Security of Digital Banking Systems in Poland: Users Study 2019

Wojciech Wodo and Damian Stygar
Department of Computer Science, Wroclaw University of Science and Technology, Wybrzeze Wyspianskiego 27,

Keywords: Banking, Electronic Banking, Mobile Banking, Security, Biometrics, 2FA.

Abstract: Our aim of this study was to discover believes, behaviors, thoughts and habits of digital banking users in Poland, we wanted to understand their motivation and drivers while using electronic and mobile financial services. Thanks to using Design Thinking research methodology we empathized users deeply and defined personas - representing user groups of common features and way of thinking and acting. Our desk research and users interview resulted in the identification of a number of aspects of e-banking, that can/should be taken into consideration by its users and, possibly, providers in order to assess the security of the service from the perspective of usability. We have interviewed 62 people in Poland (age span 16-72, different professions and familiarity level with e-banking solutions) in a form of qualitative study – in-depth survey (one hour per person) and discussed security issues with several Polish banks representatives. This paper is essence extract of full research conducted in this area. It presents and summarises the main assumptions and results.

1 INTRODUCTION

The year 2019 for the development of digital services and digitization of administration in Poland was very significant. We mean both state administration services, where tax settlement has been fully started for the first time - Your e-PIT (Ministry of Finance, 2019), new ID cards have been introduced with the electronic layer (Ministry of Digital Affairs, 2019a), the mObywatel application (Ministry of Digital Affairs, 2019b) enabling confirmation of identity, but above all preparing the financial sector for the implementation of the PSD2 Directive (European Parliament, 2015), launching and issuing of the test API interface by the banks (Zwiazek Bankow Polskich, 2019a) and fintech reinforcement to take over the financial services sector (Zwiazek Bankow Polskich, 2019b). This state of affairs is very pleasing from the point of view of economic development and increasing the comfort of implementation of many activities, both private and business. However, behind the rapidly moving digitization comes the risk of: cybersecurity threats, lack of user awareness, room for abuse and failure to adapt legal provisions quickly. The government has taken steps to guarantee a legal basis for certain activities and services. These activities are: the Act on Cyber Security (Polish Parliament, 2018c), the Act prohibiting the production of documents imitating identity documents and documents authorizing to perform activities (Polish Parliament, 2018b), or the previously ratified, widely discussed GDPR (Polish Parliament, 2018a).

1.1 Motivation

The enormous pace of adoption of new technologies in every domain of life, both private and business[1], is not reflected in informational and education campaigns that would ensure safe and informed use of the benefits of digital services. The area of this study is electronic finance, digital banking and financial services.

We are interested in how do current users of financial services and electronic banking perceive available solutions, how do they view security issues, how do they feel like when using different forms of payment, or whether are they aware of the threats arising from various technological solutions and risky behaviors. We would like to get to know the users better, their attitudes and fears, to be able to identify areas that are worth special attention in the context of education, information, and the ability to change the formula of the services provided.

The guidelines we have developed aim to identify elements that improve the comfort and safety of using

[1] https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up

Wodo, W. and Stygar, D.
Security of Digital Banking Systems in Poland: Users Study 2019.
DOI: 10.5220/0008555202210231
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 221-231
ISBN: 978-989-758-399-5; ISSN: 2184-4356

new services. We believe that our research will help to capture aspects that were not included in the preparation and design of services and systems by banks or state administration. We want to shed new light on the financial services ecosystem from a user perspective that is not uniform. This paper is essence extract of full research conducted in this area. It presents and summarises the main assumptions and results.

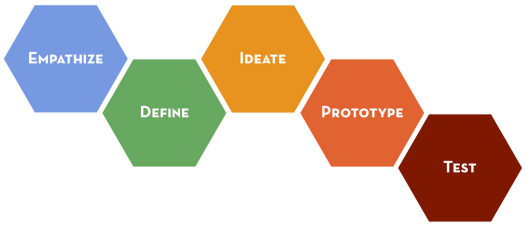
1.2 State of the Art

In the area of electronic banking, research is ongoing to monitor the state of its development, availability of services, threats and the structure of users. Thanks to the activity of the Polish Bank Association (ZBP) the Bank Cybersecurity Center was established, which monitors incidents and threats in the network, and coordinates and manages difficult situations. ZBP also regularly publishes reports on topics related to the level of adoption of banking services in the country, as well as security issues. It is worth quoting the 2018 report on the "Cybersecure Portfolio" (Zwiazek Bankow Polskich, 2018) indicating the behavior and preferences of banking customers as well as paper "PSD2 and Open Banking - Revolution or evolution?" (Zwiazek Bankow Polskich, 2019b) looking at the issues of open banking and the PSD2 directive, as well as business opportunities and threats to the fintech market. Thanks to the cooperation of the Conference of Financial Companies in Poland and EY, an annual report (since 2009) on fraud in the financial sector is created (The Conference of Financial Companies in Poland, 2018). The report presents changes in the digital banking services market, new threats and policy changes for financial institutions. In 2019, MasterCard performed research in the context of Polish consumers' attitudes towards online shopping, taking into account the upcoming changes in e-commerce payments. The result of their work is the "Secure e-shopping" report. The authors prove that biometrics will become the standard for confirming identity in payments. In addition, more than 75% of respondents believe that strong authentication of online card payments, which will enter into force in mid-September 2019, is needed, which clearly sets a new trend in banking. In 2016, Polish users' preferences, their attitudes and level of awareness in relation to the security of mobile devices and biometrics were examinded. This work resulted in the report "Security and biometrics of mobile devices in Poland. User surveys 2016" (Wodo and Ławniczak, 2016). The study distinguished four main types of users of mobile devices and applications, assigning them characteristic features, views and behaviors. Disturbingly, more than half of the users showed nonchalance and carefree approach to security aspects, they did not attach importance to the value of their data and identity. The most important conclusion of the report is that it is impossible to create one universal solution that responds to all security needs of mobile device users. Security systems should be designed with a specific audience in mind that combines similar characteristics, views and needs. The topic of corporate banking security was in turn taken up by KPMG, preparing the 2018 report on Mobile Technology Security (KPMG, 2018). The report shows that companies are more attentive to security than individual customers. Over half of the surveyed companies use mobile devices in their business practice, and 76% of organizations do not allow the processing of company data on employees' private mobile devices. Over half of the companies enforce authentication for access to a mobile device and only install mobile applications approved by the organization. Yubico sponsored research in 2019 devoted to users' approach to passwords and identity authentication security, resulting in the State of Password and Authentication Security Behaviors Report (Ponemon Institute LLC, 2019). The study was conducted in the United States, Great Britain, Germany and France on a sample of 1,761 people involved in IT technologies. Interestingly, over 57% of respondents said that due to the fact that password management is inconvenient and cumbersome, they would like to use alternative methods to authenticate their identity. 56% of respondents were in favor of using dongles. The report shows that the use of two-factor authentication is not common, 67% of respondents do not use 2FA in any form in their personal lives, and 55% do not even use it at work.

2 USERS' STUDY

In order to analyze the situation in the area of security technology of electronic and mobile banking services in Poland, exploratory research on the user market was carried out using the Design Thinking methodology. It is a method of creating innovative products and services based on a deep understanding of users' problems and needs, developed at Stanford University in California (Brown, 2009). The main assumption of this method is to focus on the user, because it is he who will bring the answer to the guiding questions related to awareness and approach to electronic banking security systems. In order for the proposed solution to reach maturity, it should undergo several project cycles during which it will verify the decisions taken and the directions of work chosen, and above

all it will collide with its final recipient - the user. The stages of the Design Thinking process are illustrated in Figure 1.



Source: www.longevity3.stanford.edu/designchallenge

Figure 1: General scheme for Design Thinking process.

We do not forget about possible limitations of our research, that is the way we would like to discuss them in following paragraphs. This paper reaches third stage of DT process - Ideation. The study involved 62 people constituting the research sample, including 32 men and 30 women aged 18 to 78 years – 18-23 (48,4%), 24-45 (32,3%), 45+ (19,4%). It should be emphasized that the conducted research is a qualitative research in which a single interview with the respondent lasts about an hour and is focused on a thorough understanding of the respondents' attitudes, thoughts and behaviors. We tried to select our research group in such a way it could be diversified both in terms of gender and age, but also education and profession, thanks to which the obtained information has a greater cognitive value and is not biased.

At the same time, a larger share of a group of people aged 18-23, i.e. a learning / studying group, was taken into account, as they are natural users of new technologies and will soon start their professional life. They will constitute a new segment of financial services clients, hence we decided that their examination is particularly important for the conclusions and recommendations for the future.

2.1 Questionaire

According to the adopted methodology, work began with the creation of an interdisciplinary research team, which due to the diverse experience of members, could look at the research problem from many perspectives. The construction of the questionnaire is the result of the diversified knowledge and experience of the team that developed it to maximize the answers to the most important questions from users. In the first phase of the Design Thinking process, a framework interview questionnaire was constructed. The rules and guidelines suggested by American process creators were taken into account, while remembering the context of the study. As it was decided to use in-depth interview, the importance of exploring the respondent's needs and fears was emphasized. Attention was also paid to behavioral aspects - i.e. behavior, gesticulation during the answers given and the inseparable expression of emotions associated with it, e.g. through the tone of voice, speed of speech or facial expressions. It was decided that the above aspects should constitute the frame of the interview, and the questionnaire should be the starting point of the conversation, which direction the questioner will decide on. Before proceeding to the interview phase, a research team of ten members was trained to conduct research correctly and uniformly to ensure consistency and quality of the data obtained. The questionnaire covered 13 areas and consisted of open questions whose purpose was to explore the area of using electronic and mobile banking. The emotional background accompanying the responses expressed in the respondents' behavior was also examined, and attempts were made to capture the motivation of their decisions. The interview also raised issues of views regarding the issue of cybersecurity. The main purpose of the questionnaire was to highlight the needs, concerns or concerns of users related to various aspects of using electronic banking and related services. The areas discussed in the interview concerned: - use of electronic and mobile payments, ways of carrying them out and authentication; - a sense of security resulting from the use of online and mobile payments; - use of mobile applications for electronic payments and their updates; - experiences and emotions (personal or loved ones) related to cyber attacks; - hygiene in using electronic and mobile banking, knowledge of security rules and compliance with them; - knowledge of issues related to cyber attacks on electronic finances and sources of information about them; - the use of payment cards and contactless payments, applicable limits and security rules; - knowledge of double verification mechanisms (2FA), ePUAP system, identity verification services such as "log in via a bank" and attitudes towards them as well as the degree of their use; - imagining an ideal security system for electronic banking services and mobile;

2.2 Collected Data Presentation

This part of the study will present data obtained from interviews, both in quantitative terms, as well as their discussion broken down into individual issues. The research areas will be provided with the users' own statements, which will allow to accurately illustrate the attitude, opinions and approach to the discussed issues. This approach allows you to more easily iden-

tify your (reader) views and behaviors with described people, because their characters become closer and more real to us through references to situations, facts and behaviors known to us from our own lives. The presented statements are only part of the interview - it is impossible to describe all dependencies in a graphic form, nevertheless those that best illustrate the purpose of the research were presented.

2.2.1 How Do You Pay for the Services and the Products? Why?

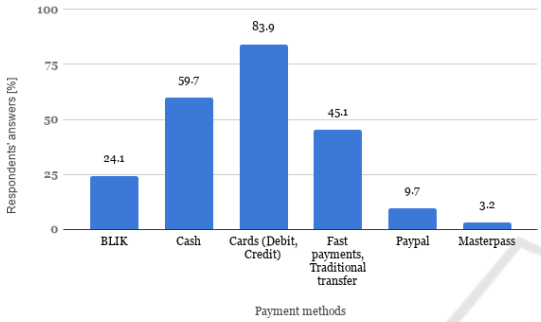


Figure 2: How do you pay for the services and the products? Why? (n=62).

The overwhelming number of people - 83.9% of respondents, pay by card (debit, credit, etc.) on a daily basis. Many answers show that mobile banking users like to "enjoy freedom" - for many, card payments are fast, and the lack of the need to have a full cash wallet with them is a convenience that has repeatedly appeared in the statements of respondents. However, it is not only speed that determines how the respondents pay.

People are more likely to choose methods they know and inspire more confidence. Thanks to such answers it can be concluded that the popularization of a given payment method and its advertising affects the number of people who will use it.

2.2.2 How Do You Pay for Online Shopping? Why?

Of all respondents, 92% pay for online purchases. Others. 8% either do not shop online at all, or ask someone close to buy, or only use cash on delivery. Fear accompanies more than one user of electronic banking. Once again, the respondents' main reasons for using selected payments are speed and convenience, which is emphasized by several of the respondents.

According to the respondents' answers, they do not consider using certain payment methods in terms of security. For example, a card payment transaction is a reasonable choice for online payments. While the respondents mention the simplicity and speed of this solution, it is worth adding that card payment is also secure, for example due to chargeback. Thanks to it, in certain cases, the owner of a payment card may apply for a refund of the transaction amount.

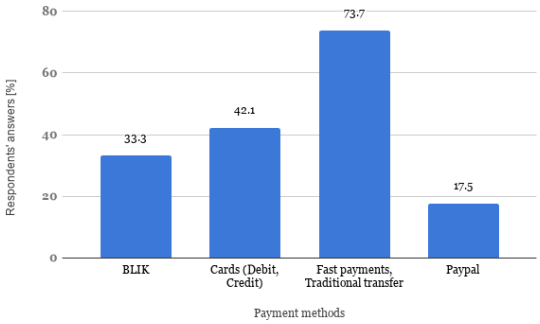


Figure 3: How do you pay for online shopping? Why? (n=57).

2.2.3 What Methods of Transaction Confirmation Do You Know and Use?

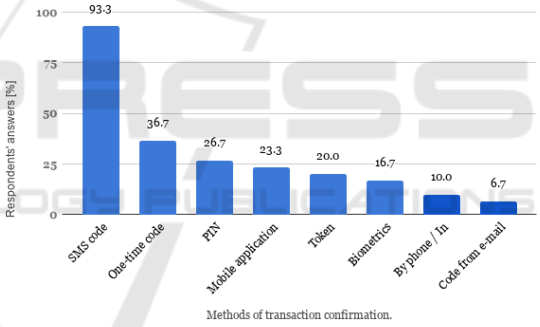


Figure 4: What methods of transaction confirmation do you know? (n=30).

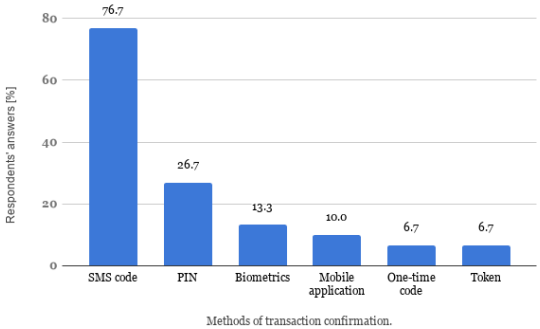


Figure 5: What methods of transaction confirmation do you use? (n=30).

In both cases, many respondents misunderstood the question. It concerned transaction confirmations, such as a one-time code, which allowed the payment

process to start. In the interpretation of some of the respondents, transaction confirmations are SMS notifications and emails that say that the payment process has been completed. Due to this interpretation error, the statistical sample for these questions is half of those surveyed.

The best-known method of confirming transactions is a one-time SMS code. This may be primarily due to their high popularity in Polish banking.

Banks encourage the use of SMS codes, withdraw other transaction authorization methods[2], and several respondents pointed out that in their bank SMS codes were the only possible option to choose.

SMS codes may not be a secure way of confirming transactions, as there is an option to add a trusted recipient. After this action, the SMS code is not required to complete the transaction. It is also possible to duplicate the SIM card and take the victim's number[3]. The implementation of the SMS code mechanism is also sometimes faulty. The code may not be associated in any way with the transaction performed by the user, so it is possible to use it at the same time for another transaction (e.g. substitution of given transactions).

2.2.4 Do You Feel Safe/Comfortable When You are Paying Online?

Anwers for this question are following (for n=56): Yes - 69,6%, No - 5,4%, Not Always - 25%.

An overwhelming number of people say that they feel safe when using the above payment. A frequent justification among the respondents was the lack of unpleasant experiences. An additional answer was distinguished - "not always".

Considering the answers and conclusions from previous questions, it can be seen that respondents in everyday life do not worry about safety. What counts is that the service works well, hence the repeated emphasis on the speed and convenience of the solution. The security of banking systems is not long in the minds of users. Most of them are unaware of lurking threats or unpleasant consequences. Many respondents personally did not experience any unpleasant incidents. This may lead to the conviction that they cannot be attack objects, which translates into a (false) sense of security.

[2]https://www.zadluzenia.com/pekao-rezygnacja-z-kart-kodow-jednorazowych/

[3]https://niebezpiecznik.pl/post/duplikat-karty-sim-kradziez-bank-mbank-bzwbk/

2.2.5 Do You Check Your Bank Account in Public Places?

The majority of respondents believe that home and work are safe places for financial operations. Sometimes, however, there is a need to carry out a financial operation in a public place and then the respondents decide to do it (44.8% of respondents), with the proviso that they use their device (25% checkers), try to find a secluded place, or at least cover the screen during entering login details or transaction data (35.7% verification). In addition, 11.5% of respondents who check the account declare that they are accompanied by a sense of discomfort. The above numbers show the respondents' concerns related to violation of the sphere of privacy or potential threat to finance. Only less than 31% of respondents perform financial activities in public places without fear and discomfort. Some of the surveyed people have developed methods that allow a greater degree of security to use electronic finances in public places, namely using a percentage slider in a banking application that reflects the account balance in relation to the set amount.

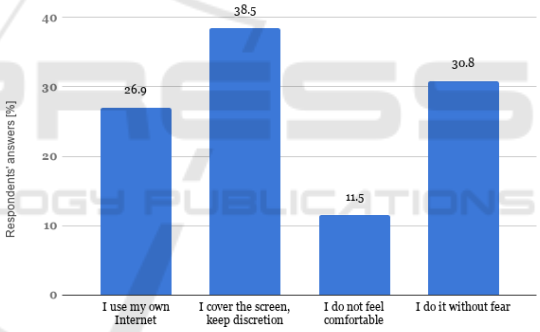


Figure 6: Behaviors and emotions among people checking a bank account in public places. (n=26).

2.2.6 Have You Heard about Cyber Attacks on Electronic Finance?

Over 88% of respondents have heard about cyber attacks on electronic finances, however, after analyzing quotes describing this information, one may get the impression that this information is rudimentary, imprecise, not bringing with it solid knowledge, what should be done to avoid such an attack in the future. Only 12.9% of those surveyed answered in the first place about such incidents.

2.2.7 Where do You Get Knowledge about Cybersecurity?

The dominant source of information on cybersecurity among the respondents are general media (approx.

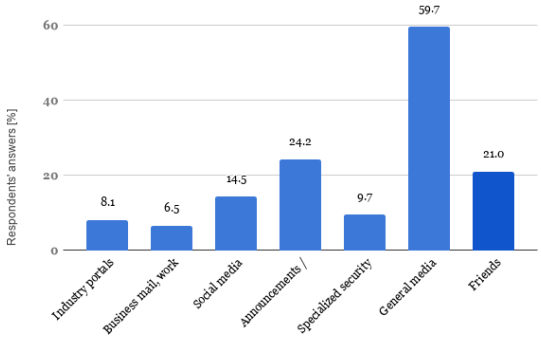


Figure 7: Where do you get knowledge about cybersecurity? (n=62).

60%), such as the Internet (information portals) as well as television and the press.

These are carriers of unprofessional information, but they should clearly be used to reach a large group of recipients, hence banks should devote more attention to them while conducting information and educational campaigns.

About 25% of respondents declare that they read ads and banking information, this would indicate an important educational and information channel.

One should work on the form of banking messages, because for the average recipient the content transmitted there is unattractive and incomprehensible, which means that they quickly lose their attention and do not have the proper effect. Over 20% of respondents advise friends on security issues, this information channel cannot be directly influenced. On social media, which for almost 15% of respondents are a source of information about security already. By addressing these communication channels, you can reach the majority of different users, so they are excellent places for educational and warning campaigns.

2.2.8 Do You Think That Cyber Attacks Apply to You?

Answers show, around 74% of people think that cyber attacks can affect them. At first, this result looks promising, because it shows that there is awareness of the threat arising from the world of cyber crime. Unfortunately, some of these people immediately underestimate the reality of such attacks by saying: ”I will not be attacked because I have no money” (∼11%) or ”I am not afraid because I have secured myself well” (∼6.5%). This is reflected in the answers to the next interview question. A large proportion of respondents (around 21%) do not believe that cyber attacks affect them, arguing with their opinions on the content of bank accounts.

The conclusions of these results are appalling, because a large group of people clearly do not realize that they can become the target of cyber criminals and that you do not need to have big money or be important. They clearly lack awareness of how such attacks take place and that in most cases they are not targeted, but automated, based on phishing and installing malware on victims’ devices.

2.2.9 Have You Personally or Someone Close Become a Victim of a Cyber-attack on Finances? What did You Feel? What did this Person Feel?

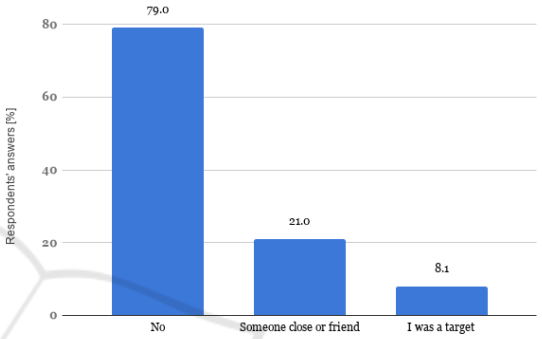


Figure 8: Have you personally or someone close become a victim of a cyber-attack on finances? (n=62).

The answers to this question are an extremely important clue, because they show that almost 80% of respondents did not experience harm and did not fall victim to a cyber attack on their finances.

Lack of such direct and strong experience makes their perception of threat less real, it is difficult for them to imagine what their situation would look like and what emotions would accompany them. It is also associated with a lack of reflection on cyberspace security issues in everyday life. It is easy to imagine what will happen if we do not close the apartment and lose our possessions, it is much harder to think about virtual money and bank accounts that are intangible and distant.

Over 21% of respondents declare that unpleasant incidents related to cyber attacks occurred in their families or friends, this experience should sensitize them to security issues, but they are not their own experience, so the impact of such situations is much smaller.

8.1% of respondents have suffered harm as a result of a cyber attack, their attitude and approach to security have changed dramatically.

2.2.10 Does Your Bank Warn You about Cyber Attacks?

Answers (for n=59) are following: Often, through various channels - 58%, Sometimes - 25%, No notifications I did not notice - 17%. It is very important to ensure the awareness of users of electronic banking. They should be kept informed of any attacks they may be exposed to. Otherwise, they can easily become victims. To the question "Does your bank warn you about cyber attacks?" As many as ∼83% of respondents said yes. This is positive information, but you should ensure that this indicator increases all the time, because it means that the remainder of ∼17% are not sent or are published in a form that remains unnoticed by users.

While answering the question, a condition was noted, which should be given special attention. About 22% of surveyed users who said they received notifications openly admit that they do not read this information.

2.2.11 What Safety Rules Do You Know?

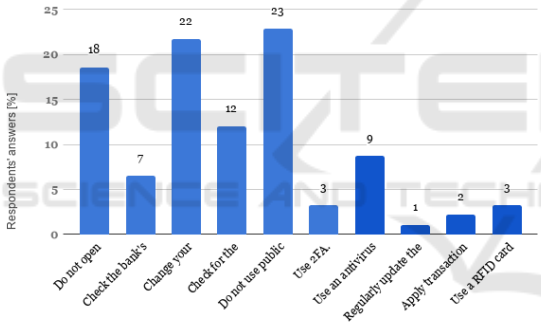


Figure 9: What safety rules do you know?

The responses show that a large proportion of respondents are aware to use strong passwords and change them regularly.

Equally popular indications were to avoid opening suspicious emails and links. It allows, among others avoid entering login details on the crafted page. The surveyed people do not use public networks when using electronic banking, fearing the interception of sensitive data. The "Regularly updated software" option definitely received the least number of indications, however, this is due to the fact that the vast majority of respondents use automatic updates and do not have to remember that on a daily basis. The rule to check the URL of the bank's website was quite popular. Some respondents use bookmarks in the browser, so they do not have to enter the address themselves.

However, it is common behavior to enter the bank name in the Google search engine and select the link that comes first from the searched items. This behavior combined with the lack of address verification can lead to dangerous situations.

2.2.12 Do You Know Any Form of Phishing?

About 15% of people openly admitted that they do not know any forms of phishing.

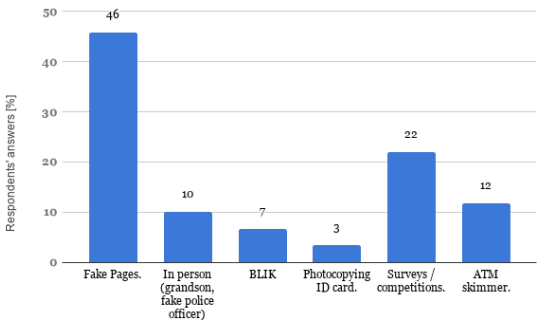


Figure 10: What forms of phishing do you know? (n=59).

Physical and virtual methods were among the types of phishing scams mentioned. The physical, which according to the answers constitute about 1/4 of the total indications, can be attributed to the method of "granddaughter", photocopying an ID card and the use of skimmers in ATMs. However, by far the most popular form among the respondents is phishing, which obtained almost 46%.

The possibility of photocopying an ID card as a form of phishing has been mentioned alarmingly rarely. The problem with this type of behavior was to be solved by the "Act of November 22, 2018 on public documents"(Polish Parliament, 2018b) , but photocopying will still be possible.

2.2.13 How Do You Verify the Bank's Website?

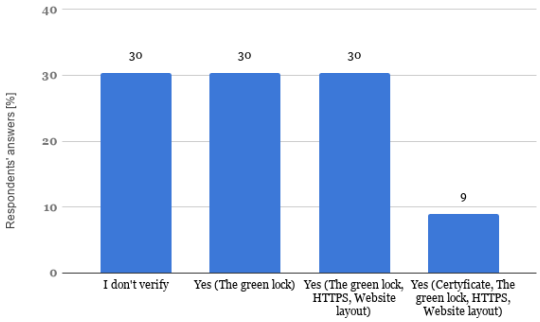


Figure 11: How do you verify the bank's website? (n=56).

About 30% of surveyed users said that they did not verify their bank's website at all. People who carry out verifications mainly check the presence of a "padlock" at the bank's address and graphic design, and

only 9% of people additionally check the certificate. A disturbing phenomenon is that the people who carry out the verification do not have adequate knowledge whether this is sufficient treatment. Therefore, they feel anxious when using electronic solutions because they are not sure if this guarantees their security.

2.2.14 Have You Heard of Two-Factor Authorization (2FA)?

As it turned out, there are often those who have heard of 2FA (69% people), 24% of respondents are not concerned with knowledge about 2FA. Only after explaining the interviewers did the respondents often realize that they knew and even used this solution.

Some users are not familiar with the names of the solutions they use. The reason for this may be the fact that banks use too superficial - descriptive names of solutions, as well as the fact that many surveyed users of electronic banking do not broaden their knowledge in the field of security.

Author's comment: It is important that banking institutions not only inform the user in a clear but also non-trivialized manner about the solutions used. A short but reliable explanation could encourage a better understanding of how a given system, method (e.g. authentication) works.

2.2.15 Do You Use Two-Factor Authorization (2FA)?

Most respondents use 2FA (67,4%). The question was asked to a group of respondents who in the previous question declared knowledge of two-factor authorization. Analyzing the answers to the above question, one can notice a certain lack of consistency of respondents. Many people want to use additional security features, although they may be less convenient than, e.g., one-factor authorization. Of course, there will be people who do not want to use additional security, because they associate it with a problem, not security. Therefore, we need to popularize authorizations such as biometrics, which is a convenient and effective way of confirming identity. Similar conclusions were made in the results of research carried out by MasterCard[4].

2.2.16 Do You Use the Application (on Your Phone / Computer) to Store Passwords / PINs for Login / Authentication?

Subjects almost equally use and do not use mechanisms to store and manage passwords for authentication services. Among those who declare the use of such mechanisms (46.7%), the most popular is remembering passwords in the browser (over 66% of use cases). The Apple user pool uses a keychain (10% of use cases). In addition, people who use these solutions indicate that not for banking applications! The attitude of the respondents to mechanisms and tools supporting the process of remembering passwords and keys for authentication services is described.

2.2.17 How Do You Imagine an Ideal Electronic/ Mobile Payment Security System?

From the answers given, it can be concluded that users feel the need to increase the level of security. The most frequent indications are the greater use of biometrics, e.g. fingerprint, iris scan. Such solutions inspire the trust of respondents, regardless of their age or experience in electronic banking. This was indicated by both younger and older people.

Based on some interviews, an image of a person is also created for whom comfort is definitely more important than safety. Such a person would gladly give up, for example, confirming activities by using SMS codes. This opens the way to the popularization of biometric solutions.

In addition, attention was paid to the problem of the multitude of data for logging in to various websites. The respondents believe in the security of banking solutions and would be more willing to use the possibility of authentication through a banking service, as it is the case with the ePUAP website. This creates a chance to introduce solutions such as myID (Krajowa Izba Rozliczeniowa, 2019).

2.3 Personas

The research allowed to deepen knowledge about users of electronic and mobile banking. Based on the analysis of the answers given by users and the accompanying emotions, three main personas were identified, combining similar behavioral traits, needs and fears. Personas distribution (for n=62) is: Naive Nadia (45%), Fearful Frak (10%) and Reasonable Rick (45%).

2.3.1 Persona 1 - Naive Nadia

This person has little knowledge of current banking systems. She is usually familiar with the very basic principles of using electronic or mobile payments, and her knowledge of attacks on electronic banking is often low or negligible. This results in Nadia's conviction that she cannot be the target of a hacker at-

[4]www.zadluzenia.com/bezpieczne-e-zakupy-mastercard/

tack, because she is an unattractive target because she does not have a large amount of financial resources and is not an important person. In banking, she values speed and convenience above all. She does not think about the security of the systems she uses, therefore she does not feel the need to explore her knowledge in this direction, believes that someone else will take care of its security. Nadia often has no need to use technical innovations and the basic payment mechanisms she is used to are satisfied with it, she does not see the benefit of using them. She is not looking for new safety information in the media. Naive Nadia in some cases is accompanied by the belief: "I do not know, so I do not care", which is dangerous for her finances. Despite the use of electronic and mobile banking, she is not interested in whether the given solution is secure. Often, elements such as payment and authentication methods are selected only on the basis of the bank's recommendations and uses factory settings.

2.3.2 Persona 2 - Fearful Frank

A person who has some concerns about electronic and mobile banking. Despite his fears, he uses modern solutions but with great uncertainty. Frank has some knowledge related to banking, but it is usually not complete, which can lead to various inaccuracies. This person derives information mainly from the internet, but not from professional sources, hence often operates on "half truths" about an attack or system. In addition, Frank may be very distrustful of financial systems, fear espionage and conspiracy, which results from a lack of his thorough knowledge and a lack of willingness to deepen it. His attitude is often represented by statements such as "they know", "everything is monitored", "I don't trust my phone". Frank feels calmer when he is aware of how the solutions he uses work. If in his opinion the application is simple and transparent, and his data is not saved anywhere, then he is not afraid of losing funds or attacks. What is most important for him in banking can summarize the statement: "The certainty that a given transaction will be carried out, that nobody will mix anything in it and the money will go to the right recipient."

2.3.3 Persona 3 - Reasonable Rick

A person well-versed in banking and new technologies, aware of the risks associated with cyberattacks on electronic finance. Rick knows and applies various security mechanisms and generally adheres to security principles. This person draws knowledge from various sources, they are often reliable and proven. Rick sometimes even visits industry portals to read some details. In addition to speed or convenience, it often mentions that security is an important feature of the banking system. It may happen that Rick overestimates his knowledge and his confidence is too high, which is expressed in beliefs such as "messages from the bank are too simple, I already know everything" and thus skips bank alerts or exposes to new threats.

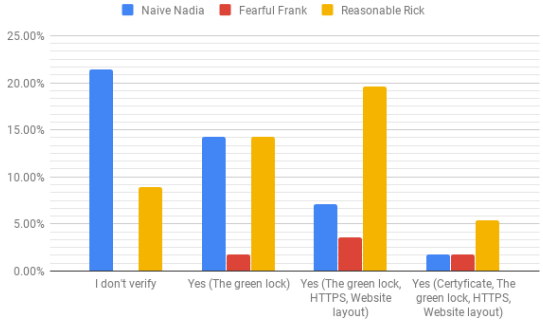


Figure 12: How do you verify the bank's website? (with personas distribution) (n=56).

Among those who do not verify the bank's website, those with the characteristics of Naive Nadia predominate. This proves that it is primarily the lack of knowledge and putting convenience over security that are the cause of exposure to potential attacks. It can be seen that as users become more aware, the number of ingredients that are verified when visiting the bank's website also increases. This is illustrated by the increased participation of people with the characteristics of Reasonable Rick in subsequent answers to this question.

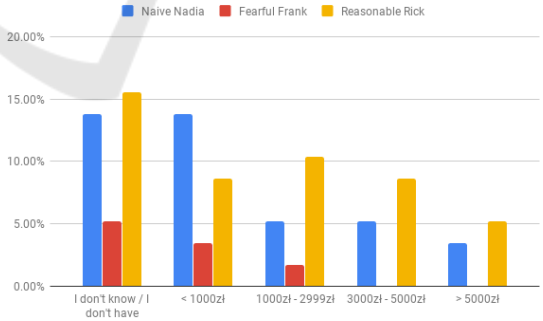


Figure 13: What is your payment limit? (with personas distribution) (n=58).

Based on the answers and distinguished people during the study, it can be concluded that people with the characteristics of Reasonable Rick set definitely higher limits than other persona. It may be related to the fact that these people feel safe because they make more effort while verifying other security mechanisms.

3 RESULTS AND FURTHER STUDY

This part of the study will summarize the research carried out and formulate the main conclusions resulting from it. In addition, recommendations will be developed for both users and financial institutions.

3.1 Main Outcomes

- Users often mention as a service that they use a specific brand of the company that provides this service. This demonstrates the strength of the brand's recognition and its impact on the recipient.
- Respondents begin to understand the need to use biometrics, trust it more and appreciate the benefits it brings.
- Users benefit from new, digital services if they experience benefits for themselves. An excellent example was the possibility of settling PIT tax in 2019, where you could log in with the help of a trusted profile or a bank. Many respondents used the ePuap platform service for the very first time.
- Respondents show confidence in banking institutions and willingly use authentication mechanisms through them (including the Trusted Profile service). This indicates a promising direction for the development of identity management services and its verification by financial institutions.
- 60% of respondents indicate television, the press and ordinary non-industry information portals as the main source of information about security. The use of these sites during socio-educational campaigns can significantly contribute to raising users' awareness.
- Market penetration through 2FA solutions is quite high, about 70% of respondents declare the use of a double authorization mechanism. The implementation of the PSD2 directive by the banking sector will further promote the use and awareness of these solutions.
- Only 3.8% of people indicated photocopying their ID as a form of phishing. This shows the lack of awareness of the consequences of such behavior among the respondents. The solution to this problem was to be the Act of 22 November 2018 on public documents (Polish Parliament, 2018b), but the interpretation of the provisions in relation to financial institutions is still not clear.
- 1/3 of respondents cannot answer at what level they have set limits, e.g. cash withdrawals or transfer amounts. 22% of respondents use limits of over PLN 3,000, including 9% set over PLN 5,000. Given the average earnings in Poland for 2019, which is PLN 3,600 net, these people risk losing almost all of their earnings.
- Over 60% of respondents verify the bank's website by checking the "green padlock", similarity of the website's graphics and the HTTPS protocol in the address bar, but they are still not sure if this is enough. Only about 9% of respondents check the site's certificate.
- Over half of the respondents (approx. 63%) are aware of the reality of cyber threats on their finances. On the one hand, it still shows a lot of room for education of users, while on the other it calms down a bit, showing that awareness of threats arising from cyberspace is growing every year (The Conference of Financial Companies in Poland, 2018).
- Only a small number of people surveyed (about 8%) directly experienced a cyber-attack on their finances or data, hence most of the respondents cannot imagine how this situation looks like and what their emotions are. It is foreign and distant to them.
- The popularity of applications for electronic payments such as GooglePay or ApplePay is not large, less than 13% of users declare their use. This is probably due to the high availability of various mobile and electronic payment mechanisms in Poland (Shoper, 2019), hence the need to use these specific is not great.

4 CONCLUSIONS AND FUTURE WORK

Summing up our research, we identify the evident need to match security solutions and communication methods to several existing client archetypes, because they are characterized by distinctly different needs and approach to the issue of electronic banking. Among the diversified surveyed group, there are still large gaps in knowledge and awareness regarding cybersecurity issues when using digital banking solutions. The good news is that an increasing number of people know and use the second verification factor as well as point out biometrics as an alternative to standard security mechanisms. Efforts should be made to constantly educate the market and customers in cooperation with institutions and companies that have recognition among customers.

As the main focus for future work in this area we would like to investigate in more detail the usage of second security factor (i.e. biometrics, tokens) in mobile banking security systems and apps. What is also important in the context of banking security is the General Data Protection Regulation (European Parliament, 2016) and its impact on security mechanism and at least data processing and storing, including backups and erasing data on customer demand. What should be addressed here is appropriate mechanisms fulfilling both banking law and GDPR, which is challenging, especially in the prospect of implementing the PSD2. We will create assesment criteria to perform preliminary evaluation of Polish and European Banks in the first place, we will quantify the answers and assign scoring for each criteria. We also want to extend our study to other coutries, in Europe as well as in Asia and North America.

ACKNOWLEDGEMENTS

We would like to express our gratitude to our colleague Klaudia Winiarska for support during investigating these issues, brainstorming and contestation of assumptions.

REFERENCES

Brown, T. (2009). *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation*. HarperBusiness.

European Parliament (2015). Directive (eu) 2015/2366 of 25 november 2015 on payment services in the internal market. Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN.

European Parliament (2016). General Data Protection Regulation. http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf/. Accessed on 21.10.2019.

KPMG (2018). Bezpieczeństwo technologii mobilnych. https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/11/pl-raport_kpmg_bezpieczenstwo_technologii_mobilnych.pdf.

Krajowa Izba Rozliczeniowa (2019). myID. https://www.mojeid.pl/. Accessed on 21.10.2019.

Ministry of Digital Affairs (2019a). eID card. https://www.gov.pl/web/e-dowod/. Accessed on 21.10.2019.

Ministry of Digital Affairs (2019b). mObywatel. https://www.gov.pl/web/mobywatel/. Accessed on 21.10.2019.

Ministry of Finance (2019). Your e-PIT. https://www.podatki.gov.pl/pit/twoj-e-pit/. Accessed on 21.10.2019.

Polish Parliament (2018a). Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf.

Polish Parliament (2018b). Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych. Journal of Laws of the Republic of Poland. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000053/O/D20190053.pdf.

Polish Parliament (2018c). Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Journal of Laws of the Republic of Poland. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/O/D20181560.pdf.

Ponemon Institute LLC (2019). State of password and authentication security behaviors report. ponemon institute research report. https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf.

Shoper (2019). Płatności. raport. https://www.shoper.pl/static/raporty/Shoper_Raport_Platnosci_2019.pdf.

The Conference of Financial Companies in Poland (2018). Nadużycia w sektorze finansowym. raport z badania. https://www.zpf.pl/pliki/raporty/raport_naduzycia_2018.pdf.

Wodo, W. and Ławniczak, H. (2016). *Bezpieczenstwo i biometria urzadzen mobilnych w Polsce. Badania uzytkownikow 2016*, pages 1–16. Oficyna Wydawnicza Politechniki Wrocławskiej, Wroclaw, Poland.

Zwiazek Bankow Polskich (2018). Cyberbezpieczny portfel. https://www.zbp.pl/getmedia/5f90b612-ac57-43fc-bc98-49870e34d555/Raport_ZBP_-_Cyberbezpieczny_Portfel.

Zwiazek Bankow Polskich (2019a). Polish API. https://polishapi.org/. Accessed on 21.10.2019.

Zwiazek Bankow Polskich (2019b). PSD2 i Open Banking - Rewolucja czy ewolucja? https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/03/pl-raport-kpmg0-zbp-psd2-i-open-banking-rewolucja-czy-ewolucja.pdf.