# IT-Security of E-Banking in Eyes of Croatian Clients

[1] Nedim Makarević
[2] Hikmet Secim
[3] Mehmet Toycan

[1] Cyprus International University, Cyprus
Doctor of Business Administration candidate
E-mail: nmakarevic@air-net.de
[2] Cyprus International University, Cyprus
Prof. Dr.
Economics/ Business Administration
[3] Cyprus International University, Cyprus
Asst. Prof. Dr.
Engineering Department

**Abstract.** The purpose of this paper is to examine clients' perceptions in Croatia towards information technology (IT) security of electronic banking (e-banking), to diagnose problems and try to give proper solutions. Methodology was survey based on six variables and specific questions assigned to each variable. Response rate was good and 203 respondents were surveyed. Findings indicated that Croatian e-banking users trust to banks when it comes to IT security of online banking. It is important to mention that clients perceive tangible features as important as they actually are. This proved that clients are aware of potential security threats, and even though they trust to bank, they are aware of their own responsibility when using e-banking services. Since there is gap in literature when it comes to research dealing with IT-security of electronic banking in Croatia, this article is both unique and good stimuli for new research in the future.

**Keywords:** Perceptions; information; IT security; online banking; privacy.

## Introduction

Handling money with no physical contact, usually via internet and making money transactions is nowadays known as "online banking". Muniruddeen Lallmahamood (2007) defines internet banking as banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments. Internet banking or online banking has created new ways of handling banking transactions for banking related services and for e-commerce related transactions such as online shopping (Lallmahamood, 2007).

Along with development of internet banking, new ways of stealing money by criminals are developed as well. Additionally, it is obvious that banks' dependence on new technologies increases, and therefore their need to protect their own and assets of their clients increases as well. This is where importance of IT security for banks' clients starts. Accordingly, it is important to know awareness level and perceptions of clients towards IT security of online banking. Since results of this research will enable banks to learn more about their clients, this research have potential to be important source of information to consider by banks when it comes to their planning and development activities. In Croatia, there is a need to do this kind of research because there is a gap in literature about mentioned issue in this country which gives even more value to this work.

Methodology of this work relies on survey which was based on specific variables. The survey has been prepared and distributed to clients who are actively using online banking. Main objective of this research is to learn perceptions of clients when it comes to IT security of online banking in Croatia. Additionally, this research has contribution in terms of providing new information to banks operating in Croatia and filling the gap in literature regarding this issue that considers population of Croatia as main target.

In the following sections of this work, through theoretical background, all necessary definitions together with brief historical facts important for understanding this topic will be explained. Accordingly, information on online banking in Croatia will be provided so readers can

be more familiar with the situation in this country. After that, used methodology will be explained. In the end, results will be analyzed, discussed and concluded.

**Theoretical background**

Muniruddeen Lallmahamood (2007) defines internet banking as banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments (Lallmahamood, 2007). On the other hand, Jagdeep Singh (2012) defines internet banking as online systems which allow customers to plug into a host of banking services from a personal computer by connecting with the bank's computer over the telephone wires. He is also mentioning some synonyms for internet banking such as online banking, PC banking, home banking or electronic banking (Singh, 2012).

According to Gordon and Loeb (2002), Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solutions and managerial actions (Gordon & Loeb, 2002).

Banks are not only dealing with intangible money transactions, but also with protection of highly sensitive information such are credit cards' PINs, data about the customers, customers bank accounts and all other kinds of information that could enable to third party conducting the criminal activities and making damage for both, customer and bank. According to Landwehr (2001), weaknesses of banks' information systems are named vulnerabilities, and it is likely that such vulnerabilities represent opportunities for crime by third parties (Landwehr, 2001).

One of the alternatives when it comes to keeping money in safer forms than cash is electronic handling of money, where no physical contact is necessary. This means that almost all transactions can be realized via different devices including computers, mail or telephone, without physical contact. Such an operation resulted in new types of crime, and some of them are still new to the legal systems. Main problem is that allowing people to make transactions with no physical contact opens the door for criminals to gain access and make transactions. Accordingly, beside the physical security systems of banks, possibility of crime is still very high. Sometimes, in order to keep public image, banks do not even investigate and prosecute cybercrimes. If they would do that, customers wouldn't deposit money in their banks (Pfleeger & Pfleeger, 2006). In short, big question emerge in heads of clients: "Is electronic way of handling money safe?"

**Online banking in Croatia**

After the war, in 1995, Croatian banking industry, along with all other industries was in recovery process. Number of banks was changing quickly since the situation was not stable yet. Process of elimination and merging the banks was accelerated after 2000 (Roncevic, 2006).

When it comes to online aspect of Croatian banks, Roncevic (2006) emphasized that in year 2000, Croatian banks provided an opportunity for clients to see different information on their web pages. Technological development resulted in quite different and improve situation till now. In 2000, only 37 banks had cash machines, only 5 banks provided sms services, and only 7% offerde services of reading status of accounts on their web. Nowadays, more than 74% of banks provides online access to data for its clients, most of the banks offer cash machines, and almost all of them offer online services (Roncevic, 2006).

According to data of Croatian National Bank, in second quarter of 2007 there was 385 000 of citizens and 120 000 businesses which used internet banking. 40.6 % of total number of transactions was electronic, and 7.6% of them was internet payment. In a case of businesses, even 18.1% of transactions was internet transactions (Ministry of Businesses, Work and Entrepreneurship, 2007).

**Literature review**

According to Shrinath (1997), statement „information is power" has nowhere been realized more significantly than in the banking industry. When discussing the risks and challenges for IT security in that period of time, Shrinath mentioned four risks: unauthorized system/data access by business users in the bank; unauthorized system/data access by application/system support personnel; unauthorized system/data access by customers; unauthorized system/data access by the

public at large. Since most people do not realize that large banks are prone to high risk of security breakdown even without going so far as the Internet, author decided to examine and explain the most critical areas (Shrinath, 1997).

Lawrence A. Gordon and Martin P. Loeb (2002) wrote an article which presents an economic model that determines the optimal amount to invest to protect a given set of information. Their model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. After analysis conducted by Gordon and Loeb (2002), they suggested that in order to maximize the expected benefit from investment in information protection, a firm s hould spend only a small fraction of the expected loss due to a security breach (Gordon & Loeb, 2002).

Authors found very important to know about perceptions of users about specific technologies. This is how technology acceptance model was born. Pikkarainen et al. (2004) conducted a study about consumer acceptance of online banking. They investigated online banking acceptance in the light of the traditional technology acceptance model (TAM). The data for their results was consisted of group interview with banking professionals, TAM literature and e-banking studies. According to their results, perceived usefulness and information on online banking on the Web site were the main factors influencing online-banking acceptance (Pikkarainen et al., 2004).

When it comes to explanation of basic concepts involved with system security, helpful was introductory chapter of book entitled „Security in computing "written by Charles P. Pfleeger & Shari Lawrence Pfleeger (2006). Their book deals with broad range of computer security related topics such are: cryptography; secure systems development; basic communications technologies; advices on planning, risk, and policies; Intellectual property; computer crime, and ethics. In short, it is possible to conclude that this book can serve as great guide to information about computer security attacks and countermeasures (Pfleeger & Pfleeger, 2006).

Interesting research was made by Luis V. Casalo, Carlos Flavian and Miguel Guinaliu (2007) who conducted it with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking. Their paper described the positive effects of security and privacy, usability and reputation on consumer trust in a web site in the online banking context. This study is very interesting and valuable since it proposes link between security, privacy and trust, amongst others, in the online banking context (Casaló et al., 2007).

Muniruddeen Lallmahamood (2007) explored the impact of perceived security and privacy on the intention to use Internet banking. He used an extended version of the technology acceptance model (TAM) is to examine the above perception and concluded that while perceived usefulness is a critical factor in explaining users' intention to use Internet banking, it is important to pay attention to the security and privacy of users' of Internet banking. According to results, convenience, ease and time saving are the main reasons for the adoption of Internet banking, whereas security, trust and privacy appear to be the top main concerns for non-Internet banking users. As author mentioned, this may also imply that security concerns and privacy protection are perceived to be part of the overall service provided by the Internet banking services providers, and he suggests that banks should gain customers' confidence through raising security levels of the bank (Lallmahamood, 2007).

Many studies that are dealing with evaluation of clients' trust when it comes to banking are including „security" as important construct. This leads to conclusion that IT security is important for getting customer's trust in banking business. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) wrote a paper with aim to examine the role of situation normality cues (online attributes of the e-banking web site) and structural assurance cues (size and reputation of the bank, and quality of traditional service at the branch) in a consumer's evaluation of the trustworthiness of e-banking and subsequent adoption behavior. One of their findings in this work stated that web site features that give customers confidence are significant for promotion of e-banking (Yap et al., 2010).

Research found to be very useful for this article is the one completed by Mohanad Halaweh (2012) who was writing about user perceptions of e-commerce security (Halaweh, 2012). In fact, both online banking and e-commerce are having common characteristic which is no physical (face to face) contact between parties involved in transaction, and using same technologies for doing transaction. This means that both of them are exposed to same risks. Accordingly, this common characteristic was very useful while identifying relevant variables for this study since some of them

are simply modified and used for this research. Results of study conducted by Mohanad Halaweh (2012) showed that user characteristics, psychological state and intangible security features have a significant influence on e-commerce security perception. Additionally, in contrast, tangible security features and cooperative responsibility have a non-significant influence (Halaweh, 2012).

Singh (2012) commented that customers, both corporate as well as retail ones are no longer willing to queue in banks, or wait on the phone, for the most basic of services. Therefore, electronic delivery of banking services is becoming the ideal way for banks to meet their clients' expectations. Accordingly, author got idea to study the scenario of e-banking, and in his study he considered opinions of 100 customers from Ludhiana. The results of this work revealed that people are aware of e-banking, but not fully. In fact, the Customers are at ease after using e-banking since it saves the precious time of the customer. It has also been found that Customer satisfaction varies according to age, gender, occupation etc. (Singh, 2012).

**Variables & survey**

For conducting this research, with aim to get closer insight into clients' perceptions towards online banking in Croatia, six variables were identified as a result of literature review. Those variables are as follows:

1.1. Privacy aspect refers to confidence in the technology and online banking service provider when it comes to protection against privacy issues such are private information of client, information about money transactions conducted by client, information about client's personal passwords etc. Pikkarainen et al (2004) stated that as the amount of products and services offered via the Internet grows rapidly, consumers are more and more concerned about security and privacy issues (Pikkarainen et al., 2004).

1.2. Control aspect - When it comes to control perspective of IT security, as it is possible to conclude from survey questions of Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010), this aspect refers to strictness of identity ascertaining when sending messages to client, or doing transactions by client, but also general control by bank when it comes to online transactions' confidentiality (Yap et al., 2010).

1.3. Psychological aspect - According to Halaweh, Mohanad (2012) The psychological aspect of security incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the payment process and performance of online transactions. Even though he made research about e-commerce, because of same nature of e-commerce and e-banking which is remote rather than face-to-face, his work was useful for preparation of survey in this study (Halaweh, 2012).

1.4. Therefore, it is possible to conclude that many customers have the misconception that the use of e-banking is vulnerable and that there is a high probability that their money will be lost.

1.5. Tangible features - Halaweh, Mohanada (2012) defines tangible indicators as those technological security features of websites that can be checked by users, such as https, padlocks and security certificates. Tangible features need to be understood and checked by the customer over the website rather than captured through social communication; this involves having knowledge and experience of these features, such as knowing what a security certificate means and how to check whether it has expired (Halaweh, 2012).

1.6. Intangible indicators - When talking about intangible indicators such are famous website and reputation, Halaweh, Mohanad (2012) says that they are not seen on the website and cannot be directly checked over the website. They are affected by society in terms of communication and the environment: where the customer lives and what they hear from others, as well as their past experience (Halaweh, 2012).

1.7. Perceived IT security Perceived IT security refers to general perception of online e-banking services by clients when it comes to IT security.

Accordingly, survey consisted of twenty questions was created. Questions were mainly adapted from previous researches considering Pikkarainen et al (2004), Casaló, Flavián, and Guinalíu (2007), Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010), Halaweh, Mohanad (2012), Muniruddeen Lallmahamood (2007). All questions prepared for the survey, along with their references they were adapted from, are presented in Table 1 available in the next page.

Pikkarainen et al. (2004) conducted group interview with banking professionals in order to learn about consumer acceptance of online banking (Pikkarainen et al., 2004). Specific questions

related to privacy aspect from his interview were adapted and used in this research to examine clients' concerns about their privacy and security issues in e-banking. Casaló, Flavián, and Guinalíu (2007) made research with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking (Casaló et al., 2007). Since they are dealing with similar issue, questions regarding security and privacy were adapted and used in this study. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) used survey to evaluate trustworthiness of e-banking and subsequent adoption behavior through several factors (Yap et al., 2010). Accordingly, several questions helpful to measure control aspect of IT security in e-banking were used in our study. Halaweh, Mohanad (2012) studied user perceptions of e-commerce security (Halaweh, 2012). Since both e-commerce and e-banking are having the same characteristics such is lack of face to face communication and physical contact which implies same issues and concerns for final users of such a services, many questions were adapted from his survey in order to measure psychological aspect, tangible and intangible indicators, and perceived IT security in general when it comes to online banking. Also, when it comes to Muniruddeen Lallmahamood (2007), one of questions used in his study was useful to adapt for this research when it comes to measuring psychological aspect of IT security (Lallmahamood, 2007).

Table 1: Review of survey questions

| **Questions** | **Adapted from** |
|---|---|
| I trust in the ability of bank to protect my privacy | Pikkarainen et al (2004) |
| I am not worried about my personal information given to bank | |
| I think that my bank's information system respects personal data protection laws | Casaló, Flavián, and Guinalíu (2007) |
| I think that my bank's information system will not provide my personal information to other companies without my consent | |
| I think that my bank's information system respects user's rights when obtaining personal information | |
| I think that bank needs to ascertains my identity before sending any messages to me | Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) |
| I think that bank needs to ascertains my identity before processing any transactions received from me | |
| I trust that my bank uses security controls for the confidentiality of online transactions | |
| I don't fear when I am using e-banking services | Halaweh, Mohanad (2012) |
| I never have misconceptions about using e-banking services | |
| I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication | |
| I feel safe when I release credit card information through Internet banking | Lallmahamood, Muniruddeen (2007) |
| I don't check the presences of http(s) in the URL when I handle money transactions online | Halaweh, Mohanad (2012) |
| I don't check the small padlock icon on the bottom right corner of the website when I handle transactions online | |
| I don't check the digital security certificate of the web site when I handle money transactions online | |
| I would use e-banking services only provided by on a reputable bank | Halaweh, Mohanad (2012) |
| I would use e-banking services only provided by local bank | |
| I think my bank shows great concern for the security of any online transactions | Casaló, Flavián, and Guinalíu (2007) |
| I believe using e-banking services online is secure | Halaweh, Mohanad (2012) |
| Using e-banking services gives me a feeling of security | |

Source: Prepared for this research

## 2. Data and Methodology

Data for this study was collected by the means of a survey conducted in Croatia in 2013. A total of 250 questionnaire forms were delivered to respondents, and most of them were answered (even 203) giving a response rate of 81.2 percent.

Surveys were filled at universities by students, academic and administrative staff, and in branches of different institutions in Croatia by randomly selected clients. This resulted in a sample that was well distributed in terms of demographic information (e.g. age, and education).

Data is mainly numerical except demographics part which is categorical. Seven point Likert scale was used in order to test the agreements of the respondents on six variables through twenty questions. The collected data is then inserted into an excel spreadsheet and analyzed descriptively. The surveys were distributed both online and personally. Online version of survey was created, and its link was sent via e-mail to potential participants.

## Results

*Demographics*

Demographics information includes respondents' department, positions within the department and their education levels, gender and age. The survey is responded by 98 males and 105 females. Their education level is found to be extremely high (only thirteen respondents have no higher education level which is 6.4% of all respondents). More details regarding education level of respondents are available in Table 2.

Table 2: Education level of respondents

| Education level of Respondents | Number of respondents | Percentage (%) |
|---|---|---|
| Other | 13 | 6.4 |
| Undergraduate | 130 | 64.0 |
| Master | 51 | 25.1 |
| Doctorate | 9 | 4.4 |
| **Total** | **203** | **100%** |

The positions of the respondents were grouped according to their similar characteristics. It is possible to conclude that many respondents are still students, even 88 of them which is almost 43.3 % of total number of surveyed respondents. Even though not all of them are employed, most of the students are studying far away from their hometown, and their parents (sponsors) are sending them money using banking services. This fact makes them considerable target for this research. When it comes to employed respondents, most of them are in managerial positions. 15 of surveyed people work in different managerial positions. Sample of 203 surveyed people has high level of variety in terms of positions, which is visible in Table 3.

Table 3: Positions of the Respondents

| Positions of the Respondents | Number of Respondents | Percentage (%) |
|---|---|---|
| Academic Staff | 27 | 13.3 |
| Accounting Officer | 9 | 4.4 |
| Administration | 29 | 14.3 |
| Electrical Engineer | 3 | 1.5 |
| Journalist | 5 | 2.5 |
| Lawyer | 3 | 1.5 |
| Librarian | 4 | 2.0 |
| Manager | 15 | 7.4 |
| Physical Worker | 5 | 2.5 |

| | | |
|---|---|---|
| Psychologist | 4 | 2.0 |
| Sales Person | 7 | 3.4 |
| Software Developer | 4 | 2.0 |
| Students | 88 | 43.3 |
| **Total** | **203** | **100%** |

*Survey results*

From Table 4, it is possible to conclude that privacy aspect of IT security in online banking of Croatia is perceived as not acceptable by clients of this region. In fact, mark of 6.191 indicates that clients agree that banks are able, and doing their best to protect their privacy.

Table 4: Privacy aspect

| PRIVACY ASPECT (6.191) | Mean |
|---|---|
| I trust in the ability of bank to protect my privacy | 6.233 |
| I am not worried about my personal information given to bank | 6.055 |
| I think that my bank's information system respects personal data protection laws | 5.978 |
| I think that my bank's information system will not provide my personal information to other companies without my consent | 5.790 |
| I think that my bank's information system respects user's rights when obtaining personal information | 6.897 |

When it comes to control aspect, clients strongly agreed with statements about ascertaining their identities while using online banking and they believed that banks are using security controls to improve confidentiality of online transactions (Table 5).

Table 5: Control aspect

| CONTROL ASPECT (6.555) | Mean |
|---|---|
| I think that bank needs to ascertains my identity before sending any messages to me | 6.787 |
| I think that bank needs to ascertains my identity before processing any transactions received from me | 6.989 |
| I trust that my bank uses security controls for the confidentiality of online transactions | 5.889 |

When it comes to psychological aspect whose results are presented in Table 6, clients' perceptions towards IT security of online banking are very interesting. In fact, respondents agreed with the statements which indicate that clients are not afraid of using e-banking services, they do not have any misconceptions and they are not anxious while using online banking. Also, they feel quite safe when releasing credit card information through internet banking.

Table 6: Psychological aspect

| PSYCHOLOGICAL ASPECT (5.659) | Mean |
|---|---|
| I don't fear when I am using e-banking services | 5.677 |
| I never have misconceptions about using e-banking services | 5.509 |
| I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication | 6.554 |
| I feel safe when I release credit card information through Internet banking | 4.896 |

Results showed that Croatian clients are aware of importance of tangible features for security while doing online transactions. In fact, clients were mainly disagreeing with statements that they are not very careful when it comes to paying attention to presence of http(s) in the URL, small

padlock icon and digital security certificate of the web site. More details about this aspect are available in Table 7.

Table 7: Tangible Features

| TANGIBLE FEATURES (3.295) | Mean |
|---|---|
| I don't check the presences of http(s) in the URL when I handle money transactions online | 2.334 |
| I don't check the small padlock icon on the bottom right corner of the website when I handle money transactions online | 3.225 |
| I don't check the digital security certificate of the web site when I handle money transactions online | 4.326 |

This research showed that marketing and intangible assets of banks are slightly influential in Croatia. Clients are paying more attention to tangible rather than intangible ones such are banks' reputation, location and its concern towards security provision for its clients when making their decision to use online banking services. This could mean that clients perceive security provision as standard that must be respected by all banks. In other words, they are aware that banks will respect their privacy especially because of the competition in banking industry. More details about influence of intangible features to clients' perceptions of IT security of online banking are available in Table 8.

Table 8: Intangible features

| INTANGIBLE FEATURES (4.683) | Mean |
|---|---|
| I would use e-banking services only provided by on a reputable bank | 5.453 |
| I would use e-banking services only provided by local bank | 2.342 |
| I think my bank shows great concern for the security of any online transactions | 6.253 |

When it comes to general opinion about IT security of online banking, from Table 9, it is possible to conclude that clients strongly believe that using e-banking services online is secure, and they use e-banking services with feeling of security.

Table 9: Perceived IT security

| PERCEIVED IT SECURITY (6.110) | Mean |
|---|---|
| I believe using e-banking services online is secure | 6.546 |
| Using e-banking services gives me a feeling of security | 5.674 |

## 3. Conclusion

This research provided important insights in the area of clients' perceptions towards IT security of online banking in Croatia. Response rate of 81.2% together with the fact that surveyed people are coming from various companies, departments and positions within those departments gives even more importance and value to the results of this work. Limitations of this research are relatively small sample and quite generic approach to problem. Accordingly, suggestions for future researches would be based on going more deeply into the issue and analyzing larger samples. This article represents very unique set of information for the banks operating in Croatia. In this research, it has been empirically proved that clients of Croatia think that banks are able to protect their privacy completely, they perceive that banks are doing their best to improve confidentiality of online transactions, their perceptions has no fear, misconceptions and anxiousity. Also, Croatian clients are completely aware of importance of tangible features for security while doing online transactions. On the other hand, this research showed that marketing and intangible assets of banks are not always influential in Croatia. In brief, when it comes to general opinion about IT security of online banking, it is possible to conclude that clients are optimistic, they trust to banks, and they are aware of their own responsibilities regarding using online services.

## References

1. Casaló, L. V., Flavián, C., & Guinalíu, M. (2007) "The role of security, privacy, usability and reputation in the development of online banking." Online Information Review, 31(5), 583–603.

2. Gordon, L., & Loeb, M. (2002) "The Economics of Information Security Investment." ACM Transactions on Information and System Security, 5(4), 438–457.

3. Halaweh, M. (2012) "Modeling user perceptions of e-commerce security using partial least square." Journal of Information Technology Management, 23 (1).

4. Lallmahamod, M. (2007) "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model." Journal of Internet Banking and Commerce, 12 (3).

5. Landwehr, C. (2001) "Computer security." International Journal of Information Security, 1(1).

6. Ministarstvo gospodarstva, rada & poduzetništva (2007). Strategija razvitka elektroničnog poslovanja u Republici Hrvatskoj za razdoblje 2007. – 2010. Retrieved December 11, 2013, from: http://www.google.ba/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.mingo.hr%2Fuserdocsimages%2Ftrgovina%2FStrategija_razvitka_e-poslovanja_u_RH_u_razdoblju_2007_-_2010.pdf&ei=aLTAUpCgBMKztAbwm4GQDg&usg=AFQjCNEJUpNVIiDjgpTZo49aDYq-LGlIug&sig2=xfKGt_dTITaitRNHszf1Iw

7. Pfleeger, C. P., & Pfleeger, S. L. (2006) Security in Computing (4th ed.). Prentice Hall.

8. Shrinath, B. (1997) "Information Security in Banks." Journal of Financial Crime, 5(1), 65–71.

9. Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004) "Consumer acceptance of online banking: an extension of the technology acceptance model." Internet Research, 14(3), 224–235.

10. Rončević, A. (2006) "Nove usluge bankarskoga sektora: razvitak samoposlužnoga bankarstva u Hrvatskoj." Ekonomski pregled, 57(11), 753-777.

11. Singh, J. (2012) "SCENARIO OF E-BANKING IN TODAY'S LIFE-A Survey." International Journal of Computing & Business Research.

12. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) "Offline and online banking – where to draw the line when building trust in e-banking?." International Journal of Bank Marketing, 28(1), 27–46.