JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2016 March Volume 5 Number 3
http://dx.doi.org/10.9770/jssi.2016.5.3(9)

ELECTRONIC BANKING SECURITY ANDCUSTOMER SATISFACTION IN COMMERCIAL BANKS

Jaroslav Belás[1], Michal Korauš[2], Felix Kombo[3], Anton Korauš[4]

[1,3] Tomas Bata University in Zlín, Fakulty of Management and Economics, Mostní 5139, 760 01 Zlín, Czech Republic
[2,4] Paneuropean University in Bratislava, Faculty of Economics and Entrepreneurship, Tematinská 10, 80000 Bratislava

E-mails: [1]belas111@gmail.com ; [2]felixkombo@gmail.com; [3]michalkoraus@gmail.com; [4]akoraus@gmail.com

Received 15 November 2015; accepted 10 Februrary 2016

Abstract. The aim of this article is to examine the selected attributes of commercial banks security in relation to customer satisfaction. We focused on electronic banking products as these represent a significant segment of today's bank activities. We compared the opinions of different social groups (men and women, university educated respondents and the others, respondents under the age of 35 and the elders). Our empirical research in the banking sector of Slovakia showed that only 71.96% of the respondents think their bank takes proper care over their money. Electronic forms of banking are used by more than 90% of the respondents, particularly by university educated ones. The trust in security of electronic payments was found to be at quite a low level of 78.19%. At the same time, 12.77% of the respondents declared they had been a target for hackers, men being a more frequent target.

Keywords: Commercial Banks, Bank security, Customer Satisfaction, Electronic Banking, Internet Banking

Reference to this paper should be made as follows: Belás, J.; Korauš, M.; Kombo, F.; Korauš. A. 2016. Electronic banking security and customer satisfaction and in commercial banks, *Journal of Security and Sustainability Issues* 5(3): 411–422.
DOI: http://dx.doi.org/10.9770/jssi.2016.5.3(9)

JEL Classifications: G21

1. Introduction

An essential determinant of efficient and stable banking is trustworthiness. It is due to the fact that this sector transports scarce financial capital for its optimal utilisation thus it exists only if there is a sufficient number of economic subjects willing to deposit their surpluses in banks and at the same time a sufficient number of subjects relying on banks in case of money deficit. In this context it can be stated that a bank trades mainly with the trust of their clients.

Security is a significant issue in commercial bank management and is connected to a large number of bank activities. Ensuring security of banking is determined by various factors. Commercial bank security is a complex system including many activities, e.g. capital management in the context of credit, market and operational risks (i.e. capital adequacy management) etc.

Process security is focused on operational risk defined as a risk of loss resulting from internal processes or human capital failure or from external conditions (Polouček et al., 2013; Peker et al. 2014; Grubicka, Matuska 2015)

Physical security is linked to protection of cash in bank branches and ATMs. The system security includes all internal and external processes realised by informational system.

In this context, security of individual customers´ deposits (managing the liquidity of a commercial bank) and their payments is crucial. Security of customers´ deposits is the key factor of success for banks as exactly this factor heavily influences acquisition, retention or loss of customers. For this reason, it is vital for a commercial bank as a business unit to undertake such measures to ensure a proper and efficient protection of customers´ deposits.

The current situation demands from commercial banks to pay extraordinary attention to electronic banking security. Compliance with consumers' needs and requirements (Bilan, 2013), comprehensive customer care and bank customers' satisfaction is currently in the centre of attention of researchers and bankers, as it represents an important marketing variable for most companies, especially those working at highly competitive markets. (Belás and Demjan, 2014) Researchers are trying to find the main determinants for bank customer satisfaction and examine these issues from various perspectives (Belás et al., 2015; Chocholáková et al., 2015; Doležal et al., 2015; Kombo, 2015; Paulík et al., 2015).

In this article, we examine the electronic banking security in the context of customer satisfaction.

2. Title of the chapter

The fast development of Information and Communication Technologies (ICT) over the past few years has led to a body of innovations in the banking sector, being electronic banking probably the most significant one. This new distributional channel offers various opportunities in the field of new financial products development and their distribution to clients through the Internet. Better technology, more distributional channels and their higher flexibility brings substantial effects in the bank products quality and after all, in higher levels of satisfying customer needs. (Sysáková and Šlahor, 2010)

According to Polouček et al. (2013), electronic banking can be defined as providing bank products and services to customers via electronic channels. The utilisation of these channels has underlined the essential role of bank Security as the Internet environment is more sensitive to system attacks. (Koskosas, 2011; Dhillon and Torkzadeh, 2006). Koskosas (2011) declares electronic banking represents huge advantages for customers due to the simplicity and transactional costs reduction. Not less important, it also comes up with new challenges for banks in the financial systems Security.

The above mentioned development of ICT has changed the view of banks on their performance and activities and also the way consumers deal with their banks. (Eriksson, Kerem and Nilsson, 2008; Sayar and Wolfe, 2007)

Currently, commercial banks intensively use the Internet and offer their services through the Internet to their clients. Internet banking can be defined as providing banking products and services via computer network (the Internet).

Customers using Internet banking have a non-stop access to their accounts, they can make payments whenever and wherever they are willing to, display the bank statement to a transaction, pay out their debts and realise many more bank transactions electronically via webpages of their bank. (Yoon and a Steege, 2013; Yoona and Occeña, 2014)

From the point of view of a commercial bank, Pikkarainen, Pikkarainen, Karjaluoto, and Pahnila (2004) state two main reasons for development of Internet banking: firstly , the reduction of costs compared to traditional distributional channels; secondly, getting the branch network leaner by decreasing number of branches.

Internet banking has created an alternative to a traditional branch visit and the usage of this distributional channel has been growing since its introduction. Not even 15 million people used Internet in 1993 (0.3% of the world population), whereas this number had increased to 3 billion users in 2014 (40.4% of the world population). The overall population growth was in decline in the same period, from 1.47% to 1.14% annually. More details can be found in Table 1.

Table 1. The growth of the world population and the Internet penetration

Year	Number of Internet users	Annual growth of number of Internet users	The world population	Annual growth of the world population	The penetration of Internet among the world population (%)
2014	2 925 249 355	7.85%	7 243 784 121	1.14%	40.4%
2013	2 712 239 573	7.99%	7 162 119 430	1.16%	37.9%
2012	2 511 615 523	10.52%	7 080 072 420	1.17%	35.5%
2011	2 272 463 038	11.71%	6 997 998 760	1.18%	32.5%
2010	2 034 259 368	16.09%	6 916 183 480	1.19%	29.4%
2009	1 752 333 178	12.18%	6 834 721 930	1.20%	25.6%
2008	1 562 067 594	13.77%	6 753 649 230	1.21%	23.1%
2007	1 373 040 542	18.62%	6 673 105 940	1.21%	20.6%
2006	1 157 500 065	12.41%	6 593 227 980	1.21%	17.6%
2005	1 029 717 906	13.15%	6 514 094 610	1.22%	15.8%
2004	910 060 180	16.89%	6 435 705 600	1.22%	14.1%
2003	778 555 680	17.49%	6 357 991 750	1.23%	12.2%
2002	662 663 600	32.37%	6 280 853 820	1.24%	10.6%
2001	500 609 240	21.09%	6 204 147 030	1.25%	8.1%
2000	413 425 190	47.20%	6 127 700 430	1.26%	6.7%
1999	280 866 670	49.38%	6 051 478 010	1.27%	4.6%
1998	188 023 930	55.70%	5 975 303 660	1.30%	3.1%
1997	120 758 310	55.95%	5 898 688 340	1.33%	2.0%
1996	77 433 860	72.69%	5 821 016 750	1.38%	1.3%
1995	44 838 900	76.15%	5 741 822 410	1.43%	0.8%
1994	25 454 590	79.74%	5 661 086 350	1.47%	0.4%
1993	14 161 570		5 578 865 110		0.3%

Source: Internet live stats, (2014)

In 2014, the penetration of Internet grew by most in the countries of Africa, namely by 17% in Eritrea, Burundi and Nigeria. Only 2% of the population have access to Internet in these countries. The lowest growth rate was recorded in developed countries, such as Sweden. Norway, Iceland where the penetration is already higher than 90%. However, the world´s highest penetration is on Bermuda Islands (97.75%), Qatar (96.65%) and Bahrain (96.53%).

As Slovakia is among countries with the highest Internet penetration in the world, the pace of penetration growth was slower than the world´s average. The statistics is based on Eurostat surveying of individuals who were online at least once in the last 12 months regardless if it was a computer or a mobile connection. For more details, see Table 2.

Table 2. The growth of the Slovak population and the Internet penetration

Year	Number of Internet users	Annual growth of number of Internet users	Slovak population	Annual growth of the Slovak population	The penetration of Internet among Slovak population (%)
2014	4 495 238	2.57%	5 415 949	0.09%	83.0%
2013	4 382 777	1.37%	5 410 836	0.12%	81.0%
2012	4 323 458	2.79%	5 404 322	0.22%	80.0%
2011	4 206 108	-1.23%	5 392 446	0.04%	78.0%
2010	4 258 424	5.49%	5 390 410	0.15%	79.0%
2009	4 036 801	5.76%	5 382 401	0.12%	75.0%
2008	3 817 005	14.58%	5 376 064	0.05%	71.0%
2007	3 331 372	10.72%	5 373 180	0.00%	62.0%
2006	3 008 840	1.82%	5 372 928	0.00%	56.0%
2005	2 954 977	3.79%	5 372 685	0.02%	55.0%
2004	2 847 094		5 371 875		53.0%

Source: Internet live stats, (2014)

Commercial banks have started to invest in Internet banking development not only to come up with an innovative way to boost the customer comfort, but also to reduce its own costs and increase its profitability. Strong competition has forced banks to search for new profitable areas where to expand. Internet banking is a profitable strategy for the newcomers in the banking sector. (Anderloni, Llewellyn, and Schmidt, 2009)

Electronic banking utilisation is closely connected to the customers´ perception of security which has its impact on customer attitudes and behaviour (Grabner-Krauter and Faullant, 2008). A perceived lack of Security is defined as a potential loss caused by a fraud or Internet banking hacking (Leeh, 2009; Featherman and Pavlou, 2003). Because of that, Security and privacy are stated as two basic determinants of customer trust in electronic banking (Kruck, Gottovi, Moghadami, Broom, and Forcht, 2002; Flavián and Guinalíu, 2006).

Customer satisfaction should be perceived as the basis of the financial performance of a bank. It is probable that satisfied customers will continue purchasing its products or even recommend this bank to other potential clients (Belás and Gabčová, 2014). Thus customer satisfaction with electronic banking could be of significant importance.

According to Nochai & Nochai (2013), Novickytė & Pedroja (2015), high quality Internet banking can increase customer satisfaction substantially as it offers access to a large scale of financial transactions. Most authors agree on these main indicators of customer satisfaction with Internet banking: ability to react, reliability, competences, data protection. When Internet banking is utilised by a large part of clients, banks have to develop strategies of ensuring customers´ trust in the quality of technology and functionality. The authors determined several basic attributes of customer satisfaction with Internet banking. Firstly, *reliability*, defined as a real time proper service providing and a fair charging for that. Secondly, *transaction efficiency*, defined as a solid accessibility of Internet banking without a big effort and additional costs connected to simplicity of using available information. The third attribute is *customer support* including the pre-sale and the post-sale support convincing customers they are treated well from the side of their bank. The fourth is *service protection* which means protecting personal and sensitive data, transactions and keeping bank secrecy. *User-friendliness* is the fifth attribute defined as simplicity to access Internet banking and keeping URL shortcuts and addresses simple. The next one is *performance,* i.e. proper functionality of Internet banking and the last attribute is *service content* defined as a need for a complex scale of services included in Internet banking.

Chu, Lee and Chao (2012) tested the relations among service quality, customer satisfaction, trust and loyalty in the context of electronic banking. Authors declare that if e-banks want to have strong relationships with clients, the essential factor is high quality of e-banking services which can have a direct impact on customer trust, satisfaction and loyalty.

Also Marimon, Yaya and Fa (2012) argue there is a direct relation between service quality and customer loyalty in electronic trade. Effectiveness is the most important determinant of customer loyalty, whereas system accessibility and privacy protection were found to have a lower impact. Effectiveness means customers can easily find everything needed, transactions are realised fast, information is well organised, there is a fast Internet connection and user-friendliness.

Chen, Hsiap and Hwang (2012) created an IBCS model (Internet Banking Customer Satisfaction) compound of six essential parts: content, accuracy, format, simplicity of use, timeliness and Security. This model emphasised that clients perceive sensitively the Internet Security. The study also found that content and format drive the highest costs what determines their crucial role in the IBCS model. The relative importance of other factors was as follows: accuracy, timeliness, user-friendliness and security. The possible explanation is that content, format, accuracy and timeliness are important requirements for giving access to private financial information via Internet banking. User-friendliness and security are other key areas by investing in which banks can attract customers to use e-services. Customers tend to have higher expectations as for user-friendly interface and Internet transactions security.

Hoffmann and Birnbrich (2012) examined security attributes of electronic banking. The aim of their research was to describe conceptual and empirical relations among bank activities in the field of protection against third party attacks, customer relationship management quality and customer loyalty. The authors declare security is crucial and is getting even more important in the current banking sector. The fraud prevention has become one of the priorities of banks, customers and even politicians as bank frauds harm both banks and customers. The results showed there is a positive relation between trustworthiness of a bank, its skills in the field of fraud prevention and customer relationship management quality. After all, customer relationship management quality has a positive influence on customer loyalty.

Regarding the differences between younger and older customers, research shows the older ones have better knowledge about security measures of banks focused on fraud prevention. At the same time, the positive impact of this awareness on the customer relations quality is less significant in the group of older clients. The possible reason could be a higher level of scepticism of older clients regarding the efficiency of the above mentioned measures. Fraud prevention is vital in customer relationship management quality for all customers regardless their education and income levels.

3. Research objective, methodology and data

The aim of the article was to examine selected attributes of commercial bank security in relation to customer satisfaction. We focused on products of electronic banking which represent a significant segment for the current banks. We compared the opinions of different social groups (men and women, university educated respondents and the others, respondents under the age of 35 and the elders).

Own research was conducted via a questionnaire survey in Slovakia in 2015. 321 respondents were reached, of which 61.37% were men and 38.63% were women. Regarding the age structure, 37.69 % of respondents were 18-30 years old, 55.76% of respondents were 31-62 years old and 6.54% of respondents were above the age of 62. The educational structure was as follows: 67.60% had a university degree, 27.41% had secondary education, and 4.98% had primary education. The random sampling method was used and the questionnaire was available online at http://www.iankety.sk/dotaznik/327968727/.

In our research, we set 5 scientific hypotheses using qualified estimation:

H1: Bank customers in Slovakia show high levels of trust in the accuracy of bank processes managing their money. More than 70% of clients believe their bank take a proper care of their money. In this area there are no statistically significant differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders.

H2: The intensity of electronic payments methods usage is high in Slovakia. More than 75% of respondents use electronic forms of banking. There are no statistically significant differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders in this area.

H3: More than 80% of Slovak bank clients believe the payments via electronic banking are safe. There do not exist any statistically significant differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders in this area.

H4: The level of Slovak bank customers´ trust in online banking security is generally high. More than 75% of clients rely on online banking security measures applied by their banks. In this area there are no statistically significant differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders.

H5: Bank customers in Slovakia have only minimal experience with hacker attacks: less then 20% have such experience. The differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders are not statistically significant in this area.

The above mentioned hypotheses were validated by Pearson statistics. The significance level (α) was estimated at 0.05. To calculate p-value using the χ^2goodness of fit test we used an online calculator available at: http://www.socscistatistics.com/tests/chisquare2/Default2.aspx. To examine the differences between the selected social groups by z-test methodology we used an online calculator available at: http://www.socscistatistics.com/tests/ztest/Default2.aspx.).

Table 3 presents the research results regarding the customers´ belief that their bank takes a proper care of their money.

Table 3. Levels of customers´ belief in their bank taking a proper care of their money according to selected social groups

Do you believe that your bank takes a proper care of your money?	Men (M) in (%)	Women (W) in (%)	University degree (UD) in (%)	Others (O) in (%)	Under 35 (-35) in (%)	Above 35 (+35) in (%)	p-value*** M/W UD/O -35/35+
1. Yes	70.56	74.19	71.89	72.11	71.08	72.90	0.4777 0.9681 0.7188
2. No	29.44	25.81	28.11	27.89	28.92	27.10	0.4777 0.9681 0.7188****
χ^2 *p-value*	0.4984* 0.4802**		0.0018 0.9664		0.1314 0.7170		

Source: own research and calculation

Notes: *χ^2comparing the responses of men and women in general, ** p-value comparing the responses of men and women in general, *** p-value using the z-test methodology, **** in case of questions with only two possible answers, p-values are identical for both answers and thus will not be calculated in the subsequent sections. P-values calculated by χ^2 test and z-test tend to be at similar levels.

The results showed in Table 3 confirmed the first part of H1 as the overall level of belief was higher than 70% and also the levels of belief in the selected social groups were in every case higher than 70 %. The test criteria (χ^2 and p-value) confirmed the second part of H1 as well. We did not find any statistically significant differences between men and women, university educated respondents and the others, respondents under the age of 35 and the elders in the question of trustworthiness of Slovak banks. *H1 was confirmed*.

The results regarding the intensity of usage of electronic banking in Slovakia are introduced in Table 4. These results show the electronic forms of banking are utilised by more than 90% of respondents what confirms the first part of H2.

The values of the test criteria (χ^2 and p-value) partially confirmed the second part of H2. We found no statistically significant differences between men and women and between the respondents under the age of 35 and the elders. On the other hand, there were statistically significant differences between university educated respondents and the others in the intensity of electronic banking usage (p-value = 0.0040). P-value of z-test showed that respondents with a university degree use electronic forms of payments more often than other respondents (p-value = 0.0041). *H2 was partially confirmed*.

Table 4. Levels of intensity of electronic forms of payments usage according to selected social groups

Do you use electronic forms of payments?	M in (%)	W in (%)	UD in (%)	O in (%)	-35 in (%)	+35 in (%)	p-value*** M/W UD/O -35/35+
1. Yes	91.37	92.74	94.93	85.58	94.58	89.03	0.6599 0.0041 0.0688
2. No	8.63	7.26	5.07	14.42	5.42	10.97	
χ^2 *p-value*	0.1923 0.6610		8.2641 0.0040		*3.3122* *0.0688*		

Source: own research and calculation

Table 5 contains the research results regarding the customers´ evaluation of electronic payment security.

Table 5. Evaluation of electronic payments security by selected social groups

Do you believe that payments via electronic banking are safe?	M in (%)	W in (%)	UD in (%)	O in (%)	-35 in (%)	+35 in (%)	p-value*** M/W UD/O -35/35+
1. Yes	80.71	74.19	80.18	74.04	81.33	74.84	0.1676 0.2113 0.1585
2. No	19.29	25.81	19.82	25.96	18.67	25.16	
χ^2 *p-value*	0.4689 0.4935		1.6507 0.1989		2.0129 0.1560		

Source: own research and calculation

The levels of trust in electronic payments security differ among the selected social groups from 74.19% (women) to 81.33% (respondents under 35). The overall trust in electronic payments security was at 78.19% thus the first part of H3 was not confirmed. However, the second part of H3 could be accepted as we found no statistically significant differences between men and women, university educated respondents and the others and respondents under the age of 35 and the elders. All in all, *H3 was partially confirmed*.

In Table 6 we display the customers´ evaluation of banks´ security measures. The first part of H4 could be accepted: 83.13% of respondents rely on the security measures applied by their bank in the area of online banking. At the same time, the second part of H4 was proved as there were no statistically significant differences between men and women, university educated respondents and the others and respondents under the age of 35 and the elders in the question of evaluation of online banking security measures. To sum up, *H4 was confirmed*.

Table 6. Customers´ evaluation of the security measures applied by banks from the point of view of selected social groups

Do you rely on the security measures of your bank in online banking?	M in (%)	W in (%)	UD in (%)	O in (%)	-35 in (%)	+35 in (%)	p-value*** M/W UD/O -35/35+
1. Yes	83.76	82.26	85.71	77.88	83.13	83.23	0.7263 0.0784 0.9840
2. No	16.24	17.74	14.29	22.12	16.87	16.77	
χ^2 *p-value*	0.1221 0.7268		3.0802 0.0793		0.0005 0.9822		

Source: own research and calculation

Moving on, Table 7 presents the research results in the question of customers having experience with hacking attacks.

Table 7 Levels of customers´ experience with hacking attacks according to selected social groups

Have you ever experienced a hacking attack or a bank fraud?	M in (%)	W in (%)	UD in (%)	O in (%)	-35 in (%)	+35 in (%)	p-value*** M/W UD/O -35/35+
1. Yes	17.77	4.84	15.21	7.69	13.25	12.26	**0.0007** 0.0588 0.7872
2. No	82.23	95.16	84.79	92.31	86.75	87.74	
χ^2 *p-value*	**11.4156** **0.0007**		3.5639 0.0591		0.0712 0.7896		

Source: own research and calculation

According to our research, 87.23% of all clients do not have any experience with hacking attacks or bank frauds. The first part of H5 was thus confirmed. Nonetheless, the second part of H5 could be accepted only partially. Although there were not any statistically significant differences between respondents with a university degree and the others and between the respondents under the age of 35 and the elders, the responses of men and women varied significantly. More men than women declared they had experienced a hacking attack or a bank fraud ($\chi^2 = 11.4156$, p-value = 0.0007). As a result, *H5 was partially confirmed*.

It is possible to view the relationship between electronic banking and bank customers´ satisfaction from different perspectives. The electronic banking security is a crucial issue in the current banking (Hoffmann and Birnbrich, 2012; Chen, Hsiao, Hwang, 2012). The quality of electronic banking can increase customer satisfaction substantially (Nochai and Nochai, 2013; Chu, Lee, and Chao, 2012). Murugiah and Akgam (2015) discovered an interesting fact within their research. They found a negative relation between customer satisfaction and bank security. The authors state that a 1% growth of bank security causes 30.3% decrease in customer satisfaction. The reasons for that are complex bureaucratic procedures, i.e. excessive documentation in case of increasing bank security. Overrated security measures (e.g. complex security certificates in Internet banking) make the communication between customers and their bank more complicated and thus deteriorate their overall satisfaction.

Survey results as for drivers of satisfaction in the Czech Republic present the fact that most clients are satisfied with the possibilities of e-banking. This answer was elected by 74.64% of respondents. In the second place, respondents were satisfied with the availability of branches (49.54%), followed by a developed network of ATMs (40.25%). The possibility of using e-banking as the most important factor of satisfaction was preferred the most by women (more than men), young people up to 30 years and clients with higher education. In the banking sector of Slovakia the most important factor of satisfaction was the possibility of using e-banking service, the second most important satisfaction determinant was the availability of bank branches and the third place was taken by developed network of ATMs. This research has shown statistically significant differences among individual social groups. The possibility of using e-banking service is more significant for younger clients and customers with higher education in Slovakia. (Belás, Cipovová, and Demjan, 2014)

Within our own research presented above, we found out only 71.96% of respondents believe their bank takes a proper care of their money. We assume that quite low level of trust is caused by a complex understanding of this question by different respondents. We assume that clients did not evaluate only the security aspects of the problem but also the economic parameters of taking care of their money (such as interest rates levels).

Moreover, our research showed more than 90% of respondents use some form of electronic banking. These results are comparable to the data in Table 2. The overall level of trust in electronic payments security was found

to be at relatively low level of 78.19%. At the same time, 12.77% of respondents stated they had experienced some kind of hacking attack or a bank fraud.

According to Furnell, Bryant and Phippen (2007), Internet currently represents the biggest threat of attacks on commercial bank clients. Clients are aware of Internet threats and know it is their duty to protect themselves against these attacks although they usually do not have sufficient knowledge to do so completely. Hackers are trying in various ways to obtain private data from bank clients in order to abuse them. Attacks on electronic banking have become more and more common over the past few years threatening mostly bank clients, their private data and financial resources.

Kaspersky Lab (2014) declares that an organised hacker gang which has attacked a hundred of banks in 30 countries all over the world (Russia, USA, Germany, China, Ukraine, Canada, Hong Kong, Taiwan, Romania, France, Spain, Norway, India, Great Britain, Poland, Pakistan, Nepal, Morocco, Iceland, Ireland, the Czech Republic, Switzerland, Brazil, Bulgaria and Australia) since 2013 has stolen more than a billion of USD. The hackers come mainly from China, Russia and Ukraine and they obtained the money via infiltration into internal systems of banks. They developed methods how to gain an access to internal systems of banks by phishing, constant monitoring of employees´ behaviour and infiltrating a malware called Carbanak. Afterwards, they were able to trace servers for security cameras what enabled them to stalk employees realising electronic payments for clients and then make cash transfers to selected accounts in China and USA. In other cases, they got into the systems of accounts management where they changed the account balances and sent the differences to their own accounts immediately. For example, they increased the balance from 1,000 USD to 10,000 USD a then they transferred the difference (9,000 USD) to their accounts. From the customer´s point of view, the account balance was kept at the same level so he/she did not even realise any fraud transaction were made via their account. Moreover, the hackers obtained money also by reprogramming ATMs from which they withdrew cash afterwards. They operated in smaller amounts not to attract the attention. From every single of the 30 hacked banks, they stole at most 10 million USD and the average attack last two-four months. Kaspersky Lab also states that currently, the hackers are trying to expand the attacks in the countries of Central and Eastern Europe, the Middle East, Asia and Africa.

Based on the described example as a representative one, it can be opined the current situation demands a permanent process of software programmes improvements. Biometric methods represent the future in the area of customer identification and authentication and there is still large space for their wider application. Despite the fact some of the biometric methods have become a standard (e.g. fingertip scanning), the opportunities of their abusage still represent security risk. It is possible to eliminate this risk by applying a combination of simpler and less expensive biometric methods. Doing so, the reliability of these methods would increase significantly and at the same time, it would optimise the costs of new technologies implementation for commercial banks.

The massive development of ICT, particularly mobile devices in the past few years has driven the need for innovative bank applications usable in smart phones and tablets interfaces. The character of such applications can vary substantially, from the QR code scanner, to contactless mobile payments via NFC technologies, to searching for the nearest ATM or branch. The future will probably bring the combination of bank applications and biometric methods what would enhance the functionality of applications and in the meantime, it would make the clients´ access to bank products and services easier. New trends in this area are also personalised applications customised according to specific needs and interests of a single client.

The protection against hacking attacks and frauds is not only the issue of commercial banks; it should also be conducted by clients themselves as they are cyber attack targets most often. The protection from the clients´ perspective means an optimal choice of antivirus, antiphishing, antispam, antispyware, firewall, private zones detection and antithreft diagnostics software programmes. The proper protection also includes regular updates of the above mentioned programmes and checking the account balance and transactions.

Conclusions

The banking sector has vastly developed electronic communication with their clients in the current years. This process was driven mostly by an increase of number of Internet users. Improving electronic distributional channels of banks is on one hand connected to better availability of products and services for clients; on the other hand it also leads to a potential risk increase. This risk is represented by a possible private data theft, then access of hackers to clients´ accounts and in the end by stealing the money from clients.

The electronic banking security is a challenge for current bank management all over the world what has been confirmed also by numerous successful attacks on commercial banks and their customers.

Our own research has shown more than 70 % of respondents in Slovakia believe their bank takes a proper care of their money. We also found electronic forms of banking are utilised by more than 90 % of clients, most frequently by university educated ones. The trust in the payments via electronic banking is at average levels as there appear hacking attacks and bank frauds from time to time.

The results thus confirmed that security issues currently influencing also customer satisfaction and loyalty have become a crucial element of bank activities. Commercial banks which base their business mostly on their own trustworthiness are forced to constantly improve applied technologies and protect themselves against potential hacking attacks. A vital component of this is also the customers´ awareness of security measures and threats. It cannot be declared that banks in Slovakia do not realise such activities but resulting from our research we opine the banks do not do it in a correct way. If they did, we assume the level of trust in electronic payments security would be at higher levels.

Acknowledgments

The authors are thankful to the Internal Grant Agency of FaME TBU No. 000/IGA/FaME/2015: The possibilities of the financial performance growth for commercial banks in the context of the credit risk of SME and the customer satisfaction, for financial support to carry out this research.

References

Anderloni, L.; Llewellyn, D. T.; Schmidt, R. 2009. *Financial Innovation in Retail and Corporate Banking.* London: Edward Elgar Publishing.

Belás, J.; Chochoľáková, A.; Gabčová, L. 2015. Satisfaction and loyalty of banking customers: a gender approach, *Economics and Sociology*, Vol. 8, No1, pp. 176–188. DOI: 10.14254/2071- 789X.2015/8-1/14

Belás, J.; Cipovová, E.; Demjan, V. 2014. Current trends in area of satisfaction of banks´clients in the Czech Republic and Slovakia, *Transformation in Business & Economics,* Vol. 13, No 3(33), pp. 219–234.

Belás, J.; Demjan, V. 2014. Bank customers satisfaction: case studies from Czech Republic. *Actual problems of economics,* No. 12(162), pp. 315–323.

Belás, J.; Gabčová, L. 2014. Reasons for satisfaction and dissatisfaction of bank customers. Study from Slovakia and the Czech republic, *International Journal of Entrepreneurial Knowledge.* Issue1, Vo.2, pp. 4–13. DOI: 10.15759/ijek/2014/v2i1/53759

Bilan, Y. 2013. Sustainable development of a company: Building of new level relationship with the consumers of XXI. Century, *Amfiteatru Economic, 15*, 687–701.

Chochoľáková, A.; Gabčová, L.; Belás, J.; Sipko, J. 2015. Bank Customers' Satisfaction, Customers' Loyalty and Additional Purchases of Banking Products and Services. A Case Study from the Czech Republic, *Economics and Sociology*, Vol. 8, No 3, pp. 82–94. DOI: 10.14254/2071-789X.2015/8-3/6

Dhillon, G.; Torkzadeh, G. 2006. Values-focused assessment of information system security in Organizations, *Information Systems Journal,* Vol. 16, No. 3, pp. 293–314.

Doležal, J.; Šnajdr, J.; Belás, J.; Vincúrová, Z. 2015. Model of the loan process in the context of unrealized income and loss prevention, *Journal of International Studies*, Vol. 8, No 1, 2015, pp. 91– 106. DOI: 10.14254/2071-8330.2015/8-1/8

Eriksson, K.; Kerem, K.; Nilsson, D. 2008. The adoption of commercial innovations in the former Central and Eastern European markets: The case of internet banking in Estonia, *International Journal of Bank Marketing*, Vol. 26, No. 3, pp. 154–169. DOI: 10.1108/02652320810864634

Featherman, M. S.; Pavlou, P. A. 2003. Predicting e-services adoption: A perceivedrisk facets perspective, *International Journal of Human-Computer Studies,* Vol. 59, No. 4, pp. 451–474.

Flavián, C.; Guinaliu, M. 2006. Consumer trust, perceived security, and privacy policy: three basic elements of loyalty to a web site, *Industrial Management & Data Systems,* Vol. 106, No. 5/6, pp. 601–620.

Furnell, S.; Bryant, P.; Phippen, A. 2007. Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* Vol. 26, No. 5, pp. 410–417.

Grabner-Krauter, S.; Faullant, R. 2008. Consumer acceptance of internet banking: the influence of internet trust. *International Journal of Bank Marketing,* Vol. 26, No. 7, pp. 483–504. DOI: 10.1108/02652320810913855

Hoffmann, A. O. I.; Birnbrich, C. 2012. The impact of fraud prevention on bank-customer relationship, *International Journal of Bank Marketing*, 30(5): 390–407. DOI: 10.1108/02652321211247435

Grubicka, J.; Matuska, E. 2015. Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence, *Entrepreneurship and Sustainability Issues* 2(4):188–197.

Chen, R. F.; Hsiao, J. L.; Hwang, H. G. 2012. Measuring customer satisfaction of Internet banking in Taiwan: scale development and validation. *Total Quality Management*, 23(7): 749–767.

Chu, P. Y.; Lee, G. Y.; Chao, Y. 2012. Service quality, customer satisfaction, customer trust, and loyalty in an e-banking context. *Social behavior and personality*, 40(8): 1271–1284.

Internet live stats. 2014. *Internet Users.* [online] [cit: 2015-7-13] Avalable from: http://www.internetlivestats.com/internet-users/

Lee, M. 2009. Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit, *Electronic Commerce Research and Applications,* Vol. 8, No. 3, pp. 130–141.

Kaspersky Lab 2014. *The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide.* Avalable from:http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide

Kombo, F. (2015). Customer satisfaction in the Kenyan banking industry, *Journal of International Studies*, Vol. 8, No 2, 2015, pp. 174–186. DOI: 10.14254/2071-8330.2015/8-2/15

Koskosas, I. 2011. E-banking security: A communication perspective in Risk management. *Palgrave Macmillan*, Vol. 13, pp. 81–99.

Kruck, S. E.; Gottovi, D.; Moghadami, F.; Broom, R.; Forcht, K. A. 2002. Protecting personal privacy on the internet, *Information Management & Computer Security,* Vol. 10, No. 2, pp. 77–84.

Marimon, F.; Yaya, L. H. P.; Fa, M. C. 2012. Impact of e-Quality and service recovery on loyalty: A study of e-banking in Spain, *Total Quality Management*, 23(7): 769–787.

Murugiah, L.; Akgam, H. A. 2015. Study of Customer Satisfaction in the Banking Sector in Libya, *Journal of Economics, Business and Management*, Vol. 3, No. 7 pp. 674–677.

Nochai, R.; Nochai, T. 2013. The impact of Internet Banking Service on Customer Satisfaction on Thailand: A Case Study in Bangkok. *International Journal of Humanities and Management Sciences,* 10(1): 2320–2344.

Novickytė, L.; Pedroja, G. 2015. Assessment of mergers and acquisitions in banking on small open economy as sustainable domestic financial system development, *Economics and Sociology*, Vol. 8, No 1, pp. 71–87. DOI: 10.14254/2071- 789X.2015/8-1/6

Paulík, J.; Kombo, F.; Ključnikov, A. 2015. CSR as a driver of satisfaction and loyalty in commercial banks in the Czech Republic, *Journal of International Studies*, Vol. 8, No 3, 2015, pp. 112–127. DOI: 10.14254/2071-8330.2015/8-3/9

Peker, S.; Tvaronavičienė, M.; Aktan, B. 2014. Sustainable risk management: fuzzy approach to volatility and application on FTSE 100 index, *Entrepreneurship and Sustainabillity Issues* 2(1): 30-36. DOI: http://dx.doi.org/10.9770/jesi.2014.2.1(4)

Pikkarainen, T.; Pikkarainen, K.; Karjakuoto, H.; Pahnila, S. 2004. Consumer acceptance of online banking: An extension of the technology acceptance model, *Internet Research*, Vol. 14, No. 3, pp. 224–235.

Polouček, S. et al., 2013. *Bankovnictví.* 2. vydání. Praha: C. H. Beck.

Sayar, C.; Wolfe, S. 2007. Internet banking market performance: Turkey versus the UK, *International Journal of Bank Marketing,* Vol. 25, pp. 122–141. DOI: 10.1108/02652320710739841

Sysáková, V.; Šlahor, L. 2010. *Peniaze a bankovníctvo.* Bratislava: Kartprint.

Yoon, H.; Occena, L. 2014. Impacts of customers ' perceptions on internet banking use with a smart phone, *Journal of Computer Information Systems,* Vol. 54, No. 3, pp. 1–9.

Yoon, H. S.; Steege, L. M. 2013. Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use, *Computers in Human Behavior,* Vol. 29, No. 3, pp. 12–29.