European Research Studies Journal
Volume XXVIII, Issue 4, 2025

pp. 29-43

Contemporary Threats in the Financial Market

Submitted 16/08/25, 1st revision 03/09/25, 2nd revision 19/09/25, accepted 10/11/25

Tomasz Grudniewski[1], Sylwia Wojciechowska-Filipek[2], Dariusz Brążkiewicz[3], Zbigniew Ciekanowski[4], Aneta Wysokińska[5]

Abstract:

Purpose: *This article analyses contemporary cyber threats to the financial market and identifies practical strategies for mitigating these threats in the context of increasing digitalisation. The study focuses on assessing the nature and impact of attacks on the financial sector and identifying measures to strengthen the resilience of economic systems.*
Design/Methodology/Approach: *The article employs theoretical methods, including literature analysis, industry reports on cybersecurity, and an examination of incidents that impacted the Polish financial system between 2020 and 2024. The first part characterises the roles of the financial market in the economy. It then analyses the consequences of the digitisation of financial services in the context of emerging cyberattacks and examines the number and value of attacks on financial institutions in Poland. The research problem is formulated as follows: What cyber threats pose the greatest challenge to the security of the financial market, and what strategies can provide adequate protection against them? The hypothesis is that integrated technology-based measures are insufficient to ensure the cybersecurity of the financial market without effective customer education, as customers are the primary participants in this market.*
Findings: *The Polish financial market is perceived by the public as the best protected against cyber threats. On the other hand, banks – as key players in the financial market – remain among the most frequently targeted entities in Poland. Compared to different industries and institutions, banks are considered leaders in cybersecurity. In this respect, Poles rate them even higher than technology companies or uniformed services. In 2024, there was an increase in the use of artificial intelligence to create convincing advertising materials for fraud, the automation of fraud processes, rapid domain changes in response to blockages, the use of current events, e.g. economic ones, and the personalisation of attacks for specific target groups (CSIRT - Computer Security Incident Response Team, KNF -*

[1]*John Paul II University in Biala Podlaska; ORCID: 0000-0003-3394-8992;*
e-mail: gisbourne2@gmail.com;
[2]*Uniwersytet Warszawski, Wydział Zarządzania, ORCID: 0000-0002-1847-1957,*
e-mail: wojciecs@wit.edu.pl;
[3]*John Paul II University in Biala Podlaska; ORCID: 0000-0002-5372-1210,*
e-mail: d.brazkiewicz@dyd.akademiabialska.pl;
[4]*John Paul II University in Biala Podlaska; ORCID: 0000-0002-0549-894X,*
e-mail: zbigniew@ciekanowski.pl;
[5]*War Studies University, ORCID: 0000-0001-9021-6355,*
e-mail: aneta.wysokinska2801@gmail.com;

Polish Financial Supervision Authority, 2024). A shift in cybercriminals' tactics was also observed — instead of advanced, technical attacks, they are increasingly using social engineering (a form of fraud in which the use of psychological and social factors is crucial to the success of the attack). This strategy involves persuading people to transfer funds to specified accounts themselves.

Practical implications: *Research confirms that institutions that prioritise cybersecurity measures not only increase their resilience to cyber threats but also improve their financial performance and increase shareholder value. It is not the scale of investment in cybersecurity itself that has a significant impact on economic performance, but rather the mere disclosure of such expenditure in reports. This reflects a shift away from a reactive approach towards integrated strategies in which cybersecurity becomes a central element of financial planning.*

Originality/Value: *Cybersecurity education plays a crucial role in the functioning of the financial market, serving as one of the foundations of its stability and trust. Raising awareness among employees and customers about digital threats significantly reduces the risk of successful attacks. Aware users are the first line of defence against security incidents, thus contributing to the minimisation of financial, operational and reputational losses. Systematic education in the field of cybersecurity enhances the resilience of financial institutions to emerging digital threats, thereby constituting an integral component of their long-term security and development strategy.*

Keywords: *Financial market, digital economy, cybersecurity.*

JEL Codes: *G10, O33.*

Paper type: *Research article.*

1. Introduction

Financial institutions are leveraging the versatility of cyberspace and digital innovations to expand their customer base and offer digital products and services. This enables transactions to be carried out without physical interaction, allowing customers to access services remotely. However, the increasing prevalence of digital innovation in financial institutions also has negative consequences (Akinbowale, Klingelhofer, Zerihun, and Mashigo, 2024), as it provides criminals and fraudsters with significantly greater opportunities to commit abuse (Laxman *et al.,* 2024). The financial sector is a prime target for cybercriminals.

On the one hand, financial institutions manage vast amounts of money, making them a natural target for extortion and payment fraud. On the other hand, they collect sensitive data that can be sold or used for identity theft. Given the importance of the

financial market to the economy and its attractiveness to cybercriminals, adequate protection against cyberattacks is a key objective for market participants.

2. The Place of the Financial Market in the Digital Economy

Technological development has reversed the traditional mode of operation of various industries and fundamentally changed the expectations and behaviour of market participants. Entities from the financial sector were pioneers in the business application of new technologies. Banks, insurance companies and investment funds naturally took advantage of technological innovations, thereby contributing to the development of digital tools and instruments. In this way, they responded to the changing needs and behaviours of their customers (Warsaw Institute of Banking, 2022).

The financial market has a significant impact on the development of digital technologies, as this sector is based on information processing, data analysis and transaction management, which makes digital technologies such as artificial intelligence (AI) and data analysis crucial. The digital economy is emerging as a new strategic area, permeating the financial space and thereby accelerating overall integration with the financial market, which in turn increases the productivity, profitability, and competitiveness of the entire industry (Ren, 2022).

The digital economy integrates the financial market with new technologies, which increases its importance as a tool supporting investment and innovation (Śledziewska and Włoch, 2024). It should be emphasised that financial activities can direct the flow of capital to meet the financial needs of the digital economy and achieve optimal allocation of resources.

Additionally, the financial market serves as a platform for aggregating information and facilitating price discovery. The mechanism of information feedback and price changes in the financial market can reflect the development of the digital economy industry. On this basis, it is evident that the digital economy and the financial market are inextricably linked (Ren, 2022). Due to their key role in the economy, financial institutions are essential for maintaining liquidity, ensuring money supply, granting loans, collecting savings and deposits, and executing payments and settlements. They serve as the backbone of the economy (Gulyas and Kiss, 2023).

Digital finance also contributes to the growth of the gross domestic product (GDP) of digitised economies by providing convenient access to a wide range of financial products and services (and credit instruments) for individuals, as well as small, medium and large enterprises, which can increase total spending and thus improve GDP levels. Digital finance can also lead to greater economic stability and increased financial intermediation, benefiting both customers and the economy (Ray, 2022).

Financial institutions are also part of critical infrastructure, alongside energy, water, and food supply, transport, communications, public administration, and emergency and defence services, which are essential for the smooth functioning of the economy (Gulyas and Kiss, 2023).

3. The Impact of Technological Developments on Financial Market Security

The current era of the world is one of digitalisation, in which financial transactions, financial investments and many other finance-related activities take place electronically and are carried out via cyberspace (Ray, 2022). Electronic transactions are less burdensome and offer customers greater freedom. In addition, they are cheaper, as banks encourage customers to use this type of transaction because it reduces transaction costs, strengthens customer retention, increases portfolio share and improves customer service (Laxman *et al.,* 2024).

It should be noted that alongside the positive aspects of technological progress in financial services, there are also negative repercussions referred to as the 'dark side of financial technology'. Examples of these negative implications include phenomena such as criminal activity and fraud, as well as cybersecurity vulnerabilities (Foguesatto, Righi, and Müller, 2024).

Security breaches encompass a wide range of illegal activities conducted on the Internet to compromise the security of personal or organisational systems or information and communication technology (ICT) architecture, facilitating fraud. Examples of these activities include phishing, spying, vishing, online theft, credit or debit card theft, malicious attacks, system hacking, data theft, and denial-of-service (DoS) attacks (Akinbowale, Klingelhofer, Zerihun, and Mashigo, 2024).

Phishing has become a significant concern for individuals and organisations as attackers use increasingly sophisticated methods to gain access to sensitive information such as personal details and login credentials (Singh, Kumar, and Kumar, 2024). To extract confidential information from unsuspecting victims, criminals employ social engineering and advanced methods, including browser file archivers, calendar phishing, fake websites or emails, content injection, voice manipulation, or other tools designed to deceive and exploit the victim's trust (Singh, Kumar, and Kumar, 2024).

Cybercriminals are increasingly targeting human firewalls rather than technical systems (Waelchli and Walter, 2025), thereby raising concerns about consumer protection. People play an integral role in 80–90% of successful cyberattacks, as persuading users to disclose confidential information is often much easier than circumventing computer security protocols (Triantafyllopoulos, Spiesberger, and Schuller, 2025).

It is worth noting that the systematic digitisation of financial transactions creates a potential risk of manipulation and exploitation of vulnerable customers. Low levels of digital and financial literacy, combined with the opacity of algorithm-based decisions, can expose consumers to complex decision-making processes and privacy and security risks (Colangelo, 2024).

Cyberattacks undermine trust in online interactions. As a result, users may be afraid to engage in online activities such as internet banking, e-commerce or online shopping. In addition to the damage caused to individual users, cyberattacks can also have serious consequences for businesses. The effects of cybersecurity breaches include significant revenue losses, legal costs, and operational disruptions. Such direct failures pave the way for a cascade of indirect losses, including loss of customer trust, damage to reputation (Singh, Kumar, and Kumar, 2024), and a sharp, abnormal decline in the market value of the organisation (Brho, Jazairy, and Glassburner, 2025).

Financial fraud is a serious problem that not only affects people's financial well-being but also has far-reaching consequences for the financial sector, government, and businesses. It is a significant factor in reducing productivity and economic growth (Nasdaq, 2024). Furthermore, research highlights the potential for new threats to spread from digital finance to traditional finance, posing a significant challenge for policymakers and regulators (Foguesatto, Righi, and Müller, 2024).

According to the 2024 Global Threat Intelligence Report by NTT and the 2023 ENISA Threat Landscape report, financial services are one of the sectors most vulnerable to cyber risks (Smaga, 2025). Not only is the number of cyberattacks increasing, but so is their intensity, sophistication and organisation (Gulyas and Kiss, 2023). Cybercriminals are using more sophisticated techniques to overcome traditional, passive defence methods (Creado and Ramteke, 2020).

The growing popularity of technologies such as deepfakes, used to impersonate other individuals, AI-generated phishing messages, and QR code-based scams is making it increasingly difficult for both financial institutions and their customers to detect fraud. The Tietoevry Banking report indicates that Europe has experienced a significant rise in the number of detected frauds. In 2022, an average of 2.65 cases of fraud per 100,000 transactions were recorded.

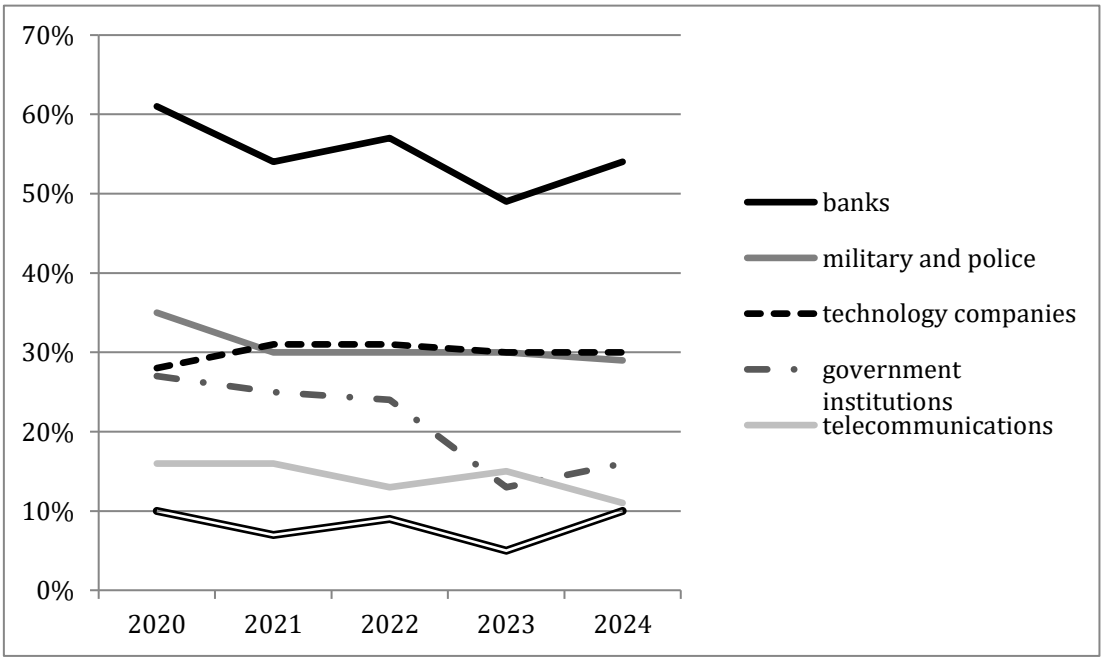
In 2023, this rate increased by nearly 47% to 3.89 cases per 100,000 transactions, and in 2024, it rose by another 43% to 5.57 cases per 100,000 transactions. In 2024 alone, the number of phishing attacks in Europe increased by 77%, while social engineering fraud rose by as much as 156% compared to the previous year (Tietoevry Banking, 2025). Currently, human error is associated with approximately 90% of all incidents, indicating that social engineering plays a significant role in most modern cyberattacks (Waelchli and Walter, 2025). Almost one-fifth of all incidents affect financial companies (Smaga, 2025).

In 2023, estimated losses from fraud and banking fraud worldwide totalled $485.6 billion. This ranks second after drug trafficking ($782.9 billion) and ahead of human trafficking ($346.7 billion) (Nasdaq, 2024). Although it can be challenging to quantify the direct costs of cyber fraud, its impact on an organisation's productivity, profitability, reputation, and customer satisfaction cannot be underestimated (Akinbowale, Klingelhofer, Zerihun, and Mashigo, 2024).

4. Threat Analysis on the Polish Financial Market

The public perceives the financial market in Poland as the best protected against cyber threats. Compared to other industries and institutions, banks are considered leaders in cybersecurity. In this respect, Poles rate them even higher than technology companies or uniformed services (Figure 1).

Figure 1. *Assessment of the level of safety in various industries by Poles*



Source: *ZBP, Reports on the perception of cybersecurity in 2020–2024.*

On the other hand, banks – as key players in the financial market – remain among the most frequently targeted entities in Poland. This is because a significant portion of social activity, including both financial transactions and citizens' interactions with public administration, has transitioned to the digital world. Banking applications have become a tool for everyday use. In addition to handling payments, financial institutions are increasingly acting as intermediaries in the use of public services.

This includes fees for public transportation, road tolls, and parking, as well as applications for social benefits and the use of e-government services. Currently, banking apps can be used not only to pay for public transport, parking or motorway tolls, but also to submit applications under the 800+ programme, access ePUAP (Electronic Platform of Public Administration Services) and ZUS, (Social Insurance Institution), or check information in the Internet Patient Account (Szpakowska, 2025).

In Poland, the leading institution responsible for researching and monitoring cyber threats in the financial system is CSIRT KNF — the Sectoral Computer Security Incident Response Team operating within the structures of the Polish Financial Supervision Authority, under the Act on the National Cybersecurity System. It plays a key role in protecting the financial sector against cyberattacks. It analyses threats faced by both professional and non-professional participants in the financial market. In 2024, the following was observed (CSIRT, KNF, 2024):

- increased use of artificial intelligence to create convincing advertising materials for fraudulent purposes,
- automation of fraud processes
- quick domain changes in response to blockages,
- using current events, e.g., economic events,
- personalisation of attacks for specific target groups.

In 2024, a shift in cybercriminal tactics was observed — instead of sophisticated, technical attacks, social engineering is increasingly being used.

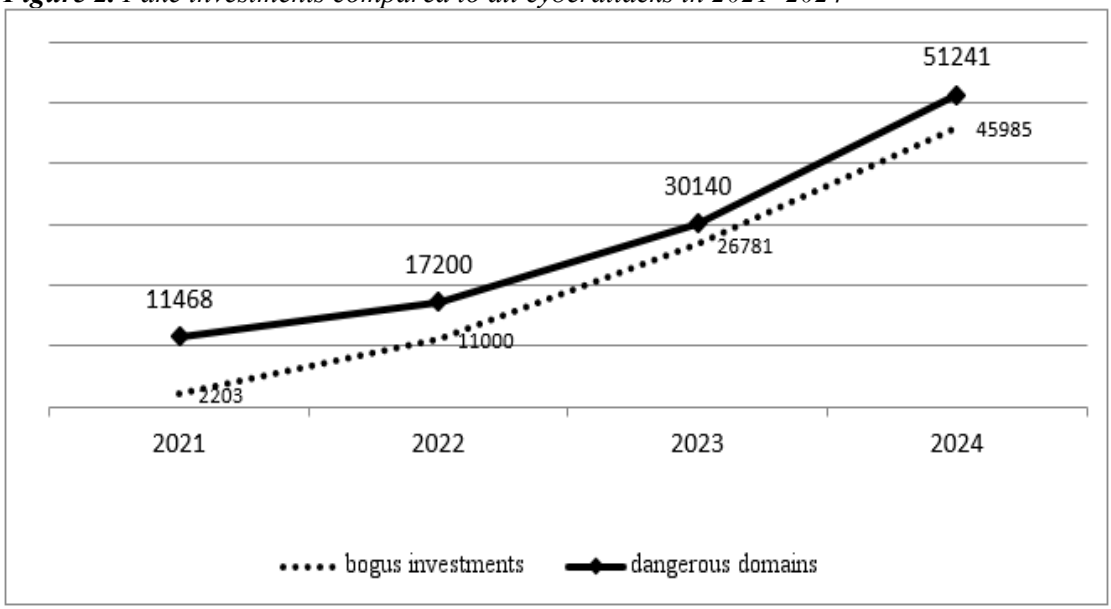
Social engineering is a form of fraud that relies heavily on the use of psychological and social factors to achieve its success (Waelchli and Walter, 2025). The strategy involves persuading people to transfer funds to specified accounts themselves. There is no technical aspect or action on computer systems involved – criminals contact their victims via messages or telephone, manipulating them into making decisions that are harmful to them. This allows them to completely bypass traditional technical defence systems (Waelchli and Walter, 2025), which unfortunately makes technological security measures ineffective. The most effective defence remains widespread education (NASK - Research and Academic Computer Network – National Research Institute, 2024).

Over the last four years, there has been a fourfold increase in attacks, indicating the intensification of cybercriminal activities. Fake (malicious) domains in the financial sector are designed to impersonate banks, stock exchanges, brokerage houses, fintechs and investment platforms. They aim to extort as much valuable data and funds as possible. In 2024, malicious domains were used to steal, among other things, electronic banking login details, payment card information and personal data (CSIRT, KNF, 2024).

Since 2022, the main category of attacks on the financial system has been fake investments. In 2024, they accounted for 89.74% of all identified attacks (Figure 2).

Fraudulent investments involve persuading victims to invest money in alleged projects or financial instruments that do not actually exist. They involve fabricated or misleading financial information, which has serious consequences for investors, market integrity, and public confidence (Rath, Haase, Melsbach, Liu, and Schoder, 2025). Cybercriminals promise quick and high returns, while assuring victims that there is no risk, to persuade as many people as possible to make deposits.

Figure 2. *Fake investments compared to all cyberattacks in 2021–2024*



Source: *Polish Financial Supervision Authority, Annual Reports (2021–2024).*

To lend credibility to their activities, they often use the image of well-known people or authorities, and the websites and investment platforms they create look almost identical to real financial services. As a result, the invested funds are diverted directly to the fraudsters, who then disappear, leaving the victims without their money (NASK, 2025).

Apart from fake investments, in 2024, the financial market was dominated by (CSIRT, KNF, 2024):

- fake surveys - attacks involving the promise of high rewards for completing a fake survey. The surveys are designed to encourage participation in competitions or research (e.g., opinion polls) and are short and easy to complete, allowing users to finish them quickly. The questions are initially

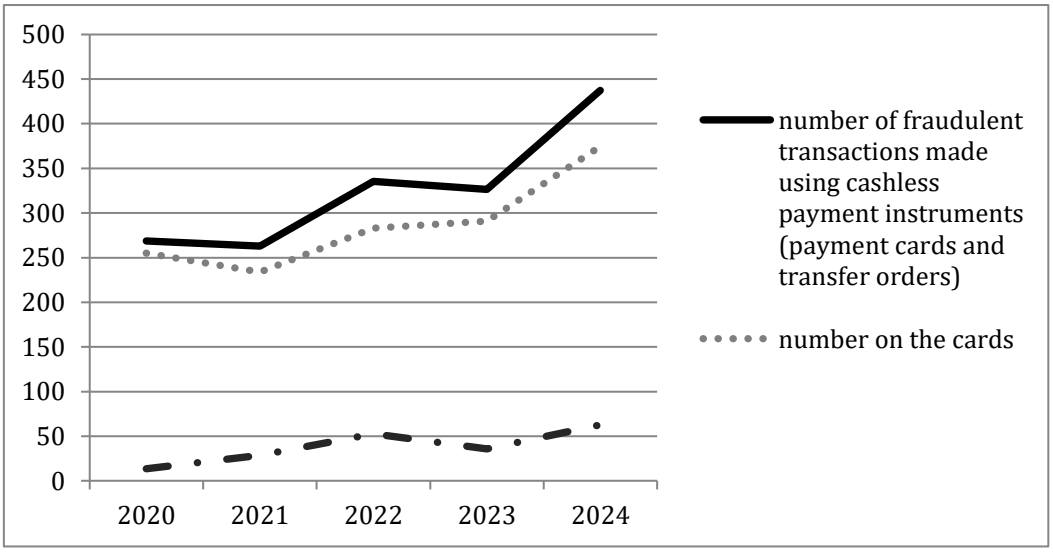
neutral, but gradually transition to requests for personal data and payment card details.

- courier/postal services - impersonating courier company employees. Fraudsters send messages containing a link to a website that appears deceptively similar to that of a bank or payment provider, informing the recipient that they need to pay extra for the shipment. These are usually amounts of up to a few zlotys.
- fake payment gateways - websites that imitate online gateways. Cybercriminals used them to intercept credit card and other payment data (CSIRT, KNF, 2023).

In Poland, there has been a significant increase in the number and value of fraudulent transactions made using cashless payment instruments (payment cards and transfer orders). Due to the varying scope of payment card fraud reported in the statements, a persistent discrepancy exists in the statistics compiled based on data provided to the National Bank of Poland by clearing agents and payment card issuers (Figure 3).

Data from payment card issuers does not include fraudulent transactions made in Poland with cards issued in other countries. On the other hand, data for payment cards provided by clearing agents do not include fraudulent transactions made outside the country with cards issued in Poland. Due to the subject of the study, the figures provided by issuers were used (NBP, 2025).

Figure 3. *Number of fraudulent transactions (in thousands)*

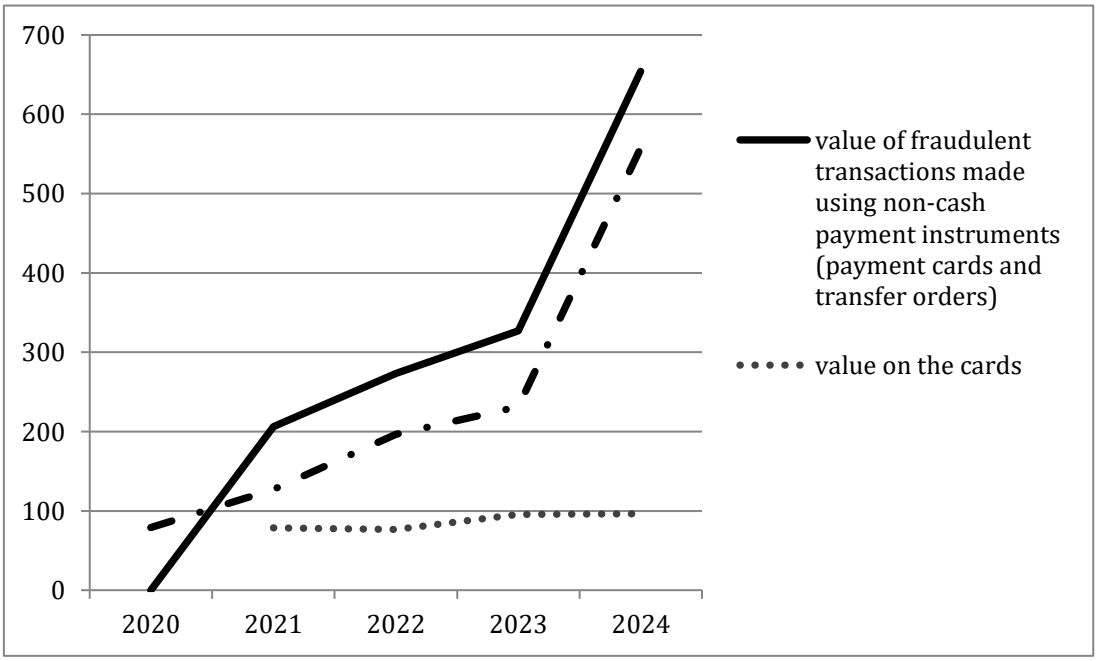


Source: *National Bank of Poland.*

Data collected by banks shows that the scale of fraud involving cashless payment instruments has increased significantly in recent years. This is also confirmed by data from the first quarter of 2025, in which, compared to the end of 2024, the number of registered fraudulent transactions increased by 7.4%, while their value increased by as much as 14.8%.

This means that not only were there more incidents, but they were also more costly for customers and financial institutions. Although the percentages appear significant, it is worth noting that the scale of the problem in relation to the market as a whole remains relatively small.

Figure 4. *Value of fraudulent transactions (in PLN million)*



Source: *National Bank of Poland.*

Fraudulent transactions accounted for only 0.0028% of the total number of transactions and 0.0010% of the total value (NBP, 2025). This means that the vast majority of card transactions and transfers are carried out smoothly and securely.

The scale of this fraud is lower than in other European countries. A report by the European Central Bank (ECB) and the European Banking Authority (EBA) on payment fraud across the European Economic Area (EEA), the total value of fraudulent direct debits, card payments, cash withdrawals and e-money transactions in the EEA amounted to €4.3 billion in 2022 and €2.0 billion in the first half of 2023. In the first half of 2023, fraud involving cards issued in the EEA accounted for 0.015% of the total number of card payments and 0.031% of the total value of card

payments. Fraud rates for bank transfers (0.001% of value and 0.003% of volume) (EBA ECB, 2024).

5. Digital Security Management

Cybersecurity is essential not only for institutions themselves, but also for a wide range of stakeholders, including policymakers, investors and consumers in general (Türegün, 2025).

Given the alarming consequences of cyberattacks and their long-term financial impact, companies must proactively invest in cybersecurity to protect their digital assets, maintain customer trust and ensure business continuity in the face of increasingly sophisticated cyber threats (Brho, Jazairy, and Glassburner, 2025). Research confirms that institutions that prioritise cybersecurity measures not only increase their resilience to cyber threats but also improve their financial performance and increase shareholder value. It should be emphasised that it is not the scale of investment in cybersecurity itself that has a significant impact on economic performance, but the mere disclosure of expenditure on it in reports.

This reflects a shift away from a reactive approach towards integrated strategies in which cybersecurity becomes a central element of financial planning (Türegün, 2025). Economic data from US companies listed on the Standard and Poor's (S&P 500) index for six years (2018-2023), as well as actual cases of cyber attacks, indicate that the investment necessary to protect against direct losses (e.g. repair costs, regulatory penalties, operational repairs and data recovery costs) accounts for approximately 4% of the total investment, while the remaining 96% covers indirect losses (i.e., reputational costs) (Triantafyllopoulos, Spiesberger, and Schuller, 2025).

To mitigate cyberattacks, several methods and tools have been developed, including various techniques for detecting and blocking phishing sites, as well as browser extensions that alert users to suspicious sites. The following can be used to detect phishing attacks (Singh, Kumar, and Kumar, 2024):

- URL-based features: phishing sites often use URLs that mimic legitimate sites, for example, by using typos or domain names similar to well-known brands;
- Content-based features: phishing emails and websites often use language and content designed to create a sense of urgency or fear in the user, or to mimic the tone and style of legitimate communications;
- Behavioural features: Phishing attacks often rely on user behaviour, such as clicking on a link or disclosing personal information. Features include analysis of click streams, time of day, and user location.

Despite significant efforts to combat URL phishing attacks using artificial intelligence (AI-phishing) through various machine learning (ML) techniques,

existing models often fail to implement the key functionality of autonomously training, testing, and updating the model with new incoming URLs (Malik, Khan, Qaisar, and Krichen, 2025), hence the search for newer and more effective methods.

In addition to processing various signals and identifying security incidents, the technology enables automatic response to security incidents (Waelchli, Walter, 2025). However, all intervention applications lie at the intersection of human-machine collaboration. The victim is ultimately responsible for interpreting and acting on signals indicating an attack (Triantafyllopoulos, Spiesberger, and Schuller, 2025). Therefore, given the importance of the human factor, cybersecurity focuses not only on protecting computer systems, networks and digital data, but also places particular emphasis on the human dimension, known as social cybersecurity, which combines applied research in computational science with computational techniques in social science to recognise, counteract and understand threats related to social communication (Mulahuwaish, Qolomany, and Al-Fuqaha, 2025). Education plays a key role in social cybersecurity, as it is the level of awareness and knowledge of users that forms the basis for protecting the entire society from digital threats.

Information on attacks, collected regularly by specialised institutions, is used for educational activities to raise customer awareness of cybersecurity. Cybersecurity education is an integral step towards creating a resilient, cyber-secure society and organisation (AlDaajeh, Saleous, and Choo, 2022). In Poland, several institutions, both public and private, are involved in financial cybersecurity education through training programmes, awareness campaigns and preventive measures. Table 1 presents the primary educational campaigns conducted by Polish cybersecurity institutions in 2024.

Table 1. *Educational cycles in 2024*

No.	Organiser	Form	Programme name
1	CSIRT KNF	CEDUR webinars Global Money Week (GMW)	Cybercriminals attack – how not to get robbed on the Internet
2	CSIRT KNF	CEDUR webinars	A secure phone – how to protect yourself from cybercriminals
3	CSIRT KNF	CEDUR webinars	Children online – cybersecurity from a parent's perspective
4	CSIRT KNF	CEDUR webinars	Investment in cybercrime – how to protect yourself
5	CSIRT KNF	CEDUR webinars	The latest methods used by cyber fraudsters – how not to get robbed online
6	CSIRT KNF	CEDUR webinars	Safe seniors – how not to get scammed online
7	CSIRT KNF	CEDUR webinars	What to watch out for and how not to get robbed online – online banking for seniors
8	CSIRT KNF	social media	The latest methods and techniques

		publications,	used by cybercriminals
9	Warsaw Institute of Banking	Cyber Genius knowledge tests	Cyber Security Project,
10	Warsaw Institute of Banking	lessons, lectures, webinars and training courses on cybersecurity	Cyber Security Project
11	Warsaw Institute of Banking	radio broadcasts/podcasts	Cyber Security Project
12	Warsaw Institute of Banking	publications and educational materials on cybersecurity	Cyber Security Project
13	Warsaw Institute of Banking	films and educational campaigns	Cyber Security Project
14	NASK CERT	push notifications sent via the mObywatel app	Information about current cyber threats
15	NASK CERT	social media channels	#KnowledgeAndInformation
16	NASK CERT	social media channels	#CyberScreen
17	NASK CERT	social media channels	#12CyberTips
18	Ministry of Digital Affairs	television, radio and internet campaigns	e-public services
19	Ministry of Digital Affairs	television, radio and the internet campaigns	cybersecurity

Source: *Reports by the Polish Financial Supervision Authority, WIB, NASK, Ministry of Digital Affairs.*

In Poland, the Ministry of Digital Affairs plays a crucial role in raising awareness and developing cybersecurity competencies. Developing digital security skills is one of the key objectives of the Republic of Poland's Cybersecurity Strategy (Government of Poland, 2025). These activities are targeted at a broad audience – citizens, public administration employees, teaching staff, and institutions that play a crucial role in ensuring the country's cyberspace security.

6. Conclusions

The financial market is crucial for economic growth, as it enables capital flows, risk assessment and investment financing. Financial institutions process vast amounts of sensitive data and conduct high-value transactions, making them a highly desirable target for cybercriminals. Aware of these threats, financial institutions are increasingly developing their technological and technical safeguards against cyberattacks.

Despite the growing sophistication of these solutions, they remain insufficient, as cybercriminals are increasingly targeting not systems but the people who are part of this market. In recent years, the Polish financial market has seen a several-fold increase in attacks, of which about 90% are fake investments, exploiting psychological factors to persuade customers to invest in alleged financial projects.

Cybersecurity education, therefore, plays a key role in the functioning of the financial market, constituting one of the foundations of its stability and trust. Raising awareness of digital threats among employees and customers significantly reduces the risk of successful attacks. Users who are aware of the threats are the first line of defence against security incidents, thus contributing to the minimisation of financial, operational and reputational losses.

Systematic education in the field of cybersecurity enhances the resilience of financial institutions to emerging digital threats, thereby constituting an integral component of their long-term security and development strategy.

References:

Akinbowale, O., Klingelhofer, H., Zerihun, M., Mashigo, P. 2024. Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. Heliyon, 10

AlDaajeh, S., Saleous, H., Choo, K. 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers and Security, 119, 102754.

Brho, M., Jazairy, A, Glassburner, A. 2025. The finance of cybersecurity: Quantitative modelling of investment decisions and net present value. International Journal of Production Economics, 279, 109448.

Colangelo, G. 2024. Open Banking goes to Washington: Lessons from the EU on regulatory-driven data sharing regimes. Computer Law andSecurity Review, 54, 106018.

Creado, Y., Ramteke, V. 2020. Active cyber defence strategies and techniques for banks and financial institutions. Journal of Financial Crime, 771-780.

EBA, ECB. 2024. Report on payment fraud. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.

Foguesatto, C., Righi, M., Müller, F. 2024. Is there a dark side to financial inclusion? Understanding the relationship between financial inclusion and market risk, The North American Journal of Economics and Finance, Tom. 72.

Gulyas, O., Kiss, G. 2023. Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, s. 84-90.

KNF, CSIRT. 2021. Podsumowanie roku. www.knf.gov.pl.

KNF, CSIRT. 2021. Cyberzagrożenia w sektorze finansowym. www.knf.gov.pl.

KNF, CSIRT. 2023. Raport roczny. www.knf.gov.pl.

KNF, CSIRT. 2024. Raport roczny. www.knf.gov.pl.

Laxman, V.I. 2024. Emerging threats in digital payment and financial crime: A bibliometric review. Journal of Digital Economy, nr 3, s. 205.

Malik, A., Khan, B., Qaisar, S., Krichen, M. 2025. AntiPhishX: An AI-driven service-oriented ensemble framework for detecting phishing and AI-powered phishing attacks. Information and Software Technology, Volume 188, 107877.

Mulahuwaish, A, Qolomany, B., Al-Fuqaha, A. 2025. A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and prospects. Computers in Human Behaviour Reports, Vol. 18, 100668.

Nasdaq. 2024. Financial crime insights European. https://www.nasdaq.com/global-financial-crime-report.

NASK, CERT, Polska. 2024. Raport roczny. www.nask.pl.

NASK, Szybki zysk czy bolesna strata. Jak rozpoznać i unikać oszustw inwestycyjnych, https://www.nask.pl/aktualnosci/szybki-zysk-czy-bolesna-strata-jak-rozpoznac-i-unikac-oszustw-inwestycyjnych.

NBP. Informacja o transakcjach oszukańczych. www.nbp.pl.

Ren, X. 2022. Can digital economic attention spill over to financial markets? Evidence from the time-varying Granger test. Journal of Digital Economy, 1, s.102.

Rath, O, Haase, F., Melsbach, J., Liu, J., Schoder, D. 2025. IT-embedded dynamic capabilities for public institutions coping with disinformation. The case of financial fake news. Government Information Quarterly, Tom 42.

Ray, P.K.A. 2022. Study on cyber financial frauds in the district of Jamtara. Jharkhand. Journal of Forensic Sciences and Research, nr 6, s. 042-044.

Singh, T., Kumar, M., Kumar, S. 2024. Walkthrough phishing detection techniques. Computers and Electrical Engineering, Tom. 118, część. A.

Smaga, P, 2025. Profiling the victim - cyber risk in commercial banks. Computers and Security, Tom 150.

Szpakowska, M. 2025. Największe ryzyko cyberataków dotyczy dziś sektora bankowego, Rzeczpospolita. www.rzeczpospolia.pl.

Śledziewska, K., Włoch, R. 2020. Gospodarka cyfrowa. Jak nowe technologie zmieniają świat. Wydawnictwo UW.

Tietoevry. 2025. Payment fraud report. https://www.tietoevry.com/en/campaigns/fraud-report/.

Triantafyllopoulos, A., Spiesberger, A., Schuller, B. 2025. Vishing: Detecting social engineering in spoken communication - A first survey and urgent roadmap to address an emerging societal challenge. Computer Speech and Language, Vol. 94.

Türegün, N. 2025. Digital transformation and cybersecurity risks. International Journal of Accounting Information Systems, Vol. 56.

Waelchli, S., Walter, Y. 2025. Reducing the risk of social engineering attacks using SOAR (Security Orchestration, Automation and Response) measures in a real-world environment: A case study. Computers and Security, 148.

Warsaw Institute of Banking. 2022. Wpływ nowoczesnych technologii na zmianę modeli biznesowych banków. WIB PAB1/2022, s. 12.

Warsaw Institute of Banking. 2023. Postawy Polaków wobec cyberbezpieczeństwa. www.zbp.pl.

Warsaw Institute of Banking. 2024. Cyberbezpieczny portfel. www.zbp.pl.