CONSIDERATIONS REGARDING THE SECURITY AND PROTECTION OF E-BANKING SERVICES CONSUMERS' INTERESTS

Marinela Vrînciantu[1*] and Liana Anica Popa[2]
[1) 2)]Academy of Economic Studies, Bucharest, Romania

Abstract

A significant number of breaches in the security of electronic banking (e-Banking) system is reported each year, drawing attention to the need to protect and inform customers about the risk of exposure to malicious actions initiated by cyber-criminals. Financial institutions and consumers recognize the fact that attacks and financial frauds are becoming more complex and are perpetrated by a different class of criminal. This class is increasingly sophisticated and uses technology as part of their strategy. Furthermore, the specialists forecast that the current global recession is likely to increase the frequency of internal fraud and security breaches.

The present research tries: (1) to analyze the potential dangers threatening the security of e-Banking services through a comprehensive investigation of the relevant literature; (2) to identify the tools and methods that can ensure the consumers' protection in E-Banking, (3) to present the results of a pilot study regarding the Romanian consumer perception on the protection and security related to E-Banking services

Keywords: E-Banking services, security, consumer protection, cyber-attack

JEL Classification: G21, H55

Introduction

For many years, electronic banking platforms have been implemented as an ever more efficient channel throughout which banking transactions can be done without effort. These e-Banking platforms are Web-based applications that are exposed over the Internet making their users a very appealing target for mal-intentioned individuals. A major challenge for e-Banking that requires further innovative approaches stems from the need to annihilate the effects of rapidly growing cyber-crime. The security related risks can cause banks to lose

[*] Corresponding author, **Marinela Vrînciantu -** marinela.vrincianu@gmail.com

the gains of Internet banking if problems are not properly addressed. One of the risks is identity theft, which can occur by using an unconventional attack like: phishing, pharming, spoofing, key logging, screen logging, Trojans horses, other malicious codes or transaction poisoning.

Another major problem is represented by the authentication schemes currently in use that base their robustness on the end-user's decisions, which make them entirely vulnerable to social engineering attacks.

According to UNCTAD (2007), another worry from the security point of view is the "trust gap", un unproven but suspected divide between those who use Internet for other tasks, and hence trust online banking, and those that do not. Once the banks start to outsource IT-related operations to other firms, there is the increased risk that the latter may not be sufficiently regulated and that the transfer of information to them and between them and the banks may increase the security risk. Many innovative schemes have been developed to solve the security problems (Singh&Malhotra, 2004; Rombel,2003). Some authors have proposed the inclusion of biometric characteristics, such as fingerprint or iris pattern (Arumuga, 2006). According to Mu (2003), there is a need to develop approaches to make sure that a combination of enough technical expertise, security support and oversight is in place when one engages in outsourcing in e-banks.

In highly exposed environments, such as the e-Banking platforms, the authentication GAP, (which is the technical term commonly used for referring to the intrinsic vulnerability of the authentication process) is reflected in the little or total lack of control the authenticating institution (bank) has on the users since no control exists on the medium (the Internet and computer connection used in accessing the home banking platform).

The purpose of this research is to analyze the typology of dangers that threat the security of e-Banking services. Also, the present study explores the impact of security breaches on e-Banking customers' behaviour and tries to recommend solutions for the protection of their interests. The final section presents the results of a pilot survey regarding the Romanian consumer perception on the protection and security related to e-Banking services and discusses the study's implications for research and practice. In our study, we used the methods of descriptive and exploratory research. The methods of descriptive research are used to obtain information concerning the major security issues in e-Banking. The research had been completed on the basis of primary data (structured questionnaire) and secondary data (online databases, scientific journals, surveys, news).

1. Security in e-Banking

The main risks associated with e-Banking are strategic, operational, legal and reputational. Security is considered the central operational risk of e-Banking. According to Sokolov (2007) some of the specific problems cut across risk categories, e.g. breach of security allowing unauthorised access to customer information can be classified as an operational risk, but such an event also exposes the bank to legal risk and reputational risk Customer education on security risks, the precautions and the knowledgeable use of technologies can play also an important role for consumer protection and for limiting reputational risk. In

Romania, many banks which are engaged in e-Banking activities have published on their websites recommendations to potential customers on how to increase the security while making transactions in online environment. The idea of E-Banking according to Essinger (1999) is: "to give customers access to their bank accounts via a web site and to enable them to enact certain transactions on their account, given compliance with stringent security checks". According to Leow (1999), the terms "PC banking", "online banking", "Internet banking", "telephone banking" or "mobile banking" refers to a number of ways in which customer can access their banks without having to be physically present at the bank branch.

Customers usually perceive risks in conducting online transactions, particularly if the transactions involve financial aspects. Many studies concluded that customers are afraid of security issues (Howcroft et al., 2002; Sathye, 1999; Hamlet&Strube, 2000). According to Agharwal (2009), it is generally considered that the risk perception could be higher for electronic banking services. It is argued that in the e-Banking context, the security issue is crucial once it involves directly the user's actives (Cockburn&Wilson, 1996; Pavlou, 2001). Korgaonkar and Wolin (1999) consider that customer-perceived insecurity in online transactions has become one of the most important obstacles in development of electronic services. Fitzergerald (2004) tries to identify current and potential customers' perceptions of online banking. He concluded that there are common perceptions regarding online banking with disregard to demographic, geographic or psychological characteristics. He argued that among the major 'non-adoption' areas are the security concerns and lack of awareness of online banking. Jun and Cai (2001) identified 17 service quality dimensions in e-Banking, security being one of these dimensions.

The study of Mattila et al. (2003) was concerned with analyzing the adoption of Internet banking among mature customers. The results show that people over the age of 65 generally tend to be late adopters of technologies. They found that mature customers who discontinued the use of online banking reported insufficient or non-existent training on how to use the technology. They also pointed that confusing web pages and complex steps discouraged their adoption of online banking, and improving security measures. Subsequently, they recommended developing three-dimensional web pages with voice recognition, using video technology to provide access to bank employees. Sohail and Shanmugham (2004) analyzed customers' preferences in e-Banking in Malaysia. Their conclusion indicates that accessibility to the Internet, awareness of e-Banking and customers' resistance to change are the main factors influencing the e-Banking services adoption.

Security perceptions are defined as the subjective probability with which consumers believe that their private information will not be viewed, stored and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations (Pavlou, 2001).

2. Typology of security risks in e-banking

The specialists consider that the main threats to the security of e-Banking platforms are: denial of service, illegitimate use, disclosure of information, information alteration, and repudiation (Florescu et al., 2009)

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two computers, thereby preventing access to a service or preventing a particular individual from accessing a service and attempts to disrupt service to a specific system or person. The DoS attacks typically target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. The illegitimate use involves the use of information by unauthorized persons or for unauthorized purposes. Because banking information may have a strategic importance for their customers, this action represents a significant risk for system security.

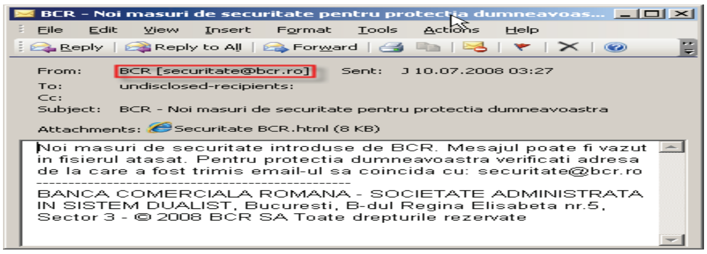
The disclosure of important information that should remain confidential, by unauthorized persons or that exceed their authority can cause significant losses for financial institutions. Alteration of information by entering, modifying or overwriting data into the system without authorization or by exceeding one's authority is a type of attack that could potentially harm greatly the banks and their customers.

Repudiation is the action of a person to deny the identity of the transmitter, the contents or the date of a communication, or transmission of an e-message. Taking into account the strategic importance of certain messages, it is important to ensure non-repudiation of financial transactions.

A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions. This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others. If this attack takes place, the data stored on log files can be considered invalid. Regarding digital security of financial transactions, the application of non-repudiation supposes: (a) a service that provides proof of the integrity and origin of data; (b) an authentication tool that with high assurance can be asserted to be genuine. A hash function is usually sufficient to establish the integrity of data. Yet, even with the hash function, it is still possible to tamper with data in transit, either through a man-in-the-middle attack, or by pharming or phising.

Man-In-The-Middle attack is the type of attack where attackers intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data.

Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. (Figure no. 1)



BCR - Noi masuri de securitate pentru protectia dumneavoas...

From: BCR [securitate@bcr.ro] Sent: J 10.07.2008 03:27
To: undisclosed-recipients:
Cc:
Subject: BCR - Noi masuri de securitate pentru protectia dumneavoastra
Attachments: Securitate BCR.html (8 KB)

Noi masuri de securitate introduse de BCR. Mesajul poate fi vazut in fisierul atasat. Pentru protectia dumneavoastra verificati adresa de la care a fost trimis email-ul sa coincida cu: securitate@bcr.ro

----

BANCA COMERCIALA ROMANA - SOCIETATE ADMINISTRATA IN SISTEM DUALIST, Bucuresti, B-dul Regina Elisabeta nr.5, Sector 3 - © 2008 BCR SA Toate drepturile rezervate

Figure no. 1: Example of phishing attack

Source: www.bitdefender.ro/NW777-ro--Clientii-e-banking-din-Romania-s-ar-putea-trezi-fara-nici-un-ban-in-cont.html [Accessed 12 January 2010]

Pharming is a type of fraud that involves diverting the client Internet connection to a counterfeit website, so that even when he enters the correct address into his browser, he ends up on the forged site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. In recent years both pharming and phishing have been used for online identity theft information. Pharming has become of major concern to businesses hosting online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat because antivirus software and spyware removal software cannot protect against pharming. One of the most effective ways of stealing information is capturing keystrokes. A very simple program captures everything the user is doing (files opened and closed, sites visited, etc.). Another and a little more sophisticated program of this type also captures text from windows and make screenshots (record everything displayed on the screen) - so the information is captured even if the user does not type anything, just opens and views the file. These programs are called Keylogging programs and represent software tools that trace all or specific activities of a user in a computer system. They form the most dangerous core of so-called spyware. Experts recommend, in this case, using a combination of three products: a personal firewall, an anti-virus and an anti-spyware - and regularly update the latter two. The threats and dangers on the Internet are changing constantly, and often extremely quickly. The most prevalent threats include viruses, Worms, Trojan Horses, drive-by downloads, spoofing-attacks. The viruses can alter data on customer computer, while the most serious cases can lead to entire hard-disk erasure. Viruses are spread via e-mail or by downloading infected files. The worms are standalone programs that do not require a host program for activation and spread themselves independently from computer to computer by exploiting security vulnerabilities or configuration errors in operating systems or applications. The Trojan horses aim to spy on sensitive data (e.g. passwords, confidential data, etc.) and send it back to their owners to gain access to third-party computers and thus take control of them remotely. Trojans are normally disguised as applications that are useful to users of the computers they infect. Drive-by downloads are mal-ware infections that happen only because the customer visited a particular website. These websites often contain legitimate content, but have been contaminated by harmful programs that smuggle malicious codes into the site. A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. A separate category of threats to the security of e-Banking systems are those resulting from the way in which the information is managed: administrative errors associated with a computerized system (wrong configuration, maintaining a user account after dismissing an employee, the wrong setting of authorities), scavenging (use of software tools for reconstruction of the magnetic information after deletion or overwriting), social engineering.

From all the above, it can be concluded that there is not any single strategy that covers all the different dangers threatening the e-Banking platforms. On the contrary, focusing on a multi-layer protection approach is the best alternative for system security and for protection of consumers' interests, including a mix of different factors that allow:

- Implementing complementary protection for the end-user's station;
- Communicating the occurrence of potential transactions frauds to the end-user;
- Shielding the authentication process from malicious activities that can affect the end user's station;
- Providing user-to-site authentication strategies which allow the end-user to verify that the connection is indeed established with the correct site;
- Implementing authentication factors that eliminate user decisions from the authentication process.

3. Effects of security breaches in e-Banking platforms

Many statistical reports provide examples about the dimension and effects of security breaches in e-Banking. According to Gartner Inc., the technology research and consulting firm (Gartner, 2005), from May 2004 to May 2005, 1,2 million consumers lost 929 million dollars due to online fraud schemes such as phishing. Symantec, in its 2006 Internet Security Threat Report on Phishing, notes that nine of the top 10 brands targeted by phishers are in the financial sector (Symantec, 2007). Approximately 7.5 percent of U.S. adults lost money as a result of some sort of financial fraud in 2008, in large part because of data breaches, according to a recent survey by Gartner Inc. Analysts said this is having an adverse effect on consumer victims who are significantly changing their financial transaction behaviours. When protection during the transmission of personal account data via the Internet is involved, many people still put their trust in the conventional PIN/TAN system. Recent reports show however that these methods are not sufficient to suppress organised cyber-crime. According to the IT national association in Germany, Bitkom, in 2007 around 4100 cases with a total loss in the region of tens of millions came to light with an average loss amount of approximately €3,700 (Mohr, 2009).

Gartner surveyed nearly 5,000 U.S. adults in September 2008 to gauge the impact of identity theft, and the leading types of financial fraud. Payment card fraud was the method most actively used by infractors, claiming 36 percent more victims in 2008 than other types of fraud. New-account fraud, in which a thief steals identity information to open a new account, occurs less frequently than payment card fraud, although Gartner estimates that up to half of all new-account frauds involve synthetic identities, and therefore many cases go unreported. Nearly twice as many people who lost money to fraud in 2008 changed their shopping, payment and e-Banking behavior.

The victims of electronic checking and/or savings account transfer fraud in 2008 were nearly five times more likely to change banks because of security concerns, when compared with the average customer. About twice as many of the victims curtailed online money transfers and bill payment used in online banking. As a result, more losses can be expected as fraudsters exploit technology to its fullest, unless the financial services industry can stay one step ahead of them.

Symantec, in its 2007 Internet Security Threat Report period, noted that Romania was home to the third most phishing Web sites globally, accounting for five percent of all phishing Web sites detected, and the most phishing Web sites in EMEA (Europe, Middle East and Africa), with 46 percent of the region's total. Although it ranked thirty-fifth worldwide and sixteenth in EMEA for overall malicious activity, it was the fifteenth ranked country in the world for phishing hosts and had the tenth highest number of phishing hosts in EMEA. Thus it would seem that the amount of phishing activity based in Romania is disproportionately high relative to the overall malicious activity originating there. These figures would indicate that phishing is the most common malicious activity originating in Romania, suggesting that attackers there may be specializing in that activity. This is borne out by numerous reports that indicate that Romania has become a growing source of online fraud (Symantec, 2008).

According to Mediafax, in Romania, in 2008, there were 652,000 online transactions by card, of which 540,000 were performed through ePayment platform. Number of fraud attempts dropped from 1.5% in 2007 to 0.7% in 2008, without major incidents recorded. The number of phising attacks in Romania increased by 20% in the first half of 2009.The vast majority of these attacks cover the e-Banking area, Raiffeissen Bank being followed in ranking by Bancpost (7% of attacks), Transilvania Bank (4%), BRD (2%), Romcard(1%).

The 2008 ranking of the most commonly forged bank identities in Romania was:

- Raiffeisen Bank (60%)
- BCR (13%)
- BRD (10%)
- Piraeus Bank (8,5%)
- Transilvania Bank (8,5%).

According to IBM X-Force Trend and Risk Report (2009), Romania is located in different tops related to spam and phishing. Thus, Romania was the tenth spam generating country in the world, the third ranked country in the landing-page top and the second ranked country with the most phishing links. (Figure no. 2)

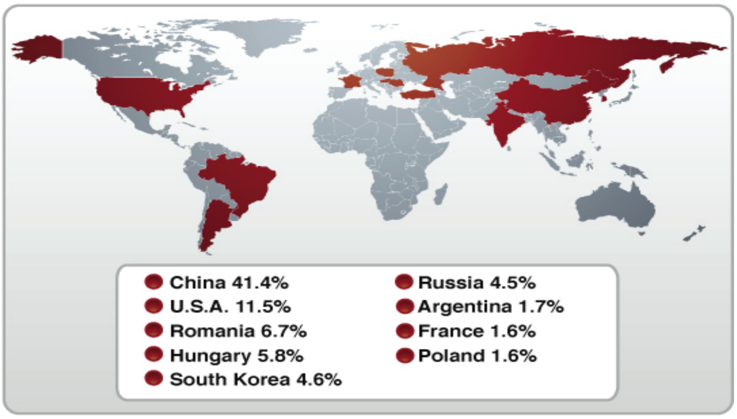


Figure no. 2: Geographical distribution of Spam URLs

Source: IBM-X Force, IBM X-Force Trend and Risk Report (2009)

4. Tools and methods to ensure the security in e-Banking services

Obviously, without great confidence in bank security, customers are unwilling to use a Internet to view their financial information online or to conduct financial transactions. Some of the security threats include invasion of individuals' privacy and confidential information theft.E-Banking platforms offer several methods to ensure a high level of security: (a) identification and authentication, (b) encryption, and (3) firewalls mechanism. The identification of an online bank takes the form of a known Internet address or Uniform Resource Locator (URL), while the customer is identified by his login ID and password to ensure only authorized users can access their accounts. On the other hand, messages between customers and online banks are all encrypted so that another person cannot view the contents of messages. The common encryption standard adopted by most browsers is called Secure Socket Layer (SSL).

A firewall is a set of related programs, located at a network gateway server that protects the resources of a bank network from users from other networks. It is a set of devices configured to permit, deny, encrypt or decrypt all computer traffic between different security domains based upon a set of rules. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification can ensure that customer account information is protected from unauthorized access.

Many institutions have therefore already reacted with improvements to their safety procedures and have started with the replacement of their previous TAN lists. A Transaction authentication number or TAN is used by some online banking services as a form of *single use* /one-time passwords to authorize financial transactions. TANs are a second layer of security above and beyond the traditional single-password authentication. But it is questionable whether changing to the mobile TAN will lead to the desired result. With this procedure, after logging on with the bank the customer receives a transaction-related TAN by SMS on his mobile phone. Since the cyber-criminal cannot simultaneously eavesdrop the customer's PC (customer to bank) and the mobile phone network (bank to customer), the mobile TAN method is regarded as relatively secure (Mohr, 2009).

A completely different alternative is protection via chip card using the HBCI (Home Banking Computer Interface) procedure. This method ensures a very high security standard – but the user needs to own software for this and a chip card reading device. These restrictions are responsible for this procedure receiving poor response in the market.

Another method of secure online banking is the TAN generator. These devices generate a TAN, which is only valid for a short period of time and is shown on the device display. The method, which is also known as "Smart TAN", substantially impedes the interception and misuse of user data. With the more intelligent "Smart TAN Plus" method the customer enters certain transaction data into a special card reader, which generates a TAN in conjunction with the bank- card. The bank computer then also computes the TAN and enables the transaction if there is a match. Since the calculated TAN can only be used for this transaction and the TAN is calculated with the aid of the bank card, this procedure is evaluated as being very secure. Only the entry of the transaction data using the keypad on the reader is sometimes regarded as inconvenient and involves the possibility of erroneous entries.

A new tool that appeared on the market to support user authentication is the electronic Identity (eID) card. Such e-ID cards have been or are being introduced in quite a number of European countries. In some countries, the issuance for these e-ID cards is managed by governments, or by private public partnership (PPP) between banks and governments, as issuing bodies. Such are Sweden, Estonia, or Luxembourg. There is, in some countries, a real interest of the banking sector to work with public authorities as close as possible on the topics of user authentication and electronic signatures.

Biometry is not currently used and is not expected to be a relevant method for authenticating users in the near future in Europe due to factors such as lack of stability, difficulty of use, and cost effectiveness.

5. E-Banking platform security and protection of consumer interests

Obviously, ensuring a high level of security for e-banking platforms will have as a final motivation, the consumers' protection of electronic services and consequently the protection of the financial institutions' interests. How a financial institution manages information security, in this case based on information and communication technologies, is essential to ensure its credibility on the ability to conduct e-banking services and to protect the confidentiality and integrity of information.

Most legal regulations regarding the protection of consumer interests by ensuring the security of e-Banking platforms are considering:

- Ensuring the security and confidentiality of customer information;
- Protection against any anticipated threats or hazards to the security or integrity of such information;
- Protection against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

In Romania, specific legislation has been created by the development of Government Ordinance no. 130/2000 on the regime of distance contracts, Law no. 455/2001 on Electronic Signatures, the Government Emergency Ordinance no. 193/2002 concerning the introduction of modern means of payment, Law no. 677/2001 on the protection of the processing of personal data and free movement of such data, with subsequent amendments, Regulations of National Bank of Romania no. 4 / 2002 concerning transactions by electronic payment instruments and the relationship between participants in these transactions, the Law no. 365/2002 on electronic commerce and the Order of the Ministry of Communications and Information Technology no. 389/27.06.2007 regarding the approval procedure of payment instruments with remote access applications such as Internet banking, home-banking or mobile banking.

This latest statute makes it mandatory to obtain an authorization in order to be able to issue remote access payment instruments. The purpose of the authorization is to check whether the financial institution in question and the corresponding software solution that intermediate the remote access payment instrument, comply with a minimal set of security needs, such as:

- Confidentiality and integrity of communications;
- Confidentiality and non-repudiation of transactions;
- Confidentiality and data integrity;
- Authentication of parties involved in transactions;
- Protection of personal data;
- Keep banking secrecy;
- Traceability of transactions;
- Continuity of customer service;
- Prevention, detection and monitoring of unauthorized access to the system;
- Restoration of information managed by the system in case of natural disasters and unforeseen events;
- Management and administration of information system;
- Any other activities or technical measures taken for the safe operation of the system.

Also, there are some legislative initiatives with regard to fighting cyber-crime: Title III in the Law no. 161/04.19.2003 regarding some measures to ensure transparency in exercising public office and in the business environment and the Law no. 64/03.24.2004 regarding the ratification of the European Council Convention on cyber-crime was adopted in Budapest on November 23rd 2001.

6. A pilot survey regarding the Romanian consumer perception on the protection and security related to e-Banking systems

6.1 Preparing the questionnaire

Main purpose of the study is to gain a better understanding of the Romanian consumer perception on the protection and security related to e-Banking services. The number of Romanian users of electronic banking services, according to the 2009 summary statements published by the Ministry of Communications and Information Technology, was 1,397,824 in the third quarter of 2009.

The method found most suitable to gather data to support this study was the online questionnaire and the questionnaire distributed directly or by phone. The survey lasted for two months starting from 15 November 2009 to 15 January 2010. A five-point Lickert scale (1=strongly disagree, 2= disagree,3=neutral,4 =agree and 5=strongly agree) , the scored question (the lowest score is 1, the highest score is 10) and the questionnaires with multiple selection were used. We also used open questions in order to obtain the opinion of interviewee. The questionnaire was designed on two sections: one section with questions of general interest (details regarding gender, occupation, use of Internet, use of e-banking) and a section with specific questions on the security and the consumer protection in e-Banking services. The total number of distributed questionnaires containing 14 questions was 350 and 154 replies were with usable answers.

The aim of a pilot study is to perform a preliminary study on a smaller scale, prior to the main investigation, in order to verify the feasibility of research and to improve the final questionnaire. Taking into account this fact and the conclusions of the pilot studies carried out on similar issues in other countries (Mahmood, 2009; Azouzi, 2009), we consider the number of 154 questionnaires as satisfactory.

6.2 Analysis of results

Replies were received from 95 male respondents and 59 female respondents. 89% of them were employed (38 % in accounting, 15% in IT, 15% in administration, 10% in customer services, 6% in management, 3% in defense industry, 2% in other activities) and 11% were unemployed (4% retirees, 9% unemployed students)

The survey reveals that:

- 79% of the respondents had access to Internet.

- It also suggests that those who are not using e-Banking provide the following reasons: lack of knowledge of current technologies, lack of security of e-Banking systems, lack of the confidence in the use of technology, the preference for face-to-face contact in financial transactions, avoiding the risk of not getting what they want.

The respondents were asked whether they agreed that the Internet was secure for conducting online financial transactions. For a clear delineation of their opinions, the question has been associated with a 5-point Lickert scale (1 = totally disagree, 2 = disagree, 3 = neutral 4 = agree, 5 = totally disagree) and the results are centralized in Table no. 1. This question was associated with question II.2 (open-up question) in which users were asked to substantiate their opinion. Only 35% of the participants consider that Internet is safe for transactions, invoking their confidence in security software.

Table no. 1: Internet is secure for conducting financial transactions (Question II.1)

Opinion	Frequency
Strongly Agree	10%
Agree	25%
Neutral	17%
Disagree	28%
Strongly disagree	20%
Sum	100%

The question II.3 was designed as a multiple selection question in order to identify the security breaches that respondents faced. Regarding the main threats and dangers in conducting online transactions, 60% of the respondents received a phishing e-mail, 56% had problems with viruses and malicious codes, 2% reported different security incidents (unexplained disappearance of money from personal accounts, failure of e-Banking computer system, unsynchronized transactions).Subsequently, the respondents were asked if they are really willing to conduct online transactions if their banks provided enough support (question II.4). The results obtained for this question, designed according to the 5-point Lickert scale are presented in Table no. 2.

Table no. 2: I am willing to conduct online transactions if my bank provided support (Question II.4)

Opinion	Frequency
Strongly Agree	40%
Agree	47%
Neutral	2%
Disagree	5%
Strongly disagree	5%
Sum	100%

Those that agreed to the idea of conducting online banking transactions with support provided by bank reached 87%. Only 10% disagreed and 2% were indifferent (table no. 2).

Regarding the accuracy and integrity of records related to personal account transactions (question II.5, designed according to the 5-point Lickert scale), 92% of respondents that use e-Banking services agreed to the idea that online customers service keeps accurate records of account transactions (Table no. 3).

Table no. 3: Online customers service keeps accurate records of my account transactions (Question II.5)

Opinion	Frequency
Strongly agree	40%
Agree	52%
Neutral	2%
Disagree	4%
Strongly disagree	5%
Sum	100%

Question II.6, designed according to a 5-point Lickert scale concerned the perception of respondents on safety of customer service.

The respondents that agreed to the idea that online customer service is secure reached 35%. Unfortunately, a 35% agreement is not a very promising statistic, especially when comparing it with 53% disagreement (Table no. 4).

Table no. 4: Online customer service is secure (Question II.6)

Opinion	Frequency
Strongly agree	20%
Agree	15%
Neutral	12%
Disagree	30%
Strongly disagree	23%
Sum	100%

Regarding the security of transactions and privacy of customer (question II.7), 35 % of respondents that use e-Banking services agreed to the idea that online customer service provides security for the transaction data and privacy, 62% disagreed and 3% were indifferent.

A relatively small group (35%) agreed their banks are putting substantial efforts in order to inform or to train them about online banking (question II.8). Question II.9, designed as a multiple selection question, aiming to identify how respondents perceive the concept of security associated with e-banking services.

For 74% of respondents, security means low risk associated with online transactions, for 54% of respondents, security means personal information safety, and for 92%, security refers online transaction safety.

Conclusions

Although electronic banking can provide a number of benefits for customers and new business opportunities for banks, it exacerbates traditional banking risks, especially security issues. Also, we can't ignore the fact that the aim of Competitive Intelligence programs is to harness disparate information resources in order to enhance the competitiveness of the financial institution while eroding the competitive advantage of its rivals. This information is often acquired through legitimate/ethical means and covert methodologies involving economic espionage (Anica-Popa&Cucui, 2009).For many years, the discussions about the next step in e-Banking security have been going on. It is difficult to appreciate at what point in time the market will actually get traction and adapt advanced new technologies. Regarding the e-Banking environment, the choice for banks is not easy. The more security they introduce, the less user convenience they get with important costs for support. The volume of attacks against e-Banking platforms continuously increases in all markets with well-established e-Banking solutions. Many banks have realized that today's available authentication tools have the same disadvantages. They do not prevent online man-in-the middle attacks; and these are the most common today. There are different solutions on the market available with the same goal: introduce a new layer of security on the customer's side so that the user has to physically confirm especially identified transactions. It can be concluded that there is not any single strategy that covers all the different dangers threatening the e-banking platform, a multi-layer protection approach being the best alternative for security processes.

References

Al-Alawi, A.I., 2005. Online banking: Security concerns and the acceptance of Mature Customers. [Online] Available at: http://www.setit.rnu.tn/last_edition/setit2005/trait-information/140.pdf [Accessed 16 January 2010]

Agarwal, S., 2009. *Customer perception towards Internet bankingw.r.f. to private and foreign banks in India 9use of MDS.* [Online]. Available at: http://www.scribd.com/doc/13282604/Customer-Perception-Towards-Internet-Banking [Accessed 15 December 2009]

Arumuga, S., 2006. Effective method of security measures in virtual banking. *Journal of Internet Banking and Commerce.* [Online], 11(1). Available at: http://www.arraydev.com/commerce/JIBC/2006-04/VB.asp [Accessed 17 January 2010]

Anica-Popa, I. & Cucui, G., 2009. A Framework for Enhancing Competitive Intelligence Capabilities using Decision Support System based on Web Mining Techniques. *International Journal of Computer, Communications&Control*, IV(4), pp.326-334.

Azouzi, D., 2009. The adoption of Electronic Banking in Tunisia: An Exploratory Study. *Journal of Internet Banking and Commerce,* [Online], 14(3). Available at http://www.arraydev.com/commerce/jibc/2009-08/SI_Dhekra.pdf [Accessed 23 November 2009]

Cockburn, C. & Wilson, T., 1996. Business use of the World Wide Web. *International Journal of Information Management*, 16(2), pp. 83-102.

Essinger, J., 1999. *The virtual banking revolution: the customer, the bank and the future*. 1st ed. London, UK: International Thomson Business Press.

Fitzergelad, K., 2004. *An Investigation Into People's Perceptions of Online Banking.* [Online] Available at: http://staffweb.itsligo.ie/staff/eward/ebus%200203/Discussion%20topics/Online%20Banking.htm [Accessed 6 June 2004]

Florescu, V. et al., 2009. *Baze de date*. Bucuresti : Editura Infomega.

Gartner, 2008. *2008 Data Breaches and Financial Crimes Scare Consumers Away,* [Online]. Available at: http://www.gartner.com/DisplayDocument?ref=g_search&id=902212&subref=simplesearch [Accessed 12 December 2009]

Gartner, 2007. *Phishing Survey,* [Online].Available at: http://www.gartner.com/it/page.jsp?id=565125 [Accessed 10 October 2009]

Gartner,2006. *Phishing Survey*, [Online]. Available at: http://www.gartner.com/it/page.jsp?id=498245 [Accessed 7 June 2008]

Gartner, 2005. *Identity Theft Survey Report* [Online] Available at: http://www.gartner.com/press releases/asset 12975411.html [Accessed 7August 2007]

Hamlet, C. & Strube, M., 2000. Community banks go online. *ABA Banking Journal's 2000 White Paper/Banking on the Internet*, March, pp. 61-65.

Howcroft, B., Hamilton, R. & Hewer, P., 2002. Consumer attitude and the usage and adoption of home-based banking in the United Kingdom. *The International Journal of Bank Marketing*, 20(3), pp. 111-121.

IBM, 2009. *IBM X-Force Trend and Risk Report* [Online] Available at: http://www-935.ibm.com/services/us/iss/xforce/trendreports/ [Accessed 10 December 2009]

Jun, M. & Cai, S., 2001. The key determinants of Internet Banking service quality: a content analysis. *International Journal of Bank Marketing*. 19(7), pp.276-291.

Korgaonkar, P. & Wolin, L., 1999. A multivariate analysis of web usage. *Journal of Advertising Research,* 39(2), pp. 53–68.

Leow, H.B., 1999. New Distribution Channels in banking Services. *Banker's Journal Malaysia*, (110), pp.48-56.

Mohr, E., 2009. Security is decisive. *Beitrag für IT Banken & Versicherungen*, 5 Oct. [Online] Available at http://www.gemalto.com/financial/ebanking/security/ [Accessed 10 January 2010]

Matilla, S. et. al., 2003. Internet banking adoption among mature customers: early majority or laggards. *Journal of Services Marketing,* 17(5), pp. 514-528.

Mahmood, Z., 2009. Attitudes towards the use of E-banking: Result of a Pilot Survey. *Communications of the IBIMA*, 8(23), pp.170-174.

Pavlou, P., 2001. Integrating trust in electronic commerce with the Technology Acceptance Model: Model Development and Validation. *AMCIS 2001 Proceedings.* [Online]. Available at: http://aisel.aisnet.org/amcis2001/159 [Accessed 3 August 2008]

Rombel, A., 2005. Next step for Internet Banking. .[Online]. Available at: http://www.gfmag.com/archives/87-87-february-2003/2176-features--next-step-for-internet-banking.html#axzz0IhUm79xl [Accessed 3 June 2008]

Sohail, M. & Shanmugham, B., 2003. E-banking and Customers' preferences in Malaysia: an empirical investigation. *Information sciences, Informatics and Computer Science: an international journal,* 150(3-4), pp. 207-217.

Sathye, M., 1999. Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, 17(7), pp. 324-334.

Sokolov, D., 2007. E-banking: Risk Management Practices of the Estonian Banks. *Working Papers in Economics. School of Economics and Business Administration,Tallinn University of Technology (TUTWPE)*, 22(156), pp.21-37.

Singh, B. & Malhotra, P., 2004. Adoption of Internet banking: an empirical investigation of Indian Banking sector. *Journal of Internet Banking and Commerce*, [Online]. 9(2) Available at: http://www.arraydev.com/commerce/JIBC/9909-05.htm [Accessed 15 October 2006]

Symantec, 2008. *Symantec Internet Security Threat Report. Trends for July-December 2007*, *Vol XIII* [Online] Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf [Accessed 12 December 2009]

UNCTAD, 2007. *Information Economy Report 2007-2008: Science and technology for development: the new paradigm of ICT* [Online] Available at: http://www.unctad.org/Templates/Page.asp?intItemID=1888&lang=1 [Accessed 12 December 2009]