ANNALS OF THE POLISH ASSOCIATION
OF AGRICULTURAL AND AGRIBUSINESS ECONOMISTS

Received: 30.12.2021
Acceptance: 28.01.2022
Published: 15.03.2022
JEL codes: G21, G41, E44, K42, R51

Annals PAAAE • 2022 • Vol. XXIV • No. (1)

DOI: 10.5604/01.3001.0015.7102

SYLWIA KLUS[*], NATALIA ŁUKASIEWICZ[*], ZUZANNA URBANOWICZ[**], LESZEK WANAT[***]

[*]Poznań University of Life Sciences, Poland
[**]Poznań University of Economics and Business, Poland
[***]Collegium Da Vinci in Poznań, Poland

E-BANKING SECURITY DILEMMAS OF USERS LIVING IN RURAL AREAS – THE CASE OF KONIN COUNTY IN WIELKOPOLSKA

Key words: e-banking, cybersecurity, financial security, rural areas, Konin County, Wielkopolska

ABSTRACT. The aim of the study was to identify selected threats to e-banking security in the opinion of rural residents, on the case of Konin County. Available e-banking services were analysed against the background of cybercrime threats. The research was conducted in the year 2019. In the spatial scope, it concerned Wielkopolska and the territory of the Konin County, which consists of 14 municipalities, including 5 urban-rural municipalities and 9 rural municipalities. Using the method of diagnostic survey, on a sample of almost 400 people invited to the study, the results were collected. The majority of respondents were rural residents. The survey questionnaire consisted of 22 closed questions and information data. Suggested answers were programmed according to a five-point Likert scale. The study used Pearson's chi-square statistical test of independence, comparative and descriptive analysis. Calculations were performed in MS Excel. As a result, a relatively high level of interest in e-banking among the residents of Konin County was indicated. More than 90% of respondents, primarily rural residents, use online banking. This is especially applicable to retail payments, as well as successive control of the household budget. E-banking's usability is mostly determined by: time saving, a widespread availability of services and convenience. Despite the awareness of risks, the level of security of online banking inspires confidence among respondents. Therefore, social and legal responsibility of the banking sector for electronic transaction security is recommended. This is justified by the majority of respondent opinions that traditional banking will be eliminated in the future by e-commerce tools, including e-banking.

INTRODUCTION

The benefits of e-banking are attractive for its universal use. It is the popularity and availability of digital services that encourages not only bank customers but also cybercriminals [Ahmad et al. 2021, Cwynar, Patena 2021]. Some features of e-banking are, as it were, "conducive" to potential infringement: a lack of actual customer-bank contact, the availability of services from anywhere in the world, provided there is good quality electronic communication, and, of course, the universality of access to digital banking for all concerned [Gąsiorowski, Podsiedlik 2015]. The potential threats are related to three different stages of customer-bank communication: on the Internet, on the bank's computer system or on the customer's device (computer or smartphone). These threats can be categorized into automated teller machine (ATM) related, payment card related or occurring in online banking [Arora, Kaur 2018, Chaimaa et al. 2021].

Online communication is particularly important for rural residents [Paszkowski et al. 2018]. It shortens and sometimes completely eliminates the distance of an institution (including a bank) to a potential customer. Digital exclusion, and therefore "banking exclusion", is one of the threats to rural development, both of households and economic activity. Local leadership [Potkański et al. 2011], promoted despite many barriers [Wanat, Potkański 2011], has an important, underestimated mission in this area. It is about both local government activities and building sustainable relationships: intermunicipal, intersectoral and inter-institutional [Chudobiecki et al. 2016, Potkański et al. 2016]. The experience of new public economy studies points to the need for changes in rural development programming [Paszkowski et al. 2019]. Competitiveness and development in this scope will be determined not only by traditional resource factors, but also by apparently "new" criteria based on cooperation and networking [Sujová, Hajdúchová 2015, Klus et al. 2021].

In the perspective of possible e-commerce domination, it seems necessary to study the ability of rural residents to implement new public economy challenges, also in spatial economy [Potkański, Wanat 2017]. There needs to be a balance between security threats and the benefits and popularization of digital communications. For these reasons, studying and gradually eliminating dilemmas in e-banking usage appears justified and necessary. This problem not only concerns individual users, including households, farmers and seniors [Sikora et al. 2018, Orłowska, Błeszyńska 2020], but also local communities in rural areas [Wanat et al. 2021]. Therefore, the aim of the study was to identify selected threats to online banking security in the opinion of rural residents, on the case of Konin County. The analysis was performed on banking services available in the selected territory in the context of cybercrime threats.

SELECTED THREATS OF E-BANKING SERVICES – STATE OF THE ART

Past studies have identified the key security threats to online banking as well as possible ways to reduce the risks [Ślażyńska-Kluczek 2016, Skowysz, Krot 2018, Zarańska, Zborowski 2018, Wanat et al. 2019, Paduszyńska, Pawlak 2020, Cwynar, Patena 2021].

The first group of security risks are all steps in the ATM transaction. A popular form of ATM fraud is known as skimming. It involves copying data from a payment card. The cybercriminal installs a special cap on the terminal that allows him to copy information from the card's magnetic strip. The thief installs a camera that records the cardholder's PIN. The captured information is applied to a new, blank card. This card can be used to make ATM withdrawals.

Another threat to ATM transactions is card trapping. This is what is known as "trapping" the card at the ATM (in which case the "prisoner" is the payment card). Once the customer has entered the PIN, the card is blocked, and the ATM returns the cards to the owner. This is the same situation as a payment terminal failure. After the customer leaves, the thief can unlock the card and withdraw cash [Gąsiorowski, Podsiedlik 2015]. Cash trapping is a similar threat. This is cash blocking at an ATM machine, prepared by a thief. The customer walks away thinking it is a payment terminal malfunction. Then the criminal removes the lock and seizes the money.

The second group of security threats are weaknesses in e-card payment transactions. The basic security device of payment cards is PIN (Personal Identification Number). It allows for the authentication of the e-card user. The most important threats include card theft, online shopping using data from another ("stolen") card and skimming [Gospodarowicz et al. 2018].

Card thieves often do not know the PIN of the actual cardholder. They then try to make as many touchless transactions as possible that do not require authorization (PIN, signature). Lost card lists are usually updated by banks once every 24 hours. Criminals, therefore, have at least 24 hours to make multiple payments or withdraw petty cash (up to the limit) from a payment card. Additionally, if the thief knows the customer's security code, he can make higher value purchases. However, this is also a higher risk for the thief because such transactions are authorized (and remembered) online [Gąsiorowski, Podsiedlik 2015].

Online shopping using another owner's payment card information is identity fraud. Of course, it is not necessary for the persons making the transaction to make the purchase online in person. Online stores require a CVC or CVV (Card Verification Code/Card Verification Value) code to authenticate the buyer. Such a code can be found on the back of the payment card. So, a payment card thief with CVC or CVV details can easily carry out his crime-target.

A popular cybercrime is skimming. This is stealing payment card data by using (taking over) the cardholder's PIN and scanning the data from the card's magnetic stripe. The thief writes the data to a new, blank card and uses it to withdraw cash or for direct purchases. It is far less likely that payment cards are stolen before they get to the owner. Most often, the thief intercepts the card while it is being sent by conventional mail to the recipient. It is equally rare for a card to be intercepted by providing false personal information, using an identity document forged or stolen from another person.

One of the biggest threats of using bank payment cards is the process of so-called contactless payments. The volume of these simple and convenient transactions is continuing to grow. Of course, the increase in the popularity of use is accompanied by an increase in crime. The data transfer between the payment card and the receiver is performed by Near Field Communication (NFC) technology. This system enables the radio transmission of data over short distances (up to 20 cm), for high frequencies. It is convenient, but not without risks, A thief with the right receiver can read data from the user's payment card, being in direct contact. The third group of cybercrimes are e-connections, made by devices with Internet access. Some studies have identified threats of using bank services via the Internet (Figure 1).

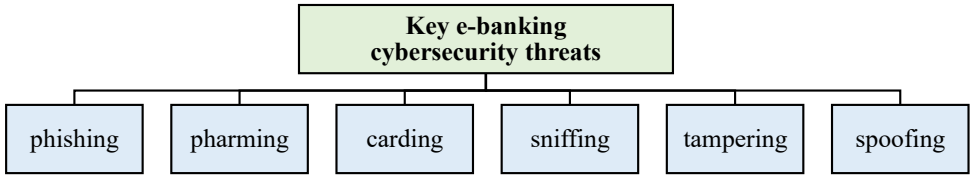

Figure 1. Selected online banking threats
Source: own elaboration based on [Gąsiorowski, Podsiedlik 2015]

Phishing is the simulation and authorization of an institution, like a bank, by a cybercriminal. The goal is to trick a bank customer into providing confidential information (authentication data) or force certain actions by that customer. Fraudsters contact customers using e-services: calling, sending SMS messages or emails. They use various methods to get the user to provide access data to online or mobile banking. Sometimes a false bank website address is sent in an SMS or email message. A customer who responds to such a message allows the thief (who controls the false start website) to save the customer's login data [Gospodarowicz et al. 2018]. Phishing also has an advanced version. This is pharming: redirecting an e-banking user to a website crafted by a cybercriminal. Fake websites can sometimes be identical ("a mirror copy") to bank websites [Gąsiorowski, Podsiedlik 2015].

Of course, banks are running public education strategies to alert customers of cybercriminal attacks. Banks are constantly implementing new security methods [Sołtysik-

Piorunkiewicz et al. 2019]. The responsibility of banks in this regard seems obvious [Szpringer 2021]. However, e-banking users should constantly learn about the threats and ways to eliminate them. The consequences of knowingly providing identification data do not fall on the thief first, but on the user. The most common is theft, which paradoxically becomes the "donation" of identity.

Not only technologies but also details of electronic fraud are being developed [Ahmad 2021]. Carding is the unlawful use of payment card identification numbers. Knowing the complete number sequence allows fraudulent online transactions. The crime is not so much about stealing the e-card, but the digital data that allows easy and correct online identification. Another threat is sniffing. That is called computer "eavesdropping". The criminal connects to the client's device through a network connection, capturing identifying data. This is a passive activity. An "extended" version of this activity is tampering. This is a combination of identification data interception and its modification by the thief. The modification may concern, for example, the bank account number in a given payment order [Gospodarowicz et al. 2018].

Spoofing is the simulation (impersonation) of a thief's website address with the actual data of the domain under attack [Wiśniewski 2018]. The fraudster intends to steal data, load malware or bypass the access control mechanism. Thus, software is also involved in cybercrime, including viruses, worms, and Trojan horses [Gospodarowicz et al. 2018]. The result of malware can be the deletion or theft of data, blocking the operation of programs used by the owner, or even loss of control of digital devices to a hacker. Some stealware or adware tools are also used to commit e-banking crimes. Stealware allows for the theft of funds, tracks the user and, when payments are made, transfers the money to the criminal's account. Adware, while displaying paid advertisements online, often simultaneously spies on the user [Wiśniewski 2018].

In Polish criminal law, identity theft is punishable by up to 3 years imprisonment [Paduszyńska, Pawlak 2020]. This is a relatively small penalty. The losses (financial and property) of online banking users may be much bigger, exposed to many new e-traps [Zarańska, Zborowski 2018]. These threats affect both young people, for whom online communication is everyday life, and for those users called digitally excluded. On behalf of seniors, necessary e-commerce transactions are often performed by the young: children and grandchildren. Threats are, therefore, not directly related to the demographic structure of the population [Popek, Wanat 2016]. These are services but also universal threats. Systematic research on e-banking security [Wojciechowska-Filipek, Ciekanowski 2019], including studies of user opinions and knowledge levels [Grzywińska-Rąpca, Grzybowska-Brzezińska 2017, Skowysz, Krot 2018, Gangadwala, Goyani 2019], especially of rural residents, is therefore justified and needed. It also draws on the experience of other international studies of rural communities using online banking [Kumar, Gupta 2020, Burra 2021].

MATERIAL AND METHODS

To identify selected security threats to e-banking users, primary data (a survey of Konin County residents) and secondary data (data from public statistics) were used. Based on the opinion of the respondents, the available e-banking services were analysed against a background of cybercrime threats.

The study was conducted in Konin County (spatial scope). The county territory consists of 14 municipalities. These are 5 urban-rural municipalities: Golina, Kleczew, Rychwał, Sompolno, Ślesin and 9 rural municipalities: Grodziec, Kazimierz Biskupi, Kramsk, Krzymów, Rzgów, Skulsk, Stare Miasto, Wierzbinek and Wilczyn. In 2018, Konin County had a population of almost 130 thousand [GUS 2020].

The opinion research was conducted in November and December 2019 (time scope) [Łukasiewicz 2020]. The survey questionnaire consisted of 22 closed questions and an information metric. The questions were related to the popularity of e-banking services in the first part and threats and methods of cybercrime reduction in the second part (subject scope). Preferences for e-banking service use were verified (the types of services, the frequency of use, the rating of service quality and availability). The proposed responses were based on a five-point Likert scale. Calculations were performed in MS Excel.

The research sample (subject scope) was selected from Konin County's population. The survey involved 267 women (68.46% of respondents) and 123 men (31.54%). A total of 403 people, selected randomly, were surveyed. Data from 390 correctly completed questionnaires were included in the calculations. The sample volume was determined based on Steczkowski's method [Steczkowski 1995]. Moreover, when analysing public statistics data describing the population of Konin County [GUS 2020], it was found that the structure of the research sample is similar to the structure of the general population. The sample adopted in the survey was, therefore, considered representative.

The ata metrics box' analysis provided basic information about the respondents. There were 23 respondents under the age of 18 (5.9%). The largest group was respondents between the ages of 18 and 26 (46.67%). In addition, there were 89 respondents aged 27 to 45 (22.82%), 59 respondents aged 46 to 65 (15.13%) and 37 respondents over 65 (9.49%).

The largest respondent group consisted of residents of rural areas (178 people). Moreover, 81 people lived in small cities (less than 4 thousand inhabitants) and 131 people came from a big city (Konin). The dominating group of 163 respondents were inhabitants of Kleczew municipality. No surveys were carried out in the following communes: Wierzbinek, Rzgów and Krzymów.

Assessing the educational level of the respondents, it was found that: 135 people declared having a secondary education, 124 were students and the smallest group only indicated primary education. A large group of respondents were employees (125 declared being on an employment contract). Only 16 unemployed people participated in the surveys.

The data collected from the survey questionnaires were verified, organized, and aggregated. Then, selected computational methods were used: Pearson's chi-square test of independence and Czuprow's coefficient of convergence (a measure of the relationship between two measurable and non-measurable variables).

The chi-square statistical test of independence is used to assess the relationship between the frequency distribution of responses for one variable, with relation to another variable. This test is used when analysing nominal variables or a nominal variable with an ordinal variable. Tested relationships are illustrated by so-called cross-tabulations.

The chi square test assesses whether the observed distribution depends on the other variable. It is calculated by comparing the observed values with the expected values. As a result, the presence of dependence or independence of response distributions can be inferred. The statistical significance of the chi-square test is calculated based on the differences between deviations and the size of the cross-tabulation being tested (the so-called "degrees of freedom"). The resulting value of the test statistic allows the value of statistical significance to be read from the table (in MS Excel).

The chi-square test bases itself on basic assumptions. If these are not met, adjusted values are used: test statistic and statistical significance (for example, Yates's continuity correction). The first assumption defines the minimum sample size ($n = 5$). The second assumption concerns the independence of groups [Słowińska 2019].

The principle of event independence means that the result for one test person should reflect one situation, not several. Of course, percentage scores (less often the "raw" number of people in a crosstab) are usually considered in assessing test scores. Different observation values may be recorded in the groups being evaluated. Meanwhile, it is about comparing proportions (values) in relation to all collected data. In the study conducted, all the assumptions necessary for the chi-square test of independence were made correctly.

USER PERCEPTION OF E-BANKING SERVICES IN RURAL AREAS

When starting the survey, it was expected that most residents of Konin County would be e-banking customers. This was confirmed by 357 respondents. It is assessed that over 37 million Poles have the potential ability to do online banking [Paduszyńska, Pawlak 2020]. Together with the respondents' age, the rate of negative answers on e-banking use increased. This trend was positively verified by performing a chi-square test with a significance level of $\alpha = 0.05$. In addition, an average correlation was found for the same attributes by determining the T-Czuprow coefficient. The results of this survey section are collected in Table 1.

Table 1. Chi-square test results: use of e-banking services

Specification (answer/age)	Observed quantities					
	< 18	18-26	27-45	46-65	> 65	total
Yes	23	182	89	53	10	357
No	0	0	0	6	27	33
Total	23	182	89	59	37	390
Theoretical quantities						
Yes	21.05	166.60	81.47	54.01	33.87	357
No	1.95	15.40	7.53	4.99	3.13	33
Total	23.00	182.00	89.00	59.00	37.00	390
Chi-square test						
$\chi^2 = 226.20$	T = 0.54					

Source: own elaboration based on [Łukasiewicz 2020]

The group of non-users of internet banking (the minority) was asked about the reasons for opting out. Most prefer personal contact with a bank employee (22 users). The others alternatively: do not have access to the Internet (10 users), lack professional knowledge (6 users) or do not trust transaction security (3 users). However, none of these users found e-banking services unnecessary or unuseful.

Respondents were asked the question: are online banking services secure? Responses were mostly positive (two-thirds) but varied (this group assesses the level of security in halves: a measure of "rather yes" and a measure of "definitely yes"). No one rated e-banking services as totally unsafe to use.

The other questions were addressed only to real users of e-services. The vast majority use e-banking from the beginning, from the beginning of the bank contract (254 users). However, 78 respondents have been long-term clients of the bank (e-banking was not yet on offer at that time). On the other hand, 25 "faithful", long-time bank customers were convinced and trusted e-commerce services.

It was supposed that the older the bank customer is (age), the more difficult it was to choose e-banking when opening a bank account. This assumption was verified by the chi-square test, with a significance level of $\alpha = 0.05$. The correlation of age and respondents' answers were confirmed (Table 2). Also, the calculated T-Czuprow coefficient confirmed the average correlation of the compared variables.

As assumed, all e-banking users use the online channel (Internet connection) for these services. A large group (292 respondents) uses this connection frequently. A similar group also uses mobile banking (278 users). Only some do not use this method at all (18 people).

Table 2. Chi-square test results: when to start using e-banking

Specification (answer /age)	Observed quantities					
	< 18	18-26	27-45	46-65	> 65	total
Yes	23	182	49	0	0	254
No (but I chose it myself)	0	0	23	2	0	25
No (no offer)	0	0	17	51	10	78
Total	23	182	89	53	10	357
Theoretical quantities						
Yes	16.36	129.49	63.32	37.71	7.11	254
No (but I chose it myself)	1.61	12.75	6.23	3.71	0.70	25
No (no offer)	5.03	39.76	19.45	11.58	2.18	78
Total	23.00	182.00	89.00	53.00	10.00	357
Chi-square test						
$\chi^2 = 340.249$		T = 0.58				

Source: own elaboration based on [Łukasiewicz 2020]

The least popular e-service distribution channel is telephone banking. The majority do not use telephone services at all (216 people, 60.5% of the respondents). Thus, it is probable that online banking services are gradually eliminating the popularity of telephone and traditional services.

However, customers use payment cards most frequently (327 frequent users, 89 daily users and only 3 non-users). The most popular bank e-card is a debit card (354 users). More than one third (124 respondents) also use credit cards. In contrast, 3 people do not use bank cards at all.

Of course, e-banking allows for many activities that do not require a visit to the bank office. This applies primarily to non-cash payments (241 people pay this way often, and 93 people even pay every day). Only 3 respondents make non-cash payments rarely or never (0.84%). Online shopping is also a very popular service. More than half of the respondents (192 people) are happy to make purchases in online stores, but only 5 people do it regularly (daily). If this survey were repeated during the pandemic (2020-2021), the group of online shoppers, out of necessity and not just conviction, would certainly be much larger.

Most respondents are likely to check their account history through e-banking (83.19% of users frequently). On the other hand, using investment e-banking is not very popular (333 people do not do it at all). It was found that all e-banking users check their account balance online (84.31% users frequently). Another less popular e-service is international bank

transfers (as many as 320 respondents do not do it at all). On the other hand, domestic bank transfers are frequently made by 279 respondents (78.15%). E-banking users are less likely to complete loan agreements online (253 people have never done so). They also rarely use e-banking to open term deposits or savings accounts (only 195 people used these e-services).

The important benefits of e-banking are those that determine the active use of online services. In the benefits group, the following were mainly noted: permanent access to the e-account (213 users) and timesaving (187 users). Low costs of the e-account were not confirmed (actually these costs are permanently increased). In the group of "other" answers, the comfort of e-banking (10 people) and the possibility of current spending control (only 2 people) were incidentally indicated.

Moreover, the potential defects of e-banking were verified. Almost half of the respondents (157 people) did not select any weaknesses. The remaining respondents noted technical breaks (85 people), that is, access denied.

The overall rating of banking e-services is positive. More than half of the customers (189 people) are satisfied with "their" e-bank. A third of them (127 respondents) prefer

Table 3. Chi-square test results: e-banking as the only form of banking in the future

Specification (answer age)	Observed quantities					
	< 18	18-26	27-45	46-65	> 65	total
Definitely yes	21	22	4	0	0	47
Probably yes	2	119	30	15	1	167
Hard to say	0	31	36	8	1	76
Probably not	0	10	14	16	6	46
Definitely not	0	0	5	14	2	21
Total	23	182	89	53	10	357
Theoretical quantities						
Definitely yes	3.03	23.96	11.72	6.98	1.32	47
Probably yes	10.76	85.14	41.63	24.79	4.68	167
Hard to say	4.90	38.75	18.95	11.28	2.13	76
Probably not	2.96	23.45	11.47	6.83	1.29	46
Definitely not	1.35	10.71	5.24	3.12	0.59	21
Total	23.00	182.00	89.00	53.00	10.00	357
Chi-square test						
$\chi^2 = 268.39$	T = 0.43					

Source: own elaboration based on [Łukasiewicz 2020]

the e-services in "their" bank. Seven surveyed customers (dissatisfied with e-services) gave the opposite opinion.

A relationship was found between the respondents' age and opinion on e-banking dominance in the future. However, the older the respondent, the less certainty of the elimination of traditional banking in questionnaire responses. This relationship was confirmed by the chi-square test at a significance level of $\alpha = 0.05$ (Table 3), but the T-Czuprow correlation strength coefficient indicated a moderate correlation between these variables.

Of course, the general trend is a strong idea (214 respondents) that e-banking will totally replace traditional banking in the future. There are few sceptics on this issue. This supposition is confirmed by the test results, summarized in Table 3. Perhaps this means not only the end of traditional banking, but also the end of traditional money [Baader 2016, 2020] and, therefore, the end of paper cash (banknotes) and coins.

E-BANKING SECURITY – RESULTS AND DISCUSSION

The second part of the survey asked e-banking users about the security of online services. Questions included: respondents' knowledge about cybercrime, methods of preventing cybercrime, e-security tools in banking and their usefulness – all in the customers' opinion. The answers were sought against the hypothesis, recognizing cybercrime as a real problem of the twenty-first century.

Customer views on the quality of information provided by financial institutions on e-banking risks varied. A large group assessed the banks' security policies positively, but almost 38% indicated a "rather yes" answer (135 users). On the other hand, almost 27% of customers are not satisfied with bank information. Another important finding is the lack of opinion of almost a quarter of respondents (87 people). It can be assumed that they are not interested in the problems of bank transaction security.

What e-banking security threats do respondents fear? When asked to identify the two biggest e-threats, respondents cited: hacking into a bank account (248 answers) and theft of personal information (236 answers). Only 7 e-banking users (1.96%) do not find any threats. Of course, any Internet user can be attacked by a hacker. Meanwhile, as many as 136 respondents believe they can handle a cyber-attack on their own. The opposite (99 users) or neutral (94 users) opinion is held by more than half of e-banking customers. The structure of respondents' answers (and therefore potential decisions) in the e-banking security threat condition is collected in Table 4.

The certainty of young people is surprising: they know the online dangers are of course known, but (in their opinion) they are easy to self-eliminate. Are they really? As the age of the respondent increases, doubts (and fear of threats) successively increase.

Table 4. Chi-square test results: user awareness of e-banking threats

Specification (answer/age)	Observed quantities					
	< 18	18-26	27-45	46-65	> 65	total
Definitely yes	14	6	2	1	0	23
Probably yes	8	90	26	11	1	136
Hard to say	1	69	17	5	2	94
Probably not	0	17	43	33	6	99
Definitely not	0	0	1	3	1	5
Total	23	182	89	53	10	357
Theoretical quantities						
Definitely yes	1.48	11.73	5.73	3.41	0.64	23
Probably yes	8.76	69.33	33.90	20.19	3.81	136
Hard to say	6.06	47.92	23.43	13.96	2.63	94
Probably not	6.38	50.47	24.68	14.70	2.77	99
Definitely not	0.32	2.55	1.25	0.74	0.14	5
Total	23.00	182.00	89.00	53.00	10.00	357
Chi-square test						
$\chi^2 = 232.602$		T = 0.4				

Source: own elaboration based on [Łukasiewicz 2020]

This hypothesis was confirmed by the chi-square test, with a significance level of $\alpha = 0.05$ (Table 4). Also, the T-Czuprow coefficient indicates a moderate correlation between the assessed attributes. Unfortunately, the volume of respondents who lack sufficient knowledge about cyber threats is alarming.

Perhaps the "ignorance" of threats is based on past experiences of e-customers. The majority of survey respondents (292 users) reported that they have not encountered cybercrime before. However, some e-bank customers understand that the threat of cyber-attack is growing: 61 people have witnessed one, and 12 people more than once.

So, what do bank customers do to use e-banking safely? First of all, they install antivirus software (304 users). More than 80% of respondents (298 people) pay attention to the correct ending of the e-bank connection (logout). A similar group (257 users, or more than 70%) consciously refuses to install software from an unknown source. However, only a small group (27 users) do not save images of their payment cards or CVC or CVV codes in the open virtual space (cloud) or on storage media. This, in turn, is a potential source for hackers. Only a few users (15 people) use additional advanced tools, protecting e-banking data. When selecting "other ways to secure data" respondents indicated: the need

for multi-step verification of login credentials (13 users) and e-banking only on personal, private digital devices (a computer, a smartphone), preferably at home. Of course, e-users (321 people, so almost all) used authorization codes, which form the basis for securing a personal bank account. However, only a few used a token (26 users) or an e-signature (22 users) for authorization.

Finally, banks (as institutions of public trust) are obliged to ensure the security of e-services to their customers. More than three quarters of respondents (273 users) get their knowledge about cybercrime from media information campaigns. Similarly, this applies to sources of knowledge about e-safety tools. Only 3.08% of respondents (11 responses), read public laws to know the details of banking e-safety. All this implies the major social responsibility of the financial sector, as well as the bank's supervision and government action. Indeed, banks are implementing e-security in their own interest. For example, most of the surveyed e-users positively assess the ending of the connection with the e-bank after a certain (not very long) period of non-activity in the application (123 users). Multistage methods of customer authentication (login) and transaction authorization are also approved (over 100 positive responses in each case). Curiously, only a small group of customers noted the need to indicate one-time or daily limits for e-transactions. Their least attention is paid to the presence of transaction limits, which was indicated by 23 respondents.

Awareness of the reality of cyberwar is a very current challenge: institutional and individual. The institutional response should be the active policy of information and education (only half of respondents assess it as sufficient). At the same time, the individual response should be permanent education. This is the first line of activity, since the respondents (346 e-users, 203 of them strongly) identified cybercrime as one of the most important problems of our century.

CONCLUSIONS

Have all e-banking security dilemmas been resolved? Of course, not. It is not possible to specify an ideal model for using online banking. Cybercrime is evolving as fast as new technologies. The priority of cybersecurity should therefore be the individual user's behaviour and decision [Łukasiewicz 2020, Kumar, Gupta 2020, Burra 2021]. Also, the key factor of cooperation cannot be ignored: institutions (the banking sector) and users of the banking system (individual customers, entrepreneurs, farmers, seniors). The banks' activities should also build on the experience of other institutions and local governments based on the best practices model [Wanat, Lis 2009, Potkański et al. 2016, Mikołajczak et al. 2020]. Real security of e-banking depends on the quality of this cooperation [Wanat et al. 2021].

The aim of the study was to identify selected threats to e-banking security, based on residents of Konin County, especially from rural areas. The e-services available in banks in the opinion of respondents were analysed. These services were assessed against the background of cybercrime threats. Based on the survey results, the following conclusions were formulated:

1. A relatively high level of e-banking interest was found among Konin County residents. More than 90% of respondents used online banking. This applies especially to payments in retail trade (housing invoices, purchases), as well as household budget control.
2. The usability of e-banking is mainly determined by: time saving, the availability of services and convenient application (52% of users). Interestingly, almost 44% of respondents do not see any defects (threats) in online banking services.
3. Almost 60% of respondents think that traditional banking could be eliminated by e-banking in the future.
4. On the other hand, the respondents identify threats concerning the security of online banking use. Threats concern not only the protection of money on a bank account (deposits), but also the possible hacking of personal and sensitive data.
5. Unfortunately, more than 55% of users do not know what to do after detecting a cyberattack. Only a few users (17% of responses) have witnessed or encountered cybercrime. Respondents try to reduce the risks by using the security solutions offered by banks: authorisation codes (90%) and antivirus software (87%).
6. E-users also accept preventive actions by banks to improve cybersecurity (82% of responses). At the same time, respondents are not independently ready to respond to digital threats but are totally dependent on bank policies and banking solutions.

The active cooperation of all e-commerce actors based on trust should be recommended [Wanat, Potkański 2010, Skowysz, Krot 2018, Klus et al. 2021]. What does this mean in practice? First of all, it is the social and legal responsibility of the banking sector for the security of financial e-transactions [Szpringer 2021]. On the other hand, it is the knowledge, conscious behaviour and individual decisions of e-banking users that will determine e-security. The alternative is – even unaware – to open the door wide for criminal behaviour, for hackers.

BIBLIOGRAPHY

Ahmad Iftikhar, Iqbal Shahid, Shahzad Jamil, Muhammad. Kamran. 2021. A systematic literature review of e-banking frauds: Current scenario and security techniques. *Linguistica Antverpiensia* 2: 3509-3517.

Arora Sangeeta, Simarpreet Kaur. 2018. Perceived risk dimensions and its impact on intention to use E-banking services: A conceptual study. *Journal of Commerce and Accounting Research* 7 (2): 18-27.

Baader Roland. 2016. *Das Ende des Papiergeld-Zeitalters: Ein Brevier der Freiheit*. Bern: Verlag Johannes Müller.

Baader Roland. 2020. *Koniec pieniądza papierowego* (The end of paper Money). Warszawa: Wydawnictwo DeReggio.

Burra Bhagyalakshmi. 2021. Use and adoption of mobile banking in rural areas of India: a descriptive study on emergence of e-banking. *Journal of Xi'an University of Architecture & Technology* 13 (2): 175-184.

Chaimaa Belbergui, Elkamoun Najib, Hilal Rachid. 2021. E-banking overview: concepts, challenges and solutions. *Wireless Personal Communications* 117 (2): 1059-1078.

Chudobiecki Jan, Tomasz Potkański, Leszek Wanat. 2016. Intermunicipal and inter-sectoral cooperation as a tool supporting local economic development. [In] *The Path Forward Wood Products: A Global Perspective*, ed. Denis Jelačić, 187-196. Zagreb: WoodEMA.

Cwynar Wiktor, Wiktor Patena (eds.). 2021. *Podręcznik do bankowości. Rynki, regulacje, usługi* (Banking manual. Markets, regulations, services). Warszawa: Wolters Kluwer Polska.

Gangadwala Dhruv R., Mukesh R. Goyani. 2019. A study of issue of e-banking from the customers perception. [In] *Emerging Trends in Global Management and Information Technology*, Sheth Ketaki, Rupal N Patel., Sanjay K. Radadiya (eds.), 73-84. New Delhi: Allied Publishers.

Gąsiorowski Jerzy, Piotr Podsiedlik. 2015. *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej* (Crimes in electronic banking in Poland. An attempt to assess from a legal and forensic perspective). Dąbrowa Górnicza: Wyższa Szkoła Biznesu w Dąbrowie Górniczej.

Gospodarowicz Andrzej, Marcin Gospodarowicz, Magdalena Kozińska, Emil Ślązak, Katarzyna Zarańska, Marek Zborowski. 2018. *Bankowość elektroniczna: istota i innowacje* (Electronic banking: essence and innovation). Warszawa: Wydawnictwo CH Beck.

Grzywińska-Rąpca Małgorzata, Mariola Grzybowska-Brzezińska. 2017. Determinanty zachowań klientów e-banków. *Roczniki Kolegium Analiz Ekonomicznych/Szkoła Główna Handlowa* 45: 335-346.

GUS. BDL. 2020. (Central Statistical Office – CSO, Local Data Bank). Baza danych za lata 2010-2020 (Database for 2010-2020), https://bdl.stat.gov.pl/BDL/star, access: 08.12.2021.

Klus Sylwia, Leszek Wanat, Tomasz Potkański, Rafał Czarnecki, Vladislav Kaputa, Władysław Kusiak, Jan Sikora, Karolina Smętkiewicz. 2021. Selected mesoeconomic indicators of regional development in Poland based on intermunicipal cooperation. *European Research Studies Journal* 24 (4 special issue): 704-715. DOI: 10.35808/ersj/2800.

Kumar Mahesh, Sanjay Gupta. 2020. Security perception of e-banking users in India: an analytical hierarchy process. *Banks and Bank Systems* 15 (1): 11-20. DOI: 10.21511/bbs.15(1).2020.02.

Łukasiewicz Natalia. 2020. *Percepcja mechanizmów bezpieczeństwa przez użytkowników bankowości elektronicznej (na podstawie badań ankietowych wśród mieszkańców powiatu konińskiego)*. Praca dyplomowa. Maszynopis (Perception of security mechanisms by users of electronic banking (based on surveys among the inhabitants of the Konin County). Thesis. Typescript. Poznań: Poznań University of Life Sciences, Faculty of Economics and Social Sciences. Department of Finance and Accounting.

Mikołajczak Elżbieta, Leszek Wanat, Katarzyna Styma-Sarniak, Rafał Czarnecki, Anna Topczewska. 2020. The prospects to applying the best practices model as one of the pillars of business management in the wood market. [In] *Management Aspects in Forestry and Forest Based Industries*, ed. Denis Jelačić, 125-136. Zagreb: WoodEMAia.

Orłowska Małgorzata, Krystyna M. Błeszyńska. 2020. Edukacja a kompetencje cyfrowe seniora (Education and digital competencies of elder adults). *Kultura-Społeczeństwo-Edukacja* 18 (2): 143-164. DOI: 10.14746/kse.2020.18.6.1.

Paduszyńska Marta, Bartłomiej Pawlak. 2020. Rynek usług płatniczych w Polsce w świetle zmian prawnych implementujących postanowienia dyrektywy PSD2 (The payment services market in Poland in the light of legal changes implementing the provisions of PSD2. *Studia Prawno-Ekonomiczne* 114: 333-349.

Paszkowski Stanisław, Łukasz Sarniak, Leszek Wanat. 2019. Regionalne uwarunkowania budowania potencjału rozwoju obszarów wiejskich w Polsce (Regional conditions for the building of development potential in rural areas in Poland). *Fragmenta Agronomica* 36 (4): 54-64. DOI: 10.26374/fa.2019.36.32.

Paszkowski Stanisław, Leszek Wanat, Łukasz Dybkowski. 2018. Różnicowanie w kierunku działalności nierolniczej jako czynnik rozwoju gospodarczego obszarów wiejskich Wielkopolski (Diversification towards non-agricultural economic activity as a factor of development of rural areas in Wielkopolska). *Rynek-Społeczeństwo-Kultura* 1 (27): 145-158.

Popek Magdalena, Leszek Wanat. 2016. Demographic threats facing Poland on the basis of apoll of students of Poznań University of Economics and Business. *WSB University in Wroclaw Research Journal* 16 (3): 91-110. DOI: 10.29015/cerem.215.

Potkański Tomasz (ed.), Andrzej Porawski, Leszek Wanat, et al. 2016. *Współpraca jednostek samorządu terytorialnego narzędziem wsparcia Polskiej Polityki Rozwoju* (Local self-government unit cooperation as a support tool for the Polish Development Policy). Poznań: Związek Miast Polskich.

Potkański Tomasz, Leszek Wanat. 2017. Dylematy rozwoju miejskich obszarów funkcjonalnych z perspektywy partnerstw międzysamorządowych (Dilemmas of development of the functional urban areas from the perspective of intermunicipal co-operation). *Studia KPZK PAN* 1: 235-245. DOI: 10.24425/118535.

Potkański Tomasz, Leszek Wanat, Jan Chudobiecki. 2011. Leadership in time of crisis or crisis of leadership? Implications for regional development. *Intercathedra* 27 (4): 45-52.

Sikora Jan, Leszek Wanat, Iwona Widerska. 2018. Solidarność, ekwiwalentność czy sprawiedliwość? Zarządzanie wiekiem emerytów w polskim powszechnym systemie emerytalnym (Solidarity, equivalence or justice? Retirement age management in the Polish public pension system). *Zeszyty Naukowe Politechniki Częstochowskiej/Research Reviews of Czestochowa University of Technology* 29: 147-163. DOI: 10.17512/znpcz.2018.1.12.

Skowysz Kinga, Katarzyna Krot. 2018. Zaufanie a skłonność do korzystania i zadowolenie z usług internetowych (The impact of trust on the tendency to use and satisfaction with internet services). *Akademia Zarządzania* 2 (4): 101-117.

Słowińska Magdalena. 2019. Wykorzystanie testu chi-kwadrat w badaniach preferencji żywieniowych konsumentów (Use of the chi-square test in consumer preferences studies). *Engineering Sciences & Technologies/Nauki Inżynierskie i Technologie* 1 (32): 24-36. DOI: 10.15611/nit.2019.1.02.

Sołtysik-Piorunkiewicz Anna, Pyszny Krzysztof, Majerczak Przemysław. 2019. Analiza metod zabezpieczeń w systemach elektronicznych płatności (Analysis of security methods and techniques for access to data in electronic payment systems). *Studia Ekonomiczne* 390: 105-124.

Steczkowski Jan. 1995. *Metoda reprezentacyjna w badaniach zjawisk ekonomiczno-społecznych* (Representative method in the study of economic and social phenomena). Warszawa, Kraków: Wydawnictwo Naukowe PWN.

Sujová Andrea, Iveta Hajdúchová. 2015. Cluster mapping: a basis for the creation of network cooperation. [In] *Management of network organizations: theoretical problems and the dilemmas in practice*, eds. Włodzimierz Sroka, Štefan Hittmár, 85-103. Cham: Springer. DOI: 10.1007/978-3-319-17347-4_7.

Szpringer Włodzimierz (ed). 2021. *Społeczna odpowiedzialność banków. Między ochroną konsumenta a osłoną socjalną* (Corporate social responsibility of banks. Between consumer protection and social protection). Warszawa: Wolters Kluwer Polska.

Ślażyńska-Kluczek Dorota. 2016. Perspektywy rozwoju innowacji na rynku usług płatniczych (Prospects for the development of innovation in the payment services market). *Kwartalnik Nauk o Przedsiębiorstwie* 41 (4): 74-84.

Wanat Leszek, Vladislav Kaputa, Sylwia Klus, Stanisław Paszkowski, Tomasz Potkański. 2021. Mesoeconomic factors of intermunicipal cooperation as a tool for the integrated development of rural areas in Poland. *Zeszyty Naukowe Wyższej Szkoły Humanitas Zarządzanie* 22 (4): 169-188. DOI: 10.5604/01.3001.0015.6946.

Wanat Leszek, Sylwia Klus, Elżbieta Mikołajczak. 2019. The economic and social dilemmas of management focused on the future of retail branches of commercial banks in Poland. *Quality Production Improvement*. De Gruyter. 1 (1): 34-41. DOI: 10.2478/cqpi-2019-0005.

Wanat Leszek, Wojciech Lis. 2009. Promotion of best practices-project proposal for the wood industry in Poland. *Intercathedra* 25: 151-155.

Wanat Leszek, Tomasz Potkański. 2010. Effective leadership as one of the pillars of development of knowledge-based economy. *Intercathedra* 26: 182-185.

Wanat Leszek, Tomasz Potkański. 2011. Barriers for effective regional leadership in time of crisis. *Intercathedra* 27 (4): 75-79.

Wiśniewski Michał. 2018. Zagrożenia nabywców usług sektora marketingu internetowego – prawnokarna analiza zjawiska domain spoofing (Online marketing services threats – legal analysis of domain spoofing). *Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa* 4 (41): 173-183.

Wojciechowska-Filipek Sylwia, Zbigniew Ciekanowski. 2019. *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki, organizacji, państwa* (Safety of functioning in cyberspace of an individual, organization, state). Warszawa: CeDeWu.

Zarańska Katarzyna, Marek Zborowski. 2018. *Charakterystyka bankowości elektronicznej. Bankowość elektroniczna. Istota i innowacje* (E-banking. Essence and innovations). Warszawa: CH Beck.

***

DYLEMATY BEZPIECZEŃSTWA UŻYTKOWNIKÓW BANKOWOŚCI ELEKTRONICZNEJ, MIESZKAJĄCYCH NA OBSZARACH WIEJSKICH – PRZYKŁAD POWIATU KONIŃSKIEGO W WIELKOPOLSCE

Słowa kluczowe: bankowość elektroniczna, cyberbezpieczeństwo, bezpieczeństwo transakcji finansowych, obszary wiejskie, powiat koniński, Wielkopolska

ABSTRAKT

Celem pracy była identyfikacja wybranych zagrożeń bezpieczeństwa bankowości elektronicznej w opinii mieszkańców obszarów wiejskich, na przykładzie powiatu konińskiego. Analizie poddano dostępne na rynku usługi e-bankingu na tle zagrożeń cyberprzestępczości. Badania przeprowadzono w roku 2019. W zakresie przestrzennym dotyczyły one Wielkopolski i terytorium powiatu konińskiego, który tworzy 14 gmin, w tym 5 gmin miejsko-wiejskich oraz 9 gmin wiejskich. Stosując metodę sondażu diagnostycznego zebrano opinie niemal 400 osób zaproszonych do badania. Większość respondentów stanowili mieszkańcy obszarów wiejskich. Kwestionariusz ankiety składał się z 22 pytań zamkniętych oraz metryki informacyjnej. Proponowane odpowiedzi zaprogramowano według pięciostopniowej skali Likerta. W studium wykorzystano statystyczny test niezależności chi-kwadrat Pearsona, analizę porównawczą i deskryptywną. Obliczenia wykonano w programie MS Excel. W rezultacie wykazano relatywnie wysoki poziom zainteresowania e-bankowością wśród mieszkańców powiatu konińskiego. Ponad 90% respondentów, w tym mieszkańców obszarów wiejskich, wykorzystuje bankowość internetową. Dotyczy to szczególnie płatności w handlu detalicznym, a także sukcesywnej kontroli budżetu domowego. O użyteczności e-bankingu decydują przede wszystkim: oszczędność czasu, powszechna dostępność usług i wygoda. Mimo świadomości zagrożeń, poziom bezpieczeństwa bankowości internetowej budzi zaufanie większości respondentów. Oznacza to stosowanie niemal wyłącznie bankowych narzędzi cyberbezpieczeństwa. Rekomendowane są zatem działania instytucjonalne, wynikające z prawnej i społecznej odpowiedzialności sektora bankowego za bezpieczeństwo transakcji elektronicznych, realizowane w praktyce. Uzasadnia to opinia większości respondentów, przekonanych, że bankowość tradycyjna zostanie w przyszłości wyeliminowana przez narzędzia gospodarki cyfrowej, w tym przez e-banking.

AUTHORS

SYLWIA KLUS, PHD

ORCID: 0000-0003-2477-8610
Poznań University of Life Sciences
Department of Finance and Accounting
28 Wojska Polskiego St., 60-637 Poznań, Poland
e-mail: sylwia.klus@up.poznan.pl

NATALIA ŁUKASIEWICZ

Poznań University of Life Sciences
Department of Finance and Accounting
28 Wojska Polskiego St., 60-637 Poznań, Poland
e-mail: natalia24.lukasiewicz@gmail.com

ZUZANNA URBANOWICZ, PHD

ORCID: 0000-0002-2701-6390
Poznań University of Economics and Business
Department of Business Activity and Economic Policy
10 Niepodległości Av., 61-875 Poznań, Poland
e-mail: zuzanna.urbanowicz@ue.poznan.pl

LESZEK WANAT, PHD

ORCID: 0000-0002-1166-9258
Collegium Da Vinci in Poznań
Department of Information Technology
10 Kutrzeby St., 61-719 Poznań, Poland
e-mail: leszek.wanat@up.poznan.pl

Proposed citation of the article:
Klus Sylwia, Natalia Łukasiewicz, Zuzanna Urbanowicz, Leszek Wanat. 2022. E-banking security dilemmas of users living in rural areas – the case of Konin County in Wielkopolska. *Annals PAAAE* XXIV (1): 115-133