SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 224

SECURITY AWARENESS REGARDING ONLINE AND MOBILE E-BANKING COMMUNICATION CHANNELS AMONG STUDENTS IN POLAND IN 2024

Marek ZBOROWSKI

Faculty of Management, University of Warsaw; mzborowski@wz.uw.edu.pl, ORCID: 0000-0003-4762-127X

Purpose: This article examines students' awareness of digital security in electronic banking. The study takes into account the following areas related to the issue: the general awareness of computer system security and the level of cybersecurity threat awareness, particularly in the context of understanding and familiarity with fundamental concepts in the use of electronic banking. In addition, the research assessed the participants' level of experience with electronic banking.
Design/methodology/approach: The survey was conducted in 2023 using the CAWI method and included more than 310 students. An analysis of the results was carried out, followed by a discussion of the findings, and concise conclusions were drawn in relation to the specific areas examined in the study.
Findings: The research revealed that respondents are aware of the risks associated with using electronic banking, tend to associate the concept of security primarily with protecting personal data, and express a need for more proactive cybersecurity education efforts from banks and key institutions in the Polish financial sector.
Research limitations/implications: The main limitation of the study, as it was conducted exclusively within an academic environment. Another limitation is related to the lack of exploration of respondents' attitudes toward the latest advancements in this field.
Practical implications: These suggestions may also serve as a valuable resource for practitioners in the financial sector seeking to develop initiatives aimed at enhancing cybersecurity awareness among their clients.
Social implications: Recommendations were formulated that may be useful for scholars interested in exploring the recognition of computer security issues in the context of electronic banking.
Originality/value: The original contribution of the article lies in presenting the current attitudes of students toward the issue of security in individual banking operations.
Keywords: IT security; electronic banking; cybersecurity; security of banking operations; security of electronic banking.
Category of the paper: Research paper.

1. Introduction

The use of information technologies, particularly those intended for widespread public use, has become a common phenomenon and will undoubtedly continue to expand. However, as this trend progresses, the number of crimes committed with the use of such technologies, i.e., cybercrime, is also increasing. On the other hand, users of technology, particularly those utilizing public networks such as the Internet, expect that the services provided through these means will ensure their security. The provider's responsibility is to secure products and services provided using the network. Still, they will be helpless if users (customers) do not follow at least the basic security principles when using information technology. The Internet, website services, and mobile applications are highly vulnerable to cybercrime. In e-banking, this will include online banking services and bank applications installed on mobile devices. They are also the primary channels for customers to communicate with their banks. Therefore, the study aimed to examine the extent to which students, who are one of the social groups most open to adopting new technologies, understand the concept of security in the context of internet communication channels and mobile electronic banking. This study complements the author's long-standing analysis of the e-banking market and public perceptions of new technologies.

The growing threat emerging from the digital space of the public Internet is clearly illustrated by recent statistics. According to *Security Magazine*, there are more than 2200 attacks daily, equating to almost one cyberattack every 39 seconds. Each year, on average, about 2220 cyberattacks are registered each day, equivalent to more than 800,000 attacks per year. According to Cobalt (Top Cybersecurity Statistics for 2024 | Cobalt, n.d.), nearly 95% of all digital breaches are caused by human error. Europe experienced 85% of all hacking attacks observed in 2023, followed by North America at 7% and the Middle East at 3% (Poireault, 2023). Similar cybercrime statistics can be observed in Poland. In 2023, the number of companies that recorded at least one cybercrime incident increased by eight percentage points to 66%. The proportion of companies reporting 30 or more security incidents increased by 6 percentage points - from 5% in 2019 to 11% in 2023. At the same time, the share of companies that reported no attacks at all declined by 14 percentage points, from 46% in 2019 to 32% in 2023. According to 70% of the organizations surveyed in 2023, organized criminal groups are perceived as a significant source of threats (Kurek et al., 2024). Among the research data cited, particular attention should be given to those related to organizations operating within the financial sector in Poland. According to the latest *Check Point Threat Intelligence* data, Polish financial institutions find themselves in a particularly challenging situation. With an average of 1728 attacks per week targeting a single organization, Poland significantly surpasses neighboring countries in terms of the scale of cyber threats: the Czech Republic, 1211; Austria, 993 or Hungary, 780. What is also worrying is that the number even exceeds the global average of 1689 attacks (Ataki Hakerskie Na Banki…, n.d.).

The growing threat emerging from the digital space of the public Internet is clearly illustrated by recent statistics. According to *Security Magazine*, there are more than 2200 attacks daily, equating to almost one cyberattack every 39 seconds. Each year, on average, about 2220 cyberattacks are registered each day, equivalent to more than 800,000 attacks per year. According to Cobalt, (Top Cybersecurity Statistics for 2024 | Cobalt, n.d.) nearly 95% of all digital breaches are caused by human error. Europe experienced 85% of all hacking attacks observed in 2023, followed by North America at 7% and the Middle East at 3% (Poireault, 2023). Similar cybercrime statistics can be observed in Poland. In 2023, the number of companies that recorded at least one cybercrime incident increased by eight percentage points to 66%. The proportion of companies reporting 30 or more security incidents increased by 6 percentage points - from 5% in 2019 to 11% in 2023. At the same time, the share of companies that reported no attacks at all declined by 14 percentage points, from 46% in 2019 to 32% in 2023. According to 70% of the organizations surveyed in 2023, organized criminal groups are perceived as a significant source of threats (Kurek et al., 2024). Among the research data cited, particular attention should be given to those related to organizations operating within the financial sector in Poland. According to the latest *Check Point Threat Intelligence* data, Polish financial institutions find themselves in a particularly challenging situation. With an average of 1728 attacks per week targeting a single organization, Poland significantly surpasses neighboring countries in terms of the scale of cyber threats: the Czech Republic, 1211; Austria, 993 or Hungary, 780. What is also worrying is that the number even exceeds the global average of 1689 attacks (Ataki Hakerskie Na Banki…, n.d.) The report prepared by KPMG, which referred to the CSIRT assessment of the Polish Financial Supervision Authority, indicated that one of the most important cyber frauds for financial market clients in 2023 are fake investment opportunities (Raport Roczny CSIRT KNF 2023, 2023). One of the main tools used by fraudsters in 2023 were fake websites and fraudulent ads posted on social media as well as emails and SMS messages; phishing using emails and SMS messages; fake bank websites; Stealer malware (Stealers are advanced forms of malware that aim to steal valuable data from infected devices) and telephone scams (Raport Roczny CSIRT KNF 2023, 2023). The data presented reveal a concerning picture of the growing threats faced by both organizations in the financial sector and their clients. For this reason, a study was undertaken to examine students' awareness of cybersecurity in the context of using electronic banking services.

To gain a proper understanding of the concept of security, it is important to refer to a definition of organizational security. The definition of Shockley-Zabalak, Ellis and Winograd states that trust is "The willingness of an organization, based on its culture and the way it communicates when operating and in its relationships with others, to be responsive and cooperative, assuming the belief that the individual, group or organization is competent, open, honest, interested and reliable, and that it identifies with common goals, norms and values" (Schwabe, 2023). This definition highlights several key elements, including the organization's intent and actions aimed at cooperating with external entities (including clients) to achieve

a state of security for itself. Security within an organization directly contributes to the level of trust it earns from its clients. In today's world, where public networks such as the Internet have become the primary channels of communication between organizations and their clients, it is important to address the issue of cybersecurity. It encompasses the protection of tools, systems, processes, concepts, methods and strategies to protect assets in cyberspace from unauthorized access and loss of information, leading to the preservation of the integrity, confidentiality and availability of resources (Taherdoost, 2022). The definition indicates achieving a state of security regarding an organization's ICT resources. Electronic banking is a special area of an organization's IT systems, including the organization itself and its customers. A secure electronic banking system can be defined as one in which the six attributes of confidentiality, integrity, authenticity, non-repudiation, availability and reliability have reached an acceptable level for the bank and its customers (Zalewska-Bochenko, Siemieniuk, 2010; Korzeń, 2007). Achieving such a state requires not only strong commitment from the organization itself, namely, the bank, but also relies significantly on clients' awareness of potential threats and their corresponding behaviors. In the case of large organizations such as banks, a kind of imbalance of knowledge about cyber threats enters the picture. It is evident that banks and their clients face different types of threats; however, it should be recognized that both parties share the responsibility for maintaining the security of the bank's information systems, and, consequently, their own security as well.

Effective cyber-security of electronic banking requires the integration of advanced technical defense mechanisms with tailored educational strategies for its users that take into account awareness gaps, cognitive biases and cultural factors. In the literature, the phenomenon of cybersecurity in the field of electronic banking is typically examined within several contexts, including strategic, technical, educational, risk factor analysis and regulatory perspectives.

In the strategic context, special attention was paid to a comprehensive analysis of cybercrime incidents, assessing the financial impact of cyberattacks, evaluating the effectiveness of the existing cybersecurity framework and making strategic recommendations to strengthen cybersecurity measures.(Oyewole et al., 2024) Another important concept was recognizing the digital technologies being implemented in the banking industry and their impact on the growth of digital fraud, with a particular focus on online banking fraud.(Ahmad et al., 2024) In the technical context, attention was paid to the security measures used. These include: authentication methods (multi-component authentication (Karim et al., 2024; Malinka et al., 2022), biometrics). It was pointed out that the methods improve security, but require user acceptance and trust (Hajjisaaid, Ahmed, 2020). The aspect of utilizing artificial intelligence and machine learning has also been taken into consideration. It was pointed out that they support the detection of anomalies and improve the accuracy of predictive analytics. It was shown that their use improves the effectiveness of combating advanced attacks, such as: polymorphic malware or fraud (Deshmukh, 2024). In the area of mobile banking, there has been a noted increase in attacks targeting mobile platforms, highlighting the need for secure API interfaces,

the use of application sandboxing and user education on threats specific to mobile devices (Kangapi, Chindenga, 2022). In the educational context, studies have shown gaps in awareness of cybersecurity principles among vulnerable populations (A Study on Customer Awareness…, 2025). In the context of the behavioral approach, it has been indicated that gamification and active learning are preferred over traditional methods of merely informing users about precautionary behaviors. The above mentioned approaches are characterized by higher effectiveness in the long-term formation of safe habits (Prevention Of Cyber Frauds…, n.d.). Studies have pointed to the importance of promoting a safety-conscious culture through institutional policies and education in the regulatory and risk factor context. These approaches play a crucial role in reducing user-induced security breaches. The literature on the subject also examined how new regulations (e.g., PSD2) strengthen the implementation of secure multi-factor authentication practices (Malinka et al., 2022; A Regulatory Framework…, 2024).

As previously noted, most literature sources on cybersecurity in electronic banking concentrate on areas such as strategy, technology, user education, risk assessment or regulatory frameworks. However, relatively few studies specifically explore users' perceptions of cybersecurity in the context of online and mobile banking.

This article aimed to assess the level of students' understanding of computer system security, their awareness of common cybersecurity threats and their prior experiences in this field. The research, based on survey data and subsequent analysis, focuses specifically on students' perceptions of cybersecurity in electronic banking, with particular attention paid to two access channels: online and mobile banking. The analyses will help determine the extent of students' knowledge regarding cybersecurity when using online and mobile banking services.

In realizing the article's purpose, the following research questions were adopted: Which threats in using computer systems are recognized by their users? How do the respondents understand the issue of cybersecurity? How do the respondents perceive the security issue in their electronic (online and mobile) banking? How do respondents assess the banks' activities in raising respondents' knowledge of the risks of using electronic banking?

The article is divided into five parts: introduction, literature review, research methodology, discussion of results and conclusions. The introduction provides an overview of the research topic and outlines the context for the study. The second section reviews the current state of research on individual users' perceptions of computer security in electronic banking. It also highlights areas related to user perceptions of cybersecurity in electronic banking that have not yet been sufficiently explored. The following section includes a presentation of the research procedure adopted and the research sample characteristics. The fourth section presents the research results and compares them with findings from the existing literature on the subject. The article's final section presents the conclusions drawn from the analysis and discussion, outlines the study's limitations and suggests directions for future research.

This article is part of the author's ongoing, cyclical research on how consumers perceive changes in behavior related to e-banking phenomena (Chmielarz, Zborowski, 2024; Chmielarz et al., 2021).

2. Perception of cybersecurity

The issue of e-banking security is typically analyzed across several broad dimensions, including strategic, technical, educational, risk assessment and regulatory aspects. However, relatively few studies focus on how bank customers perceive security when conducting online and mobile banking transactions.

From a strategic perspective, Oyewole et al. (Oyewole et al., 2024), based on their research, emphasized that the banking sector should adopt a holistic approach to cybersecurity, involving coordinated investments in technology, user education and inter-organizational collaboration. Further recommendations include the integration of Big Data analytics, artificial intelligence and continuous risk assessment to respond to diverse and emerging forms of cyber threats effectively. The authors pointed to the need for a more substantial commitment by banking institutions to strengthen cybersecurity to protect financial assets and maintain customer trust. Dawodu et al. (Cybersecurity Risk Assessment In Banking, 2023) emphasize the importance of continuous monitoring and incident response planning as part of banks' cybersecurity. The authors point out that these measures are essential for detecting and responding to cyber threats in a timely manner. In the technical context, Priyadarshini and Geetha (E-Banking, n.d.) discussed experimental models for improving online banking security, and Mohammed and Mohammed (Mohammed, Mohammed, 2024) proposed a Role-Based Access Control (RBAC) model for enhancing authentication security in online banking. These studies point to the growing role of technological innovation in securing financial transactions. The banking sector is increasingly becoming a target for cybercriminals using advanced techniques to breach security. Dawodu et al. (Cybersecurity Risk Assessment In Banking, 2023) emphasize the critical role of cybersecurity risk assessment in banking, pointing to the need for banks to identify, analyze and assess threats. This process is essential for implementing controls to mitigate risks and comply with regulations. The study underscores the importance of adopting quantitative and qualitative risk assessment approaches, including threat modeling and scenario analysis. Garba, Kaur and Ibrahim (Garba et al., 2023) studied the human factors influencing cybersecurity culture among online banking users in Nigeria. Their research underscores the importance of cybersecurity awareness, policy and education in promoting the right attitudes and behaviors to enhance cybersecurity. The study reveals a clear knowledge gap in cybersecurity and highlights the under-researched influence of social norms and interpersonal trust in shaping cybersecurity culture. In one of the publications covering institutional awareness and risk management, Tiwari et al. (A Survey of Cybersecurity Threats…, n.d.)

presented the results of the study in which they surveyed 750 financial professionals in India. The survey identified critical gaps in the effectiveness of protection measures against cyber threats. They also identified a need for greater emphasis on training programs. Dongol and Chatterjee (Dongol, Chatterjee, 2019) examined cybersecurity practices at Nepalese banking institutions, finding weaknesses in security implementation. Arora et al. (Arora et al., 2022) analyzed cybersecurity case studies in both developing and developed countries, categorizing security threats and methodologies. Ahmad et al. (Ahmad et al., 2024) analyzed the relationship between digital banking technologies and the rise of fraud threats such as phishing and denial-of-service attacks. Cele and Kwenda (Cele, Kwenda, 2024) reviewed the literature using 58 previous studies to identify cybersecurity threats hindering the adoption of digital banking worldwide. The authors highlighted that phishing, malware and identity theft are major obstacles to the spread of e-banking. Regulatory perspectives have a significant impact on shaping global cybersecurity practices. Gupta et al. (Gupta et al., 1 C.E.) analyzed the U.S. Federal Financial Institutions Examination Council (FFIEC) guidelines for electronic banking authentication. The researchers discussed their implications for the security policies of financial institutions.

Within the context of this article, special attention is devoted to studies examining customers' perspectives on cybersecurity in both online and mobile banking operations. Alghazo et al. (Alghazo et al., 2017) conducted an extensive survey of 1044 online banking users in Saudi Arabia, Pakistan and India. The survey revealed gaps between users' cybersecurity practices and institutional expectations. Similarly, Matlala (Behavioural Insights…, 2024) used structural equation modeling (SEM) to assess the behavioral determinants of cybersecurity intentions among 338 South African e-banking customers. Sanusi (Sanusi, 2015) surveyed 237 Nigerian banking users, reporting high awareness of basic security measures. The author of the study considered it essential to place greater emphasis on educating users about safe practices in the use of electronic banking services. The cited studies underscore the role of user awareness in maintaining a high level of cybersecurity, but it is essential to keep in mind their regional nature. Naturally, this does not diminish their significance within the broader scope of research on electronic banking security.

The research presented in the subsequent sections of the article contributes to the broader international academic literature by offering insights into the level of awareness regarding security issues in the use of computer systems for electronic banking, as observed within a selected research group. The study adopted the following contexts: understanding of the issue of security of computer systems, awareness of the risks specific to cybercrime, learning about the participants' previous experience of cybercrime in the use of electronic banking and indications of expectations of initiatives on the part of banks in the area of cybersecurity. The research focused on analyzing the mentioned contexts in customer communication with banks in online and mobile banking channels. It is important to note that the study is regional and limited to the academic community.

3. Research methodology

3.1. Characteristics research methodology and survey questionnaire

In reference to the author's previous analyses and research (Zborowski, Chmielarz, 2023, 2024) on the perception of new technologies, a research procedure was developed, which generally includes: literature research, creation of a research survey, use of the CAWI method, calculation and interpretation of the obtained results.

The individual stages of the adopted research procedure are as follows:

- conducting literature review and consulting with experts on the theory of computer systems security and awareness of the perception of this phenomenon in society, with a particular focus on students,
- preparing the first version of the survey questionnaire, based on the above considerations, combined with the author's own expertise and observations of the studied phenomenon, stemming from his extensive experience cooperating with IT teams,
- verifying the clarity and relevance of the survey questions through a pilot study conducted on a randomly selected group of respondents,
- developing the final version of the survey questionnaire and selecting student groups at random for the implementation of the study,
- sharing the link to the survey questionnaire (using the CAWI method – Computer-Assisted Web Interview) with the previously selected student groups,
- collecting the survey questionnaires, presentation of their results, subsequent analysis and discussion of the data,
- drawing conclusions and presenting potential directions for further research.

The analysis of theoretical material, combined with consultations with experts in the studied field, enabled the formulation of requirements for a survey on the perception of computer system security, with a particular focus on electronic banking. It was assumed that the questionnaire, in addition to assessing participants' perceptions of key concepts, should also serve as an informative tool, increasing respondents' awareness of potential threats present online. This approach represents a specific response to the issues outlined in the introduction of the article. In addition, the survey draws respondents' attention to the key risks that may occur in using electronic banking in the area of cybercrime. The survey was aimed at students of management, who are expected to assume managerial roles upon graduation and will have a tangible impact on shaping the attitude of their organizations both in terms of the awareness of implementing security policies and also, among other things, communicating to clients that their security also depends on their own actions.

Taking the above requirements into account, the first version of the survey consisted of a series of sequential questions: frequency of Internet use; the type of e-banking preferred when communicating with the bank; understanding of the definition of cyber-security and its main components; awareness of the risks that occur when using a computer network; recognition of the most common types of attacks on the network and experience with them; awareness of the sources of threats on the Internet and the intentions of the authors of the attacks; the characteristics of application-level threats; the respondent's personal experiences with cybercriminal activities; their assessment of personal sense of security in electronic banking; and educational initiatives undertaken both by banks and by institutions acting in the interest of the security of the banking sector and its clients.

Appropriate revisions were made after consultations with students (a pilot group of twenty randomly selected individuals) regarding their understanding of the survey questions and the clarity of the provided answer options. The corrections to the survey form consisted of removing two questions and adding one assessing the respondent's level of trust in the bank's computer systems. The final version of the survey included 26 content questions and five questions related to respondents' demographic characteristics.

The survey was conducted from May to June 2023 among second-year students of the Finance Management and Accounting program at the Faculty of Management, University of Warsaw. The results were collected by the CAWI method using LimeSurvey software. The survey questionnaire was hosted on the Faculty of Management's servers. Upon completion of the study, the results were processed in MS Excel using pivot tables. Subsequently, relevant charts were prepared to illustrate the findings.

3.2. Characteristics of the research sample

The data were collected and categorized based on gender, age, level and field of education, place of residence as well as professional status and financial situation. The characteristics of the research sample are shown in Table 1.

Table 1.
Basic characteristics of the sample

Characteristics	Percentage share
Gender	
woman	75.81%
man	24.19%
Age	
19-24	96.77%
25-34	2.90%
35-55	0.32%
Education	
Bachelor's degree	78.71%
incomplete higher education	12.90%
secondary	6.77%
higher education	1.61%

Cont. table 1.

Place of residence	
town of 21,0000-50,000 residents	4.84%
city of 51,000-200,000 residents	4.84%
town of up to 20,000 residents	10.00%
city with over 200,000 residents	16.45%
village	63.87%
Field of study (present or completed)	
social sciences, including management, psychology, sociology, economics, pedagogy, administration, law	75.81%
other	16.13%
science, including mathematics, computer science, physics, chemistry	8.06%
Financial situation	
very good (I can afford everything I need, and I can save some money)	20.00%
good (I am not complaining, but it could be better)	51.61%
satisfactory (I can still make ends meet)	2.58%
I am a student, I am not financially independent	8.71%
average (I have enough money to live frugally)	17.10%
Professional status	
I am a student	43.87%
I work on a casual basis (on a contract for work/contract)	31.29%
I work on a full-time or part-time employment contract	17.10%
other	7.10%
I run my own business	0.65%

Source: own work.

An analysis of the data presented in Table 1 indicates that the research sample was characterized by a relatively high degree of diversity. However, it encompassed a total of over 310 individuals who are among the most active participants in the labor market in terms of education and age (Batorski, 2015).

In the survey sample analyzed (Table 2), the standard deviation values are highest for age at 54.96%, and lowest for work situation at 13.91%.

Table 2.
Statistical analysis of input data from the research sample

Characteristics	Percentage share
Age	
Variance	30.20%
Standard deviation	54.96%
Education	
Variance	11.02%
Standard deviation	33.19%
Place of residence	
Variance	6.24%
Standard deviation	24.98%
Field of study (present or completed)	
Variance	13.69%
Standard deviation	37.00%
Financial situation	
Variance	3.60%
Standard deviation	18.97%
Professional status	
Variance	1.94%
Standard deviation	13.91%

Source: own work.

Analyzing the data in Table 2, the greatest variation occurred in terms of the age of the respondents, with a variance of 30.20% and a standard deviation of 54.96%. Despite the high values of both measures of dispersion in the data, the survey was conducted on a relatively homogeneous group of students from one department in the second year of study. The other measures can be considered low, highlighting the homogeneity of the group.

4. Discussion

The CAWI survey conducted among students of the Faculty of Management at the University of Warsaw consisted of the following sections: infrastructure of network activities, recognizing the issue of computer system security, cybersecurity threat awareness and experience in using electronic banking.

The first section began with an assessment of the respondent's level of familiarity with Internet technology, followed by an examination of how they use it in their interactions with banking services. This was assessed by examining the frequency of the respondent's use of the Internet and the types of commonly used devices they utilize for this purpose. The use of the Internet in contact with the bank was verified by examining which channels in the area of electronic banking the respondent uses to communicate, whether he considers himself an active user of electronic banking, and which of the devices used for this purpose he considers the most secure.

Out of the available response options: *I am connected to the Internet all the time*, *Several times a day*, *Once a day*, *Several times a week*, *Once a week*, *Several times a month*, *Once a month*, *Never,* 84.84% said they are connected to the Internet all the time, and 15.16% said they access the Internet several times a day. Respondents most frequently accessed the Internet using: a smartphone and a PC (desktop or laptop), 58.39%. The second most frequently selected answer was *Other combination of equipment* (e.g., tablet and PC, desktop and smartphone) 23.87%. The least commonly selected option was *only a smartphone* 17.74%. The results obtained may indicate that when browsing the Internet content, the respondents use multiple devices almost simultaneously. They do not limit themselves to only a specific device.

The most frequently selected response regarding access to the respondent's own resources held at their bank was: *banking app on smartphone* (69.03%), followed by *a website on PC and banking app on smartphone* (20.00%). The remaining answers were a combination of channels: *an app and a website on a smartphone, a website on a PC or a smartphone*, and *a website on a smartphone*, which were selected by less than 6%. Therefore, the variance and standard deviation had high values, respectively: 7.1% and 26.63%. Detailed responses are presented in Figure 1.

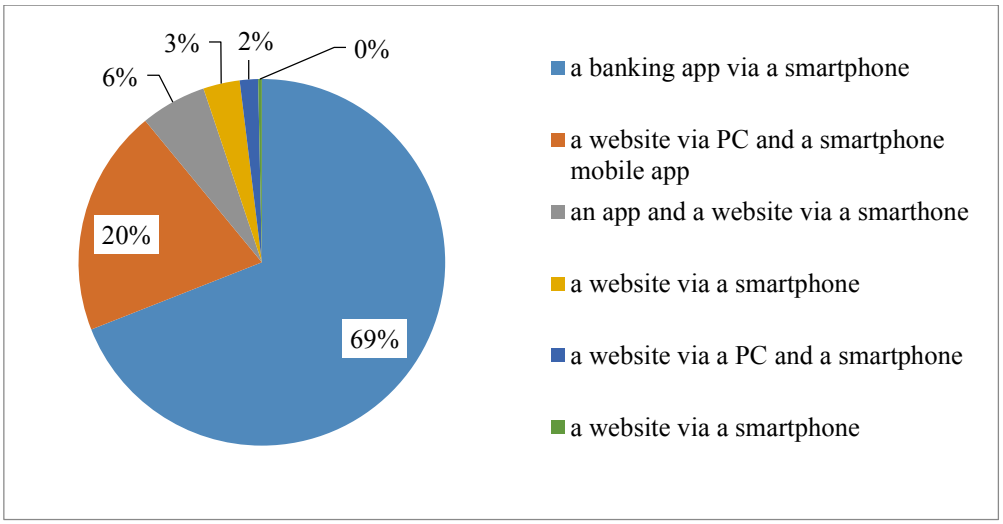

Figure 1. Percentage share of communication media used by respondents to access banking services.
Source: own work.

With regard to self-perception as active users of electronic banking (bank account), respondents most commonly indicated that they access e-banking services a few times a day (38.39%) and a few times a week (36.45%). Electronic banking is used once a month by 20.65% of respondents. The least frequently selected answer was *Once a day* and was selected in 0.65% of cases. For the responses to this question, the variance was 2.7%, and the standard deviation was 16.55%. Detailed responses are presented in Figure 2.

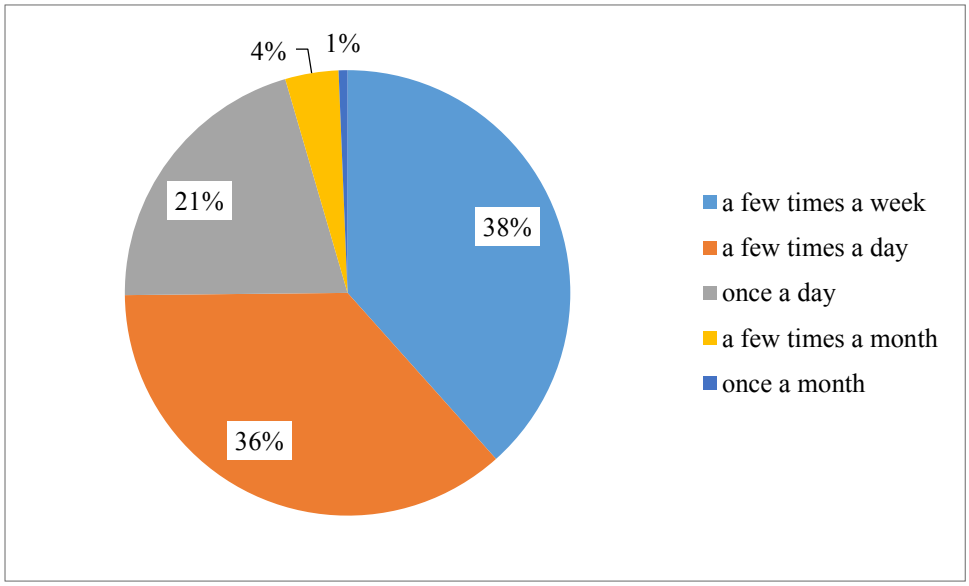

Figure 2. Bank customers' activity as reported by respondents (in %).
Source: own work.

The final question in this section focused on assessing the respondents' subjective perception of the security of specific devices used in interactions with the bank. Of the four possible answers, i.e. *smartphone*, *PC*, *desktop computer*, *tablet*, respondents identified the *smartphone* 42.26% as the safest for using electronic banking. *The PC* was perceived as 8.71 percentage points less secure, with the *desktop computer* rated an additional 9.35 percentage

points lower in terms of security. An interesting observation is that none of the respondents indicated the *tablet* as a secure device, which may suggest that, since they primarily associate it with entertainment and simple tasks, they do not perceive it as safe. Calculations point to a variance of 0.82% and a standard deviation of 9.03%.

Table 3.
Overview of cybersecurity definitions

No.	Definitions (Labels)	Share %
1.	Computer security includes measures and regulations that ensure the confidentiality, integrity and availability of information system assets (goods), including hardware, software, pre-built programs (firmware) and processed, stored and communicated information (Stallings, Brown, 2019)	30.97%
2.	Computer security, cybersecurity or information technology security (IT security) protects computer systems and networks from disclosure of information, theft or damage to hardware, software or electronic data, and disruption or improper performance of services (Informatycznej, 2021)	50.97%
3.	Information systems security relates to the totality of measures designed to secure data stored in a computer so that it cannot be exploited by unauthorized persons or exposed to permanent loss (Wyrębek, 2012)	9.35%
4.	An information system is secure if its users can rely on it and the installed software works according to its specifications (Garfinkel et al., 2003)	1.61%
5.	I see no difference in the definitions.	7.10%

Source: own work.

The next section of the survey, Recognizing the Issue of Computer Systems Security, included a series of questions on aspects such as the definition of cybersecurity, understanding and relevance to the respondent of the components of this issue. The survey presented respondents with four popular definitions of the concept of computer security and added a response of *I don't see a difference in the definitions*. The definitions and the shares of responses are shown in Table 3.

Respondents pointed to the second most accurate definition of cybersecurity, as shown in Table 3 (51% of cases). The second most frequently chosen characteristic of computer security was indicated by 30.97% of respondents. Other options, i.e., the third and fourth, are rated at a similarly low level, 9.35% and 1.61% respectively. The selection of the definitions used in the survey was purposeful. The first two definitions represent a broad approach, encompassing aspects such as devices, software, actions and legal considerations, whereas the third definition focuses more narrowly on actions aimed at preventing data loss. While still correct, the last definition appears to be the least precise. This response structure suggests that respondents are generally aware of issues related to computer system security, demonstrating an understanding of its various aspects.

Table 4.
Components of cybersecurity and their definitions

No.	Cybersecurity characteristics	Percentage share	Definition of cybersecurity features	Percentage share
1.	Data confidentiality	31.72%	Data confidentiality ensures that private or confidential information is not shared or disclosed to unauthorized persons.	34.32%
2.	Data integrity	27.31%	Data integrity (data integrity) ensures that information and programs are subject to change only in specific and authorized ways.	22.72%
3.	Privacy (assurance)	13.33%	Privacy ensures that individuals exercise control or influence over which information concerning them may be collected and stored, and by whom and to whom that information may be disclosed.	23.08%
4.	Responsibility	12.47%	Accountability refers to a security objective that requires an individual's actions to be clearly and uniquely attributable to that individual. This is helpful in achieving: undeniability, containment, fault isolation, violation detection and prevention as well as in corrective actions and legal proceedings after the fact.	1.89%
5.	Authenticity (in the sense of originality)	7.20%	Authenticity (originality). Certainty (conviction, confidence) as to the reliability of a transmission, message or their creator (origin).	2.96%
6.	System integrity	6.45%	System integrity ensures that the system performs the intended functions without interference (is fully operational), unaffected by intentional or unintentional unauthorized manipulation.	8.76%
7.	Availability	1.52%	Availability ensures that systems operate without delay and do not deny services to authorized users.	6.27%
	Variance	1.25%	Variance	1.54%
	Standard deviation	11.20%	Standard deviation	12.43%

Source: own work based on (Stallings, Brown, 2019).

From the listed areas, respondents were asked to select the three they most closely associate with computer security. The most frequently selected answer was *Data Confidentiality, 31.72%, while the least commonly selected answer was Availability,* 1.51%. The detailed response values are presented in Table 4 in columns 2 and 3.

Referring to the values in Table 4, columns 2 and 3, the responses *Data Confidentiality* and *Data Integrity* were selected with similar frequency - in about 30% of cases. The second most frequently selected pair was *Privacy* (13.33%) and *Accountability* (12.47%). The third pair was *Authenticity* (7.20%) and *System Integrity* (6.45%). From the data presented, it can be concluded that the issue of computer security is most often associated primarily with data security. The other elements do not yet exist so strongly in respondents' minds. When definitions were added to each concept, the order of relevance of cybersecurity features changed slightly (columns 4 and 5). *Data Confidentiality* remained the most important concept, with its significance increasing by approximately three percentage points, reaching a value of 34.32%. The second position was already taken by *Privacy* (23.08%). It is worth noting that the definition of this term includes the word *information*, though it is used in a context more characteristic of the term *data*. This confirms the observation made earlier that cybersecurity is

associated with data protection. The third most frequently selected feature was *Data integrity* (22.72%)

The third section of the survey, *Cybersecurity Awareness*, examined recognition of threats present in computer networks, awareness of types of attacks in cyberspace, active and passive threats and sources of both human and software threats.

When surveyed on awareness of key threats, of the three main ones, i.e., *random internal*, *random external* and *intentional threats*, a large majority of respondents indicated the third option. *Intentional threats*, that is, *those carried out deliberately and strategically, typically as part of industrial espionage, vandalism, terrorism, or acts of retaliation, etc.,* were selected in almost 85% of cases. This was followed by *random internal threats* (nearly 12%) and *random external threats* (only about 4%). The answers indicate that respondents perceive the concept of *danger* as having a conscious and premeditated character.

In a question combining both the recognition of the types of attacks in cyberspace and their adverse effect in relation to the resulting use of electronic banking, one can notice three groups of answers. The first: *malware* and *phishing* were selected in 45.39% of cases, the second: *cracking*, *sniffing* and *spoofing* in 45.58%, and the third: *cross-site scripting (XSS)* and *SQL Injection* in 9.04% of cases. A detailed presentation of the significance of the various types of attacks is shown in Figure 3. It is worth mentioning that in the survey form, a definition of each term was presented next to it.

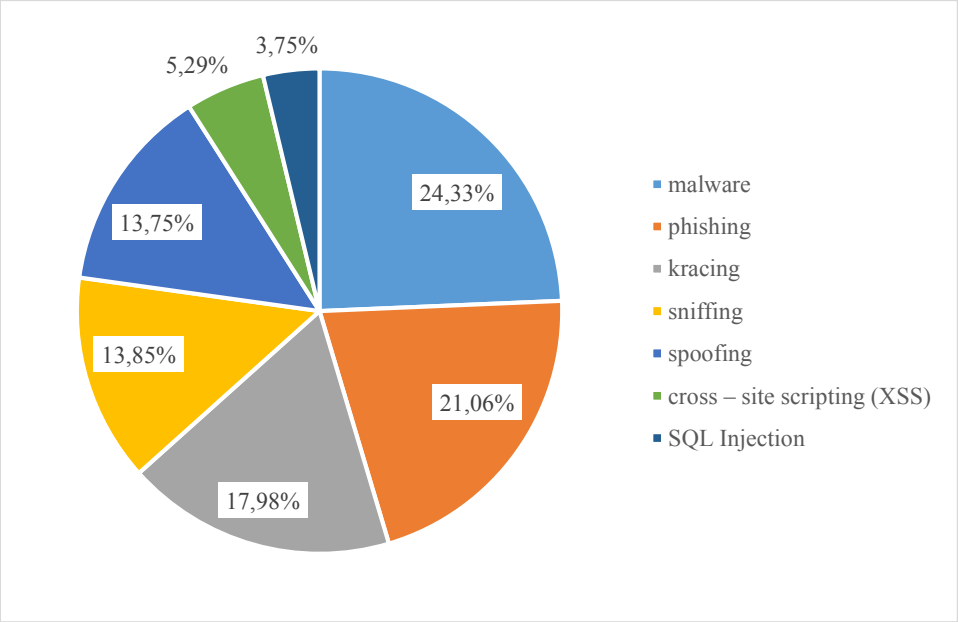

Figure 3. Percentage of responses regarding the significance of different types of cyberattacks.
Source: own work.

The results presented in Figure 3 indicate that respondents identified the following as the most recognizable and dangerous types of attacks: *malware* (24.33%), no less dangerous was *phishing* (21.06%). Slightly less critical is *cracking* (17.98%), *sniffing* and *spoofing* are

practically at the same level around (13%) and *Cross-site scripting (XSS)* and *SQL Injection* (each less than 6%).

One of the main categorizations of network threats is their division into passive and active. Passive threats include eavesdropping, network traffic analysis or revealing emissions. Respondents were asked whether they or their relatives had direct contact with such threats. The majority indicated that they have not encountered these types of problems (41.94%) or do not know if they have had contact with them (32.58%). Contact with this type of threat was mentioned by only 25.48% of respondents. In the case of active threats, understood as the conscious or unconscious actions of bank employees themselves, the majority of respondents (65.81%) indicated that they or their relatives had no contact with this threat. Meanwhile, 25.16% of respondents indicated that they do not know, and fewer than 10% confirmed having encountered such threats. The responses may suggest that the respondents or their close contacts have not encountered passive or active threats. This could indicate either a sense of security or a limited awareness of potential threats.

In understanding the concept of cybersecurity, awareness of the sources of threats is just as important as their classification. In the area of awareness of sources of threats to online and mobile banking, the distribution of variant responses is relatively even, with a variance of 0.03% and a standard deviation of 1.70%. Of the eight sources of threats, respondents were asked to select five. The most frequently indicated responses were: *information contained in banking documentation was previously maintained in paper form; however, with the advancement of computer systems, the vast majority of this information has been transferred to digital systems* (15.23%), and *data held in computer systems can be easily modified by at least two authorized persons: the owner of the data and the system administrator* (15.03%). Detailed data on the responses is provided in Table 5.

Table 5.
Sources of threats to online and mobile banking

Sources of threats to online and mobile banking	Percentage of responses
information contained in banking documentation was previously maintained in paper form; however, with the advancement of computer systems, the vast majority of this information has been transferred to digital systems, where, of course, they can be processed more easily, but are also more susceptible to loss or unauthorized copying (Olczak et al., 2015)	15.23%
data held in computer systems can be easily modified by at least two authorized persons: the data owner and the system administrator (Bandera, Grzywacz, 2016)	15.03%
due to the high costs and the risk associated with low awareness of the importance of data and computer system security, there is a potential risk that IT solutions may be inadequately protected, particularly among managerial staff (Krzysztoszek, 2017)	14.26%
there is also a frequent issue of relying on companies responsible for computer system security that lack proper certification	13.68%
every system, including IT systems, to a greater or lesser degree is always subject to errors, errors in the code, as well as the error of its use (*FTBS 2023*, 2023)	12.06%
the increasing availability of online content has also led to a greater volume and easier access to software that facilitates unauthorized access to organizational computer systems (Siemieniuk, Zalewska-Bochenko, 2017)	11.61%

Cont. table 5.

in the modern economy, the most valuable good has become data and information, the increase in demand for this good causes an increase in the number of actors willing to enter into possession of data by illegal means (Hajduk-Stelmachowicz, Iwan, 2018)	11.03%
any incidents involving unauthorized access to data within a specific institution pose a real threat to its public image. As a result, such institutions often choose not to disclose these occurrences, which in turn may further encourage cybercriminals to attempt gaining access to sensitive data and information (Mazurek, 2023)	7.10%
Variance	0.03%
Standard deviation	1.70%

Source: own work.

Threats to computer system security do not stem solely from malicious software; they can also originate from human actions. In the area of human threats, two answers were indicated at virtually the same level, at about 43% each, as among three possible answers: *the desire to make a profit* and *espionage, which involves stealing valuable information and passing it on to a competing bank*. The response: *the desire to gain publicity by revealing the fact of the intrusion, regardless of whether it was combined with, for example: data theft, changes in the bank's software or not,* was selected significantly less frequently, at a rate of 13.55%. In the area of software-related threats that may have the most adverse effects when using online and mobile banking, where respondents were asked to indicate the three most significant ones, the most frequently selected response was: viruses (29.07%), followed by rats and Trojan horses (22%) each. The least frequently indicated were bacteria and denial of service attacks at about 3% each. It is worth mentioning that the survey form provided respondents with definitions of each type of threat. The detailed distribution of responses is presented in Figure 4.

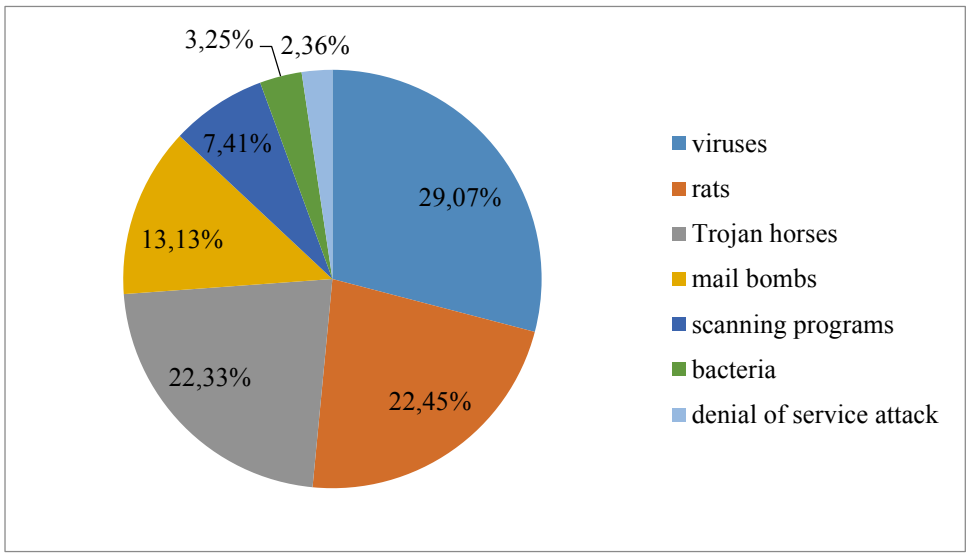

Figure 4. Percentage of responses regarding the relevance of cyber threats.

Source: own work.

Analyzing the data presented in Figure 4, it is worth noting that the selected responses were related to various methods of accessing data. It can be concluded that in the area of electronic banking security (both mobile and online), data breaches are perceived by respondents as the greatest threat, while denial-of-service (DoS) attacks are considered relatively insignificant.

The fourth part of the survey, *Experiences in the use of electronic banking*, examined such aspects as personal experience with cybercrime in the use of electronic banking, perceptions of the security of banking services provided by the respondent's bank, educational activities in the area of computer security undertaken by both the respondent's financial institution and well-known institutions working in the interest of banking sector security and customers.

In the area of the respondent's own experience with the issue of cybercrime, as well as their understanding of the concept, the vast majority of respondents (72.26%) are certain that they have not encountered the problem. 17.74% indicated that they did not know if they had encountered it. Only 1.61% gave the answer that *I don't quite understand the concept*. Less than 10% gave a positive answer. The structure of the responses indicates that respondents perceive the use of electronic banking as safe.

Among those who have experienced cybercrime, the most common responses are: *phishing attempts, theft of personal information, phishing attempts for login credentials, fake text messages, fake bank websites, fake BLIK payment authorization requests* and *phishing attempts for payment card details*.

In terms of overall trust in the security of the respondent's bank's computer systems, the vast majority rated it as *good* (61.61%), while only 20.65% rated it as *very good*. The remaining responses, i.e., *I did not consider it*, *I have no opinion*, *average*, and *poor*, accounted for a total of 17.75% of all responses. Detailed information on the responses provided is presented in Figure 5.

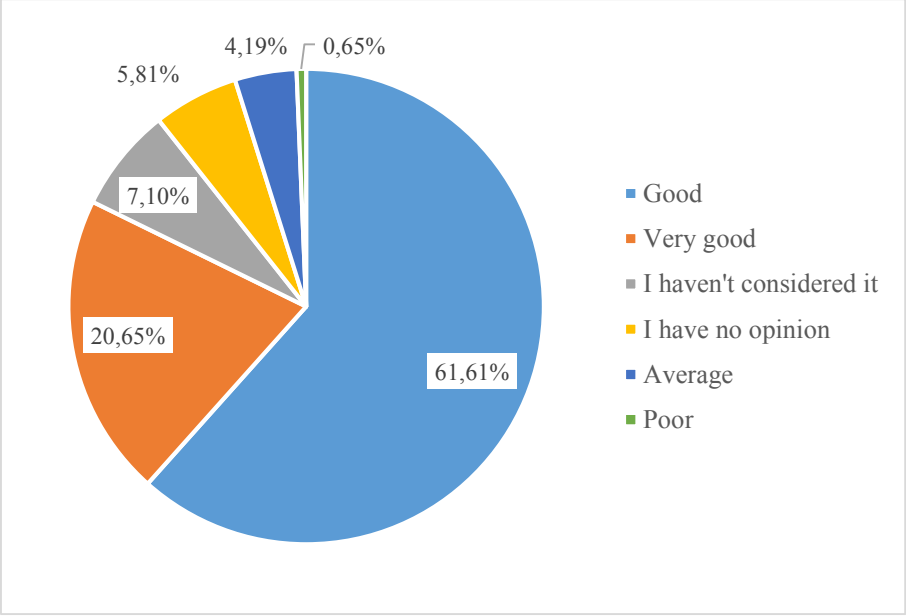

Figure 5. Percentage of responses regarding trust in the security of the respondent's bank's computer systems.

Source: own work.

In assessing the educational activities undertaken by the bank, respondents rated the banks' performance in this area as *good* (33.55%). The answer *very good* was selected by only 12.26% of respondents. The least frequently selected answer was *bad* (0.32%). Detailed information on the evaluation of the initiatives of firm institutions in educational activities is presented in Table 6.

Table 6.
Evaluation of banks' educational behavior regarding cybersecurity

Response	Percentage share
Good	33.55%
Average	20.97%
Very good	12.26%
I have encountered it once, but I don't remember exactly	10.97%
I haven't noticed any	9.35%
I haven't considered it	6.77%
I have no opinion	2.90%
Poor	2.90%
Bad	0.32%
Variance	1.09%
Standard deviation	10.46%

Source: own work.

Referring to the data presented in Table 6, it is worth noting that the responses: *I have encountered it once, but I don't remember exactly*, *I haven't noticed any*, *I haven't considered it*, account for as much as 27.09%. Such a high percentage of responses depicting respondents' uncertainty may suggest that respondents believe banks should engage more strongly in educational activities. These activities would likely raise understanding of the risks involved in using electronic banking.

According to the respondents, institutions such as the Financial Supervision Commission, the Polish Bank Association and the Ministry of Finance should be interested in building awareness of electronic banking security. In the survey, respondents mostly rated the involvement of the aforementioned institutions as *average* (28.71%), while the second most frequently chosen answer was *good* (26.13%). The answer *very good* was selected by only 4.19% of respondents. The remaining responses were negative, with a total of 40.64% of respondents indicating either a lack of knowledge about the subject or no interest in it. The response statistics presented may indicate that respondents expect these types of organizations to undertake a broader commitment to educational activities in the area of computer security.

5. Conclusions

In summary, the results of this study reveal a picture of cybersecurity perception, in which respondents demonstrate great trust in electronic banking systems. In addition, they have not encountered significant threats in cyberspace, but are aware of them. This is evident in the educational needs reported by respondents addressed to institutions supervising the financial market in Poland.

The detailed conclusions include:

- in communication with banks, among all available channels, respondents most frequently chose banking applications installed on smartphones,
- respondents used e-banking several times a day, which may indicate a high level of confidence in such solutions,
- respondents are aware of issues related to computer system security and understand its various aspects; however, they primarily interpret it as protection against data disclosure,
- the majority of respondents have not encountered, or do not know if they have encountered, passive threats, which may indicate the respondents' high confidence in using computer networks,
- similar to the recognition of attack types, when it comes to the perceived significance of cyber threats, viruses were identified as the most recognizable, followed by Trojan horses and Remote Access Trojans (RATs),
- the vast majority of respondents have not personally encountered cybercrime while using e-banking, confirming the high level of confidence in this type of solution,
- in terms of confidence in the security of the respondent bank's computer systems, the majority of respondents regarded them as good and very good, indicating high confidence in the solutions provided by this type of financial institution,
- in evaluating banks' educational efforts in the area of cybersecurity, respondents described them as good or average, which may indicate that they expect their financial institutions to take more proactive measures in this domain,
- respondents indicated medium involvement of institutions such as the Polish Bank Association (Związek Banków Polskich) and the Financial Supervision Commission (Komisja Nadzoru Finansowego) in building awareness of cybersecurity. This indicates an expectation of stronger involvement of the mentioned institutions in educational activities in the area of digital security.

The results of the survey indicate that respondents have a high awareness of cyber threats that can occur when using e-banking services. The research also showed that awareness of cybersecurity issues is known to respondents, but is perceived as insufficient. In addition,

respondents indicate the need for banks to increase educational activities related to their security in using online and mobile e-banking communication channels.

The research conducted also had some limitations. The first was that the research sample was limited to the academic community. The second limitation was related to conducting the research only in one country. The third referred to conducting the analyses only from the point of view of bank customers who are users of electronic banking. The study did not include banks themselves as the second key entity, highly exposed to threats originating from computer networks.

The analysis conducted fits into the research gap in the area of perception of computer security by individual users of electronic services provided by banks to the mass customer. The presented research can also be useful for practitioners operating in the financial sector to create ventures aimed at raising awareness of cybersecurity among their customers.

Further research in this area should be expanded in three main directions. The first is to expand the research group to include other electronic banking users. The second would be to study the factors influencing the development of cybersecurity awareness with a particular focus on the solutions used by banks. The third direction should be an attempt to use international comparisons to examine whether, for example, cultural factors and the level of IT adoption in a given country affect cybersecurity awareness.

References

1. *A Regulatory Framework for Improving E-banking Security* (2024, June 24). SciSpace - Paper. https://doi.org/10.1109/icccnt61001.2024.10724553
2. *A Study on Customer Awareness Towards Cyber Security in Banking Industry with Special Reference to Sulthan Bathery Municipality* (2025). ResearchGate. https://doi.org/10.55041/IJSREM40978
3. *A survey of cybersecurity threats and countermeasures in the Indian financial sector | Request PDF* (n.d.). ResearchGate. https://doi.org/10.47974/JIOS-1568
4. Ahmad, I., Khan, S., Iqbal, S. (2024). Guardians of the vault: Unmasking online threats and fortifying e-banking security, a systematic review. *Journal of Financial Crime*, *31*(6), 1485-1501. https://doi.org/10.1108/JFC-11-2023-0302
5. Alghazo, J.M., Kazmi, Z., Latif, G. (2017). C*yber security analysis of internet banking in emerging countries: User and bank perspectives.* 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), 1-6. https://doi.org/10.1109/ICETAS.2017.8277910
6. Arora, D., Garg, M., Mongia, S. (2022). *Global Case Studies, Domains and Used Methodologies Concerning Cyber Security in Online banking: A Review.* 2022 10th

International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1-7. https://doi.org/10.1109/ICRITO56286.2022.9965094

7. Bandera, R., Grzywacz, J. (2016). Zagrożenia bezpieczeństwa w bankowości elektronicznej. *Zeszyty Naukowe PWSZ w Płocku. Nauki Ekonomiczne*, *2(24)*, 151-168.
8. Batorski, D. (2015). Technologies and Media in Households and Lives of Poles. *Contemporary Economics*, *9*(4), 367-389.
9. *Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa* (2024). ResearchGate. https://doi.org/10.55927/ijba.v3i4.5515
10. Cele, N.N., Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31-48. https://doi.org/10.1108/JFC-10-2023-0263
11. Chmielarz, W., Zborowski, M. (2024). On Comparison of the Results of Selected Multicriteria Methods Applied in the Assessment Banking Websites in Poland in 2022. In: M. Hernes, J. Wątróbski (Eds.), *Emerging Challenges in Intelligent Management Information Systems* (pp. 268-288). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-66761-9_22
12. Chmielarz, W., Zborowski, M., Fandrejewska, A., Atasever, M. (2021). Poland–Turkey Comparison of Mobile Payments Quality in Pandemic Time. *Journal of Risk and Financial Management*, *14*(9), Article 9. https://doi.org/10.3390/jrfm14090426
13. Cybersecurity Risk Assessment In Banking: Methodologies And Best Practices (2023). *Computer Science & IT Research Journal*, *4*(3), Article 3. https://doi.org/10.51594/csitrj.v4i3.659
14. Deshmukh, K. (2024). Risk Analysis in Online Banking Systems. *IJFMR - International Journal For Multidisciplinary Research*, *6*(3). https://doi.org/10.36948/ijfmr.2024.v06i03.21892
15. Dongol, R., Chatterjee, J. (2019). *Robust Security Framework for Mitigating Cyber Threats in Banking Payment System: A Study of Nepal*. https://www.semanticscholar.org/paper/Robust-Security-Framework-for-Mitigating-Cyber-in-A-Dongol-Chatterjee/96db0a7d729dfedbbc913aad97370844df70522c
16. Dziennik Internautów (n.d.). *Ataki hakerskie na banki—Rosnące zagrożenie dla polskiego sektora finansowego.* Retrieved from: https://di.com.pl/ataki-hakerskie-na-banki-rosnace-zagrozenie-dla-polskiego-sektora-finansowego-70912, May 9, 2025.
17. *E-banking: Online Transactions and Security Measures* (n.d.). ResearchGate. https://doi.org/10.19026/rjaset.7.766
18. *FTBS 2023: Cyberbezpieczeństwo banków – zagrożenia i nowe perspektywy* (2023, June 5). https://bank.pl/ftbs-2023-cyberbezpieczenstwo-bankow-zagrozenia-i-nowe-perspektywy/

19. Garba, J., Kaur, J., Ibrahim, E.N.M. (2023). Design of a conceptual framework for cybersecurity culture amongst online banking users in Nigeria. *Nigerian Journal of Technology*, *42*(3), Article 3. https://doi.org/10.4314/njt.v42i3.13
20. Garfinkel, S., Spafford, G., Schwartz, A. (2003). *Practical UNIX and Internet Security*. O'Reilly Media, Inc.
21. Gupta, M., Lee, J., Rao, H.R., Gupta, M., Lee, J., Rao, H.R. (1 C.E.). *Implications of FFIEC Guidance on Authentication in Electronic Banking* (implications-ffiec-guidance-authentication-electronic). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-59904-855-0.ch022
22. Hajduk-Stelmachowicz, M., Iwan, K. (2018). Zarządzanie bezpieczeństwem informacji w obszarze bankowości elektronicznej wobec zjawiska cyberprzestępczości—Aspekt indywidualny. *Roczniki Kolegium Analiz Ekonomicznych, no. 49, Społeczno-ekonomiczne aspekty rozwoju gospodarki cyfrowej : koncepcje zarządzania i bezpieczeństwa*. Szkoła Główna Handlowa, 489-499.
23. Hajjisaaid, A., Ahmed, Y.A. (2020). Secure Electronic Banking Authentication—Survey. *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 1-4. https://doi.org/10.1109/ICCIT-144147971.2020.9213767
24. Informatycznej, R.B.K. (2021, April 23). *Zabezpieczenia systemów informatycznych—Profesjonalny Outsourcing IT Warszawa dla firm—Kompania Informatyczna*. https://kompaniainformatyczna.pl/2021/04/23/zabezpieczenia-systemow-informatycznych/
25. Kangapi, Thembakazi, M., Chindenga, E. (2022). Towards a Cybersecurity Culture Framework for Mobile Banking in South Africa. *2022 IST-Africa Conference (IST-Africa)*, 1-8. https://doi.org/10.23919/IST-Africa56635.2022.9845633
26. Karim, N.A., Khashan, O.A., Kanaker, H., Abdulraheem, W.K., Alshinwan, M., Al-Banna, A.-K. (2024). Online Banking User Authentication Methods: A Systematic Literature Review. *IEEE Access*, *12*, 741-757. https://doi.org/10.1109/ACCESS.2023.3346045
27. Korzeń, K. (2007). *Bankowość elektroniczna jako kanał dystrybucji usług bankowych*. Intelgraf - Anna Dygas.
28. Krzysztoszek, M. (2017). *Bankowość elektroniczna w teorii i praktyce Materiały edukacyjne dla środowiska szkolnego*. Komisji Nadzoru Finansowego. https://www.knf.gov.pl/knf/pl/komponenty/img/Bankow%C5%9B%C4%87%20elektroniczna%20w%20teorii%20i%20praktyce_60154.%20Materia%C5%82y%20dla%20%C5%9Brodowiska%20szkolnego_60154.pdf
29. Kurek, M., Burzyk, P., Kieszkowski, M. (2024). *Barometr cyberbezpieczeństwa 2024, Na fali, czy w labiryncie regulacji?* KPMG Poland. https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf

30. Malinka, K., Hujňák, O., Hanáček, P., Hellebrandt, L. (2022). E-Banking Security Study—10 Years Later. *IEEE Access*, *10*, 16681-16699. https://doi.org/10.1109/ACCESS.2022.3149475
31. Mazurek, W. (2023). Bankowość elektroniczna w Polsce w opinii klientów indywidualnych w świetle wyników badania własnego. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *12*(7), 9-31. https://doi.org/10.7172/2299-5749.IKAR.7.12.1
32. Mohammed, J.A., Mohammed, J.S. (2024). Authenticated E- Bank System Based on RBAC Model. *International Research Journal of Innovations in Engineering and Technology*, *8*(5), 150-155. https://doi.org/10.47001/IRJIET/2024.805023
33. Olczak, M., Brakoniecki, M., Sterczała, P., Borek, J. (2015). *Bezpieczeństwo bankowości elektronicznej, II Raport Specjalny*. Obserwatorium.biz. https://obserwatorium.biz/wp-content/uploads/2018/11/2_PL.pdf
34. Oyewole, A.T., Okoye, C.C., Ofodile, O.C., Ugochukwu, C.E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643. https://doi.org/10.30574/wjarr.2024.21.3.0707
35. Poireault, K. (2023, November 30). Manufacturing Top Targeted Industry in Record-Breaking Cyber Extortion. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/manufacturing-top-targeted-orange/
36. *Prevention Of Cyber Frauds In The Banking Sector* (n.d.). ResearchGate. https://doi.org/10.55041/ISJEM01341
37. *Raport Roczny CSIRT KNF 2023* (2023). Urząd Komisji Nadzoru Finansowego. https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_roczny_CSIRT_KNF_88762.pdf
38. Sanusi, I.B. (2015, June 1). *Assessment on User Awareness of Security Aspects in E-Banking*. https://www.semanticscholar.org/paper/Assessment-on-User-Awareness-of-Security-Aspects-in-Sanusi/019bd8ea329d9b9871be030c7594f1b1f5671b08
39. Schwabe, M. (2023). Zaufanie jako niezbędny element funkcjonowania organizacji. *Studia i Prace Kolegium Zarządzania i Finansów*, *189*, Article 189. https://doi.org/10.33119/SIP.2023.189.7
40. Siemieniuk, N., Zalewska-Bochenko, A. (2017). Bezpieczeństwo systemów informatycznych w instytucjach bankowych. *Roczniki Kolegium Analiz Ekonomicznych, no. 44, Uwarunkowania funkcjonowania gospodarki cyfrowej*. Szkoła Główna Handlowa, 55-67.
41. Stallings, W., Brown, L. (2019). *Bezpieczeństwo systemów informatycznych. Zasady i praktyka (VI).* Helion. https://helion.pl/ksiazki/bezpieczenstwo-systemow-informatycznych-zasady-i-praktyka-wydanie-iv-tom-1-william-stallings-lawrie-brown,bsi41v.htm
42. Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, *215*, 483-487. https://doi.org/10.1016/j.procs.2022.12.050

43. *Top Cybersecurity Statistics for 2024 | Cobalt* (n.d.). Retrieved from: https://www.cobalt.io/blog/cybersecurity-statistics-2024, May 9, 2025.
44. Wyrębek, H. (2012). Bezpieczeństwo w zarządzaniu informacją na poziomie systemów informatycznych. *Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie*, *22*. https://bazawiedzy.uws.edu.pl/info/article/UPH6f5ecdbd560f40568fb33822137d0f36/
45. Zalewska-Bochenko, A., Siemieniuk, Ł. (2010). Bankowość, bankowość elektroniczna a etyka. *Ekonomia-Polityka-Etyka. Tom III.* A.F. Bocian (ed.), 235-244.
46. Zborowski, M., Chmielarz, W. (2023). *Sensitivity analysis of the criteria weights used in selected MCDA methods in the multi-criteria assessment of banking services in Poland in 2022*. 1217-1222. https://doi.org/10.15439/2023F3745
47. Zborowski, M., Chmielarz, W. (2024). On The Application Of The Conversion Method For Website Evaluation Of Polish Banks In 2022. *Humanities and Social Sciences*, *31*(3), Article 3. https://doi.org/10.7862/rz.2024.hss.38