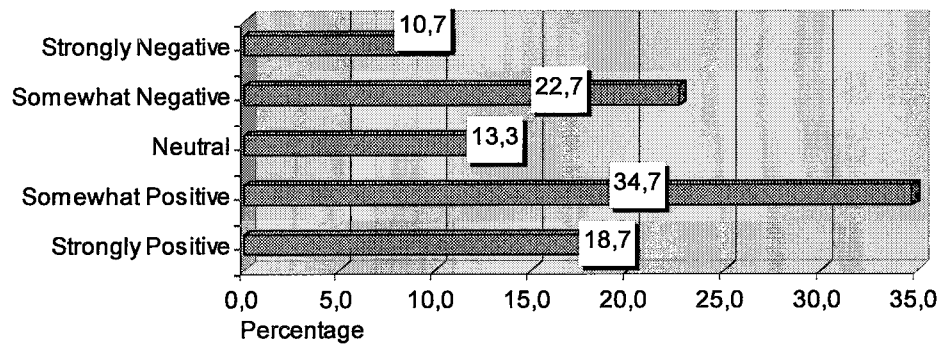


Figure 5.4 Virtual keyboard usability

Continuing to research on respondents' adoption on usability considerations, they were asked to choose from a five-scale option list indicating their feeling about having to type an extra transaction password in the middle of an operation. Respondents are told given information about transaction passwords and were asked their adoption on having to use transaction passwords through their operations concerning usability. The results are given in the Figure 5.5. A homogeneous distribution exists (both one third of the sample) among the respondents who feel comfort when using an auxiliary transaction password and those who do not.

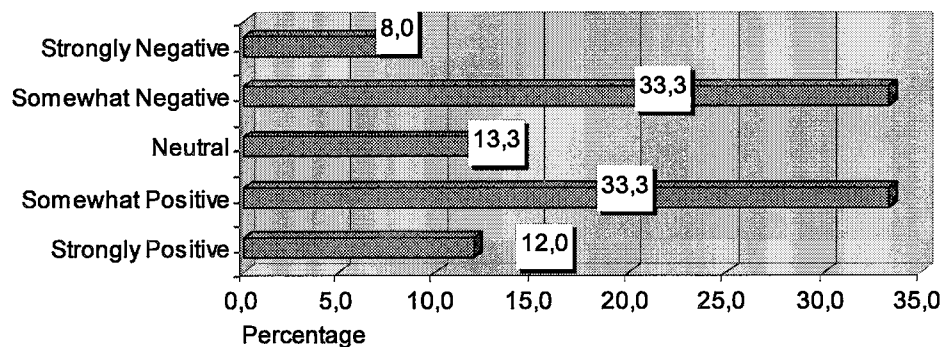


Figure 5.5 Transaction password usability

The last variable targeting research on customers' adoption on usability considerations of their Internet Bank, asks the respondents to choose from a five-scale option list indicating their feeling about session timeouts. Respondents are told about auto logoff feature and were asked their adoption on that issue concerning usability. The results are given in the Figure 5.6. These figures show us that, with 65.3 % (above average of respondents) rating, auto logoff feature gives the respondents an extra feeling of comfort.

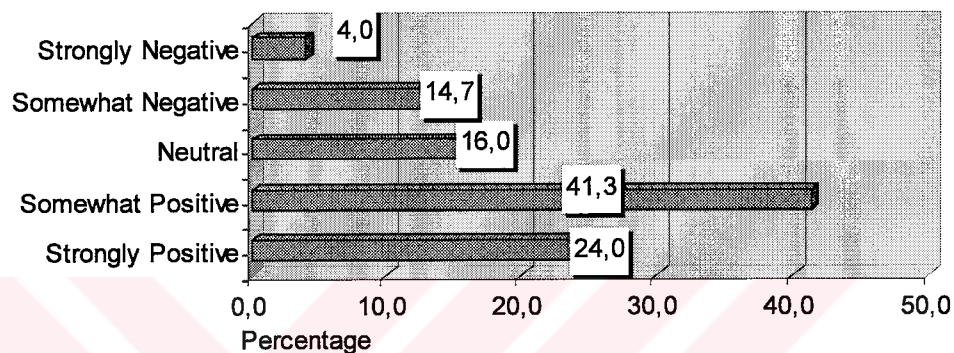


Figure 5.6 Session timeout usability

5.2.3. Standardization considerations

In this section, respondents were asked how they find advertising pop-ups, inserts and notification pages which make promise of promotions. In addition, survey inquiries respondents' opinion on using one formal common Internet Banking interface which interconnects more than one online bank site in a single application. To achieve this, respondents were asked in what level usable they find using different interfaces for the same kind of operations in the case they use different online banks. Under standardization considerations section, survey includes the following topics and corresponding dependent variables to each of the inquiry which are given in Table 5.9.

Table 5.9 Standardization based Internet banking services variables.

Standardization variables	
Advertising preference	advertis
Usability in unstandard interfaces	standaru

Results on these variables in this category are listed below with a brief discussion about the outputs:

In order to learn respondents' opinion on advertising pop-ups, inserts and notification pages that make promise of promotions, they were asked through four different options. The results are shown in Figure 5.6. Results show that the long portion of the respondents finds the advertisings to be obstructive and indicates that to be changed. Only 14.8% of the respondents find it useful.

Table 5.10 Respondents' willingness on facing advertising and inserts in an Internet banking environment.

Advertisers	
	Percent checked
Useful	14,8
Does not hinder	38,3
Uncomfortable and obstructive	40,7
Feel negative, must be changed.	6,2
Total	100,0

It was hypothesized that, there is a potential seek and demand for using standard and serious interfaces for an environment which interconnects all of the banks that the customer actively using and registered. In Figure 5.7, results show that the 36.0 percent of the respondents find somewhat positive using different and unstandard interfaces in the case they use more than one banking interface. That was a surprising figure however, as shown in Table 5.11, approximately one third of the respondents think that it will be beneficial to have a standard interface interconnecting all the banks that respondents are currently registered.

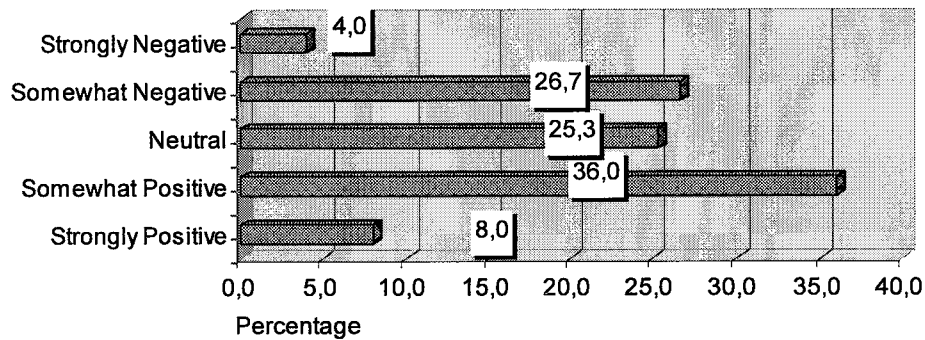


Figure 5.7 Using unstandard interfaces in scalar
 Table 5.11 Respondents' opinion on using same interface for all the banks they are registered.

Standard interfaces	
	Percent checked
Rather trying different styles	10,4
Does not hinder	54,5
Uncomfortable and obstructive	28,6
Feel negative, must be changed.	6,5
Total	100,0

5.3. Data Consistency and Reliability

The Bivariate Correlations used to compute the pairwise associations for a set of variables and display the results in a matrix which is useful for determining the strength and direction of the association between two scale or ordinal (such as the five-scaled option list) variables.

Security Section

The correlations reported in the tables are all above zero. According to Pearson's correlation coefficient, the association between Overall Security and Login mechanism is fairly strong at the 0.05 level. Also the association between Overall Security and Session Timeout is strong at the 0.05 level. This means that people's approach on login mechanism and session timeout is statistically consistent with overall security understanding. Statistical figures are shown in Table 5.12.

Table 5.12 Correlation table concerning security

Correlations			
		Overall Security	Login mechanism
Overall Security	Pearson Correlation	1	0,296 *
	Sig. (2-tailed)		0,010
	N	75	75
Login mechanism	Pearson Correlation	0,296 *	1
	Sig. (2-tailed)	0,010	
	N	75	75
		Overall Security	Virtual Keyboard
Overall Security	Pearson Correlation	1	0,077
	Sig. (2-tailed)		0,509
	N	75	75
Virtual Keyboard	Pearson Correlation	0,077	1
	Sig. (2-tailed)	0,509	
	N	75	75
		Overall Security	Txn. Password
Overall Security	Pearson Correlation	1	0,119
	Sig. (2-tailed)		0,310
	N	75	75
Txn. Password	Pearson Correlation	0,119	1
	Sig. (2-tailed)	0,310	
	N	75	75
		Overall Security	Session Timeout
Overall Security	Pearson Correlation	1	0,256 *
	Sig. (2-tailed)		0,026
	N	75	75
Session Timeout	Pearson Correlation	0,256 *	1
	Sig. (2-tailed)	0,026	
	N	75	75

***. Correlation is significant at the 0.05 level (2-tailed).**

Usability Section

The correlations reported in the usability section tables are also all above zero. According to Pearson's correlation coefficient, the association between Overall Usability and using Virtual Keyboard is fairly strong at the 0.05 level. This means that people's approach on using a virtual keyboard is statistically consistent with overall usability understanding. Statistical figures are shown in Table 5.13.

Table 5.13 Correlation table concerning usability

Correlations			
		Overall Usability	Login mechanism
Overall Usability	Pearson Correlation	1	0,127
	Sig. (2-tailed)		0,279
	N	75	75
Login mechanism	Pearson Correlation	0,127	1
	Sig. (2-tailed)	0,279	
	N	75	75
		Overall Usability	Virtual Keyboard
Overall Usability	Pearson Correlation	1	0,238 *
	Sig. (2-tailed)		0,040
	N	75	75
Virtual Keyboard	Pearson Correlation	0,238 *	1
	Sig. (2-tailed)	0,040	
	N	75	75
		Overall Usability	Txn. Password
Overall Usability	Pearson Correlation	1	0,106
	Sig. (2-tailed)		0,366
	N	75	75
Txn. Password	Pearson Correlation	0,106	1
	Sig. (2-tailed)	0,366	
	N	75	75
		Overall Usability	Session Timeout
Overall Usability	Pearson Correlation	1	0,214
	Sig. (2-tailed)		0,066
	N	75	75
Session Timeout	Pearson Correlation	0,214	1
	Sig. (2-tailed)	0,066	
	N	75	75

***. Correlation is significant at the 0.05 level (2-tailed).**

6. DISCUSSION AND CONCLUSION

As technology evolves, online banking became an important subject that came into our daily life in the late 90's. The technology permits growing of capabilities which let the users easily perform time consuming banking activities with a single click. Users enjoy having this financial freedom available 7 / 24. Bankers are glad since a new delivery channel was invented without great sacrifices. However in parallel to rapid development, it did not take a long time for both of the actors to begin paying for freedom. What is meant for payment is not the operational fees and any innovation expenses. The people should pay for their trust expectations. That resembles to make a payment to a brick and mortar bank to let your jewels be kept in a safer place rather than your own case at home.

Security is all about risks and associated costs. One cannot achieve perfect security, so at some moment in time, despite all security measures something will always go wrong. Even the best solution relies on the assumption that the end-point of the systems is trusted. Concerning the client, this means that the electronic banking system should run within a trusted environment that has not been tampered with. The user must be responsible for maintaining his computing environment and keeping it trustworthy. The users must also protect the secret elements that are used in the system such as passwords, private keys and tokens. While inherently more secure environments will considerably improve the overall security of an online banking system, education of users has an even more significant impact on its overall security (Claessens et al., 2002)

In order to emphasize the scope and the education factor as a key matter for the problem, we refer to Brian McKenna (McKenna, 2004). A senior banking source in the City of London confirmed to Infosecurity Today, that the phishing problem, while “not brand new” is a “big concern that can probably only really be solved by business engaging the ISPs — who do not always give the degree of attention they could to the content that they host. It's an industry-wide problem, really, and is about the policing and governance of the internet, which is an inescapably international matter. At root, this is a social engineering problem. Customer education and awareness is the key (McKenna, 2004).

Those looking for some greater reassurance can at least look for signs of the vendor's commitment to security in other ways. A baseline would be to see some evidence of the site having a credible privacy and security policy –which at least indicates some recognition of the issue being a concern for customers. Online banking sites have utilized a more substantial challenge-response process, requiring the user to enter personal information such as date of birth along with randomly selected digits from a secret security number (thus reducing the possibility of someone capturing the information – e.g. via a keystroke logging worm – and then being able to repeat it for a subsequent successful login). The downside, of course, is that this process may be perceived as too time-consuming or complex by potential customers (Furnell, 2004).

This study has aimed on researching people's understanding of online banking services in Turkey with respect to security and usability issues. According to a similar research established by APACS it is stated that, despite their apparent concerns about security, most users will actually know very little about it –and indeed may find it difficult to define their requirement much more specifically than saying that their personal and financial details need to be protected. As such, provided that they have been explicitly authenticated, and are then assured that the transit of sensitive data is protected from prying eyes, the majority of users will feel that there is little else to worry about (Furnell, 2004).

Our findings are not very different from those statements of APACS. The results of our research indicates that, when security is the concern, a large population feels secure and satisfied from the overall service point of view. This idea is also supported by the various security variables which are applied one by one (virtual keyboards, having to give a bunch of personal details when login to bank etc.)

One other key point that our research has identified is that; people are likely to adapt to an online banking environment which is not easy to use but offering a wide range of security options. This is due to the fright of being a victim of an online banking incident. Customers are likely to put up with all the precautions despite all the usability expectations.

People in Turkey are not enough introduced with single sign on financial institutions which keep track of every property of a customer. So we believe that opinion of using a single interface for unified online banking is not evaluated well by the participators. We also

believe that a transactional based, single sign on unified online banking environment supported by hardware tokens such as smart cards would highly be welcomed by online customers.

6.1. Recommendations for Further Research

Since it is impossible that this work would have solved all the problems associated with the area of study, we provide the recommendations for further research section. The section includes suggestions about how the work can be improved as well as discussions about possible solutions from an author point of view. We should state that further researches mentioned below will likely to be conducted by both the technical and business entities together.

6.1.1. E-signature

A serious and scientific approach needs to be handled, perhaps with the leadership of the law makers. Beginning by the year 2005, both public and private sector in Turkey are introduced with the electronic signature (e-signature) technologies. This technology, which permits to make it possible to identify the originator and the recipient of any electronic information, will have to be used to lessen fraud. Basically, e-signature uses Public Key Cryptography infrastructure which is based on communication between two parties over secure channels such as SSL.

Utilizing e-signature might be a part of an integrated Internet banking application and hence provide a secure and trustworthy mechanism for online banking. From a security point of view, Public Key Cryptography is the best solution and the only non-repudiation one. However in this solution the clients' (the customer) private key (the Cryptographic element which identifies the customer) is in practice often stored in software and only protected by a password. Smart cards and readers constitute a solution that still seems to be too expensive or complicated.

6.1.2. Internet browser changes

According to John Pescatore, vice president and research fellow in Gartner Research, there is a need to see the basic Internet infrastructure support a "Caller ID" function to give consumers at least the equivalent defense of what they have on telephone solicitations.

This would need innovation at the browser end, which has been sorely lacking for the past several years (McKenna, 2004).

This solution argues that currently used Internet banking infrastructure is based on client-server architecture and client side is the internet browser such as MS Internet Explorer. The 'Caller ID'-like function could be implemented on the browser fairly easily. But that would require Microsoft to change IE, and it's not been too innovative there — because of lack of competition (McKenna, 2004).

6.1.3. SMS issues

The widespread adoption of mobile phones and SMS text messaging offers an alternative channel between the user and the bank. Whilst it is neither authenticated nor encrypted, it is in practice infeasible for an attacker to compromise both the SSL/TLS channel and the SMS channel to a particular user simultaneously. Several vendors already offer the option of one-time-password distribution via SMS as a cost-effective alternative to password-generating tokens. However, this independent channel also offers a way around the man-in-the-middle. To achieve this, it is necessary to move away from session-based security (based on a secure log-in), to message-based security (based on explicit authentication of individual transactions) (Tuliani, 2004).

In this scenario, the user would log on using his username and password, exactly as he does today. For each transaction entered, a summary would be returned to the user together with a one-time-password, in the form of an SMS. For example, 'Pay £50 to British Gas a/c 12345? Confirm: ADJPEQ'. Any tampering with the transaction details would be evident at this point. Assuming all is correct, the user enters the one-time-password into his PC to confirm the transaction (Tuliani, 2004).

Customized level of security can be achieved through SMS. A SMS agent is setup and every action that is preferred to be monitored such as login to bank, performing an EFT transaction through internet will be logged and alerted to customer's phone and mailbox through SMS gateway. Any critical action which is optional to customer will be confirmed by the customer.

6.1.4. Single sign-on features

Increased complexity in the digital identities of the users and the growing complexity of the business scenarios (related to both security and usability) will require the right identity management solutions to allow for the use of the services that hides that complexity from the end user, while preserving the user's privacy and security. Due to this foreseen complexity a necessity to create a networked world in which customers and banks could more easily interact with one another while respecting the privacy and security of shared identity information.

In this point, we mention the “Single Sign On” feature which means that user can access different services or service providers without authenticating at each one. These service providers range from traditional banks to any financial institute such as online brokerage corporations and insurance agencies. Simply, identity management functions such as authentication to each of these services are handled by one trusted operator. The system enables customers of all banks to receive a unified view of their activities in all accounts, at all banks. Single sign on is a way of getting users to aggregate their accounts at a single institution.

Although not well-known in Turkey, ability to access all bank accounts with a single authentication step is a widely used alternative to traditional banking online. Single sign on to all banks and having a unified view of banking statements from all banks through a single interface has many advantages which are given below in brief:

- Concentrates the customer’s banking information on a single platform, enabling him to compare the terms in his various accounts with regard to both deposits and loans.
- Enables the customer to monitor activity in his checking accounts, securities portfolios, credit cards, etc.
- Enables customers to monitor unusual activities in all bank accounts. This permits an independent analysis of every account transaction according to criteria entered by the customer.
- The customer receives financial "tips" based on his personal data - volume of activity, account status, etc.

- Confidentiality - The data is encrypted in the customer's personal computer, and he alone enjoys direct and exclusive access to it. (Fibi.co.il, 2005).

A successful implementation reference of such an environment is Money which is a comprehensive money management system from Microsoft. It makes it easier to manage where customers' money goes and how it grows; giving everything customers need to accomplish their core financial tasks.

A common banking environment might be setup for use in online banking services which permits single sign on feature. This system might involve currently used online services presented by banks as well as new features such as creating a monthly budget, analyzing cash flow by creating reports and graphs, tracking net worth, give the ability to customers to optimize their investments and even create a long-term plan. This environment might include the use of digital certificates that permits the use of e-signature, embedded in a smart card. It should be noted that a great effort needs to be made for Turkish banks to make their Internet banking services are compatible with such an environment.

APPENDICES

APPENDIX A: QUESTIONNAIRE – TURKISH VERSION

Genel Değerlendirme (1/8)

İnternet bankacılığını kullanmaya çekiniyor musunuz?	
<input type="checkbox"/>	Hayır, rahatlıkla kullanıyorum.
<input type="checkbox"/>	Çekiniyorum fakat sıklıkla kullanıyorum.
<input type="checkbox"/>	Çekiniyorum, gerekmedikçe kullanmıyorum.
<input type="checkbox"/>	Çekiniyorum ve kullanmıyorum.

Genel Değerlendirme (2/8)

Bankanızın internet bankacılığı hizmetleri ve bu konudaki güvenlik tedbirleri hakkında düşünceniz? (Birden fazla seçenek seçilebilir.)					
<input type="checkbox"/>	Güvenilir ve tatminkar buluyorum.				
<input type="checkbox"/>	Güvenlik tedbirleri fazla, fakat gerekli.				
<input type="checkbox"/>	Genel olarak tatmin edici değil.				
<input type="checkbox"/>	Olumsuz buluyorum, sistem yenilenmeli.				
	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Güvenlik Açısından	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kullanışlılık Açısından	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Reklam ve Promosyonlar (3/8)

İnternet bankacılığı sitelerinde reklam, branding ve promosyon vadeden işlemler, ekranlar, insertler hakkında ne düşünüyorsunuz? (Birden fazla seçenek seçilebilir.)	
<input type="checkbox"/>	İşime yarıyor, olumlu buluyorum.
<input type="checkbox"/>	Bu durum beni engellemiyor.
<input type="checkbox"/>	Sıkıcı ve engelleyici.
<input type="checkbox"/>	Sistem yenilenmeli, olumsuz buluyorum.

Banka İşlemleri (4/8)

Birden fazla banka kullanıyorsanız aynı işlem çeşidi için farklı tarzda menüler, farklı girdi ve çıktı (makbuz gibi) arayüzleri , farklı ekranları kullanma konusundaki düşünceleriniz? Yani; bir bankada yapmak istediğiniz bir işlemi diğer bankada farklı menü opsiyonlarını kullanarak yapmak zorunda kalmanız durumu. (Birden fazla seçenek seçilebilir.)

<input type="checkbox"/>	Her banka için farklı arayüzler olmalı.				
<input type="checkbox"/>	Farklılık beni engellemiyor, rahatsız etmiyor.				
<input type="checkbox"/>	Farklılık rahatsız ediyor.				
<input type="checkbox"/>	Bence bu değiştirilmeli, olumsuz buluyorum.				
	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Kullanışlılık Açısından	☺	☺	☺	☺	☺

Bankaya Güvenli Giriş (5/8)

Banka sitesine, müşteri numarası, parola, şifre, özel tanımlayıcı bilgilerinizi verme işlemleri gibi bir çok adımdan geçerek giriş yapma hakkında ne düşünüyorsunuz? (Birden fazla seçenek seçilebilir.)

<input type="checkbox"/>	Güvenimi artırıyor, olumlu buluyorum.				
<input type="checkbox"/>	İşi uzatıyor, ama gerekli.				
<input type="checkbox"/>	Rahatsız edici veya kolay kullanımı engelliyor.				
<input type="checkbox"/>	Bence bu değiştirilmeli, olumsuz buluyorum.				
	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Güvenlik Açısından	☺	☺	☺	☺	☺
Kullanışlılık Açısından	☺	☺	☺	☺	☺

Bankaya Güvenli Giriş (6/8)

Parola veya şifre girişi sırasında şifre klavyesinin kayması, dinamik olması ve sadece sanal klavyeden giriş yapılabilmesi hakkında ne düşünüyorsunuz? (Birden fazla seçenek seçilebilir.)

Güvenimi artırıyor, olumlu buluyorum.

İşi uzatıyor, ama gerekli.

Rahatsız edici veya kolay kullanımı engelliyor.

Bence bu değiştirilmeli, olumsuz buluyorum.

	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Güvenlik Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kullanışlılık Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Banka İşlemleri (7/8)

Bazı işlemlerde sizden ayrıca bir onay şifresi istenmesi sizi nasıl etkiliyor? (Örneğin Havale işlemi sırasında parola veya sisteme giriş şifrenizden farklı bir işlem şifresi sorulabiliyor.) (Birden fazla seçenek seçilebilir.)

Güvenimi artırıyor, olumlu buluyorum.

İşi uzatıyor, ama gerekli.

Gereksiz ve engelleyici.

Bence bu değiştirilmeli, olumsuz buluyorum.

	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Güvenlik Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kullanışlılık Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

İşlem Sonlandırma (8/8)

Bankanıza girdikten bir süre sonra, belli süre işlem yapmadığımızda sistemin sizi atması hakkında düşünceleriniz? (Birden fazla seçenek seçilebilir.)					
<input type="checkbox"/>	Güvenimi artırıyor, olumlu buluyorum.				
<input type="checkbox"/>	Bu durum beni engellemiyor.				
<input type="checkbox"/>	Gereksiz ve engelleyici.				
<input type="checkbox"/>	Bence bu değiştirilmeli, olumsuz buluyorum.				
	Çok Olumsuz	Olumsuz	Kararsız	Olumlu	Çok Olumlu
Güvenlik Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kullanışlılık Açısından	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



APPENDIX B: QUESTIONNAIRE – ENGLISH VERSION

Overall View (1/8)

Do you hesitate using Internet banking?	
<input type="checkbox"/>	No, using comfortably.
<input type="checkbox"/>	Hesitate, but using frequently..
<input type="checkbox"/>	Hesitate, and rather not using..
<input type="checkbox"/>	Hesitate and not ever using.

Overall View (2/8)

Your view about your Internet Banking services and about security precautions taken by bank? (More than one choice can be selected.)					
<input type="checkbox"/>	Feel secure and satisfied.				
<input type="checkbox"/>	So much precaution, but must have.				
<input type="checkbox"/>	Generally dissatisfactory.				
<input type="checkbox"/>	Feel negative, must be changed.				
	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Security Viewpoint	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Usability Viewpoint	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Advertising and Promotions (3/8)

Your view about advertising and promotion figures appearing on the Internet Banking sites? (More than one choice can be selected.)	
<input type="checkbox"/>	Useful.
<input type="checkbox"/>	Does not hinder.
<input type="checkbox"/>	Uncomfortable and obstructive.
<input type="checkbox"/>	Feel negative, must be changed..

Banking Operations (4/8)

Your view about using having to use different interfaces for input and output for the same style of operation when you use more than one Internet banks. (More than one choice can be selected.)

<input type="checkbox"/>	Rather trying different styles.				
<input type="checkbox"/>	Does not hinder.				
<input type="checkbox"/>	Uncomfortable and obstructive.				
<input type="checkbox"/>	Feel negative, must be changed.				
	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Usability Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Secure Login to Bank (5/8)

Your view about, when login to bank, having to pass through multiple authentication steps such as supplying customer ID, password, ATM key etc.? (More than one choice can be selected.)

<input type="checkbox"/>	Feel secure, positive.				
<input type="checkbox"/>	So much precaution, but must have.				
<input type="checkbox"/>	Uncomfortable or hinders usability.				
<input type="checkbox"/>	Feel negative, must be changed.				
	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Security Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Usability Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Secure Login to Bank (6/8)

Your view about, when login to bank, having to use a sliding virtual keyboard and when it is the only way that you can log in? (More than one choice can be selected.)					
<input type="checkbox"/>	Feel secure, positive.				
<input type="checkbox"/>	So much precaution, but must have.				
<input type="checkbox"/>	Uncomfortable or hinders usability.				
<input type="checkbox"/>	Feel negative, must be changed.				
	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Security Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Usability Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Banking Operations (7/8)

Your view about, having to supply an additional confirmation password, especially when performing operations containing an outgoing money flow?(More than one choice can be selected.)					
<input type="checkbox"/>	Feel secure, positive.				
<input type="checkbox"/>	So much precaution, but must have.				
<input type="checkbox"/>	Uncomfortable or hinders usability.				
<input type="checkbox"/>	Feel negative, must be changed.				
	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Security Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Usability Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Auto Logoff (8/8)

Your view about, auto logoff of the system when you have not performed a transaction for some short time period? (More than one choice can be selected.)

- Useful and trustworthy.
- Does not hinder.
- Uncomfortable and obstructive.
- Feel negative, must be changed..

	Strongly Negative	Somewhat Negative	Neutral	Somewhat Positive	Strongly Positive
Security Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Usability Viewpoint	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



REFERENCES

- Antiphishing.org, "Phishing Home Page". Available on site <http://www.antiphishing.org/>, accessed on Jul, 13 2005 14:00 PM.
- Akhtar, R., Dong Y., 2004, "Internet Banking: A Comparative Study from Sweden and China", Department of Business Administration and Social Sciences, Division of Industrial Marketing and e-Commerce, Lulea University of Technology.
- Bankersonline.com, "What is the definition of e-banking?". Available on site http://www.bankersonline.com/technology/gurus_tech081803d.html, accessed on Jul, 13 2005 14:00 PM.
- Bankrate.com, "What is online banking?". Available on site <http://www.bankrate.com/brm/news/emoney/technoguide2004/ebanking-intro1.asp>, accessed on Jul, 13 2005 14:10 PM.
- Barth, J. R, Brumbaugh Jr, R. D, 1995, "Your Home Computer Will Soon be Your Banker and Broker", The Wall Street Journal, A15
- Chung, W., Paynter, J., 2002, "An Evaluation of Internet Banking in New Zealand", Department of Management Science and Information Systems School of Business, The University of Auckland, Private Bag 92019, Auckland, New Zealand.
- Claessens, J., Dem, V., Cock, D.D., Preneel, B., Vandewalle, J., 2002, "On the Security of Today's Online Electronic Banking Systems", Computers & Security 21(3):pp 257-269.
- Clark, T.H., Lee, H.G., 1998, "Security First Network Bank: A Case Study of an Internet Pioneer", Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong.
- Clarke, R., 1997, "Promises and threats in electronic commerce". Available on site www.anu.edu.au/people/Roger.Clarke/EC/Quantum.html, accessed on Jul, 17 2005 14:20 PM.
- Cooper, R.G., 1997, "Examining some myths about new product winners, in Katz, R. (Ed)", The Human Side of Managing Technological Innovation, Oxford, pp 550-560.
- Crosby, L.A., Evans, K.R., 1990, Cowles, D., "Relationship quality in services selling: an interpersonal influence perspective", Journal of Marketing, 54 (3): pp 68-81.
- Daniel, E., 1999, "Provision of electronic banking in the UK and Republic of Ireland", International Journal of Bank Marketing, 17(2): pp 72-82.
- Fibi.co.il, "A Unified View of Your Banking Statements From All Banks". Available on site http://www.fibi.co.il/fibi/site/en/fibi.asp?pi=1408&doc_id=2692, accessed on Jul, 13 2005 14:20 PM.

Ffiec.gov, "E-Banking, Introduction". Available on site http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_00_intro_def.html, accessed on Jul, 13 2005 14:25 PM.

Furnell, S., 2004, "E-commerce security: a question of trust", Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, United Kingdom.

Gefen, D., 2000, "E-commerce: the role of familiarity and trust", *Omega*, 28(6): pp 725–737.

Granova, A., Eloff, JHP., 2004, "Online banking and identity theft: who carries the risk?", Information and Computer Security Architectures (ICSA) Research Laboratory, Department of Computer Science, University of Pretoria, South Africa.

Grazioli, S., Jarvenpaa, S.L., 2000, "Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet", *IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems and Humans*, 30(4): pp 395–410.

Groenfeldt, T., 2000, "Room to improve", *United States Banker*, 110(9): pp 54-60.

Hamlet, C., 2000, "Community banks go online", *ABA Banking Journal*, 92(3): pp 61-64.

Hinde, S., 2004, "All you need to be a phisherman is patience and a worm", Group Information Protection Manager, BUPANet

HSBC.com, "Online Security", Available on site <http://www.hsbc.com/hsbc/security>, accessed on Jul, 18 2005 15:20 PM.

Khan, B.S., 2004, "Consumer Adoption of Online Banking: Does Distance Matter?"

Lockett, A., Littler, D., 1997, "The Adoption of Direct Banking Services", *Journal of Marketing Management*, 13: pp 791-811.

McKenna, B., 2004, "Banks put customers on phishing alert. But whose pigeon is it?"

Miles, M.B., Hubberman, A.M., 1994, "Qualitative Data Analysis", Sage Publications Inc, (2), Thousand Oaks, California.

Mxes.org, "Tracking the reputation of Mail eXchangers , Glossary". Available on site <http://www.mxes.org/glossary/>, accessed on Jul, 13 2005 10:20 AM.

O'Connel, B., 1996, "Australian Banking on the Internet – Fact or Fiction?", *The Australian Banker*, pp 212-214.

Polatoglu, V.N., Ekin, S., 2001, "An Empirical Investigation of The Turkish Consumers' Acceptance Of Internet Banking Services", *International Journal of Bank Marketing*, 19 (4): pp 156-165.

- Ramayah, T., Ling, K.P., 2003, "Internet As A New Distribution Channel For Financial Services: Awareness And Acceptance Of Internet Banking", School of Management Chairman, Operations Management
- Ratnasingham, P., 1998, "The importance of trust in electronic commerce", *Internet Research: Electronic Networking Applications and Policy*, 8(4): pp 313–321.
- Robinson, T., 2000, "I-banking: Still not a perfect marriage", *Informationweek.*, (782): pp 104-106.
- Sathye, M., 1999. "Adoption of Internet banking by Australian consumers: an empirical Investigation: *International Journal of Bank Marketing*", 17(7): pp 324-334.
- Stafford, B., 2001, "Risk management and I-banking: What every banker needs to know", *Community Banker*, 10(2): pp 48-49.
- Stewart, K., 1999, "Transference as Means of Building Trust in World Wide Web Sites", *Proceedings of the 20th. ICIS, Charlotte, North Carolina.*
- Tuliani, Dr J., 2004, "The future of phishing", UK Technical Manager, Cryptomathic
- Williams, K., 2000, "Are you ready for I-banking", *Management Accounting*. 81(10): pp 23-82.
- Yan, G., Paradi J.C., 1998, "Internet - The Future Delivery Channel for Banking Services?", *Centre for Management of Technology and Entrepreneurship, University of Toronto.*

CV OF THE AUTHOR

Gökhan AFACAN was born in 1978 in Eskişehir. After graduating from Eskişehir Kılıçođlu Anatolian High School, he took his bachelors degree from Computer Engineering department of Ege University, İzmir at the year of 2000. He worked as an Analyst Programmer at Banksoft, a software house company located in İstanbul which serves Personal Banking software solutions for banks. After completing his military service, he began working in Akbank T.A.Ş. as a software developer. By the end of year of 2004, he has been working for TUBITAK UEKAE, the National Electronics and Cryptology Research Institute of Turkey, with the title of Data Systems Administrator for a project of e-signature in the frame of e-government. He may be reached via e-mail from the addresses of gokhan.afacan@kamusm.gov.tr or gokhan.afacan@gmail.com .

