JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 March Volume 8 Number 3
http://doi.org/10.9770/jssi.2019.8.3(3)

Scopus®

SECURITY ASPECTS: PROTECTION OF PEOPLE IN CONNECTION WITH THE USE OF PERSONAL IDENTIFICATION NUMBERS

Antonín Korauš[1], Ján Dobrovič[2], Jozef Polák[3], Stanislav Backa[4]

[1]Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava 35, Slovak Republic
[2,3,4]University of Prešov in Prešov, Faculty of Management, Konštantínova 16, 080 01 Prešov, Slovak Republic

E-mails: [1]antonín.koraus@minv.sk , [2]jan.dobrovic@unipo.sk , [3]jozefpolak64@gmail.com, [4]stanislav.backa@gmail.com

Received 10 May 2018; accepted 10 January 2019; published 30 March 2019

Abstract. User identifiers for financial transactions are widely used for personal identification numbers (PINs). PIN numbers are deposited at ATMs, card payments at POS terminals and electronic banking services. Bank card (ATM) credit card fraud has dramatically increased over the last decade. When analyzing the most common attacks and the reasons for successful frauds, it is clear that the main problem is PIN authentication, which itself does not produce any security features (except for the use of stars). This means that security is based solely on user behaviour. Research has focused on areas where personal protection and security is most failing, and that's where the user is carrying a PIN along with a credit card, whether he or she changed the PIN on the payment card, and whether the PIN does not specify the date or year of his birth.

Keywords: personal identification number, security, PIN, payment card, credit card fraud, ATM, electronic banking services

Reference to this paper should be made as follows: Korauš, A.; Dobrovič, J.; Polák, J.; Backa, S. 2019. Security aspects: protection of people in connection with the use of personal identification numbers, *Journal of Security and Sustainability Issues* 8(3): 319-330. http://doi.org/10.9770/jssi.2019.8.3(3)

JEL Classifications: F5, F52, K42, K24

1. Introduction

Increasing possibilities of hardware and software, growing Internet speed and importance of wired and wireless data transfer, the emergence of big data and cloud computing services, take-over by smart phones of increasingly more human communication functions, and emerging of other functions important to people means that information technologies play an increasingly more important role in our lives (Štitilis et al. 2016; Štitilis et al. 2017; Fuschi, Tvaronavičienė 2014; Tvaronavičienė et al. 2016; Cseh Papp et al., 2018; Tvaronavičienė 2018a; 2018b; Limba, Šidlauskas 2018; Radu, 2018; Kovaľová & Kulčár, 2017; Korauš, Kelemen 2018; Korauš et al. 2017; Korauš et al. 2018; Šišulák 2017; Benešová, Hušek 2019; Kazansky, Andrassy 2019).

When users enter a PIN, they are vulnerable to shoulder and key logging attacks. When entering PIN numbers using virtual keyboards, it is possible to mitigate attacks caused by piano playback but increases the risk of surfing on the shoulders. A series of resistive keyboards for the shoulder were designed. However, many of them offer inadequate security and are useless. They also require important user information, training, user memory and other PIN input devices. Since PIN security should not be made on the basis of unpleasant user experience, it is important to mention the risks that arise from the first PIN entry.

Today, security is very much essential for all kind of activities. Illegal activities are happening in every place today. Therefore, government and corporate sections are concentrating mainly on the security levels with their

every invention. In today's technically advanced world, autonomous systems are gaining rapid popularity. Quantitative systematic risk assessment methods are preferred such as RM/RA CRAMM (Mullerova 2016, Mamojka, Mullerova 2016, Palková 2018) to be combined with crime forecast maps (Mullerova, Mamojka 2017). Systematic detection of UBO is dependent upon the development and introduction of new software based on scientific methods. As the social computer and automation has been increased and the ATM and credit card has been installed and spread out to simplify the financial activity, and the banking activity. However the crime related with financial organization has been increased in proportion to the ratio of spread out of automation and devices. Those crimes for the financial organization have been increased gradually from year 1999 to 2003, little bit decreased in 2004, and then increased again from year 2005 (Narmada, Priyadarsini, 2016). Payment cards represent a contemporary tool of cashless payment systems (Kocisova, Gavurova and Sopko 2018), which are commonly used to cover expenses and realize cash withdrawals.

An automated or automated ATM (ATM), also known as an automated ATM, is a computer telecommunication device. Nowadays many people use ATMs to select, deposit money, account information, recharge credit on mobile phones, and more. Therefore, not only personal protection and security but also security at the centre of ATM is important. These protection practices are designed to prevent users who have been attacked by foreigners during money withdrawals in particular by innovative ideas designed to improve security.

ATM card is a plastic card that contains a unique card number and security information such as expiration date. It has a 4 - digit PIN number for authentication. ATM card is inserted into the ATM machine enter the PIN number, machine identifies the customer and completes the transaction. CPU (Central Processing Unit), magnetic card, crypto - processor, a display device, function key buttons, record printer, and vault these devices used in ATM centre. Most ATMs are connected to an interbank network enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account. This is a convenience, especially for people who are travelling: it is possible to make withdrawals in places where one's bank has no branches, and even to withdraw local currency in a foreign country, often at a better exchange rate than would be available by changing cash. ATMs rely on Authorization of a Transaction by the card issuer or other authorizing institution via the communications network.

Transaction via an ATM payment card requires privacy to maintain personal protection and user safety. Privacy must be secured around the world. Therefore, in the idea of bringing privacy through the security level, an ATM security system has been developed, which mainly uses three divisions, such as IR sensors, a metal detector and a biometric sensor. Each unit has its own main role over the protection model. The IR sensor serves to enable one person at a time. Transaction is safer. A metal detector mounted on metal detection doors, knife, gun, etc. If a user is not educated or unconscious about an ATM, then the proposed work is given at that time the authorized person providing security protection only to help customers with a biometric fingerprint (Sako, Miyatake, 2004; Vlacseková, Mura 2017). People need to know about the ATM's working condition without going to the ATM centre. It was linked to a global mobile communications system (GSM) an ATM network that provides all ATM information working conditions for payment card users (Hamad et al., 2006).

2. Theoretical background

Banks currently use sophisticated tools to track and detect fraud and fight against them at every stage of the buying process, even before they buy. Banking experts are constantly expanding and enhancing technology to take a step forward from fraudsters, so that once MasterCard identifies smartphone clips as its own, no one else can shop with client mobile credentials. Card payer cardholders are also able to make safer digital payments even through tokenisation - the process of exchanging a token card master account number.

The smart cards are equipped with an additional security element, which is embedded in the form of an inserted microchip, safely storing user data.

The service provider is assigned or the user selects the Personal Identification Number (IPIN) numbers that

contain 3 to 6 digits. PIN numbers are typically associated with different types of banking services. If a user completes a transaction, it is a requirement for users to enter their PIN assigned to their account. User numbers will be verified based on saved numbers. Sometimes a dynamically generated number called a one-time password (OTP) can be used as a PIN. Although PINs are simple and effective in securing accounts, they are prone to attacking the shoulder. When attacking the shoulder surf, the attacker follows the user authentication process and identifies the PIN number. Using virtual keyboard shortcuts makes it easier for an attacker to make keyboard entries on the screen. A security precaution to prevent this attack ensures that no one is entered before the PIN is entered. But in public places such as ATMs, cyber cafes, department stores, etc. It's hard to push. Another option is to use OTP for transactions. However, additional costs and delays could arise. OTP attacks are also prevalent (Raddum et al. 2010).

In the case of a human arm attack, the attackers rely on their ability to observe and remember the details they have observed (De Angeli et al. 2005, Tari et al. 2006, Roth and Richter 2006; Hitka et al., 2017; Mura, Vlacseková 2018; Mészáros, 2018; Zulova et al., 2018; Vlacseková, Mura 2017). When entering a PIN on a virtual keyboard, a user clicks the numbers one at a time and gives enough opportunity for the observer to see individual digits reconstruct the entire PIN. So any security mechanism that prevents direct entry of numbers and increases the trouble of the attacker tracking the pin input to track the real number is enough to alleviate attacks on the shoulder. But when the attack on the shoulder is surfing with a recording device such as a mobile camera or malware that could record video activity on the screen, it is very difficult to defend (Wu 2014). This is because the attacker could view the recorded video several times and reproduce the PIN number in succession. There are many suggestions to limit recorded attacks on the shoulder. Such models are more complicated for implementation and follow-up for regular users.

Recognizing the potential for PIN attacks during the PIN process, many scientists have focused on developing new schemes to mitigate these attacks. A survey of many virtual keyboards takes place in (Kölsch and Turk 2002). Method (Wilfong 1999) requires that the user performs a math operation on each digit of his / her random number PIN provided by the authenticators. The result is entered by the user. At the end of the server, the same digits are repeated to get digits. Verified based on actual saved PINs. This approach requires users a certain level of competence to perform mathematical computations, and may lead to several erroneous inputs.

In the mobile environment, there is a high risk of the observing attacks which is the way to steal a password, because many people have a camera-equipped mobile phone and a miniature camera. The biometric authentication technology is one of the methods to solve this problem. However, some equipment does not have the device of biometric authentication. Moreover, some system requires PIN or password when failing in the biometric authentication. The PIN or password authentication is still used widely (Fujita, Hirakawa, 2008).

3. Research objective and methodology

The results of the conducted survey and its subsequent analysis are a contribution to the enhancement of knowledge and comprehension of the behaviour of payment card users from the point of view of their security. The study analyzes one of the basic security features of payment cards and is focused namely on PIN code and basic rules for its use. The survey as well as the selection of a representative sample was carried out as follows:

- Time horizon of the survey: 20/02/2018 - 20/07/18
- Representative sample: 1 012
- Number of questionnaires issued: 4 700
- Number of (completed) questionnaires collected: 3 288

The representative sample of 1,012 of fully-completed questionnaires was selected by random number generator from the total count of 3,288 to represent the SR population over the age of 18 in terms of gender, age, education, settlement categories, and regional breakdown.

The research file is represented by 5 age categories. Respondents aged 18-30, 31-40, 41-50, 51-60 and over 60 years. In the category from 18 to 30 years, there are 206 respondents, representing 20.22% of the research population. The second age category represented by age from 31 to 40 years is defined by 212 respondents, representing 20,80%. The third age category from 41 to 50 years contains 192 respondents, which is 18.84% in relative terms. The age category from 51 to 60 years is represented by 196 respondents (19.23%) and the age category over 61 years by 213 respondents (20.90%). The survey was attended by 540 men, representing 52.99% and 479 women representing 47.01%. As per geographical region, 134 respondents were from Prešov region (13.15%), 140 respondents from Košice region (13.74%), 117 respondents from Banská Bystrica region (11.48%), 127 respondents from Žilina region (12.46%), 127 respondents from Nitra region (12.46%), 144 respondents from Trenčín region (14.13%), 112 respondents from Trnava region (10.99%) and 118 respondents from Bratislava region (11.58%). In terms of achieved education, 300 respondents were with basic education (29.44%), 438 respondents with secondary education (42.98%) and 281 respondents with higher education (27.58%). The structure of respondents participating in the survey in age groups of 18-30 and over 60 years, is presented in Figures 1 and 2.

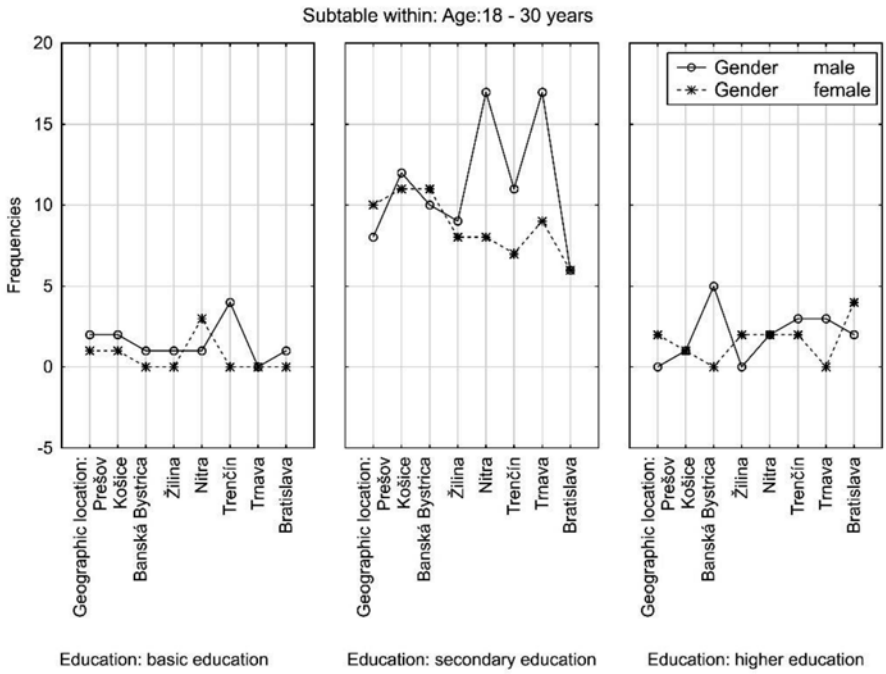

Figure 1 Structure of respondents aged 18 – 30 years

Source: own research

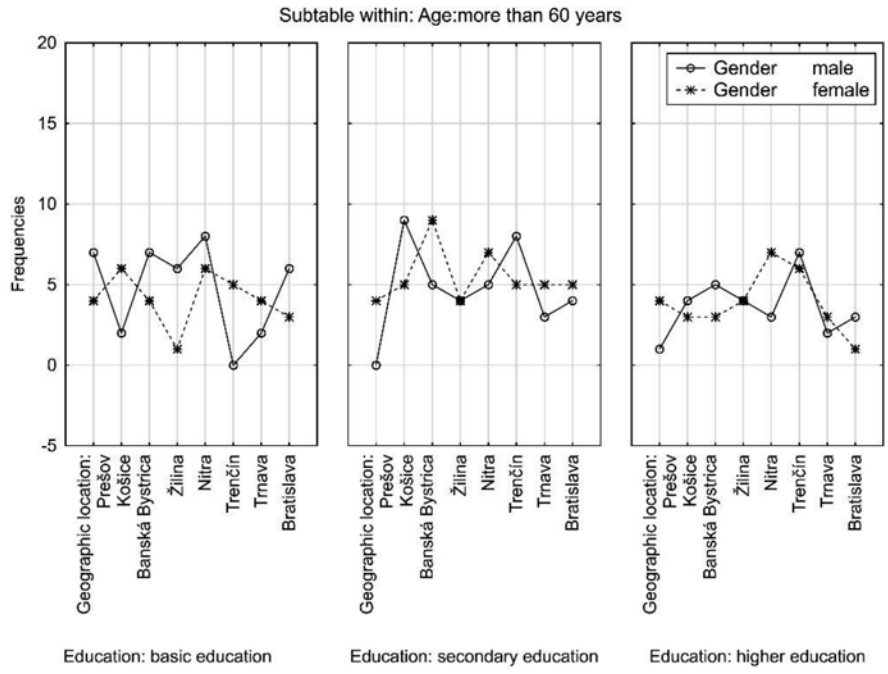

Figure 2 Structure of respondents in the age category over 60 years

Source: own research

As seen from Table 1, the result of the analysis of responses to question No 1 of the questionnaire as to whether the respondents would carry a PIN along with their credit card showed that 13.24% of those aged 18-30 years chose the answer of "definitely not". The same response was reported by 10.79% of respondents aged 31-40, 9.12% aged 41-50, 9.42% of respondents aged 51-60 and 9.81% aged over 60. Overall, 52.40% of all respondents answered by choosing this option while 24.34% of the respondents opted for a "no" option. The answer "I do not know" was chosen by 1.37%, "yes" by 9.72% and "certainly yes" by 12.17%.

Table 1 Table of respondents' relative answers to question Q1 in relation to respondents' age

	Percentages of Total Row Variables: Age (5) Column variables: Q1(5)					
	Definitely not	No	I do not know	Yes	Certainly yes	Total
18 - 30 years	13.24828	5.78999	0.000000	0.294406	0.88322	20.2159
31 - 40 years	10.79490	5.29931	0.294406	1.864573	2.55152	20.8047
41 - 50 years	9.12659	5.88813	0.196271	1.079490	2.55152	18.8420
51 - 60 years	9.42100	3.72915	0.490677	2.747792	2.84593	19.2345
More than 60 years	9.81354	3.63101	0.392542	3.729146	3.33660	20.9028
Total	52.40432	24.33759	1.373896	9.715407	12.16879	100.0000

Source: own research

Q1 - Do you carry a PIN along with a credit card?

Based on results of the correspondence analysis at total value of $\chi 2 = 76.6831$ and degrees of freedom df = 12, the significance value of p = 0.0001 is achieved. Therefore, at the level of significance of $\alpha = 5\%$, we can say that there is a significant relationship between the age of respondents and fact of carrying the PIN code along with the payment card. More detailed results of the correspondence analysis are shown in Figure 3 in form of a correspondence map.

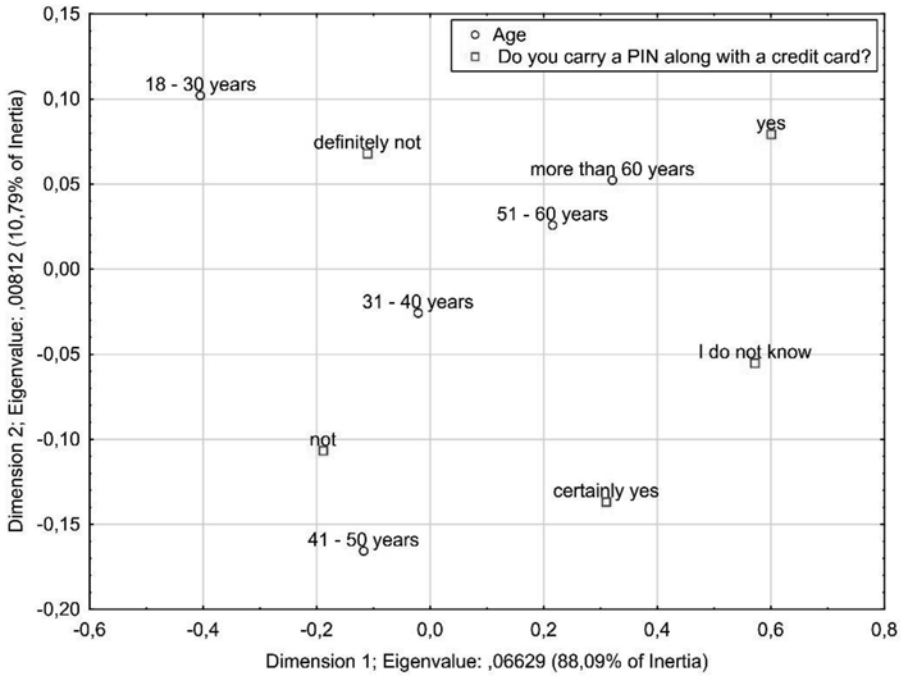

Figure 3 Correspondence map of dependence of respondents' answers to question Q1 (Do you carry a PIN along with a credit card?) and age

Source: own research

From more detailed results, it is clear that respondents aged 18-30 years have statistically significantly leaned toward the "definitely not" option. Respondents aged between 41 and 50 years were inclined to answer "no" while those aged 51-60 and over 60 years were inclined to answer "yes". In a way, the latter results are not surprising. The fact that people from older categories tend to prefer carrying a PIN along with their credit cards reflects the aspect of losing confidence in recollecting their PIN. This however brings about a huge security risk and in case of theft it may result in subsequent misuse of the payment instrument.

As to the relationship between gender of respondents and answers to question No. 1 (Do you carry a PIN along with a credit card?), the level of achieved significance of the x2 test ($p = 0.8701$) as well as that of geographical distribution of the respondents ($p = 0.8555$) clearly displays that both cases did not show a significant relationship. Thus, it is possible to state that both men and women preferred roughly equal answers to question No. 1 of the questionnaire while even not reflecting the difference in geographic distribution with respect to the choice of preferred answer.

As to education, the percentage of responses to the question Q1 (Do you carry a PIN along with a credit card?) are shown in Table 2.

Table 2 Table of respondents' relative answers to question Q1 in relation to the achieved education of respondents

	Percentages of Total Row Variables: Education (3) Column variables: Q1(5)					
	Definitely not	No	I do not know	Yes	Certainly yes	Total
Basic education	13.64082	6.57507	0.294406	3.827282	5.10304	29.4406
Secondary education	20.90285	9.61727	0.981354	5.397448	6.08440	42.9833
Higher education	17.86065	8.14524	0.098135	0.490677	0.98135	27.5761
Total	52.40432	24.33759	1.373896	9.715407	12.16879	100.0000

Source: own research

Q1 - Do you carry a PIN along with a credit card?

The above table shows that 13.64% of respondents with primary education, 20.90% of respondents with secondary education and 17.86% of those with university education chose the option of "definitely not" to the question "Do you carry a PIN along with a credit card?". Together, 52.40% of all respondents chose this option. The option "no" was chosen by 6.57% of respondents with primary education, 9.62% with secondary education and 8.15% with university education. According to the analysis, the PIN code is carried along with the card (options "yes" and "certainly yes") by 8.93% of respondents with basic education, 11.47% of those with secondary education and only 1.57% of university graduates.

Based on the results of the correspondence analysis at the total value of $\chi^2 = 71{,}1715$ and degrees of freedom df = 8, the significance value p = 0,0001 is achieved. Thus, at the level of significance of $\alpha = 5\%$, we can state that there is a significant relationship between the level of education achieved by the respondents and fact of carrying the PIN code along with the payment card. More detailed results of the correspondence analysis are shown in Figure 4 in form of a correspondence map.

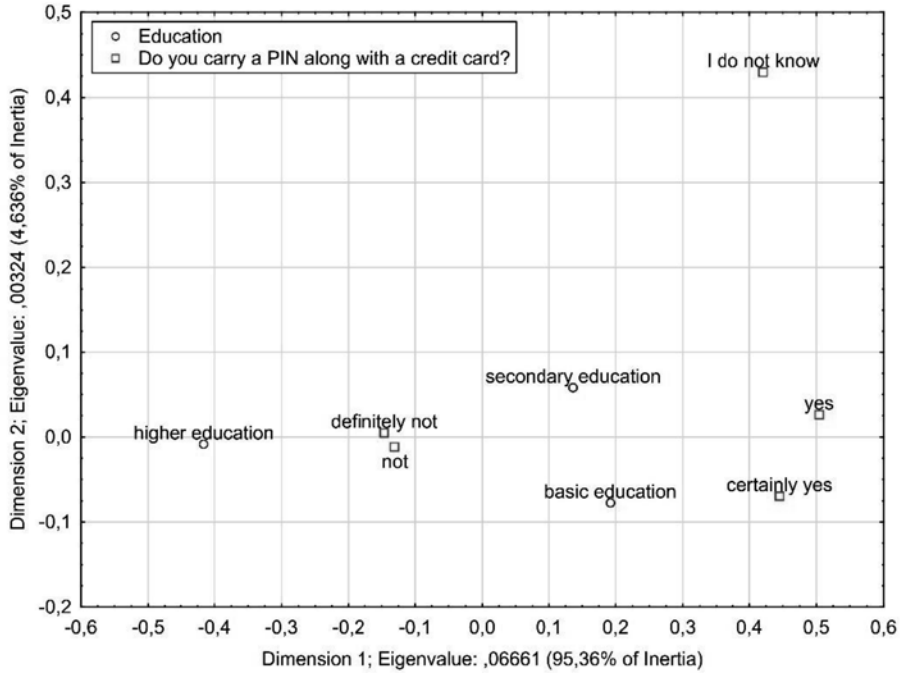

Figure 4 Correspondence map of dependence of respondents' answers to question Q1 (Do you carry a PIN along with a credit card?) and achieved education

Source: own research

The correspondence map (Figure 4) shows that respondents with basic education tend to carry a PIN code along with a payment card, while respondents with higher education tend to answer "no" or "certainly not".

The relative responses of the respondents to question No. 2 of the questionnaire (Did you change your PIN on your credit card?) are given in Table 3. The table shows that regardless of their age, 13.15% of the respondents did not change their payment card PIN. Out of these respondents, only 0.39254% were aged 18-30. In age categories of 31-40, and 41-50 years, the PIN code was certainly not changed in 2.06084% and 1,6683%, respectively. More than a 100% increase is seen in respondents over the age of 51. On the other hand, we can see that the payment card PIN code was certainly changed in 49.36212% of the respondents, while among them, the largest number of respondents were aged 18-30. With the increasing age, there is a decrease in the number of respondents who have surely changed their PIN, namely to 7.65456% at the age over 60.

Table 3 Table of respondents' relative answers to question Q2 in relation to the age of respondents

	Percentages of Total Row Variables: Age (5) Column variables: Q2(5)					
	Definitely not	no	I do not know	Yes	Certainly yes	Total
18 - 30 years	0.39254	0.588813	0.392542	6.47694	12.36506	20.2159
31 - 40 years	2.06084	0.785083	0.785083	6.18253	10.99117	20.8047
41 - 50 years	1.66830	0.883219	0.883219	5.59372	9.81354	18.8420
51 - 60 years	4.90677	1.373896	0.686948	3.72915	8.53778	19.2345
More than 60 years	4.12169	2.158979	0.883219	6.08440	7.65456	20.9028
Total	13.15015	5.789990	3.631011	28.06673	49.36212	100.0000

Source: own research

Q2 - Did you change your PIN on your credit card?

Based on the results of the correspondence analysis at the total value of $\chi 2 = 90.7877$ and degrees of freedom df = 16, the significance value of p = 0.0001 is achieved. Thus, at the level of significance of $\alpha = 5\%$, we can say that there is a significant relationship between the age of respondents and change in payment card PIN code. More detailed results of the correspondence analysis are shown in Figure 3 in form of a correspondence map.

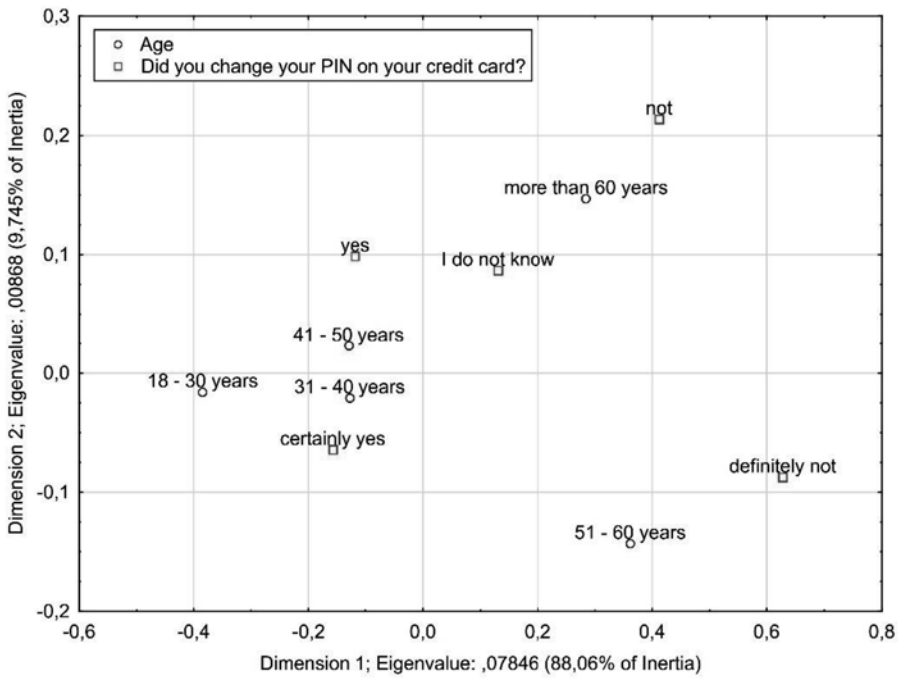

Figure 5 Correspondence map of dependence of respondents' answers to question Q2 (Did you change your PIN on your credit card?) and age

Source: own research

From a more detailed analysis in form of a correspondence map (Figure 5), it is clear that respondents aged 18-50 years statistically significantly incline to answer "certainly yes". Therefore, the respondents from these age groups have certainly changed their payment card PIN codes. On the other hand, respondents from the group aged 51-60, leaned toward the answer of "definitely not" while respondents aged over 60 years chose the option of "do not know" or "no".

As to the level of achieved education, the table of percentage answers of respondents to question No. 2 of the questionnaire (Did you change your PIN on your credit card?), clearly displays that the payment card PIN code was definitely not changed by 5.49558% of respondents with basic education. Up to 7.26202% of respondents with secondary education chose the same answer. Thus, they definitely did not change the PIN code while only 0,39254% of respondents with university education chose this option. On the second pole of the Likert scale, we can see that the PIN code has certainly been changed by 19.33268% of respondents with secondary education and 17.95878% of university graduates. Altogether, the answer of "certainly yes" was opted for by 49.36212% of all respondents.

Table 4 Table of respondents' relative answers to question Q2 in relation to achieved education of respondents

	Percentages of Total Row Variables: Education (3) Column variables: Q2(5)					
	Definitely not	No	I do not know	Yes	Certainly yes	Total
Basic education	5.49558	2.158979	1.079490	8.63592	12.07066	29.4406
Secondary education	7.26202	3.140334	1.668302	11.57998	19.33268	42.9833
Higher education	0.39254	0.490677	0.883219	7.85083	17.95878	27.5761
Total	13.15015	5.789990	3.631011	28.06673	49.36212	100.0000

Source: own research

Q2 - Did you change your PIN on your credit card?

Based on the results of the correspondence analysis at the total value of $\chi 2 = 72{,}4810$ and degrees of freedom df = 8, the significance value of p = 0,0001 is achieved. Thus, at the level of significance of $\alpha = 5\%$, we can say that there is a significant relationship between age of the respondents and change in payment card PIN code. More detailed results of the correspondence analysis are shown in Figure 3 in form of a correspondence map.

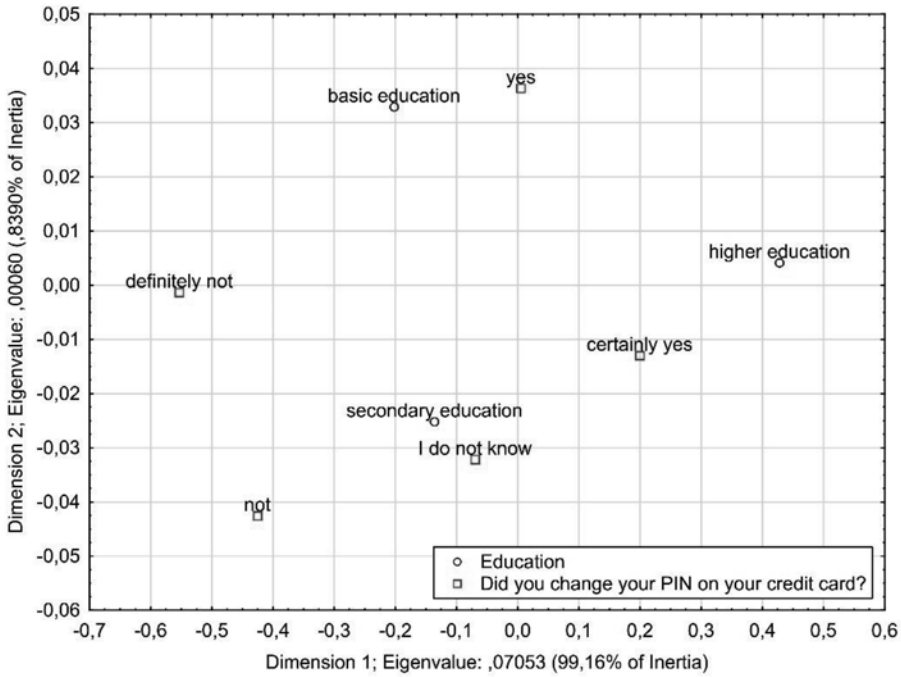

Figure 6 Correspondence map of dependence of respondents' answers to question Q2 (Did you change your PIN on your credit card?) and achieved education

Source: own research

From the more detailed results in form of a correspondence map (Fig. 6) it is obvious that the respondents with secondary education preferred answering "I do not know", while those with higher education chose the option of "certainly yes" and those with basic education opted for "yes".

Conclusions

Automatic ATMs are widely used thanks to their simplicity and extensive availability. In the coming years, ATM systems will no longer use a magnetic stripe (magstripe) access card and a fixed personal identification number (PIN) to authenticate. At present, clients use a chip and a PIN that sometimes has a magstripe if the chip fails as a backup for identification purposes. This method is not very safe and creates prerequisites for the increase in crime. For these reasons, a new, simple and secure access method is needed. In such a method, the user is generated a PIN, and this PIN is available on the ATM system through the Subscriber Identity Module (SIM) on the mobile phone of the user. Such information is reported to the Global System for Mobile Communications (GSM) module, which is inserted into the ATM's functional framework. This security method is significantly better than the traditional methods currently in use because it is dynamic in view of the ability to change the user-defined PIN (UDPIN) in each transaction. The problem that occurred with the loss of the access card and the need for immediate deactivation is eliminated. The access card can be enhanced with additional security features without the need for a large number of modifications. After the implementation of the prototype of the access card where the security features were used, the results were verified by extensive testing and proved to be a simpler and better security measure.

The use of mobile phone devices is expanding rapidly and they become essential tools that offer competitive business advantages in today's growing world of global computing environments. A mobile phone device is a suitable tool for a multifactor authentication that could provide powerful and easy to use authentication device to access any service securely such as an ATM terminal as well as would increase the level of protection for critical and sensitive information.

References

Benešová, D.; Hušek, M. (2019). Factors for efficient use of information and communication technologies influencing sustainable position of service enterprises in Slovakia. *Entrepreneurship and Sustainability Issues,* 6(3): 1082-1094. http://doi.org/10.9770/jesi.2019.6.3(9)

Cseh Papp, I., Varga, E., Schwarczová L., Hajós, L. (2018). Public work in an international and Hungarian context. *Central European Journal of Labour Law and Personnel Management*, 1 (1), 6 – 16. http://doi.org/10.33382/cejllpm.2018.01.01

De Angeli, A.. Coventry, L. M., Johnson, G., Renaud, K. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. Published in International Journal of Man-Machine Studies, Vol. 63, pp. 128 – 152. DOI:10.1016/j.ijhcs.2005.04.020

Fujita, K.; & Hirakawa, Y. (2008). A study of password authentication method against observing attacks. In SISY 2008 - 6th International Symposium on Intelligent Systems and Informatics [4664927] https://doi.org/10.1109/SISY.2008.4664927

Fuschi, D.; & Tvaronavičienė, M. (2014). Sustainable development, Big Data and supervisory control: service quality in banking sector, Journal of Security and Sustainability Issues 3(3): 5-14. http://dx.doi.org/10.9770/jssi.2014.3.3(1)

Hamad, M.; Kassem, A.; Jabr, R.A.; Bechara, C.; & Khattar, M. (2006). PIC based microcontroller design laboratory. Proceedings of the IEEE Workshop on System and Chip for Real Time Applications. Cairo, Eqypt, pp. 66-69, ISBN: 1-4244-0898-9. DOI: 10.1109/IWSOC.2006.348266

Hitka, M.; Lorincova, S.; Bartakova, G.P.; Lizbetinova, L.; Starchon, P.; Li, C.; Zaborova, E.; Markova, T.; Schmidtova, J.; & Mura, L. (2018). Strategic Tool of Human Resource Management for Operation of SMEs in the Wood-processing Industry. *Bioresources*, 13(2): 2759-2774. https://doi.org/10.15376/biores.13.2.2759-2774

Kazansky, R.; Andrassy, V. 2019. Conflict resolution approaches towards smart sustainability of internal relations, *Entrepreneurship and Sustainability Issues* 6(3): 1268-1284. https://doi.org/10.9770/jssi.2019.6.3(29)

Kocisova, K.; Gavurova, B.; & Sopko, J. (2018). Do more cards and terminals guarantee higher efficiency? The case of European Union banking. *Journal of International Studies*, 11 (2): 49-62. https://doi.org/10.14254/2071-8330.2018/11-2/4

Kölsch, M.; & Turk, M. (2004). Robust hand detection In FGR' 04 Proceedings of the Sixth IEEE international conference on Automatic face and gesture recognition, pp. 614-619, Seoul, Korea — May 17 - 19, ISBN:0-7695-2122-3

Kovaľová, M.; & Kulčár, L. (2017). Innovation management and information acquisition. *Acta Oeconomica Universitatis Selye* 6 (2): 101 – 108. ISSN 1338-6581

Korauš, A.; & Kelemen P. (2018). Protection of persons and property in terms of cybersecurity in Economic, Political and Legal Issues of International Relations 2018. Faculty of International Relations of Univerzity of Economics in Bratislava,1. - 2. juni 2018, Virt, Editor: EKONÓM, 2018, ISBN 978-80-225-4506-8, ISSN 2585-9404

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. (2019). Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3): 1101-1012. http://doi.org/10.9770/jesi.2019.6.3(3)

Limba, T.; & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)

Mamojka, M.; & Müllerová, J. 2016. New methodology for crisis management RM/RA CRAMM and its legal frame. In: Production management and engineering sciences. - Leiden: CRC Press/Balkema, 2016. pp 185-190. ISBN 978-1-138-02856-2.

Mészáros, M. (2018). "Employing" of self-employed persons. *Central European Journal of Labour Law and Personnel Management*, 1 (1), 46 – 67. https://doi.org/10.33382/cejllpm.2018.01.04

Müllerová, J. 2016. *RM/RA CRAMM as a new risk management method for prevention of ecology disasters*, 16th International Multidisciplinary Scientific GeoConference SGEM 2016, SGEM2016 Conference Proceedings, June 28 - July 6, Book5 Vol. 1, pp. 607-612. ISBN 978-619-7105-65-0 / ISSN 1314-2704

Müllerová, J.; & Mamojka, M. 2017. Legal possibilities of the rescue forces during the emergency event. In: SGEM2017 Conference Proceedings, 29 June - 5 July, 17 (51): 605-612, ISBN 978-619-7408-08-9 / ISSN 1314-2704. DOI: 10.5593/sgem2017/51/S20.079

Mura, L.; Havierniková, K; & Machová, R. (2017). Empirical results of entrepreneurs' network: Case study of Slovakia. *Serbian Journal of Management*, 12 (1): 121-131 https://doi:10.5937/sjm12-10418

Mura, L.; & Vlacseková, D. (2018). Motivation of public employees: case study of Slovak teaching and professional staff. *Administratie si Management Public*, (31): 67-80. https://doi.org/10.24818/amp/2018.31-05

Narmada, D., & Priyadarsini, J.V. (2016). Design and implementation of security based atm using ARM11 Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016, 2016, art. no. 7830124. https://doi.org/10.1109/INVENTIVE.2016.7830124

Pálková, M.; Müllerová, J.; Endrizalová E. 2018. Risk management system in Czech Republic. In: SGEM 2018 conference proceedings. 30 June - 9 July 2018 Albena, Bulgaria [print]. Sofia: STEF92 Technology 18(5.2), pp. 1049-1056. ISSN 1314-2704/ISBN 978-619-7408-47-8.

Raddum, H.; Nestås L.; & Hole K. (2006). "Security Analysis of Mobile Phones used as OTP Generators," in Proceedings of Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices, Passau, pp. 324-331. ISBN: 3-642-12367-8 978-3-642-12367-2. doi>10.1007/978-3-642-12368-9_26

Radu, L. D. (2018). Green ICT: some challenges and potential solutions. Acta Oeconomica Universitatis Selye 7(2): 141 – 150, ISSN 1338-6581

Roth V.; & Richter, K. (2006). "How to Fend off Shoulder Surfing," Journal of Banking and Finance, 30(6): 1727-1751. ISBN:1-58113-961-6 doi>10.1145/1030083.1030116

Sako, H. & Miyatake, T. (2004). Image recognition technologies towards advanced automated teller machinen. Proceedings of the 17th International IEEE Conference on Pattern Recognition.Cambridge, United Kingdom, pp. 282-285. August 23 – 26. ISBN: 0-7695-2128-2

Šišulák, S. (2017). Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5 (2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Štitilis, D.; Pakutinskas, P.; Laurinaitis, M.; & Malinauskaitė, I. (2017). A model for the national cyber security strategy. The Lithuanian case. *Journal of Security and Sustainability Issues* 6(3): 357-372. https://doi.org/10.9770/jssi.2017.6.3(3)

Štitilis, D.; Pakutinskas, P.; Kinis, U.; & Malinauskaitė, I. (2016) Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197-210. https://doi.org/10.9770/jssi.2016.6.2(1)

Tari F., Ozok A., & Holden S., (2006). "A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords," In Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, pp. 56-66. ISBN: 1-59593-448-0 doi>10.1145/1143120.1143128

Tvaronavičienė, M. (2018a). Towards sustainable and secure development: energy efficiency peculiarities in transport sector, *Journal of Security and Sustainability Issues* 7(4): 719-725. https://doi.org/10.9770/jssi.2018.7.4(9)

Tvaronavičienė, M. (2018b). Towards internationally tuned approach towards critical infrastructure protection, *Journal of Security and Sustainability Issues* 8(2): 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

Tvaronavičienė, A., Žemaitaitienė, G., & Bilevičienė, T. (2016). Ecosystem for sustainable entrepreneurship: towards smart public procurement review procedures. *Entrepreneurship and Sustainability Issues* 4(1): 39-52. http://dx.doi.org/10.9770/jesi.2016.4.1(4)

Vlacseková, D.; & Mura, L. (2017). Effect of motivational tools on employee satisfaction in small and medium enterprises. *Oeconomia Copernicana*, 8(1): 111-130. https://doi.org/10.24136/oc.v8i1.8

Wilfong, G. (1999). "Method and Apparatus for Secure PIN Entry," U.S. Patent 5940511A

Wu, T.; Lee, M.; Lin H.; & Wang, C. (2014). Shoulder-Surfing-proof Graphical Password Authentication Scheme. *International Journal of Information Security*, 13(3): 245-254. doi>10.1007/s10207-013-0216-7

Zulova, J., Svec, M., & Madlenak, A. (2018). Personality aspects of the employee and their exploration from the GDPR perspective. *Central European Journal of Labour Law and Personnel Management*, 1(1): 68 – 77. http://doi.org/10.33382/cejllpm.2018.01.05

Short biographical note about the contributors at the end of the article (name, surname, academic title and scientific degree, duties, research interests):

Ass.Prof.Ing. Antonín KORAUŠ, PhD., LL.M., MBA is an associate professor at Academy of the Police Force in Bratislava, Slovak republic. Research interests: economy security, finance security, cyber security, energy security, finance, banking, management, AML, economy frauds, financial frauds, marketing, sustainability.
ORCID ID:
https://orcid.org/0000-0003-2384-9106

Ass.Prof. Ing. Ján DOBROVIČ, PhD, is an associate professor in the Department of Management, Faculty of Management at the University of Prešov in Prešov since 2006. Since 2013, he works as head of the Department of Management, and he teaches school subjects: management, operations management, and logistics. From 1996 to 2001 he was appointed Regional Director of the Slovak Trade Inspectionin the Prešov Region Prešov. Between 2001 - 2005 he became the municipal office in Prešov. Between 2006 - 2010 he held the position of Deputy for International Relations, Director General of the Slovak Tax Directorate. He is also involved in public offices as a member of the city council and deputy Prešov Self-Governing Region.
ORCID ID:
https://orcid.org/0000-0002-0637-106X

Ing. Jozef POLÁK, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak republic
ORCID ID:
https://orcid.org/0000-0003-4733-0851

JUDr. Stanislav BACKA, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak republic
ORCID ID:
https://orcid.org/0000-0002-0411-4158