• F I N A N S E I P R A W O F I N A N S O W E •
• JOURNAL OF FINANCE AND FINANCIAL LAW •
Czerwiec/June 2025 • vol. 2(46): 19–35

Funding information: The publication of the article was funded by a subsidy for maintaining and developing the research potential of the University of Economics in Katowice. **Conflicts of interests:** None. **Ethical considerations:** The author represents individuals affected by cybercrime in legal action against banks, including individuals whose cases are described in the case study presented in this article (at the time of publication, the author no longer represents these individuals). This potential conflict of interest is disclosed in the interest of full transparency.

ATTACKS ON POLISH BANK CUSTOMERS DURING THE PANDEMIC: CYBERSCAMS AND THE ROLE OF SECURITY ALERTS

Wojciech Kaczmarczyk*

https://doi.org/10.18778/2391-6478.2.46.02

ATTACKS ON POLISH BANK CUSTOMERS DURING THE PANDEMIC: CYBERSCAMS AND THE ROLE OF SECURITY ALERTS

ABSTRACT

The purpose of the article. The publication aims to determine the extent to which changes in the use of e-banking during the COVID-19 pandemic influenced the methods and scale of cyberscams in Europe (including Poland). Additionally, it seeks to assess whether Polish banks conducted a proper information policy and were able to practically implement the adopted solutions during the examined period.

Methodology. First, an analysis of the available literature, applicable laws, and reports from state institutions was conducted. Then, security announcements from the five largest banks regarding cyberscams were examined. Additionally, a case study of three different incidents was carried out, including a review of complaint and court documentation.

Results of the research. The study demonstrates the growth and expansion of banking cyber scams in Europe (including Poland) during the COVID-19 pandemic. The analysis of security alerts highlights the need for improvements in the actions taken. Additionally, the case study points to the existence of systemic and organizational shortcomings. These findings facilitated the identification of potential changes to reduce the scale of the phenomenon. The obtained results may be useful for both researchers and practitioners working in the banking or supervisory sector.

Keywords: cybercrime, cyberscams, e-banking, COVID-19, banking services.

JEL Class: G21, G28.

* MSc in Finance and Accounting, MA in Law, University of Economics in Katowice, https://orcid.org/0000-0003-2037-2568 , Corresponding Author. E-mail: wojciech.kaczmarczyk@ue.katowice.pl

Attacks on Polish Bank Customers During the Pandemic: Cyberscams and the Role of Security Alerts

The Covid-19 pandemic forced numerous changes in the lives of residents of the Western world, significantly accelerating the digitization of the economy, including the banking sector. Handling most matters via phone, email, or dedicated applications has become the new normal, also in Poland (Rybacka, 2023).

These changes did not go unnoticed by cybercriminals, who had already been exploiting human naivety and lack of knowledge about modern technologies before the pandemic to fraudulently obtain significant sums of money. The subject of the presented research is a significant portion of cybercrimes committed against e-banking customers, specifically those that exhibit characteristics of fraud.

This publication aims to shed light on the issue of banking cyberscam in Poland in the context of increasing cyber scam number in Europe, determine the impact of the pandemic on its scale, including the evolution of fraud methods, and assess the security of e-banking in Poland. It is addressed to both professional entities (regulators, banks, researchers) and e-banking customers. The conclusions drawn from the study may contribute to improving the security of e-banking usage.

Considering the objectives of the publication, the following research hypotheses have been adopted:

1. During the Covid-19 pandemic in selected European countries there was an increase and development of e-banking cyberscam.
2. During the Covid-19 pandemic, the largest banks in Poland published public security alerts about cybercrime threats at the same time.
3. During the Covid-19 pandemic in Poland there were no organizational problems limiting the effectiveness of customer protection in case of cybercrimes.

Methodology

As part of the conducted research, a review of financial and legal literature, applicable legal acts, and reports related to the security of banking sector and the fight against cybercrime was carried out. As a result, the subject of the study was characterized, security-related obligations were identified, and the impact of the Covid-19 pandemic on the scale of banking cyberscam in Europe (including Poland) and its evolution in Poland were determined.

Next, an analysis was conducted on security communications published by the five largest banks in Poland. These communications were evaluated quantitatively, categorized by year, and assessed for their adequacy in relation to emerging scenarios of selected cyberscam cases (identified based on the aforementioned review).

The final element of the study consisted of case studies of cyber scams committed against e-banking customers during the Covid-19 pandemic in Poland. Based on the documentation related to

criminal and civil proceedings, the exact mechanisms of committed crimes were determined, and an assessment was made regarding whether they could have been prevented.

The Concept and Characteristics of Banking Cyber Scam

Crimes targeting e-banking can generally be divided into two categories: those directly affecting banking systems and those impacting users (consumers) of e-banking services (Lotko, 2024). This publication focuses on the second type of cybercrime.

For this reason, the term banking cyberscam will be understood as offenses committed to the detriment of e-banking customers, penalized under article 286 § 1 of the Penal Code (Act of 6 June 1997) and classified as cybercrime. According to this provision, fraud is defined as an offense involving the deception of a victim through fraudulent practices that create a false perception of reality (Kulik, 2022). Meanwhile, cybercrime refers to an illegal act directed against IT systems, in which a computer is either a tool or the target itself (Stefanowicz, 2017).

Cyberscam can be committed in various ways. In the literature, these crimes are most often characterized basing on the method used to gain access to e-banking. The most common types include obtaining data that allows for banking transactions, using malware that enables banking operations (Górnisiewicz et al., 2014), and scams that deceive the victim into performing the necessary banking transactions themselves (Rynkowska, 2017).

Data theft can be carried out using various phishing methods, ranging from fraudsters impersonating bank employees in phone conversations to advanced techniques involving redirection to a fake online banking website that captures login credentials (Czyżak, 2016). More sophisticated form of phishing is spearphishing, which involves creating personalized messages based on information gathered about the victim (Konieczny, 2023).

Due to the wide range of phishing methods, various taxonomies of this phenomenon can be found in the literature. Aleround & Zhou (2017) propose categorizing phishing according to the following criteria:

- communication media (e-mail, website, messengers, social networks, blogs, mobile apps etc.);
- target devices (personal PC, smart phones, voice and Wi-Fi Devices);
- attack techniques (methods of: attack initialization, data collection and system penetration);
- countermeasures.

Another method of data theft is *spoofing*, which originated as a technique for impersonating the addresses of other Internet users (Radoniewicz, 2021). Today, it is just as frequently used to impersonate another user of a telephone network, meaning that the victim believes they are receiving a call from a trusted institution (Deng et al., 2018). Spoofing that involves disguising a phone number is referred to as *smishing* (when SMS messages are used, e.g., containing links to malware) or *vishing* (when voice

calls are used). These terms are combinations of the words SMS, voice, and phishing (Mangut & Datukun, 2021).

The use of malicious software can take various forms, ranging from programs that capture the data necessary for banking transactions to those that provide remote access to the victim's computer (Czyżak, 2016). This type of software is collectively referred to as *malware* (Stawińska, 2021). However, for the purposes of this publication, the term will also include legitimate software, provided that it was installed at the initiative of the perpetrators and used in an unlawful manner.

The *scam* mechanism relies on gaining the victim's trust through traditional correspondence, email, online services, or direct contact, persuading them to take specific actions (Rynkowska, 2017). This type of cyberscam originates from the Nigerian scam, which became popular as early as the 1980s. It involved sending messages in which a wealthy benefactor is claiming that he wants to transfer a large sum of money to the recipient – but only after various fees were paid upfront (Dyrud, 2005). Interestingly, the Nigerian scam mechanism is still actively used in Poland today (Łęski et al., 2023).

Frauds that primarily rely on obtaining confidential information through human interaction (manipulation) are referred to as *social engineering attacks* (Radoniewicz, 2021). Additionally according to Salahdine & Kaabouch (2019), social engineering attacks can be categorized into the following types:

- human based and computer based;
- or technical based, social based and physical based.

Increasingly, complex strategies that are emerging also incorporate elements of advanced technical knowledge. A social engineering attack may include aspects of phishing, malware, or scam (Gryszczyńska, 2021).

Basic Obligations of Banks in e-Banking Security

One of the fundamental obligations of a bank is to ensure the security of e-banking customers, although, naturally, the complete elimination of cybercrime is impossible (Lisowska & Waściński, 2021). The fundamental provisions are contained in the Banking Law (Act of August 29, 1997). Pursuant to Article 50 par. 2 thereof, "a bank shall exercise special diligence in ensuring the security of the funds entrusted to it". The aforementioned provision indicates that ensuring the security of entrusted funds is one of the most significant obligations of a bank (Judgment of April 14, 2003), which should be associated with strict authentication procedures for transactions on the account, even if they are burdensome (Kociucki, 2020).

The European PSD2 directive is also of significant importance, as it imposes substantial transaction security requirements on banks, such as the strong authentication procedure, while also greatly enhancing consumer protection, for instance, through the procedure for reporting unauthorized transactions. In the case of an unauthorized transaction being reported, the bank is obligated to promptly

refund the lost amount unless there is suspicion of the customer's involvement in fraud (Paduszyńka & Pawlak, 2020). These regulations were implemented into the national law through the Payment Services Act.

The scope of "special diligence" should be assessed, among other things, through the lens of Recommendations issued by the Financial Supervision Authority under Article 137 point 5 of the Banking Law and Article 102 point 2 of the Payment Services Act (Act of August 19, 2011). Among these, particular importance is given to Recommendation D on the management of information technology areas and the security of the IT environment in banks (Resolution No. 7/2013) and the Recommendation on the security of online payment transactions executed by banks, national payment institutions, national electronic money institutions, and cooperative savings and credit unions (Resolution No. 584/2015).

Banks use transaction monitoring systems available on the market, provided by leading software manufacturers. Such a system should detect changes in login locations, modifications in the usage patterns of e-banking (navigation paths), excessively fast transaction execution, and unusual transactions, such as international transfers, termination of all deposits, or the use of all available funds (Iwaszczuk & Jarzęcka, 2016).

The literature mentions several possible channels for reporting incidents, including a dedicated email inbox, a designated section in online banking, encrypted and digitally signed emails, and the bank's helpline (Iwaszczuk & Jarzęcka, 2016).

The Growth of Bank Cyberscam during the Pandemic in Poland and Europe

The COVID-19 pandemic intensified the phenomenon of bank cyberscams, with criminals developing fraud schemes based on fear and the desire for pandemic-related information (Stawińska, 2021), leading to large-scale fraudulent activities (Tang et al., 2021). Due to the lockdown, consumer habits changed, including among older and less-educated individuals, who increasingly used e-banking and the Internet, making them targets for specially designed cyberscams (Naeem & Ozuem, 2021).

The sudden increase in online activity was also accompanied by a significant rise in cybercrime in Poland (Gryszczyńska, 2021), including a noticeable increase in fraudulent transactions using payment cards online in years 2018–2019 (Zalewska-Bochenko, 2023). This is confirmed by the rise in crimes related to e-banking identified by law enforcement agencies and the number of incidents classified by CERT as online fraud. However, it is important to note that such an increase was not observed in incidents described by CERT as belonging to the banking sector (likely because only reports directly related to banking systems are considered) or in the statistics provided by the Supreme Audit Office (there is no known distinction between the classification of crimes according to NPH and SAO data, while SAO figures pertain to reported crimes rather than confirmed ones). Also the number of cybercrime incidents reported by CSIRT increased in analyzed period.

A trend analysis was conducted, assuming a significance level of alpha = 0.1 due to the limited study period (2018–2021). Based on the obtained p-values, it can be inferred that a trend is present in the NPH, CERT (online fraud), and CSIRT data, however, the results are affected by a high margin of error due to a low number of observations. In the case of CERT data for the banking sector, the trend was not confirmed for reasons previously discussed. Similarly, the trend in card fraud data was not confirmed, as it appears to be only a one-time increase. Detailed data is presented in Table 1.

Table 1

Data related to cybercrimes committed and reported in Poland in thousands

	2018	2019	2020	2021	p-value
Confirmed crimes related to e-banking (National Police Headquarters)	3,6	6,3	6,7	14,5	0,0889
Online fraud reported to Police (Supreme Audit Office)	–	48,12	49,44	37,79 (50,38*)	–
Incidents handled described as banking sector (CERT Poland)	0,64	1,05	1,00	0,95	0,3845
Incidents handled described as online fraud (CERT Poland)	1,88	4,08	8,31	25,47	0,0947
Number of cybercrime incidents (CSIRT)	6,24	12,4	23,31	26,90	0,0164
Number of card frauds (Payment Systems Department)	44,4	62,4	63,9	61,8	0,2458

* Only data for three quarters has been provided, and the number in parentheses represents an estimated figure for the entire year, assuming the same quantity as in previous quarters.

Source: own work based on Boczoń (2022), CERT (2018; 2019; 2020; 2021), NIK (2022), Zalewska-Bochenko (2023), Statista (2024a).

A significant increase in online fraud was also observed in other major European countries during the pandemic. It is important to note that the data obtained for France, Germany, and the United Kingdom come from different sources with varying reporting methods and definitions of counted cases, so they should not be compared between countries. In all cases, a substantial rise was recorded, with the significance of the trend for France and Germany also confirmed by a low p-value. For these countries, it seems that the increase during the pandemic was not as pronounced as in Poland. Meanwhile, the United Kingdom recorded a similar rise to Poland, however, due to incomplete data (only three observations), the calculation of the p-value was omitted. Detailed information is presented in Table 2.

An additional source of information may also be the Eurojust statistics on cooperation in cybercrime cases. Here, too, a clear increase was observed: 2018: 99, 2019: 125, 2020: 174, and 2021: 188. The calculated p-value is 0.0198, which means that, given the adopted assumptions (along with the indicated limitations), the parameter is statistically significant, and in this case, a trend is also present.

Table 2

Number of online fraud incidents in France, Germany and United Kingdom (in thousands)

	2018	2019	2020	2021	p-value
France	79,3	99,0	124,5	149,8	0,0017
Germany	66,28	78,2	105,0	113,0	0,0210
United Kingdom	–	25,8	56,0	72,6	–

Source: own work based on Statista (2024b; 2024c; 2025).

Evolution of Bank Cyberscam during the Pandemic in Poland

During the pandemic, the number of cybercrimes not only surged dramatically but also gave rise to innovative methods of cyberscams. Among these new tactics were shocking, but not true online messages (e.g., about the number of infections), as well as mass-distributed SMS messages offering access to a paid vaccine, a fake food support, or claims that the government had frozen funds for special reserves – each time including a link to a fraudulent website or malicious software (CERT, 2020).

The further stages of the pandemic saw the emergence of additional fraud methods, among which the following were particularly notable: fake applications spread via SMS, such as STOP COVID, supposedly informing users about contact with infected individuals; mObywatel, allegedly allowing access to a third dose of the COVID-19 vaccine; and parcel delivery apps, especially those imitating InPost (CERT, 2021). Other scams included home quarantine (KNF, 2021) and the PKO BP Super campaign, falsely advertised on social media as offering a 200 PLN bonus (CERT, 2020).

Existing fraud schemes were also enhanced, including the previously common bank helpline scam, in which victims were persuaded to install malware or transfer money using Blik codes. During the pandemic, criminals combined these manipulation techniques with vishing, making the bank's actual helpline number appear on the victim's phone screen. Victims often verified the phone number, and its authenticity increased their trust in the caller (Rzecznik Finansowy, 2021).

Particularly noteworthy is the rapid growth of cyberscam schemes based on various investment opportunities, including fake investment platforms promising exceptionally high returns on cryptocurrencies and, from the second half of 2021, fraudulent investment offers imitating well-known companies, especially PKN Orlen. In both cases, victims were deceived through fabricated news articles, made more convincing with numerous photos and statements from celebrities and prominent politicians. After believing the content, victims provided their phone numbers to scammers and, following a persuasive phone conversation, invested a small amount. Through continuous manipulation, they were convinced to transfer additional funds and install remote-access software on their devices used for e-banking (CERT, 2021).

The described modus operandi of criminals during the Covid-19 pandemic indicates the development and significant complexity of methods used to defraud funds. Changes during the

pandemic have led to crimes committed against e-banking customers relying predominantly on social engineering and often incorporating elements of phishing (including spoofing), malware exploitation, and scenarios typical of scams.

Analysis of Security Alerts Published by the Largest Banks in Poland

As part of the research, an analysis was conducted on security alerts published on the websites of the five largest banks in Poland (based on total assets), namely PKO Bank Polski, Bank Pekao, Santander Bank Polska, ING Bank Śląski, and mBank, during the period from 2018 to 2021. Only warnings about potential cyberscams targeting customers were considered as security announcements, regardless of the level of detail in the warning (technical information, such as changes in e-banking, was excluded). A comprehensive summary of the results is provided in Table 3.

Table 3

Number of security alerts published on the website by the five largest banks in Poland in the years 2018–2021

	PKO Bank Polski	Bank Pekao	Santander Bank Polska	ING Bank Śląski	mBank
2018	5	0	–*	10	11
2019	6	2	5	9	7
2020	17	6	15	6	12
2021	10	3	14	10	12

* Rebranding and website change at the end of 2018.

Source: own work.

A diverse approach to publishing security notices is evident among the analyzed banks, particularly in the case of Bank Pekao, which significantly lags in terms of the number of notices (it also lacked a visible section dedicated solely to security updates). Notably, there was an increase in the number of published notices during the Covid-19 pandemic – 26 notices were published in 2018, 29 in 2019 (24 excluding Santander Bank Polska), 56 in 2020 (41), and 49 in 2021 (35). This observed trend appears to support findings regarding the rise in cyberscam cases during the pandemic.

It should be emphasized that a bank's website is not the only channel used for communicating security announcements. Banks can also display alerts during logging in, send messages to users, and more. Additionally, in cases of recurring cyberscam schemes, instead of publishing a new notice, banks may simply update a previous one (for example, ING Bank Śląski highlights certain notices as “Top Threats”).

As the next element of study, six characteristic bank cyberscam scenarios were selected, which, according to the analyzed reports, emerged or reached a significant scale during the pandemic. The study

further analyzed if and when the examined banks issued announcements regarding these threats. The detailed dates are presented in Table 4.

Table 4

Publication of the first security alerts regarding selected cyberscam scenarios in the years 2018–2021 (the five largest banks in Poland)

	PKO Bank Polski	Bank Pekao	Santander Bank Polska	ING Bank Śląski	mBank
Bank helpline fraud*	–	11.12.2020	21.09.2021	03.09.2019	05.11.2020
Paid vaccine	–	–	16.03.2020	25.03.2020	–
Funds blockage	13.03.2020	–	16.03.2020	25.03.2020	14.03.2020
Food support	–	–	16.03.2020	25.03.2020	14.03.2020
Fake inpost app	–	–	–	01.07.2020	27.01.2021
Cryptocurrency scam	04.09.2020	05.02.2020	14.07.2020	10.02.2020	28.01.2020
PKN Orlen scam	–	–	–	–	–

* Only announcements regarding the potential use of vishing.

Source: own work.

The first selected scenario was the so-called bank helpline scam, focusing solely on its latest version, which relies on deceiving victims through vishing. This choice was made due to the significant role that phone number confirmation plays in the effectiveness of the manipulation. As a result, numerous notices published by PKO Bank Polski were excluded, as none of them mentioned the possibility of vishing; instead, they merely encouraged verifying the caller by dialing the official helpline number. For the remaining four banks, warnings about this scam were published over a period of two years.

Cyberscam schemes related to the early days of Covid-19 in Poland were also identified. These included fraudulent SMS messages falsely informing recipients about faster vaccinations for a fee, blocked funds allocated to a special reserve, and food support due to the pandemic. The first announcement was issued by PKO Bank Polski on March 13, 2020, but it only addressed SMS scams related to fund blocking. The following day, mBank published an announcement, providing a detailed description of the fund-blocking messages while mentioning the food support scam only briefly in a single sentence. Three days later, Santander Bank Polska released a statement covering all three scam types. ING Bank Śląski also warned against all three scams, but on March 25, 2020, whereas Bank Pekao did not issue any warning. A similar cyberscam scheme was also analyzed – one based on SMS messages claiming that a package was waiting for pickup at an InPost parcel locker. Only two banks issued warnings about this scam: ING Bank Śląski on July 1, 2020, and mBank on January 27, 2021 – half a year later.

The last group consisted of fraudulent investment offers, specifically the so-called cryptocurrency scam and the PKN Orlen scam. All of the analyzed banks issued announcements about

the cryptocurrency scam, with mBank being the first to do so on January 28, 2020, and PKO Bank Polski being the last, nearly nine months later, on September 4, 2020. However, none of the banks issued warnings about the PKN Orlen scam, possibly due to their earlier communications on investment-related cyberscam.

It can also be perceived that, in the case of the analyzed cyber fraud scenarios, there is a potential relationship between the publication of security alerts and the nature of the bank's dominant owner. Banks controlled by the State Treasury published only two alerts each, while banks controlled by the public sector published five or six alerts. However, this may be merely an apparent correlation related to the selection of the analyzed scenarios, especially since, in terms of the overall number of security alerts, a lower number is observed only in the case of Pekao.

Cyberscams Committed during the Pandemic in Poland – Case Studies

The final part of the research consisted of case studies of three specific cyberscam incidents committed during the pandemic. The analysis was based on information from official documents issued by law enforcement authorities, correspondence between the victims and their banks, and documents submitted as part of mediation proceedings before the Financial Ombudsman or civil court proceedings. To maintain the anonymity of the victims, the timeframe of each crime was limited to indicating the quarter in which it occurred, and the financial loss was rounded to the nearest PLN 5,000. Each victim was a customer of a different bank, and in all cases, the dispute between the victim and the bank remains ongoing. A short summary of the analyzed cases is presented in Table 5.

Table 5

Basic information on the examined cases of cyberscams

Case	A	B	C
Quarter	Q1 and Q2 of 2020	Q3 of 2021	Q4 of 2021
Detriment	80.000 PLN	50.000 PLN	40.000 PLN
Scenario	cryptocurrency scam	bank helpline scam	bank helpline scam
Methods	scam, phising, malware	vishing	vishing, malware
Source of funds	funds in bank account, online loans	funds in bank account, funds from other bank accounts	funds in bank account, online loans
Method of taking funds	transfers to foreign banks	physical withdrawals and deposits using Blik codes (ATM)	transfers to domestic banks

Source: own work.

Case A involves a cryptocurrency scam. In the first quarter of 2020, the victim, encouraged by a mobile advertisement, created an account on a fraudulent investment platform, unknowingly installing an application that enabled remote access. Initially, they deposited a small amount in euros, which was

allegedly “lost” in full. Several months later, the victim received a call from a fake investment consultant claiming that an automated trading system had generated a significant profit. A few days later, the consultant informed the victim that the funds were available for withdrawal and advised them to simultaneously open the investment platform and log in to their online banking. Within a short period, multiple transactions were carried out, including signing two online loan agreements, maxing out a credit card twice, and making two euro transfers to a foreign bank account. An attempt was also made to transfer funds directly from the credit card, but it failed due to exceeding the credit limit. These transactions drained all available funds from the victim’s account. They were executed by the bank without additional verification, relying solely on SMS codes, resulting in a total financial loss of approximately 80,000 PLN. The bank’s online banking expense analysis service categorized these transactions as unspecified financial expenses and household bills.

The victim realized the crime the following day, immediately notifying the bank and filing a criminal complaint. However, no funds were recovered, and the criminal investigation was discontinued due to the perpetrators remaining unidentified. The victim had never previously taken out online loans or made transfers of such high amounts. The only prior foreign transfer victim had executed was the initial small deposit to the fraudulent investment platform. The transactions carried out by the cybercriminals were clearly characteristic of fraudulent activities described in the literature and should have been flagged by the bank’s fraud detection system, as outlined in the Security Recommendation (Recommendation 10), rather than being misclassified. The bank rejected all complaints filed by the victim, who was left repaying the fraudulent loans for over four years. In 2024, a court ruled that the bank was liable for all unauthorized transactions, and in 2025 the refund from the bank of the majority of the remaining disputed amounts.

Case B, a cyberscam based on the bank helpline scam, is particularly notable because the crime was carried out solely through vishing and advanced social engineering, without the use of any malware. In the third quarter of 2021, the victim was contacted by a fake bank consultant. The victim verified the helpline number on the bank’s website and reviewed the bank’s security announcement, none of which mentioned the possibility of vishing. The fraudster also possessed extensive personal information about the victim, including full name, bank account number, and details of authorizations for other bank accounts. The scammer informed the victim that an attempted hack had been detected on all accounts, including an attempt to take out a loan. To protect funds, the scammer instructed the victim to:

- change transaction limits;
- transfer all funds from various accounts into a main account;
- visit a bank branch with a cash deposit machine.

Following further instructions, the victim withdrew money from an ATM and deposited it into a cash deposit machine using Blik codes, allegedly transferring the funds to a “special reserve account” for security reasons. As a result of multiple transactions, the victim lost a total of PLN 50,000.

The victim's actions were interrupted by a bystander, who immediately accompanied them to the police. The victim and the witness attempted to contact the real bank helpline, but were only able to get through after a significant delay. The police accepted the criminal complaint, and a criminal court convicted minor accomplices (while the main perpetrators were never identified). The victim managed to recover approximately 1/4 of the lost amount from them. Regardless of the method using Blik codes to transfer funds, the case suggests that if a vishing warning had been available on the bank's website, the victim likely would not follow the scammer's instructions. Additionally, the victim suspects that personal data was leaked from the bank.

Crime committed in case C was also based on the bank helpline scam scenario, but in this instance, the fraudsters additionally used malware. In Q4 2021, the victim was contacted by a fake bank consultant (using vishing) who informed them about an alleged attempt to hack their account. The scammer then convinced the victim to install and activate a remote access application, which allowed the fraudsters to take out an online loan and execute six transfers to three different accounts, totaling PLN 50,000. The bank processed all transactions without any additional verification, leading to the complete drainage of the victim's account.

During the call with the fake consultant, the victim went to a bank branch, where employees advised them to end the conversation. The bank staff spent over 30 minutes trying to contact headquarters, eventually deciding to send the information via email. As a result, they managed to block PLN 5,000, which was later returned to the victim after the criminal case was discontinued. However, the bank rejected all complaints. Similar to Case A, the fraudulent transactions carried out by cybercriminals matched patterns well-documented in financial fraud literature and should have been detected by the bank's security system. Additionally, concerns arise regarding:

- whether the bank had adequate procedures for handling such incidents;
- the extent to which bank employees were familiar with those procedures.

A lawsuit against the bank is currently ongoing.

Conclusion

A significant portion of the analyzed data for Poland indicates that during the COVID-19 pandemic, there was a substantial increase in cybercrimes targeting online banking customers. This rise is particularly evident in data provided by the National Police Headquarters, the number of online fraud incidents handled by CERT, and the number of cybercrime incidents reported by CSIRT. Additionally, in these cases, the existing trend was statistically confirmed.

Not all of the analyzed data confirmed this phenomenon. A particularly surprising inconsistency arises between the number of reported online fraud cases (Supreme Audit Office) and the number of confirmed crimes related to e-banking, as well as online fraud incidents handled by CERT. Given that these events appear similar, an increase should also be observable in SAO data. Unfortunately, the

precise methodology behind the SAO-released data remains unknown, including the specific types of crimes recorded and the counting methods used. Furthermore, data from banking sector incidents and card fraud indicate that the rise in cybercrime is not linked to an increased number of attacks reported by banks or a higher use of payment cards.

A similar phenomenon is also observed in the major European countries included in the study. The number of online fraud incidents increased in all examined countries, namely France, Germany, and the United Kingdom. Additionally, in the case of the first two countries, a statistical analysis indicates a high significance of the trend (p-value of 0.02 or lower, while for the United Kingdom, the lower number of observations affects statistical significance). Thus, 1st hypothesis has been positively verified.

The analysis of security alerts indicates that Poland's largest banks lacked a unified policy for publishing such announcements, with significant differences observed between institutions. Notably, there were also big time discrepancies in warnings about the same cyberscams schemes published by different banks (even more than one year). The examined banks fulfilled their information obligations to varying degrees, meaning that at least some did not take all necessary actions immediately. As a result, 2nd hypothesis has been negatively verified.

Additionally, the case studies revealed deficiencies in existing security measures, particularly:

- the lack of effective systems for detecting fraudulent transactions, including wrong categorization of transactions (household bills etc.);
- problems with reaching bank hotlines in case of emergency;
- inadequate employee training at bank branches resulting in failure to take fast and appropriate action.

For this reasons 3rd hypothesis has also been negatively verified.

The research results indicate that during the pandemic, the number of crimes increased drastically, both in Poland and across Europe. Enhanced customer education policies were essential. Moreover, considering the significant inconsistencies in banks' security alerts, the development of a centralized system for disseminating security-related information warrants consideration. It also became essential to enhance fraud detection systems, even at the cost of reducing the convenience of online banking (even like wider transaction delays for high-risk transfer). Finally, modifications to existing procedures are necessary to ensure an immediate response to scam reports. This requires not only raising employee awareness (including appropriate training programs) and improving system infrastructure but also implementing better procedures, such as dedicated fraud hotline or specialized in-app feature for reporting cyberscams.

References

Act of August 19, 2011 on Payment Services [Ustawa z dnia 19 sierpnia 2011 roku o usługach płatniczych], t.j. Dz.U. 2024, poz. 30 ze zm.

Act of August 29, 1997 – Banking Law [Ustawa z dnia 29 sierpnia 1997 roku Prawo bankowe], t.j. Dz.U. 2024, poz. 1646 ze zm.

Act of June 6, 1997 – Penal Code [Ustawa z dnia 6 czerwca 1997 roku Kodeks karny], t.j. Dz.U. 2024, poz. 17 ze zm.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 3–12. https://doi.org/10.1016/j.cose.2017.04.006

Boczoń, W. (2022, November 30). Pandemia sprzyja cyberprzestępczości. Lawinowy wzrost ataków na klientów banków. *Bankier.pl*. https://www.bankier.pl/wiadomosc/Pandemia-sprzyja-cyberprzestepczosci-Lawinowy-wzrost-atakow-na-klientow-bankow-8285514.html

CERT. (2018). *Annual Report on the Activities of CERT Polska 2018*. NASK – National Research Institute [*Raport roczny z działalności CERT Polska 2018*. Państwowy Instytut Badawczy]. https://cert.pl/uploads/docs/Raport_CP_2018.pdf

CERT. (2019). *Annual Report on the Activities of CERT Polska 2019*. NASK – National Research Institute [*Raport roczny z działalności CERT Polska 2019*. Państwowy Instytut Badawczy]. https://cert.pl/uploads/docs/Raport_CP_2019.pdf

CERT. (2020). *Annual Report on the Activities of CERT Polska 2020*. NASK – National Research Institute [*Raport roczny z działalności CERT Polska 2020*. Państwowy Instytut Badawczy]. https://cert.pl/uploads/docs/Raport_CP_2020.pdf

CERT. (2021). *Annual Report on the Activities of CERT Polska 2021*. NASK – National Research Institute [*Raport roczny z działalności CERT Polska 2021*. Państwowy Instytut Badawczy]. https://cert.pl/uploads/docs/Raport_CP_2021.pdf

Czyżak, M. (2016). Cyberprzestępczość bankowa i środki jej zwalczania. *Ekonomiczne Problemy Usług*, *123*, 205–206. http://dx.doi.org/10.18276/epu.2016.123-19

Deng, H., Wang, W., & Peng, C. (2018). CEIVE: Combating Caller ID Spoofing on 4G Mobile Phones Via Callee-Only Inference and Verification. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking* (pp. 369–370). https://doi.org/10.1145/3241539.3241573

Dyrud, M. (2005). "I brought you a good news": An analysis of Nigerian 419 letters. In *Proceedings of the 2005 Association for Business Communication Annual Convention* (pp. 2–4).

Eurojust. (2018). *Eurojust Annual Report 2018*. https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_2018_annual_report_en.pdf

Eurojust. (2019). *Eurojust Annual Report 2019*. https://www.eurojust.europa.eu/sites/default/files/assets/ar2019_en.pdf

Eurojust. (2020). *Eurojust Annual Report 2020*. https://www.eurojust.europa.eu/sites/default/files/assets/2021_04_14_eurojust_annual_report_2020_final.pdf

Eurojust. (2021). *Eurojust Annual Report 2021*. https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-annual-report-2021.pdf

Górnisiewicz, M., Obczyński, R., & Pstruś, M. (2014). *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną. Poradnik usług finansowych.* KNF.

Gryszczyńska, A. (2021). Wykorzystanie Covid-19 w scenariuszach ataków opartych na socjotechnice. *Rocznik Bezpieczeństwa Morskiego: Przestępczość teleinformatyczna 2020*, 137–161.

Iwaszczuk, N., & Jarzęcka, A. (2016). Porównanie wybranych aspektów bezpieczeństwa płatności internetowych kilku banków działających na polskim rynku. *Przedsiębiorczość i Zarządzanie*, *XVII* (8, part. III), 210–211.

Judgment of the Supreme Court of Poland dated April 14, 2003, in case no. I CKN 308/01 [Wyrok Sądu Najwyższego z dnia 14 kwietnia 2003 roku, w sprawie o sygn. akt I CKN 308/01], LEX/el. nr 157324.

KNF. (2021). *2021 Year in Review at CSIRT KNF. Description of Selected Attacks*. Polish Financial Supervision Authority [*2021 Podsumowanie Roku w CSIRT KNF. Opis wybranych ataków*. Komisja Nadzoru Finansowego]. https://cebrf.knf.gov.pl/images/Raporty/RaportCSIRTKNF_76474.pdf

Kociucki, L. (2020). Art. 50. In B. Bajor, J.M. Kondek, K. Królikowska & L. Kociucki (Eds.), *Prawo bankowe. Komentarz do przepisów cywilnoprawnych*. LEX/el.

Konieczny, M. (2023). Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość. *Annuals of The Administration and Law, 23*, 37–38. https://doi.org/10.5604/01.3001.0016.3776

Kulik, M. (2022). Art. 286. In M. Mozgawa (Ed.), *Kodeks karny. Komentarz aktualizowany*. LEX/el.

Łęski, Z., Kurkowski, M., Gozdecki, B., & Steingartner, W. (2023). Czy można zakochać się w Jessice? – czyli o Nigeryjskim Przekręcie z perspektywy Analizy Transakcyjnej. *Przegląd Policyjny*, *4*(152), 253–254. https://doi.org/10.5604/01.3001.0054.4340

Lisowska, A., & Waściński, T. (2021). Bezpieczeństwo bankowości internetowej i mobilnej na rynku finansowym. *Systemy Logistyczne Wojsk*, *54*, 162. http://dx.doi.org/10.37055/slw/140380

Lotko, M. (2024). Bezpieczeństwo płatności w erze cyfrowej. *Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu*, *2*(105), 13. https://doi.org/10.58683/dnswsb.1999

Mangut, P., & Datukun, K. (2021). The Current Phishing Techniques – Perspective of the Nigerian Environment. *World Journal of Innovative Research*, *10*, 38–39. https://doi.org/10.31871/WJIR.10.1.9

Naeem, M., & Ozuem, W. (2021). The role of social media in internet banking transition during COVID-19 pandemic: Using multiple methods and sources in qualitative research. *Journal of Retailing and Consumer Services*, *60*, 8. https://doi.org/10.1016/j.jretconser.2021.102483

NIK. (2022). *State actions in preventing and combating the effects of selected cybercrimes, including identity theft*. Supreme Audit Office [*Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*. Najwyższa Izba Kontroli]. https://www.nik.gov.pl/plik/id,27206,vp,30013.pdf

Paduszyńka, M. & Pawlak, B. (2020). Rynek usług płatniczych w Polsce w świetle zmian prawnych Implementujących postanowienia dyrektywy PSD2. *Studia Prawno-Ekonomiczne*, *CXIV*, 340–341. https://doi.org/10.26485/SPE/2020/114/18

Radoniewicz, F. (2021). Hacking w Kodeksie karnym – wybrane zagadnienia techniczne i karne. *Rocznik Bezpieczeństwa Morskiego: Przestępczość teleinformatyczna 2020*, 179–194.

Resolution No. 584/2015 of the Polish Financial Supervision Authority of November 17, 2015, on the issuance of a Recommendation concerning the security of payment transactions performed online by banks, national payment institutions, national electronic money institutions, and cooperative savings and credit unions [Uchwała Nr 584/2015 Komisji Nadzoru Finansowego z dnia 17 listopada 2015 r. w sprawie wydania Rekomendacji dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe], Dz.Urz. KNF 2015, poz. 56.

Resolution No. 7/2013 of the Polish Financial Supervision Authority of January 8, 2013, on the issuance of Recommendation D concerning the management of information technology and cybersecurity in banks [Uchwała Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach], Dz.Urz. KNF 2013, poz. 5.

Rybacka, J. (2023). Wpływ pandemii covid-19 na sposób korzystania z usług bankowych oraz na postrzeganie banków w Polsce – na podstawie badania empirycznego. *Journal of Finance and Financial Law*, *2*(38), 91–109. https://doi.org/10.18778/2391-6478.2.38.05

Rynkowska, M. (2017). Bezpieczeństwo danych osobowych w cyberprzestrzeni. *Rocznik Bezpieczeństwa Morskiego*, *XI*, 185–200.

Rzecznik Finansowy. (2021). *Podejrzany telefon z infolinii banku? Rzecznik Finansowy ostrzega przed nową metodą oszustów*. https://archiwum.rf.gov.pl/2021/08/13/podejrzany-telefon-z-infolinii-banku-rzecznik-finansowy-ostrzega-przed-nowa-metoda-oszustow/.

Salahdine, F. & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89, 3-4. https://doi.org/10.3390/fi11040089

Statista. (2024a). *Cybercrime and cybersecurity in Poland*. https://www.statista.com/study/66683/cyber-crime-and-cyber-security-in-poland/

Statista. (2024b). *Nombre d'infractions pour escroquerie en ligne enregistrées par les forces de l'ordre en France entre 2016 et 2023*. https://fr.statista.com/statistiques/1464740/escroquerie-numerique-infraction-france/

Statista. (2024c). *Number of internet banking fraud incidents in the United Kingdom (UK) from 1st half 2019 to 1st half 2024*. https://www.statista.com/statistics/1426076/uk-internet-banking-fraud-incidents/

Statista. (2025). Anzahl der Fälle von Computerbetrug in Deutschland von 2009 bis 2024. https://de.statista.com/statistik/daten/studie/419459/umfrage/faelle-von-computerbetrug-in-deutschland/

Stawińska, W. (2021). Pandemia a zjawisko cyberprzestępczości. *Media i Społeczeństwo*, *14*, 239–240. https://doi.org/10.53052/MiS.2021.14.15

Stefanowicz, M. (2017). Cyberprzestępczość – próba diagnozy zjawiska. *Kwartalnik Policyjny*, *4*, 20.

Tang, Z., Miller, A., Zhou, Z, & Warkentin, M. (2021). Does government social media promote users' information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, 38, 1. https://doi.org/10.1016/j.giq.2021.101572

Zalewska-Bochenko, A. (2023). Rynek płatności elektronicznych z perspektywy bezpieczeństwa transakcji. *Roczniki Ekonomiczne Kujawsko-Pomorskiej Szkoły Wyższej w Bydgoszczy*, *16*, 71–72.

Received: 30.03.2025
Accepted: 11.05.2025
Available online: 30.06.2025