DOI: 10.1515/orga-2016-0022

User Experience with Security Elements in Internet and Mobile Banking[1*]

Aleksandra Svilar[1], Jože Zupančič[2]

[1] Nova Ljubljanska banka, d.d., Trg republike 2, 1000 Ljubljana, Slovenia
Aleksandra.Svilar@yahoo.com

[2] University of Łódź, School of Economy and Sociology, 90-255 Łódź, 3/5 POW Street, Poland and
University of Maribor, Faculty of Organizational Science, Kidričeva 55a, 4000 Kranj, Slovenia
joze.zupancic@fov.uni-mb.si

Background/Purpose: Maintaining a balance between security and a positive user experience in mobile and Internet banking is becoming increasingly difficult for the providers of banking services. The goal of our research is to analyse user opinions about the current situation: how users perceive security and how the authentication methods they are using affect user experience.
Methodology: Data were collected using an online survey among the users of 15 banks operating in Slovenia, and statistical methods were applied to analyse them. Results of the users' study were evaluated and commented by a limited number of interviewed banking security experts.
Results: The results indicate that the use of mobile banking in Slovenia is relatively low, as only 30 percent of respondents use mobile banking along with Internet banking. Slovenian users perceive security to be the most important factor in mobile and online banking, closely followed by reliability. We also verified whether the users knew which authentication methods they were using: 69% of respondents selected the correct authentication method. The opinion of 88% of respondents was that authentication methods do not limit them when using mobile and Internet banking. Results of the study of user's opinions did not surprise the experts, although experts' views about the balance between security and usability diverged considerably.
Conclusion: Our results indicate that, in Slovenia, users of the Internet and mobile banking services regard security to be the most important element in mobile or Internet banking and find user experience less important while they absolutely do want products that are easy to use.

Keywords: *Internet banking; mobile banking; security; user experience*

1 Introduction

Internet and mobile banking are part of a broader range of banking services, under the term of "electronic banking". The ever wider use of mobile commerce has led to the development of various applications that offer the user easy access to information and made it possible for the user to carry out various actions at all times. The usefulness of the product and the user experience are becoming increasingly important. The UXPA (User Experience Professional Association), referring to the international standard ISO 9241-11, defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"[1]. The ISO 9241-210 international standard defines customer experience as "a person's perceptions and responses that result from the use or anticipated use of

1* This article is the revised and expanded text of the paper presented at 35th International Conference on Organizational Science Development "Sustainable Organization" (http://fov.uni-mb.si/konferenca/archive-of-past-conferences/2016/), which was held 16th–18th March 2016 in Portorož, Slovenia.

1 Source: *http://uxpa.org/resources/definitions-user-experience-and-usability*, 2015

Received: 29th May 2016; revised: 17th August 2016; accepted: 11th October 2016

a product, system or service[2]". The definition further states that "user experience (UX) involves a person's emotions about using a particular product, system or service. User experience highlights the experiential, affective, meaningful and valuable aspects of human-computer interaction and product ownership. Additionally, it includes a person's perceptions of the practical aspects such as utility, ease of use and efficiency of the system."

With the development and availability of different applications, users are becoming increasingly demanding regarding Internet and mobile banking. Thus, the search for the best possible user experience is becoming more important. One of the greatest obstacles to better user experience is the need to provide and maintain a high level of security and privacy in Internet and mobile banking.

Internet and mobile banking applications provide a particularly interesting target for various abuses and intrusions. Therefore, banks must pay special attention to the security of these applications. In most cases, the provision of security affects the ease of use of an application, which is one of the main criteria of customer satisfaction (Liao & Cheung, 2008; Lee, Moon, Kim & Yi, 2015).

Historically, the majority of Slovenian banks have tended to use security features that provided maximum security. These security features are, in most cases, quite rigid and restrict the users from conducting transactions. Complex and demanding security features otherwise may give good protection against external intrusions, while severely hindering users during normal communication via the Internet or mobile bank, and thereby jeopardize internal security. Complex security procedures promote poor security habits of users, such as writing down passwords and procedures to access their accounts, which may invalidate the security measures prescribed to the users by the bank (French 2012). Ensuring a balance between the security of Internet and mobile banking applications and a better user experience is becoming an increasingly demanding task for providers of Internet and mobile banking.

Therefore, we decided to investigate how the security features applied by banks affect the user experience. In the literature, we can find numerous studies that investigated user satisfaction in a broader context, but only a few studies deal with the impact of applied security features on customer satisfaction. Therefore, we focused on the security aspects of using Internet and mobile banking.

The purpose of this paper is to explore how Internet and mobile banking users in Slovenia perceive the security provided by the security features used by Slovenian banks. Does the use of these elements interfere with or restrict the use of Internet and mobile banking? How important is security to users of Internet and mobile banking?

2 Literature review

In recent years, a growing number of institutions have become engaged in Internet and mobile banking security. In 2013, the European Central Bank (ECB, 2013) published a directive with 14 guidelines to ensure the security of Internet payments, with February 1, 2015 as the deadline for their introduction. The document states that the payment service provider must implement a high level of authentication for the implementation of Internet payments and for access to sensitive banking data. A high level of authentication is defined as a process of authentication that uses elements from two or more of the following three categories: something a user knows (e.g. a password), something the user has (e.g. mobile phone, smart card, etc.), and something that the user is (biometrics, such as fingerprints, retina or iris scans, etc.). With this ECB directive, banks in Europe are required to introduce additional security features that can be expected to have a mainly negative impact on the user experience.

When reviewing the literature, we found many studies conducted in different countries and in quite different ways. They examined user satisfaction with e-banking and the adoption of Internet and mobile banking from different perspectives. For example, Nasri and Cherfeddine (2012) used the information technology acceptance model (TAM) and the theory of planned behaviour (TPB) to investigate the acceptance of Internet banking in Tunisia. They emphasized that it is very important that banks develop a technology that is easy to use, while also putting great emphasis on security and privacy. Tella and Abdulmumin (2015) studied users' satisfaction with an e-payment system in a specific environment (university). Koo, Watti and Chung (2014) extended DeLone and McLean's IS success model to electronic banking, adding trust as a success variable. They tested the model by comparing Internet and mobile banking in Indonesia.

In a study of the use and acceptance of Internet banking in Pakistan, the authors similarly conclude that perceived usefulness and security have a major impact on the adoption of Internet and mobile banking; but when the users get used to the technology and begin regularly to use e-banking, their satisfaction is mostly determined by the ease of use and usefulness (Mashari et al., 2014). Liébana-Cabanillas, Muñoz-Leiva and Rejón-Guardia (2013) analyse the relationship between the main determinants of the TAM model (accessibility, user confidence, ease of use, usefulness) and satisfaction of users of Internet banking. They point out that both the usefulness and ease of access to banking applications and data - the main determinant of TAM model - directly affect customer satisfaction.

Investigating mobile banking adoption among young people (e.g. students), Akturan and Tezcan (2012) observed that perceived usefulness, social risk, performance

2 Source: https://en.wikipedia.org/wiki/User_experience, 2015

risk and potential benefit directly affect attitudes towards mobile banking. Some recent research focuses on user satisfaction, but it does not include security as one of the determinants of customer satisfaction, and focuses, for example, on the impact of accessibility, trust and ease of use on the satisfaction of Internet banking users (e.g. Liébana-Cabanillas, Muñoz- Leiva and Rejón-Guardia, 2013), or the impact of simplicity and interactivity on usability and user satisfaction (e.g. Lee et al., 2015).

The supervision of the risks of online banking is a much more important factor than providing its benefits is. Because it is much harder to provide risk-free online transaction environments than benefits for customers, online banking should look for strategies to reduce the risks to the prospective clients, which will help inspire their confidence (Lee 2009). Similar conclusions were also reached by Cheng, Lam and Yeung (2006), as they pointed out that in addition to the perception of usefulness, the perception of Internet security has a direct impact on the end use of Internet banking. In the beginning, most of these studies paid no specific attention to security and trust, but the results of their studies highlighted the issue of security. Only a few investigations have directly addressed the impact of security features on customer satisfaction.

Krol, Philippou, De Cristofaro and Sasse (2015) have studied the impact of two-level authentication on user experience in British banks. Test users have expressed much frustration about providing additional information when using online banking, in particular, they did not like to use one-time passwords (OTP) with devices (hardware token). Considering the diversity of the users' abilities, needs and preferences, they suggest that banks offer customers various options for two-level authentication. Furthermore, users complained about the number of steps required for authentication, so the authors suggested that banks carefully eliminate all the steps that do not provide real security.

The authors suggest the introduction of a number of different options for additional authentication, such as the replacement of one-time passwords on dedicated devices with SMS one-time passwords, or OTPs generated by applications on smartphones. From the user's point of view, this is interesting and desirable, but does have some drawbacks. Additional authentication can also be very expensive for the banks, because it requires the parallel maintenance of several products. In contrast, a user might be even more confused, because he or she has to make the choice of products, even though he or she might not understand what the consequences of the choice are. Moreover, not all of the proposed alternatives provide the same level of security.

Yoon and Occeña (2014) investigated the interactions between security and usability and ease of use for mobile banking. Their empirical study, which was conducted in the USA, showed that both the security and the perceived usefulness and perceived ease of use have a significant impact on the use of mobile banking: although many users perceive the risk of using e-commerce and specifically e-banking, they are willing to use these electronic channels because of their ease of use and their usability.

Banks use diverse security features and combinations of them; however, identification mechanisms are not standardized. Choubey and Choubey (2013) analysed the authentication procedures and other security features used by major banks in seven English-speaking countries. Their study revealed that banks use very different approaches to security, from simple username and password to fairly complex structures with one-time passwords generated by an external device. This diversity can be problematic for users when they want to change banks, or when they are doing business with several banks.

Therefore, these authors suggest the standardization of the security mechanisms used by banks. Regarding security, standardization would facilitate the development of interfaces that would be better protected against intrusions by phishing; it would also be easier to upgrade the standards, and to achieve better protection against different mechanisms of intrusion. Based on an analysis of identification of the mechanisms the online and mobile banking, Choubey and Choubey (2013) propose a unification of these mechanisms, to facilitate the use of banking services, and to find the optimal mechanism and ways for its standardization.

3 Methodology

Based on the literature review and Internet/mobile banking market analysis, we prepared a survey questionnaire. The first part of the questionnaire included demographic questions, and questions about respondents' habits when using online and mobile banking. Our aim is to examine how users perceive security, to what extent they are familiar with the security features they use, and how these features hinder their transactions. By analyzing what security features and the combinations thereof are provided by the banks that are active on the Slovenian market, we prepared a list of all the security elements used by the banks. Respondents were asked to specify which bank or banks they are using, what security features they use, and how these security features impact or hinder their use of Internet and mobile banking. We also compared the security features selected by respondents with security features used by their banks. Additionally, we measured users' general attitude towards mobile and online banking and any preference between the two. Nasri and Cherfeddine (2012) and Cheng, Lam and Yeung (2006) asked similar questions in their empirical research on the factors that influence the use of Internet banking.

Liao and Cheung (2008) in their analysis identified six attributes of quality service that can be mapped to online banking: usefulness, ease of use, reliability, security, re-

sponsiveness and implementation of changes. Our survey questionnaire presented these attributes to respondents and asked them to rate their importance using a five-point Likert scale.

Most of the questions in the survey questionnaire were the closed-end type. The survey was prepared via an online service. To obtain the widest possible range of responses from customers of different banks, we used e-mail and social networks such as Facebook to distribute the questionnaire; we also asked friends and acquaintances for help when communicating the questionnaire to potential respondents. The collected data were then analyzed using statistical methods.

Data provided by the users was consolidated and presented to a limited number of banking security experts. Structured interview was used to collects experts' opinions and their comments.

4 Results

One hundred-and-one (101) respondents returned a completely filled questionnaire: 15 (15%) of them did not use Internet or mobile banking and were therefore, eliminated from further analysis. Data from the remaining 86 questionnaires were further analysed. Table 1 shows the demographic data of the respondents, which illustrates the diversity of the population. For each demographic data element, except for gender, minor deviations from the overall population characteristics are evident. The age structure shows a very small percentage of the youngest and oldest respondents. Before their first employment, young people do not have much need to use banking services, while older people sometimes avoid using technology and stick with the traditional way of doing business with their banks. The educational structure of respondents reveals that very few respondents finished only primary or vocational education. Compared to the educational structure in Slovenia, published by the Statistical Office of Slovenia (SURS), a relatively larger percentage of respondents have at least

Table 1: Demographic data

Gender	male	43%
	female	57%
Age	Up to 24	1%
	25 to 34	44%
	35 to 44	24%
	45 to 54	14%
	55 to 64	13%
	65 or more	3%
Education	Elementary School	1%
	Three-year professional education	1%
	Middle School	26%
	Associate degree	34%
	University degree	29%
	Master degree, Doctorate	9%
Occupation	Student	6%
	Unemployed	6%
	Retired	8%
	Employed	64%
	Self-employed	13%
	Manager/Company owner	3%
Computer knowledge – self-assessment	Very limited	0%
	Basic	30%
	Advanced	48%
	Expert	22%

upper secondary education in comparison to the general population.

Most users of online and mobile banking come from the population of people between the completion of education and retirement: employees, self-employed and managers/business owners and the unemployed. Respondents were asked to self-assess their computing skills; none of them considered his or her skills to be very limited, almost a third of them estimated them to be basic, almost half as advanced, and a fifth of the respondents described their skills as being professional.

The respondents were customers of 14 Slovenian and one foreign bank. We asked them what security features they were using in Internet or mobile banking. Their answers were compared with the security features used by banks, which revealed that 69 percent of the respondents had chosen the correct security features. Table 2 shows that banks use a wide variety of security elements and their combinations. A similar diversity was found by a survey carried out by Choubey and Choubey (2013) in English-speaking countries.

Table 2: Security features used by Slovenian banks

Security features in Slovenian banks
Digital certificate stored on the computer, mobile phone, tablet computer, etc.) and a password (Access via browser where the digital certificate with a pre-set password is stored; this password must be entered on the bank's entry web page.)
Digital certificate on a smart card or USB key and a password (and/or a PIN code) (Digital certificate is stored on an external device, which can be connected to the computer directly via a USB port, or a reader. Access to the external device requires a PIN code and sometimes an additional password is required to access the Internet/mobile bank.)
Digital certificate on a payment card (MasterCard, Maestro, etc.) and a password (and PIN code). (Digital certificate is stored on the card's chip that connects to the computer via a reader. Access to the card requires a PIN code, and access to the bank's program an additional entry password)
Username and one-time password on a token or a payment card (hard token OTP). (On the bank's entry page, the username is entered, and a one-time password is obtained from the screen on a payment card or from the screen on a dedicated token (hard token) the has been provided by the bank. The token is a small, handheld, dedicated device that has a screen; the one-time password is displayed on the token's screen.)
Username and one-time password from the program on a smartphone (soft token OTP) (On the bank's entry page, the username is entered; a one-time password is generated by the program that has been installed on the user's smartphone by the bank and is additionally protected by a PIN code. In some cases, an additional password is required.)
Username and one-time password via SMS (SMS OTP) (On the entry web page, the username is entered; a one-time password is obtained from an SMS sent by the bank.)
Username and one-time password acquired from a portable reader and a card (hard token OTP) (On the entry page, the username is entered; a one-time password is acquired from the reader and a card provided by the bank.)
Additional security password (Additional security password intended to protect specific transactions in Internet/mobile bank (for example transferring money to a recipient who is not yet included in the user's list of recipients of payments). Internet/mobile bank requires the entry of a few characters of the password; randomly selected by the bank).
Username and password (On the bank's entry page. the username and (the whole) password that was given to the user when registering with the bank are entered. Changing the password frequently is recommended)
Username and a few characters of the password (On the entry page, the username and a few randomly selected characters from the password are entered. The password has been set for the registration with the bank. The required randomly selected characters are specified by the bank each time Internet/mobile banking is used.)

Table 3: Summary of user opinions on security and usability of Internet and Mobile Banking

Usability of authentication features	Very limiting (1)	Limiting (2)	Undecided (3)	Not limiting (4)	Not limiting at all (5)	**Average**	**Standard deviation**
Are authentication features you are using limiting you when using Internet or mobile banking?	1	2	8	29	46	4.36	0.80
Criteria of satisfaction with electronic banking	Very important (1)	Important (2)	Undecided (3)	Unimportant (4)	Very unimportant (5)	**Average**	**Standard deviation**
Accessibility – Internet/mobile bank is accessible from different devices, with different operating systems, etc.	35	14	19	7	11	2.36	1.40
Usability – services provided are useful indeed.	35	21	8	9	13	2.35	1.50
Ease of use – use is simple, intuitive.	42	20	9	5	10	2.08	1.40
Reliability– functioning reliably, with no mistakes and/or interruptions.	51	12	3	3	17	2.10	1.60
Security – well provided security for the user	56	9	4	2	15	1.97	1.50
Responsiveness – the banking program must be fast, must respond with no delays	41	21	7	7	10	2.12	1.40
Implementation of changes – Internet/mobile banking application is kept up-to-date.	17	21	32	11	5	2.60	1.10
Additional passwords	Very unnecessary (1)	Unnecessary (2)	Undecided (3)	Necessary (4)	Really necessary (5)	**Average**	**Standard deviation**
Do you think that additional passwords, requested during usage of Internet or mobile banking, while verifying certain transactions, are needed?	5	9	10	17	45	4.02	1.30
Using passwords	Strongly disagree (1)	Disagree (2)	Undecided (3)	Agree (4)	Strongly agree (5)	**Average**	**Standard deviation**
Selecting a password is easy and simple.	6	6	9	25	40	4.01	1.20
Changing the password periodically (for example every month) does not bother me.	15	12	18	17	24	3.27	1.50
I am using the same password for several applications: (Internet/mobile bank, Facebook, Twitter, etc).	34	9	15	14	14	2.59	1.50
Selecting long passwords is easy and doesn't bother me.	7	8	17	28	26	3.67	1.20
Restrictions for passwords (upper/lower case letters, digits, special characters) are not a problem.	7	9	20	22	28	3.64	1.30
I can easily remember passwords that I have selected.	10	7	20	27	22	3.51	1.30
I need too many passwords in my life.	9	3	12	16	46	4.01	1.30

Table 3: Summary of user opinions on security and usability of Internet and Mobile Banking (continued)

Usability of Internet and Mobile Banking	Strongly disagree (1)	Disagree (2)	Undecided (3)	Agree (4)	Strongly agree (5)	**Average**	**Standard deviation**
Using the Internet/Mobile Banking would enable me to accomplish my tasks more quickly.	6	2	1	8	69	4.53	1.10
Using the Internet/Mobile Banking would make it easier for me to carry out my tasks.	4	2	4	9	67	4.55	1.00
I would find the Internet/Mobile Banking useful.	4	3	0	5	74	4.65	1.00
Overall, I would find using the Internet/Mobile Banking to be advantageous.	4	2	4	11	65	4.52	1.00
Ease of Use of Internet and Mobile Banking							
Using the Internet/Mobile Banking service is easy for me.	4	3	8	32	39	4.15	1.00
I find my interaction with the use of the Internet/Mobile Banking services clear and understandable.	3	6	16	23	38	4.01	1.10
It is easy for me to become skillful at the use of the Internet/Mobile Banking services.	4	6	8	26	42	4.12	1.10
Security of Internet and Mobile Banking							
I would feel secure sending sensitive information across the Internet/Mobile Banking.	4	9	28	36	9	3.43	1.00
The Internet/Mobile Banking is a secure means through which to send sensitive information.	1	9	29	40	7	3.50	0.80
I would feel very safe providing sensitive information about myself over the Internet/Mobile Banking.	5	15	35	22	9	3.17	1.00
Overall, the Internet/Mobile Banking is a safe place to transmit sensitive information.	3	14	31	32	6	3.28	0.90
Attitude towards Internet and Mobile Banking							
Using Internet/Mobile Banking is a good idea.	5	0	2	17	62	4.52	1.00
I would say that using Internet/Mobile Banking is pleasant.	4	0	7	15	60	4.48	1.00
In my opinion, it would be desirable to use Internet/Mobile Banking.	2	2	15	28	39	4.16	1.00
In my view, using Internet/Mobile Banking is a wise idea.	4	3	13	24	42	4.13	1.10
Influences of Technology on Internet and Mobile Banking							
Advances in Internet/Mobile security technology provide for safer Internet banking.	3	1	18	23	41	4.14	1.00
Faster Internet/Mobile access speed is important for Internet banking.	2	9	17	27	31	3.88	1.10

Respondents were asked to rate items presented in the questionnaire using a five-step Likert scale. The results (number of replies, averages and standard deviation) are shown in Table 3.

Replies to the open-ended part of the questionnaire indicate that respondents think that security features do not hinder them. Respondents were also given the possibility to comment on their replies. Their comments were mainly related to time-consuming installation and lack of mobility, and to the time needed for entering multiple passwords.

Five banking security experts coming from four companies and banks (Halcom, d.d., Infinum, d.o.o., Abanka Vipa, d.d in NLB, d.d.). responded our invitation to participate in the interview. Three of them have worked in the field of electronic banking for more than 15 years, two of them were developers of e-banking applications with more than five years of experience in the area. Four of the participants had technical educational background, while one of them held a management-oriented degree. All the five were members of teams who decide about what security elements are included in the applications offered to the users by the banks.

Interviewees were also asked to rank listed e-banking security features by importance. The results of ranking are given in Table 4.

The summary of experts' opinions presented in Table 4 indicates that – on average – usability and security are considered as the most important features, followed by reliability, accessibility, ease of use, responsiveness and implementation of changes as the least important feature. In general, experts' opinion vary considerably.

At the end of the interview, we presented the experts a summary of the results of our user investigation. The results did not surprise them; their opinion was that our results give a realistic picture of users' views. They noticed the low rank of the feature *introduction of changes*, but experts' also ranked this feature as the least important of all. They criticised the age distribution of the surveyed users, since there were only of few respondents of age 24 or younger, and they remarked that the percentage of users who use e-banking services daily is relatively high. This could be attributed to the method of selection of the sample.

5 Discussion

The survey results show that the attitude of the respondents towards the Internet and mobile banking is generally positive, and they mostly agree that the use of these forms of banking is helpful. From Table 3, it is evident that the respondents regard security as a major criterion of satisfaction, followed by reliability and responsiveness. The majority of users consider additional passwords to be necessary. Regarding the usability of Internet and mobile banking, respondents mostly agree that banking applications are useful products, they are mostly easy to use, and consider it easy to learn how to use them.

Regarding the security of online and mobile banking, respondents are more cautious. In general, they see this form of banking as safe, but a large proportion of respondents are undecided. We believe that the reasons for this can be found in several facts, including the recognition that financial services are attractive to potential criminals, and fear of the unknown. Most of the average users do not understand well how the security features work and are not aware of what they can do to contribute to the greater security of Internet and mobile services that they use. Smart cards or USB keys with qualified digital certificates are used by a large majority of Slovenian banks. It is important that the user know that he or she should remove the card from the reader, or the USB key from the computer, to eliminate potential abuse via remote access.

Respondents largely agree that the use of these forms of banking is a positive thing. They also mostly agree that advances in Internet security provide secure online and mobile commerce, while they consider the Internet data transmission speed to be somewhat less important. Respondents who use both online and mobile banking were also asked which method they find more useful. Most (59%) of the respondents prefer Internet banking and 32% of them mobile banking, while 9% responded that they cannot provide an answer because they do not use either form of banking. We asked them for an opinion about why they consider one form of banking better than another; 51% of responses cited the benefit of online banking, mainly by better security and transparency, a broader range of services and better usability. A few respondents stated that they did not like smartphones or mobile banking, because they have not tried it. The preference for mobile banking was explicitly expressed by seven respondents. Nearly all of them have emphasized the fact that mobile banking is always at hand and thus more useful.

Our study has several limitations. The survey was conducted only in Slovenia on a relatively small sample of users of Internet and mobile banking. Thus, a comprehensive statistical analysis was not possible.

6 Conclusion

In the past two years, the European Central Bank raised the level of security required in Internet payments, which naturally also has an impact on Slovenian banks and on Slovenian users of online banking. The results of our study show that users in Slovenia are aware that security in online and mobile banking is the most important criterion. While 87% of respondents thought that security features used by banks operating in Slovenia mostly do not hinder usability, security is important or very important to 75% of respondents.

Reducing the number of steps involved in authenti-

Table 4: Ranking of e-banking security elements by experts

	Interview participant					
	1	**2**	**3**	**4**	**5**	**Mean**
Accessibility – e-bank is accessible form several devices, systems, etc.	1	7	2	2	6	3,6
Usability – the services offered are usable for the customers	5	5	7	4	5	5,2
Simplicity of use – use of services is simple, intuitive	4	3	3	6	2	3,6
Reliability – services are reliable, functioning is reliable, no errors and failures occur	6	4	6	5	3	4,8
Security – security is assured	7	6	5	7	1	5,2
Responsiveness – services are delivered without delay and waiting	3	2	4	3	4	3,2
Implementation of changes – the bank regularly implements novelties in e-banking services	2	1	1	1	7	2,4

cation is essential. An ideal authentication process would require fewer steps and not demand the use of additional devices for one-time passwords according to Krol, Philippou, De Cristofaro and Sasse (2015); our results fully support their findings. Despite the fact that our electronic banking users, and experts in e-banking security, are aware of how important security is, they certainly prefer the best possible user experience. Banks can invest much effort into the development of applications that are user-friendly, which would provide the best user experience. However, without resolving the problem of user authentication at the entrance into the application, we cannot expect that users would be satisfied, because the application makes a negative impression from the start.

A possible solution has been suggested by the recommendations of the European Central Bank[3]: using biometric data for the authentication of the individual. Years ago, producers of laptops implemented fingerprint reading technology in their hardware and software, but progress in this direction has not continued. Some researchers suggest a combination of biometrics and "classic" data, such as password and PIN (for example, Suganya, Sujatha & Alex, 2012), which increases the number of steps required for authentication. Currently, a possible solution for mobile banking is the development of fingerprint authentication on smartphones. This service is mostly used to unlock the phone itself, or access application stores, but it is also available for use to other applications[4]. Thus, banks can still provide a very high level of security with minimal additional effort for the user. Of course, such a proposal has some shortcomings:

Phones with biometric scanners are very expensive and consequently not widespread, which means that another alternative for all other users must be available:

This proposal does not solve the problems of online banking, since the user must copy something into a computer or have an additional device for reading fingerprints, together with associated software.

Nevertheless, we believe that banks should look to the future and, in addition to useful and well-designed content, provide users with safe and easily accessible Internet and mobile banking applications. In this way, they will be attractive and competitive, and users will be more satisfied. Internet and mobile bank users do not use the bank for enjoyment, but as a necessity to perform their transactions. They are obtaining the information they need and performing desired transactions. The faster and easier they can carry it out, the greater will be their satisfaction and the greater the likelihood that they remain loyal to their bank.

Literature

Akturan, U., & Tezcan, N. (2012). Mobile banking adoption of the youth market. *Marketing Intelligence & Planning*, 30(4), 444-459, http://dx.doi.org/10.1016/j.im.2014.12.001

Cheng, T.C.E., Lam, D.Y.C., & Yeung, A. C. L. (2006). Adoption of Internet banking: an empirical study in Hong Kong. *Decision support systems*, 42(3), 1558-1572.

Choubey, J., & Choubey, B. (2013). Secure User Authentication in Internet Banking: A Qualitative Survey.

3 Source: ECB, available from *http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityInternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf?2805486a1e803833e3596ccb3e73bf66*, 2015

4 Source: *http://www.wired.com/insights/2014/10/go-ahead-and-touch-id/*, 2016

International Journal of Innovation. Management and Technology, 4(2), 198-203. Retrieved from http://www.ijimt.org/papers/391-D0493.pdf

French, A. M. (2012). A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information. *Journal of Internet Banking and Commerce*, 17(2), 1-14. Retrieved from http://www.arraydev.com/commerce/JIBC/2012-08/AaronFrenchv02.pdf

Koo, C., Watti, J., & Chung, N. (2014). A study of mobile and Internet banking service: applying for IS success model. *Asia Pacific Journal of Information Systems*, 23, (1), 65-86. Retrieved from: http://www.apjis.or.kr/pdf/MIS023-001-4.pdf

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). »They brought in the horrible key ring thing!« Analysing the Usability of Two-Factor Authentication in UK Online Banking. *To appear in NDSS Workshop on Usable Security (USEC 2015)*. Retrieved from http://arxiv.org/abs/1501.04434v1

Lee, D., Moon, J., Kim, Y. J., &Yi, M. Y. (2015.) Antecedents and consequences of mobile phone usability: Linking simplicity and interactivity to satisfaction, trust, and brand loyalty. *Information & Management*, 52(3), 295–304, http://dx.doi.org/10.1016/j.im.2014.12.001

Lee, M. (2009). Factors affecting the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit, *Electronic Commerce Research and Applications,* 23, 130-141, http://dx.doi.org/10.1016/j.elerap.2008.11.006

Liao, Z., & Cheung, M.T. (2008). Measuring Customer Satisfaction in Internet Banking: A core Framework. *Communications of the ACM*, 51(4), 47-51, http://dx.doi.org/10.1145/1330311.1330322

Liébana-Cabanillas, F., Muñoz-Leiva, F., & Rejón-Guardia, F. (2013).The determinants of satisfaction with e-banking. *Industrial Management & Data Systems*, 113(5), 750-767, http://dx.doi.org/10.1108/02635571311324188

Mazhar, F., Rizwan, M., Fiaz, U., Ishrat, S., Razzaq, M.S., & Khan, T.N. (2014). An Investigation of Factors Affecting Usage and Adoption of Internet & Mobile Banking In Pakistan. *International Journal of Accounting and Financial Reporting*, 4(2), 478-501, http://dx.doi.org/10.5296/ijafr.v4i2.6586

Nasri, W., & Charfeddine, L. (2012). Factors affecting the adoption of Internet banking in Tunisia: An integration theory of acceptance model and theory of planned behaviour. *The Journal of High Technology Management*, 23, 1-14.

Suganya, M., Sujatha, S., & Alex, M. E. (2012). Secure user authentication using biometrics in mobile banking. *The Business & Management Review*, 2(1), 226-231. Retrieved from http://search.proquest.com/docview/1328550116?accountid=28931

Tella, A. & Abdulmumin, I. (2015). Predictors of Users' Satisfaction with E-payment System: a Case Study of Staff at the University of Ilorin, Nigeria. *Organizacija*, 48(4), 272-284, http://dx.doi.org/10.1515/orga-2015-0018

Yoon, H.S., & Occeña, L. (2014). Impacts of Customers' Perceptions on Internet Banking Use with a Smart Phone. *The Journal of Computer Information Systems*, 54(3), 1-9. Retrieved from http://search.proquest.com/docview/1526661130?accountid=28931

Aleksandra Svilar has a master's from University of Maribor, Faculty of Organizational Science. She has been working in Nova Ljubljanska banka d.d., for many years. Her current work area is planning and development of corporate internet and mobile banking.

Jože Zupančič has a PhD from University of Ljubljana, Faculty of Electrical and Electronic Engineering. He is retired professor of information systems at University of Maribor, Faculty of Organizational Science and currently visiting professor at University of Lodz, Poland. His primary research interests are information systems management, and user acceptance of information systems, acceptance of IT among elderly population.

Vpliv varnostnih elementov na delo s spletnimi in mobilnimi bankami

***Ozadje in namen**. Zagotavljanje ravnotežja med varnostjo v aplikacijah spletnega in mobilnega bančništva ter čim boljšo uporabniško izkušnjo postaja vse težja naloga za ponudnike spletnih in mobilnih bank. Cilj naše raziskave je ugotoviti kakšno mnenje imajo uporabniki o trenutnem stanju, predvsem kako trenutni varnostni elementi, ki jih uporabljajo, vplivajo na njihovo uporabniško izkušnjo.*

***Metodologij**a. Podatke smo zbrali s spletno anketo med uporabniki 13 bank v Sloveniji in jih analizirali s statističnimi metodami. Rezultate študije med uporabnikov je analiziralo manjše število strokovnjakov na področju varnosti elektronskega bančništva.*

***Rezultati**. Rezultati kažejo, da je mobilno bančništvo v Sloveniji še vedno relativno malo uporabljena oblika bančništva, saj ga uporablja le blizu 30% uporabnikov spletnega bančništva. Varnost je uporabnikom najpomembnejši element v spletnem ali mobilnem bančništvu, blizu pa ji sledi zanesljivost. Preverili smo tudi, koliko uporabniki vedo katere varnostne elemente uporabljajo banke s katerimi poslujejo. Skoraj 69%vprašanih je izbralo pravilen varnostni element. Kar 88% vprašanih pa je mnenja, da jih ti varnostni elementi pri delu ne ovirajo. Poleg raziskave z uporabniki smo v intervjujih za mnenje povprašali tudi strokovnjake s tega področja. Tudi strokovnjaki so v povprečju varnost postavili na prvo mesto, ob boku z uporabnostjo, vendar so mnenja posameznikov zelo raznolika. Rezultati raziskave mnenj uporabnikov strokovnjake niso presenetili.*

***Zaključek**. Kaže, da je v Sloveniji uporabnikom najpomembnejša varnost, uporabniška izkušnja pa je manj pomembna, čeprav si nedvomno želijo imeti čim lažje uporabne produkte.*

***Ključne besede:** spletno bančništvo; mobilno bančništvo; varnost; uporabniška izkušnja*