AGATA WITEK
Uniwersytet WSB Merito w Poznaniu
Wydział Ekonomiczny w Szczecinie
e-mail: witek.agata123@gmail.com

Cyberzagrożenia a poczucie bezpieczeństwa i poziom świadomości klientów banków w Polsce w świetle badań własnych[1]

Streszczenie. Celem artykułu jest analiza zagrożeń cybernetycznych w polskim sektorze bankowym w perspektywie rosnącego znaczenia bankowości cyfrowej oraz wynikającego z niej ryzyka nadużyć. Badanie przeprowadzono w formie anonimowej ankiety, którą wypełniły 152 osoby. Skoncentrowano się na ocenie poczucia bezpieczeństwa klientów banków w Polsce oraz poziomu ich wiedzy z zakresu zabezpieczeń przed fraudami. Wyniki badania wskazują na bardzo wysokie poczucie bezpieczeństwa, mimo doświadczenia próby oszustwa przez niemal połowę ankietowanych. Ujawniono również bardzo wysoki poziom zaufania do sektora bankowego, mimo ograniczonej wiedzy ankietowanych w zakresie cyberbezpieczeństwa. Wyniki podkreślają konieczność intensyfikacji działań edukacyjnych ze strony sektora bankowego, jak również transparentnej komunikacji mającej na celu realne wzmocnienie bezpieczeństwa użytkowników.

Słowa kluczowe: cyberbezpieczeństwo, oszustwa finansowe, nadużycia w bankowości
https://doi.org/10.58683/dnswsb.2105

1. Wprowadzenie

Sektor bankowy, będący jednym z filarów globalnej gospodarki, w drugiej i pierwszej połowie trzeciej dekady XXI wieku przeszedł gwałtowną transformację — współcześnie niemal w całości opiera się na technologiach cyfrowych i na powszechnej, mobilnej dostępności wszelkich oferowanych przez niego usług. Choć rozwiązania te wiążą się z niekwestionowaną wygodą dla ich użytkowników, równocześnie niosą za sobą poważne zagrożenia w postaci przestępczości cyfrowej polegającej na *phishingu*, atakach *malware* czy trojanach bankowych. Instytucje finansowe stają tym samym przed koniecznością nieustannego wzmacniania

[1] Artykuł został przygotowany na podstawie pracy magisterskiej pt. „Geneza, konsekwencje i przeciwdziałanie nadużyciom finansowym w polskim sektorze bankowym. Perspektywa cyberbezpieczeństwa", napisanej pod kierunkiem prof. dr. hab. Stanisława Flejterskiego.

systemów ochrony. Innowacyjnym technikom zabezpieczeń stale towarzyszy jednak rozwój sposobów i metod nadużyć, co prowadzi do nieustannego wyścigu technologicznego między cyberprzestępcami a instytucjami finansowymi. Celem niniejszego artykułu jest analiza nadużyć finansowych zagrażających polskiemu sektorowi bankowemu oraz ocena świadomości i poczucia bezpieczeństwa klientów banków w Polsce, których wiedza i praktyki mają istotny wpływ na skuteczność systemów ochrony oraz odporność całego sektora na zagrożenia cyfrowe.

2. Przegląd literatury — ramy teoretyczne

Nadużycia finansowe wydają się zjawiskiem równie mocno złożonym, co nieustannie ewoluującym. Tym samym nie sposób jest podać jednej, spójnej i w pełni uniwersalnej definicji tego zjawiska. Tezę tę zdaje się potwierdzać mnogość definicji występujących zarówno w literaturze naukowej, jak i w tekstach prawnych i branżowych. Dokładne zrozumienie tego pojęcia jest jednak nieodzowne w kontekście rozważań prowadzonych w niniejszym artykule.

Słownik języka polskiego określa nadużycie jako „nieuczciwy, niezgodny z prawem postępek, zwłaszcza przestępstwo finansowe" (Kubisa-Ślipko, 2000). Z ujętej w ten sposób definicji wyłania się dualistyczny charakter nadużyć — nie są to wyłącznie czyny niezgodne z normami prawnymi, ale i czyny „nieuczciwe", a zatem przekraczające normy o charakterze społecznym, moralnym czy zawodowym. Jednocześnie związanie pojęcia „nadużycie" z przestępstwem finansowym nie tylko uwypukla jego wymiar ekonomiczny, ale i sygnalizuje potrzebę odróżnienia nadużycia od przestępstwa. Przestępstwa gospodarcze są bowiem funkcjonalnie wydzieloną klasą przestępstw, których podstawowym przedmiotem naruszenia jest obrót gospodarczy (Zawłocki i Gałęski, 2024). Każde przestępstwo gospodarcze stanowi zatem kwalifikowaną postać nadużycia gospodarczego, jednak nadużycie gospodarcze można określić mianem przestępstwa gospodarczego wyłącznie w przypadku, gdy dany czyn przekracza normy prawnokarne (Kutera, 2010).

Na podstawie licznych definicji terminu „nadużycie finansowe", wypracowanych w dorobku instytucji finansowych oraz środowisk naukowych, wyodrębnić można pewne cechy wspólne, które charakteryzują omawiane zjawisko (Rajewski, 2020):

1. intencjonalność — działanie stanowiące nadużycie podejmowane jest przez sprawcę celowo, z premedytacją, wykluczone są zatem wszelkie incydenty dotyczące przypadkowych, niezamierzonych błędów czy nieprawidłowości;

2. intratność — centralnym motywem dopuszczenia się nadużycia jest osiągnięcie korzyści przez sprawcę bądź osobę trzecią; korzyści te najczęściej mają wymiar majątkowy, biznesowy lub osobisty;
3. podstępność — sprawca w celu osiągnięcia korzyści posługuje się szeroko rozumianą dezinformacją, zatajeniem prawdy czy innego rodzaju manipulacją.

Ogólnikowy charakter wskazanych cech nadużyć finansowych wynika przede wszystkim z różnorodności form, jakie przyjmują, co z kolei przekłada się na istnienie licznych podejść do ich systematyzacji. Jednym z podstawowych kryteriów klasyfikacji jest kryterium legalności, wyróżniające nadużycia (Fabisiak i Michnik, 2016):

1. legalne — które są zjawiskiem niepożądanym, lecz nie znajdują odzwierciedlenia w przepisach prawnych;
2. nielegalne — wszelkie nadużycia zabronione obowiązującymi przepisami prawa.

Kolejnym kryterium jest możliwość ujawnienia. Można tu wyodrębnić nadużycia (Jasiński, 2013):

1. rzeczywiste — czyny stanowiące nadużycia finansowe nieakceptowane w ramach działalności przedsiębiorstwa ani społecznie;
2. ujawnione — nadużycia już wykryte oraz zgłoszone odpowiednim organom i podmiotom;
3. nielegalne — wszelkie ujawnione nadużycia, przeciwko którym odpowiednie organy wszczęły procedurę śledczą celem zbadania wypełnienia przez nie znamion przestępstwa;
4. osądzone — których przestępność stwierdzona została prawomocnym wyrokiem w ramach prowadzonego w ich sprawie postępowania karnego.

Nadużycia finansowe klasyfikowane mogą być również ze względu na ich przedmiot, tj. dobro, przeciwko któremu są skierowane. Tym samym wyróżnia się nadużycia popełnione na szkodę (Ciszewska, 2016):

1. osób fizycznych — w szczególności klientów oraz konsumentów, wierzycieli czy kontrahentów sprawcy, ale i samych przedsiębiorców reprezentowanych i kierowanych przez osoby fizyczne osobiście czy w postaci organu kolegialnego, tj. wszelkie piramidy i łańcuszki finansowe, parabanki, oszu-

stwa inwestycyjne, *phishing*, *skimming*, jak również tzw. wyłudzenie „na wnuczka" i inne;
2. instytucji finansowych oraz emitentów papierów wartościowych — w szczególności na szkodę banków i innych instytucji sektora bankowego pośredniczących w obrocie pieniądza i instrumentów finansowych, m.in. wyłudzenia kredytów, tzw. pranie brudnych pieniędzy, przestępstwa czekowe czy przestępstwa wekslowe;
3. Skarbu Państwa — wszelkiego rodzaju oszustwa i wyłudzenia podatkowe, w tym unikanie uregulowania bądź terminowego uregulowania należności fiskalnych oraz uzyskanie nienależnych zwrotów podatku czy nienależne pomniejszenie podstawy opodatkowania.

W kontekście niniejszego artykułu kluczowe znaczenie mają oszustwa popełnione na szkodę osób fizycznych, charakteryzujące się niejednokrotnie nawiązaniem bezpośrednich relacji z osobą pokrzywdzoną — relacji opartych na technikach manipulacji, wywierania wpływu oraz bezpośredniego nacisku. Ofiary skłonne są do obdarzenia oszusta zaufaniem i podjęcia pochopnych, ryzykownych decyzji finansowych i zarządczych, skuszone wizją osiągnięcia gwarantowanych, wysokich zysków czy dokonania intratnej inwestycji, często bez należytej weryfikacji otrzymanych danych oraz bez konsultacji ze specjalistami lub profesjonalnymi doradcami finansowymi. Ponadto, tego rodzaju nadużycia nierzadko pozostają bezkarne ze względu na ograniczone zasoby poszkodowanych w zakresie ich wykrywania oraz dochodzenia sprawiedliwości. Wiele przypadków nie jest zgłaszanych odpowiednim organom z uwagi na brak wiary w odzyskanie utraconych środków, złożoność i biurokratyczność procedur, jak również wstyd i poczucie winy, które towarzyszą ofiarom manipulacji. Tym samym są to czyny niezwykle szkodliwe społecznie — uderzają w podmioty o słabszej pozycji, pozbawione specjalistycznej wiedzy, jak i zasobów umożliwiających jej pozyskanie. Dlatego priorytetem winno być szerzenie społecznej świadomości, stanowiącej fundament skutecznej prewencji wobec nadużyć.

Ze względu na możliwość osiągnięcia szybkich i znaczących korzyści sektor bankowy pozostaje jednym z głównych celów przestępców. Analiza nadużyć finansowych w bankowości pozwoliła na wyodrębnienie na potrzeby niniejszej pracy trzech podstawowych kategorii:

1. nadużycia popełniane przez podmioty trzecie, w tym wyłudzenia kredytów lub „pranie pieniędzy", których ofiarą jest sama instytucja bankowa;
2. nadużycia popełniane przez podmioty trzecie, m.in. wyłudzenia danych poprzez wiadomości e-mail i SMS lub rozmowy telefoniczne i wykorzy-

stywanie ich do wyprowadzania środków z rachunków klientów banku, jak również ataki hakerskie wprost na systemy bankowe w celu kradzieży danych wrażliwych lub ulokowanych w banku środków, których celem są klienci instytucji bankowych, popełniane przez sprawców wykorzystujących usługi świadczone przez instytucje bankowe;
3. nadużycia popełniane przez pracowników instytucji bankowych bądź same instytucje bankowe, m.in. kradzież i sprzedaż danych klientów banku, fałszowanie danych w systemach bankowych czy wyprowadzenie pieniędzy klientów banku lub funduszy banku, a także łamanie przez podmioty zobowiązane zasad realizujących tzw. politykę AML (ang. *Anti-Money Laundering*).

Jedną z najczęściej spotykanych form oszustw w przestrzeni cyfrowej jest *phishing*, polegający na podszywaniu się pod zaufany podmiot (osobę, instytucję) w celu wyłudzenia od poszkodowanego danych wrażliwych bądź poufnych (np. danych logowania do konta bankowości elektronicznej), nakłonienia poszkodowanego do wykonania określonej, korzystnej dla sprawcy czynności (np. dokonania przelewu środków na wskazane konto) lub w celu zainstalowania na urządzeniu poszkodowanego złośliwego oprogramowania. Jak wynika z raportu z badania przeprowadzonego przez SMSAPI dotyczącego oszustw internetowych i zagrożeń komunikacji mobilnej w Polsce (Raport 2024: Bezpieczeństwo cyfrowe Polaków, 2024), niemal co piąty ankietowany przyznał, że padł ofiarą oszustwa internetowego w ciągu 6 miesięcy poprzedzających badanie (17,8%), a ponad połowa ankietowanych (53,7%) otrzymała w tym samym okresie tzw. podejrzane treści, tj. próby wyłudzenia danych, podszywanie się pod instytucje, prośbę o dopłatę do zamówienia lub rachunku itd. (Bezpieczeństwo cyfrowe Polaków, 2024).

W literaturze wyróżnia się wiele odmian *phishingu*. Do najpopularniejszych zaliczyć można (Król, 2024):

1. *Smishing* (*SMS phishing*) — wykorzystujący wiadomości SMS, które wyświetlają fałszywy identyfikator nadawcy, dzięki czemu oszuści podszywają się pod określony podmiot, np. bank poszkodowanego;
2. *Vishing* (*Voice phishing*) — polegający na telefonicznym podszywaniu się pod inny podmiot, poprzez wyświetlanie spreparowanego identyfikatora osoby dzwoniącej;
3. *Quishing* (*QR phishing*) — stosujący adresy URL umieszczone w kodzie QR, które odsyłają do zainfekowanych stron internetowych podszywających się pod strony instytucji (np. bankowych) lub do pobrania zainfekowanych plików;

4. *AIshing* (*AI phishing*) — używający do oszustwa szeroko pojętej sztucznej inteligencji, która z pewnością w niedalekiej przyszłości może stanowić w tym obszarze największe wyzwanie dla sektora bankowego.

Współczesna cyberprzestępczość przybiera rzecz jasna różne formy, a ich skutkiem nie są wyłącznie straty finansowe, choć i te są bezsprzecznie dotkliwe, ale i utrata zaufania klientów i dobrej reputacji podmiotów sektora bankowego. Tym samym zobligowanie do doskonalenia metod i mechanizmów wykrywania i przeciwdziałania oszustwom finansowym nie wynika wyłącznie z wymogów prawnych, lecz także z konieczności sprostania wymogom bezpieczeństwa obrotu finansowego nakładanym przez społeczeństwo. Jednym z podstawowych narzędzi wykorzystywanych w walce z fraudami w bankowości jest wewnątrzsektorowa wymiana danych i informacji. Dzięki współpracy z partnerami z rynku finansowego doświadczenia zdobyte przez jedne podmioty mogą posłużyć do uszczelnienia systemów bezpieczeństwa u innych (Majka, 2024). W walce z nadużyciami związanymi z kradzieżą tożsamości niezwykle pomocny stał się również prowadzony przez ministra cyfryzacji rejestr zastrzeżeń numerów PESEL, który działa jako swoista blokada przed wyłudzeniem kredytu, pożyczki lub leasingu, zawarciem nieautoryzowanej umowy rachunku oszczędnościowego lub konta osobistego czy przed jednorazową wypłatą gotówki w kwocie przekraczającej trzykrotność minimalnego wynagrodzenia (Kisiel, 2024).

Niezwykle skutecznym narzędziem prewencyjnym są również metody oparte na tzw. biometrii, których rozwój i popularyzację można było zaobserwować na przestrzeni ostatnich lat. Jest to jedno z narzędzi umożliwiających uwierzytelnienie oraz autoryzację transakcji bankowej dokonanej w bankowości *online* bądź *onsite*, polegające na wykorzystaniu indywidualnych i specyficznych cech klienta, które silnie, a niekiedy nawet jednoznacznie odróżniają go od innych osób. Wyróżnić można dwa główne rodzaje biometrii wykorzystywane w instytucjach bankowych (Biometria w bankowości elektronicznej — rynek, technologia, klient, 2022):

1. biometria behawioralna — oparta na cechach behawioralnych, takich jak głos, pismo odręczne czy sposób korzystania z urządzeń;
2. biometria fizyczna — oparta na cechach fizycznych (głównie odciski palców, tęczówka oka, wygląd twarzy czy układ żył w palcach lub w siatkówce oka).

Jako że osoby poddane manipulacji zachowują się w sposób odbiegający od normy, kluczową zaletą biometrii behawioralnej jest fakt, iż pozwala ona na wykrycie usiłowania popełnienia oszustwa z wykorzystaniem socjotechniki — kiedy to sam klient dokonuje transakcji (Majka, 2024). Rozwiązania korzystające z bio-

metrii mają jednak wszechstronne zastosowanie — używane mogą być do celów identyfikacji klienta w oddziałach banku lub bankomatach, do logowania się na konto, do uwierzytelnienia przelewu, pożyczki lub płatności kartą czy do założenia nowego rachunku (Wieprow, 2022).

Narzędziem, które na przestrzeni ostatnich lat odgrywa coraz większą rolę w sektorze bankowym, jest również szeroko rozumiana sztuczna inteligencja (AI). Jedną z największych zalet tej technologii jest umiejętność tzw. monitorowania danych w czasie rzeczywistym, dzięki czemu nie tylko znacznie skracany jest czas reakcji na podejrzane transakcje bądź zachowania użytkowników konta, ale i zaoszczędzony jest czas, który trzeba by było poświęcić na tradycyjne metody analizy. Co więcej, dla systemów sztucznej inteligencji możliwe jest stałe analizowanie i monitorowanie potężnej ilości danych, praktycznie niemożliwych do przetworzenia przez człowieka, co daje szansę wychwycenia nawet najdrobniejszych odstępstw od normy i najsubtelniejszych, powtarzalnych wzorców. W końcu, istnieje możliwość szkolenia systemów AI w celu wykrywania całkowicie nowych metod dokonywania nadużyć, na podstawie dostarczonych przez bank informacji na temat metod dotychczasowych (Gratkowska, 2024).

Choć technologia często odgrywa kluczową rolę w walce z cyberzagrożeniami, nie wszystkie rozwiązania mają charakter *stricte* techniczny — równie istotne jest równoległe, praktyczne wspieranie świadomości klientów, poprzez wyposażenie ich w narzędzia ułatwiające kontrolę nad własnymi środkami i rachunkami, m.in. w weryfikację dwuetapową, powiadomienia o nowych transakcjach, wprowadzanie limitów wydatków, transakcji czy wypłat lub też po prostu wyświetlanie ostrzeżeń w aplikacjach i stronach bankowych na temat potencjalnych oszustw. Dzięki tego typu działaniom klienci mają możliwość kompleksowego podejścia do kwestii bezpieczeństwa, a ryzyko pasywnej postawy wobec wszelkich prób nadużyć zostaje zminimalizowane.

Polski sektor bankowy nie zanotował wielu skutecznych ataków na infrastrukturę bankową. Jeden z takich przypadków miał miejsce w 2015 roku, kiedy Plus Bank padł ofiarą serii ataków hakerskich, których skutkiem była kradzież wrażliwych danych z systemu bankowego. Według oświadczeń rzekomego włamywacza łupem miały paść m.in. numery kilkuset kart płatniczych, dane osobowe klientów banku oraz loginy i hasła do rachunków bankowych (Haertle, 2015). W 2024 roku miał natomiast miejsce pierwszy znany napad *ransomware* w polskiej bankowości — jego ofiarą padł Bank Spółdzielczy w Zambrowie, który poinformował swoich klientów o ataku skutkującym zaszyfrowaniem ich danych i brakiem dostępu do bankowości elektronicznej oraz aplikacji mobilnej banku. Klienci przez kilka dni pozbawieni byli możliwości realizowania płatności oraz zarządzania środkami zgromadzonymi na rachunkach (Ransomware w Banku Spółdzielczym, 2024).

W trzeciej dekadzie XXI wieku największym zagrożeniem w Polsce pozostają domeny phishingowe. W samym 2024 roku zidentyfikowano ich aż 51 241, z których najwięcej wykorzystano do promowania fałszywych okazji inwestycyjnych, przeprowadzania oszustw ankietowych, oszustw kurierskich i pocztowych, do podszywania się pod instytucje bankowe oraz rozpowszechniania złośliwego oprogramowania (Raport roczny CSIRT KNF, 2024). Cyberzagrożenia w bankowości nie mają zatem wyłącznie wymiaru technologicznego — przyjmują również wymiar społeczny. Ataki wycelowane w podmioty nieprofesjonalne mogą skutkować wielomilionowymi zyskami dla świata przestępczego. Kluczowe zatem staje się zbudowanie zbiorowej świadomości tak, aby bezpieczeństwo nie opierało się wyłącznie na skuteczności stosowanych przez bank zabezpieczeń, ale również na umiejętności rozpoznawania i unikania zagrożeń przez samych użytkowników usług bankowych.

3. Metodyka badań

Niniejsze badanie przeprowadzone zostało w celu oceny poczucia bezpieczeństwa klientów banków w Polsce, przede wszystkim w kontekście cyberzagrożeń i cyberbezpieczeństwa, jak również w celu zbadania potencjalnych luk w świadomości i edukacji klientów na temat prewencyjnych praktyk stosowanych podczas korzystania z bankowości internetowej i mobilnej.

Podmiotem badań byli klienci polskich banków, przede wszystkim będący czynnymi użytkownikami bankowości internetowej lub mobilnej — badanie koncentrowało się na ich indywidualnych doświadczeniach i opiniach.

Główne pytania badawcze były następujące:

1. czy istnieje związek między poczuciem bezpieczeństwa klientów polskich banków a doświadczeniem przez nich próby oszustwa?
2. czy istnieje związek między oceną poziomu zabezpieczeń stosowanych przez banki w Polsce a stosowaniem przez ich klientów podstawowych praktyk bezpieczeństwa?

Na podstawie powyższych pytań sformułowano następujące hipotezy:

1. doświadczenie próby oszustwa przez klientów polskich banków negatywnie wpływa na ich poczucie bezpieczeństwa;
2. stosowanie praktyk bezpieczeństwa przez klientów polskich banków poprawia ocenę poziomu zabezpieczeń stosowanych przez banki w Polsce.

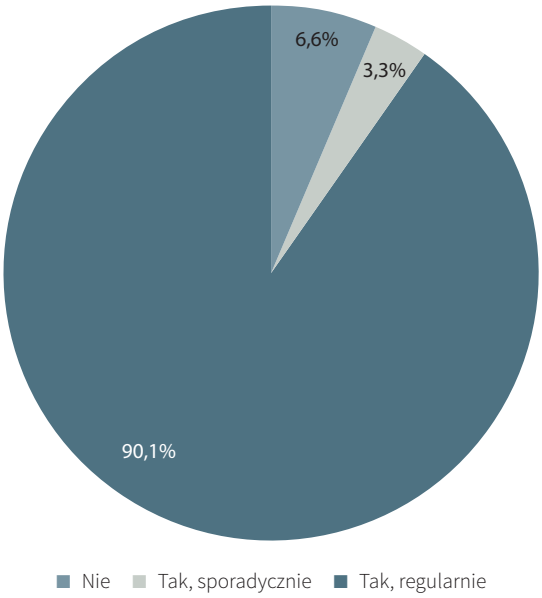
W celu zebrania opinii wykorzystano anonimową ankietę przeprowadzoną online w dniach 11–21 marca 2025 roku za pomocą formularza Google Forms — ankieta składała się z 15 pytań zamkniętych.

W badaniu wzięły udział 152 osoby. Wśród ankietowanych kontrolowano zmienne takie jak wiek, płeć oraz status zawodowy, które to dane były brane pod uwagę przy analizie wyników badania. Spośród badanych 58,6% stanowiły kobiety (89 osób), 38,8% stanowili mężczyźni (59 osób), a 2,6% osoby innej płci (4 osoby). Respondentów podzielono na pięć grup wiekowych, z czego najliczniejszą grupę stanowiły osoby między 26. a 35. rokiem życia (28,9%), następnie osoby w wieku 36–50 lat (25,7%), osoby w wieku 18–25 lat (20,4%), osoby w wieku 51–65 lat (16,4%) oraz najmniej liczna grupa osób powyżej 66. roku życia (8,6%). Wśród ankietowanych dominującą grupę stanowili pracownicy etatowi (96 osób), następnie kolejno przedsiębiorcy (18 osób), emeryci i renciści (15 osób), studenci (13 osób), osoby z innym statusem zawodowym (7 osób) oraz osoby bezrobotne (3 osoby).

Ze względu na metodę zbierania danych (ankieta internetowa) struktura respondentów nie odzwierciedla w pełni struktury demograficznej ogółu klientów banków w Polsce. W szczególności w badanej grupie odnotowano prawdopodobną nadreprezentację osób w wieku produkcyjnym (szczególnie 26–35 lat) oraz niedoreprezentację osób powyżej 51. roku życia. Taki rozkład jest jednak uzasadniony tematem badania, który koncentrował się na aktywnych użytkownikach bankowości internetowej i mobilnej. Dominacja osób młodych i aktywnych zawodowo pozwala na dokładniejszą analizę zachowań grupy najintensywniej korzystającej z nowoczesnych kanałów bankowości, choć wnioski nie powinny być bezkrytycznie generalizowane na grupę seniorów, którzy stanowili najmniejszy odsetek badanych, a którzy potencjalnie mogą stanowić dużą część ofiar cyberprzestępstw w obszarze usług bankowych.

4. Wyniki badań

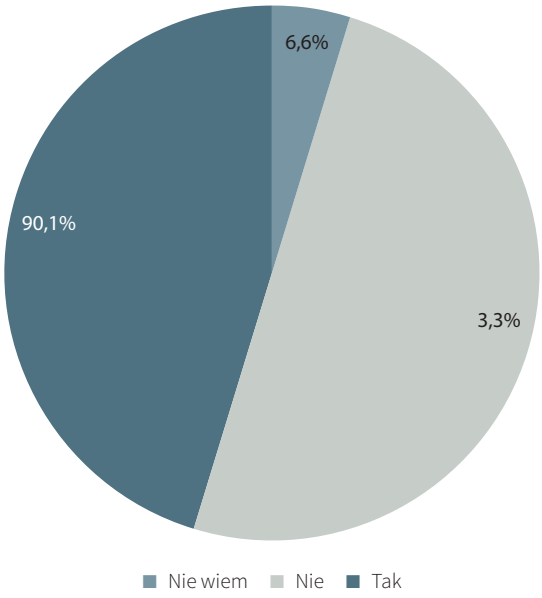
W kontekście głównego przedmiotu przeprowadzanej ankiety w pierwszej kolejności zbadano powszechność korzystania z cyfrowych usług oferowanych przez polskie banki w celu określenia stopnia, w jakim usługi te stanowią kanał komunikacji łączący instytucje bankowe z ich klientami, co przedstawiono na wykresie 1. Z udzielonych odpowiedzi wynika, że aż 90,1% ankietowanych deklaruje częste korzystanie z bankowości internetowej lub mobilnej, a kolejne 3,3% ankietowanych przyznaje, że z bankowości internetowej lub mobilnej korzysta sporadycznie. Jedynie 6,6% respondentów w żadnej mierze nie korzysta z tego rodzaju usług.



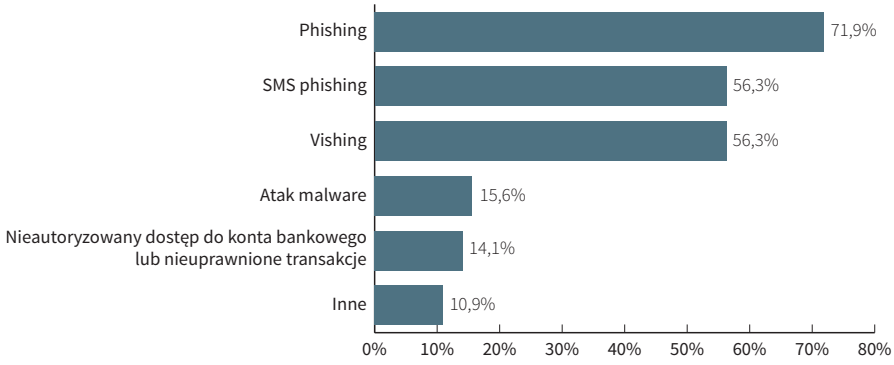
Wykres 1. Częstotliwość korzystania z bankowości internetowej lub mobilnej wśród badanych
Źródło: Badanie własne

Ukształtowana w ten sposób struktura podkreśla znaczącą rolę zdalnego kanału dostępu do bankowości jako priorytetowego ogniwa w zakresie oferowania usług przez instytucje finansowe, jak również w zakresie budowania relacji z klientem. Tym samym wyraźnie uwypukla ona potrzebę kładzenia szczególnego nacisku na cyfrową sferę funkcjonowania w ramach oceny ryzyka działalności, projektowania strategii bezpieczeństwa, jak również planowanych działań edukacyjnych — kanały elektroniczne powinny stanowić punkt ciężkości dla banków planujących skuteczną ochronę swoich klientów oraz budowanie ich cyfrowych kompetencji.

Rosnące znaczenie bankowości cyfrowej przekłada się na potencjalne ryzyko doświadczenia w tym obszarze prób cyberoszustwa. Zgodnie z wynikami badania, przedstawionymi na wykresie 2, narażona na nie była niemal połowa ankietowanych, co pokazuje, że choć poziom zabezpieczeń stosowanych przez polskie banki jest stosunkowo wysoki, a organy ścigania nieustannie pracują nad wykrywaniem przestępców cyfrowych, ich działania wciąż stanowią realne i powszechne zagrożenie dla klientów. Ponadto warto zauważyć, że niecałe 5% badanych nie było w stanie stwierdzić, czy doświadczyło próby cyberoszustwa, co sugerować może niewystarczający poziom wiedzy ankietowanych lub istnienie zaawansowanych technik oszustw, które niejednokrotnie mogą pozostać niezauważone.



Wykres 2. Doświadczenie przez respondentów próby oszustwa cybernetycznego lub ataku hakerskiego w ramach korzystania z usług bankowych
Źródło: Badanie własne

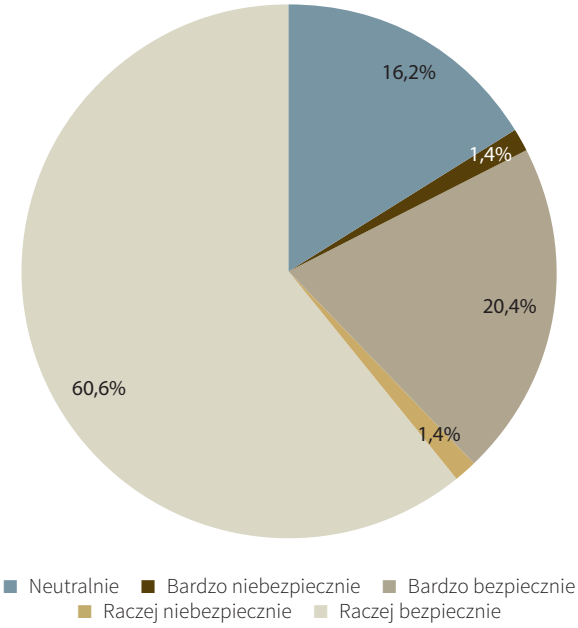


Wykres 3. Rodzaje oszustw cybernetycznych związanych z usługami bankowymi, których doświadczyli badani
Źródło: Badanie własne

Spośród grupy badanych, która deklarowała doświadczenie próby cyberoszustwa, zdecydowana większość zetknęła się z klasycznym phishingiem, SMS phishingiem oraz Vishingiem (ankietowani mieli możliwość wyboru więcej niż jednej odpowiedzi), co przedstawione zostało na wykresie 3. Wyniki badania potwierdzają

skalę i powszechność zagrożenia, jakim są ataki phishingowe. Przestępstwa tego typu zazwyczaj mają charakter masowy i są stosunkowo łatwe do przeprowadzenia — ich skuteczność opiera się w głównej mierze na braku świadomości klientów oraz na manipulacji ich emocjami. W efekcie jest to zagrożenie docierające do szerokiego grona potencjalnych ofiar niemal równocześnie, co raz jeszcze wskazuje na konieczność dalszego uczulania użytkowników na cyberprzestępstwa oraz wzmacniania umiejętności ich rozpoznawania.

Zważywszy, iż niemal połowa ankietowanych padła ofiarą co najmniej próby oszustwa cybernetycznego, naturalne staje się pytanie o ocenę poczucia bezpieczeństwa użytkowników w zakresie korzystania z cyfrowych usług bankowych. Jak wskazano na wykresie 4, nieoczekiwanie aż 60% ankietowanych deklaruje, że czuje się w tym zakresie raczej bezpiecznie, a kolejnych 20% ocenia korzystanie z bankowości cyfrowej jako bardzo bezpieczne.

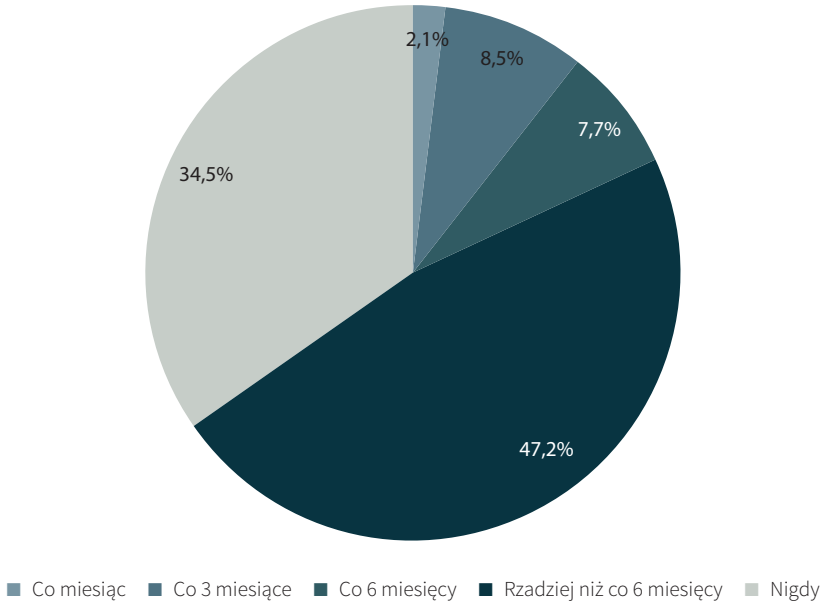


Wykres 4. Ocena poczucia bezpieczeństwa badanych podczas korzystania z bankowości internetowej/mobilnej
Źródło: Badanie własne

Co ciekawe, aż 43% z grupy osób pozytywnie oceniających swoje poczucie bezpieczeństwa zadeklarowało zetknięcie się z próbą oszustwa, a jedynie 25% z grupy badanych, którzy wystawili w tym pytaniu ocenę negatywną, faktycznie doświadczyła próby oszustwa. Wydaje się zatem, że paradoksalnie samo zetknię-

cie się z próbą oszustwa cybernetycznego, rozumiane jako rozpoznanie próby oszustwa, np. w formie phishingowej wiadomości lub podejrzanego kontaktu, nie ma większego wpływu na poczucie bezpieczeństwa ich użytkowników. Może być to zrozumiałe szczególnie w przypadku, gdy doświadczenie to nie zakończyło się stratą dzięki odpowiedniej reakcji klienta lub skutecznej interwencji banku. Tak wysoka ocena poziomu bezpieczeństwa może być również związana z ogólnym zaufaniem społeczeństwa do banków i stosowanych przez nich zabezpieczeń, co z pewnością byłoby pozytywnym wskaźnikiem dla sektora bankowego. Nie można jednak wykluczyć, że klienci banków, jako stali użytkownicy przestrzeni cyfrowej, mogą traktować próby oszustwa po prostu jako nieunikniony element dzisiejszego świata technologicznego, w którym nadużycia cyfrowe stopniowo ulegają normalizacji i przestają budzić należytą czujność.

W kontekście postawionych pytań badawczych nieodzowna stała się również analiza korzystania przez ankietowanych z podstawowych praktyk wzmacniających bezpieczeństwo przeciętnego użytkowania bankowości cyfrowej, szczególnie pod kątem korelacji między ich stosowaniem a tak wysoką deklarowaną oceną poczucia bezpieczeństwa.



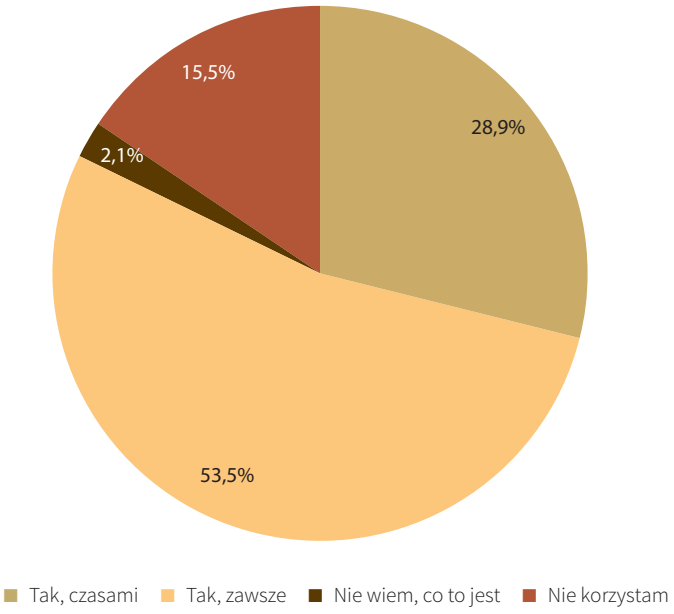
Wykres 5. Częstotliwość zmiany hasła przez badanych do internetowego/mobilnego konta bankowego
Źródło: Badanie własne

Jedną z podstawowych dobrych praktyk wydaje się regularna zmiana hasła do bankowości internetowej/mobilnej. Tymczasem, jak przedstawiono na wykresie 5,

aż 34% ankietowanych przyznało, że nigdy tego nie zrobiło, a kolejne 47% dokonuje takiej zmiany rzadziej niż co 6 miesięcy — tym samym jedynie niecałe 20% ankietowanych dba o tę formę zabezpieczenia co najmniej co pół roku.

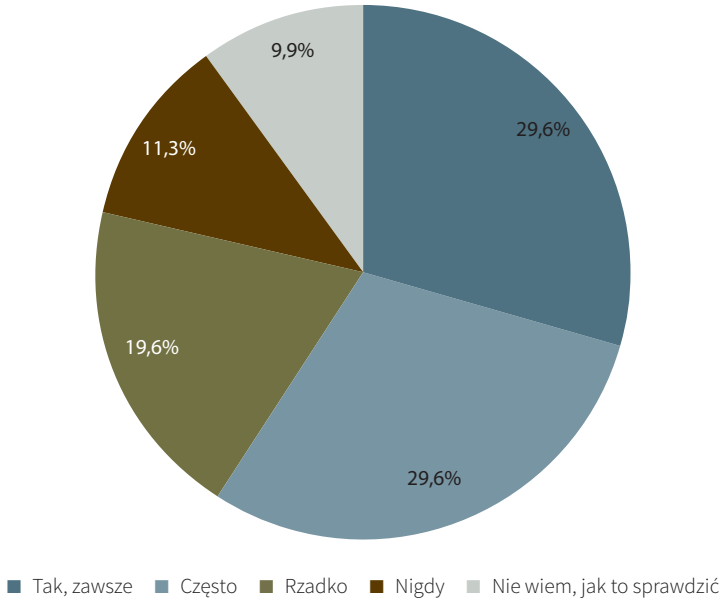
Kolejne pytanie miało na celu sprawdzenie częstotliwości korzystania przez ankietowanych z dodatkowych form zabezpieczeń podczas procesu logowania do bankowości internetowej. Jedną z najbardziej powszechnych metod w tym zakresie jest stosowanie cyfrowych certyfikatów potwierdzających tożsamość klienta, korzystanie z geolokalizacji, biometrii bądź z tzw. uwierzytelniania dwuskładnikowego (2FA), polegającego na dodaniu kolejnego etapu weryfikacyjnego (po wprowadzeniu danych logowania) w postaci kodu SMS, kodu z aplikacji uwierzytelniającej lub innych.

Wyniki badania przedstawione na wykresie 6 są w tym przypadku znacznie bardziej optymistyczne — aż 53,5% respondentów deklaruje, że takie zabezpieczenia stosuje zawsze, a niecałe 29% korzysta z nich przynajmniej czasami. Choć jest to wyraźny sygnał rosnącej świadomości w tym obszarze, liczba użytkowników nieznających tej formy zabezpieczenia oraz z niej niekorzystających pozostaje na tyle duża, iż konieczne staje się podejmowanie dalszych, systematycznych działań informacyjnych mających na celu zwiększenie wiedzy i zrozumienia wśród odbiorców.



Wykres 6. Częstotliwość korzystania przez badanych z dodatkowych zabezpieczeń, takich jak weryfikacja dwuetapowa (2FA), podczas logowania do bankowości internetowej
Źródło: Badanie własne

W ramach przeprowadzonego badania ankietowani zostali również poproszeni o wskazanie swoich nawyków związanych z oceną bezpieczeństwa stron internetowych przed realizacją transakcji online (wykres 7). Podstawową metodą w tym zakresie jest sprawdzenie obecności certyfikatu SSL, potwierdzającego tożsamość witryny — bezpieczne połączenie można rozpoznać za pośrednictwem protokołu HTTPS widocznego w adresie strony oraz ikony zamkniętej kłódki.

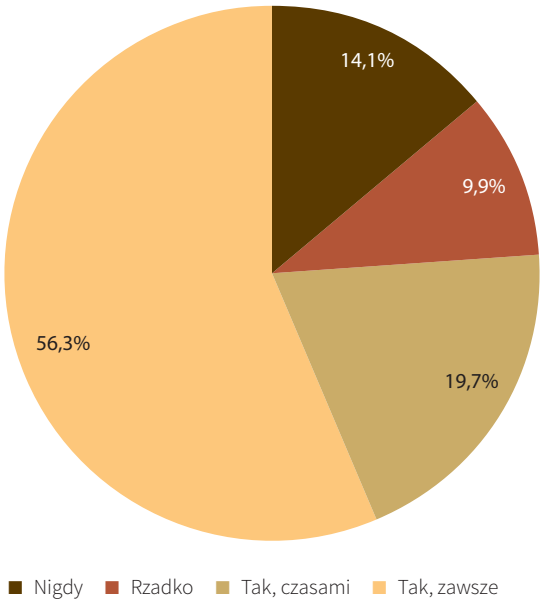


Wykres 7. Częstotliwość sprawdzania przez badanych zabezpieczenia strony internetowej przed dokonaniem transakcji online (np. poprzez protokół HTTPS)
Źródło: Badanie własne

Jak wskazano na wykresie 7, niecałe 60% ankietowanych deklaruje, że często (29,6%) lub zawsze (29,6%) weryfikuje bezpieczeństwo witryny przed zakupami online. Równocześnie jednak prawie 10% badanych stwierdziło, że nie ma wiedzy na temat takich zabezpieczeń, co w połączeniu z poprzednim pytaniem, gdzie brak wiedzy zgłosiło około 2% respondentów, wskazywać może na rozbieżności w poziomie świadomości respondentów.

Z odpowiedzi wynika, iż co piąty badany użytkownik jest stale narażony na ryzyko wycieku danych wrażliwych ujawnianych podczas realizacji transakcji, gdyż nie sprawdza bezpieczeństwa witryny (11,3%) lub nie wie, jak to zrobić (9,9%). Dodatkowo prawie 20% użytkowników zadeklarowało, iż robi to jedynie rzadko. Wyniki te ponownie wskazują na potrzebę dalszego wzmacniania kompetencji cyfrowych użytkowników polskiej bankowości online.

Ostatnie pytanie z zakresu bezpiecznych praktyk dotyczyło zabezpieczenia urządzenia wykorzystywanego do logowania się do bankowości internetowej/mobilnej poprzez zainstalowanie oprogramowania antywirusowego lub użycie innych znanych narzędzi zabezpieczających (np. wirtualnej sieci prywatnej VPN, tworzącej szyfrowane połączenie między urządzeniem a siecią internetową) (wykres 8).



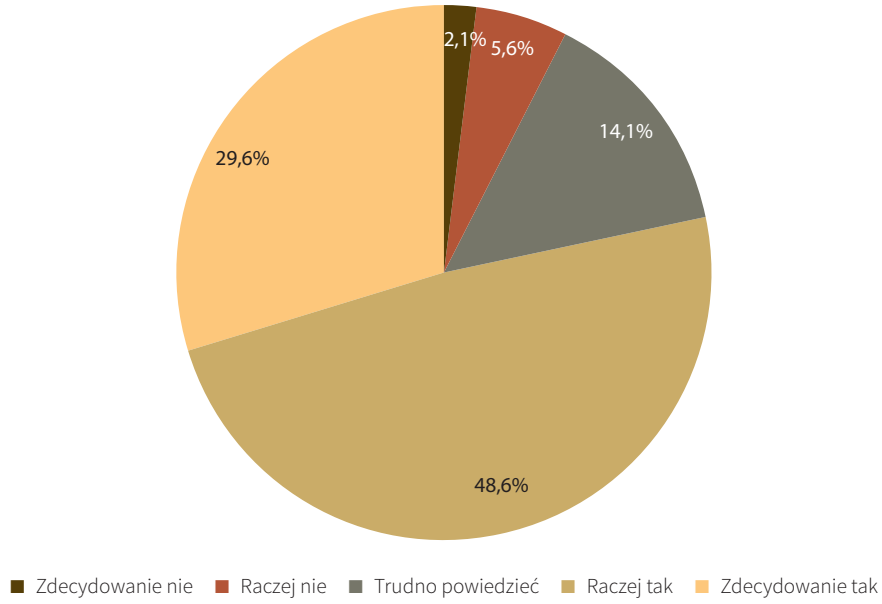
Wykres 8. Częstotliwość korzystania przez badanych z oprogramowania antywirusowego lub innych narzędzi zabezpieczających urządzenie, z którego logują się do bankowości internetowej/mobilnej
Źródło: Badanie własne

Wyniki badania w tej kategorii wydają się stosunkowo optymistyczne — ponad połowa respondentów deklaruje stałe korzystanie z tego typu zabezpieczeń, a kolejne 19,7% przyznaje, że korzysta z takich narzędzi czasami. Niestety, wciąż niemal co czwarty badany należy do grupy wysokiego ryzyka, która z takich narzędzi korzysta rzadko (9,9%) lub nigdy (14,1%). W konsekwencji, choć również w tym przypadku większość badanych użytkowników zdaje sobie sprawę z wagi ochrony swoich danych finansowych i osobowych podczas korzystania z cyfrowych usług sektora bankowego, istotna część ankietowanych wciąż narażona jest na wysokie ryzyko padnięcia ofiarą oszustwa ze strony cyberprzestępców.

Omówione wyniki dotyczące stosowania dobrych praktyk zwiększających bezpieczeństwo korzystania z bankowości online ujawniły dość znaczące luki w edukacji i świadomości badanych na temat zagrożeń związanych z bezpieczeństwem cyfrowym oraz metod ich minimalizowania. W świetle powyższego nieodzowne

wydaje się zbadanie oceny poziomu informacji przekazywanych w tym przedmiocie swoim klientom przez instytucje bankowe.

Wyniki przedstawione na wykresie 9 mogą wydawać się zaskakujące — jedynie niecałe 8% respondentów stwierdziło, że poziom ten jest zdecydowanie (2,1%) lub raczej (5,6%) niewystarczający. Spośród tej grupy ponad 80% nigdy nie zmieniło hasła do konta bankowego lub zmienia je rzadziej niż co 6 miesięcy, a 55% nigdy nie sprawdza bezpieczeństwa witryny lub robi to rzadko. Co jednak ciekawe, akurat ta część ankietowanych ani razu nie zadeklarowała braku wiedzy dotyczącej stosowanych metod zabezpieczeń — paradoksalnie aż 93% respondentów przyznających, że nie wie, jak sprawdzić zabezpieczenie strony internetowej przed dokonaniem transakcji online, równocześnie ocenia pozytywnie poziom informacji dostarczanych im przez bank.

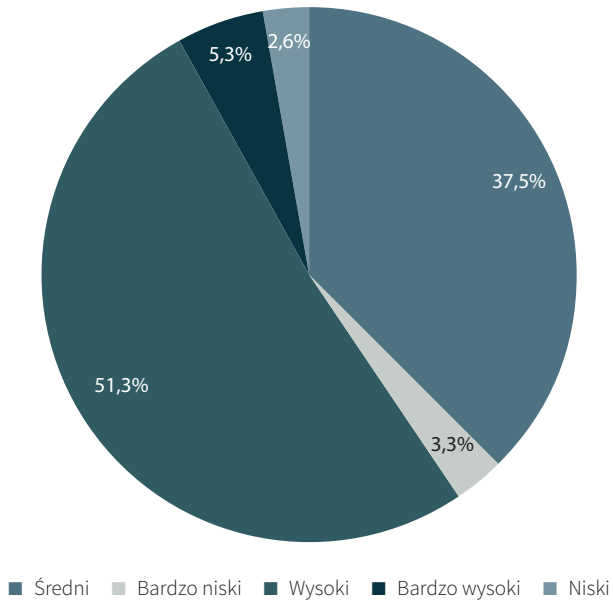


Wykres 9. Ocena wystarczalności poziomu informowania klientów przez instytucje bankowe o zagrożeniach związanych z cyberbezpieczeństwem oraz o metodach zabezpieczania się przed tego rodzaju zagrożeniami
Źródło: Badanie własne

Wskazane wyniki ponownie świadczą o wysokim poziomie zaufania społeczeństwa do instytucji bankowych i całego sektora bankowego. Wydaje się, że właśnie dzięki temu respondenci mogą wydawać się dostatecznie poinformowani, choć w rzeczywistości nie dysponują adekwatnym poziomem wiedzy w kwestii cyberbezpieczeństwa. Nie można jednak wykluczyć, że tak wysoka ocena poziomu

informacji związana może być również z brakiem świadomości klientów, jakiego zakresu informacji brakuje im w celu maksymalizacji swojego bezpieczeństwa. Wskazałoby to na potrzebę przeprowadzania działań edukacyjnych w sposób nie tylko jasny i zrozumiały dla przeciętnego odbiorcy, ale i w sposób kompleksowy, tak aby podnoszenie poziomu wiedzy miało charakter realny.

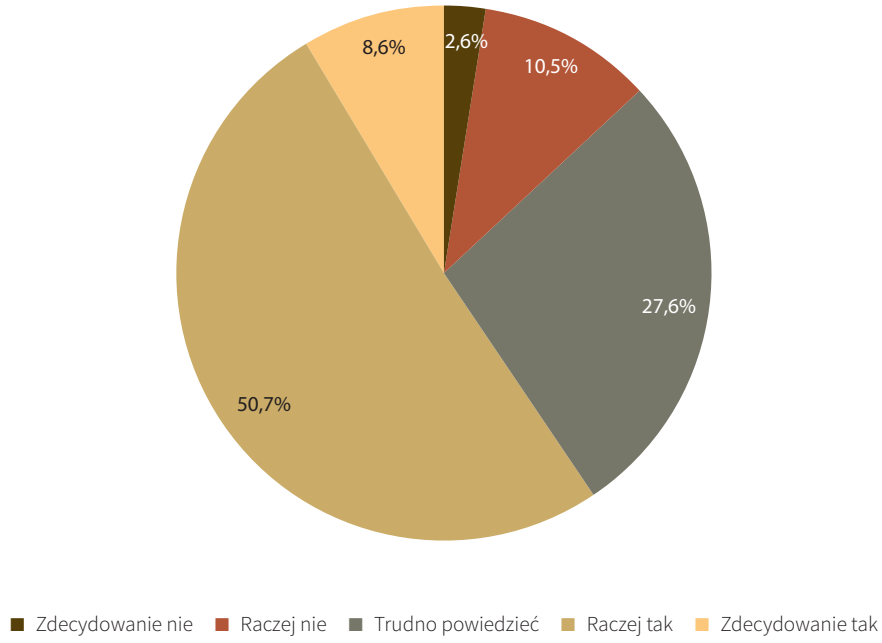
Postrzeganie poziomu i jakości komunikacji w zakresie cyberbezpieczeństwa stanowi jedynie jeden z potencjalnych filarów poczucia bezpieczeństwa użytkowników usług bankowych. Równie ważne wydaje się zbadanie tego, jak klienci oceniają ogólny poziom zabezpieczeń stosowanych przez banki w zakresie wykrywania i zwalczania nadużyć finansowych dokonywanych zarówno ze strony klientów banku, jak i osób trzecich. Odpowiedzi zobrazowane na wykresie 10 wskazują, iż ponad 56% respondentów pozytywnie oceniło poziom zabezpieczeń, a jedynie 6% ankietowanych zadeklarowało ocenę negatywną. Zaskakujące wydaje się natomiast grono osób oceniających zabezpieczenia jako średnie, które stanowi aż 37,5% spośród badanych.



Wykres 10. Ocena poziomu zabezpieczeń stosowanych przez polskie banki w ramach zwalczania prób nadużyć i oszustw ze strony klientów banku oraz osób trzecich
Źródło: Badanie własne

Podobną ostrożność ankietowani wykazali, odpowiadając na pytanie o ocenę ochrony danych finansowych oraz danych osobowych przetwarzanych przez bank, gdzie niecałe 28% wybrało opcję „trudno powiedzieć", co ukazane zostało

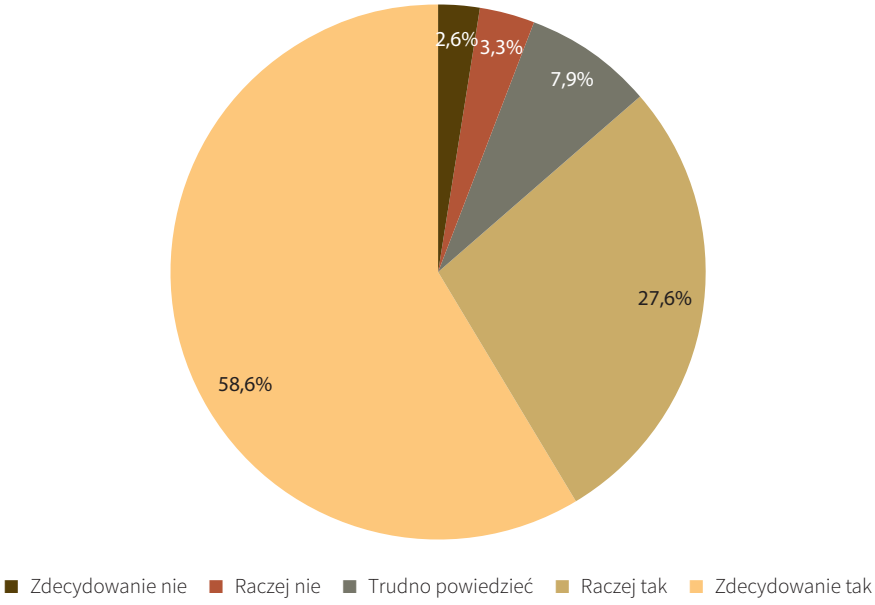
na wykresie 11. W tym przypadku niecałe 60% ankietowanych pozytywnie oceniło poziom ochrony swoich danych, a nieco ponad 13% zadeklarowało ocenę negatywną.



Wykres 11. Ocena wystarczalności poziomu ochrony danych osobowych i finansowych w instytucjach bankowych według respondentów
Źródło: Badanie własne

Rozbieżność między pozytywną oceną poziomu informacji przekazywanych przez banki a umiarkowaną oceną samych metod zabezpieczeń i ochrony danych może wynikać z braku wystarczającej wiedzy technicznej, pozwalającej w sposób rzetelny ocenić ich skuteczność. Wydaje się, że ankietowani wykazali się pewnego rodzaju ostrożnością wobec nowoczesnych technologii, jak również wobec rosnącej świadomości na temat zagrożeń, z którymi wiąże się cyberprzestrzeń. Tezę tę wydają się potwierdzać odpowiedzi ankietowanych na pytanie o potencjalne zwiększenie ryzyka cyberprzestępczości w sektorze bankowym, w kontekście rozwoju technologii cyfrowych, które przedstawiono na wykresie 12.

Aż 58,6% badanych uważa, że rozwój technologii zdecydowanie zwiększa, a kolejne 27,6% deklaruje, że raczej zwiększa omawiane ryzyko. Wyniki te odzwierciedlają powszechne obawy badanych przed dynamicznie zmieniającym się środowiskiem cyfrowym, które jednak, jak wcześniej wskazano, nie zawsze przekładają się na stosowanie najwyższych praktyk zwiększających bezpieczeństwo użytkowników.



Wykres 12. Opinie respondentów na temat wpływu rozwoju technologii cyfrowych na zwiększenie ryzyka cyberprzestępczości w bankowości
Źródło: Badanie własne

Wnioski płynące z niniejszych badań znajdują częściowe potwierdzenie w opublikowanym w październiku 2025 roku ogólnopolskim raporcie wykonanym przez SW Research na zlecenie Warszawskiego Instytutu Bankowości i Związku Banków Polskich (Postawy Polaków wobec cyberbezpieczeństwa, 2025). Przede wszystkim niniejsze badania wykazały paradoks polegający na tym, iż doświadczenie próby oszustwa nie wpływa negatywnie na poczucie bezpieczeństwa respondentów. Wniosek ten znajduje potwierdzenie w danych ogólnokrajowych: mimo iż co piąty badany (21%) przyznał, że padł ofiarą phishingu, a 22% miało do czynienia ze zhakowaniem konta w social mediach, ogólny poziom poczucia bezpieczeństwa Polaków w sieci wzrósł w ciągu roku o 7 punktów procentowych i w 2025 roku wyniósł 62%. Potwierdzenie może również znaleźć postawiona na gruncie niniejszej pracy teza o kluczowej roli zaufania do instytucji bankowych — w raporcie banki zostały wskazane przez respondentów jako bezapelacyjni liderzy cyberbezpieczeństwa (40% wskazań), znacznie wyprzedzając inne podmioty, w tym policję (25%) oraz firmy technologiczne (24%). Przytoczony raport podkreślił istnienie luk w wiedzy i brak konsekwencji użytkowników w stosowaniu zabezpieczeń — przykładowo, jedynie 31% respondentów zadeklarowało weryfikowanie tożsamości dzwoniącego pracownika banku, a blisko połowa (49%) ocenia swoją wiedzę o cyberbezpieczeństwie jedynie jako orientacyjną. Omawiany raport prezentuje jednak nieco bardziej

optymistyczny obraz świadomości klientów banków, wprost wskazując na trend wzrostowy — odsetek osób oceniających wiedzę jako bardzo dobrą w 2025 roku wzrósł do 30%. Autorzy raportu sugerują, iż to właśnie rosnąca wiedza o tym, jak się bronić, przekłada się na wyższe poczucie bezpieczeństwa. Wnioski płynące z niniejszego artykułu są w tym aspekcie nieco bardziej krytyczne i sugerują, że wysokie poczucie bezpieczeństwa respondentów wynika raczej z „przeniesienia odpowiedzialności" i nadmiernego zaufania do zabezpieczeń bankowych, a nie z ich rzeczywistych kompetencji, które w praktyce bywają niewystarczające.

Wyniki niniejszych badań wydają się jednak wpisywać w szerszy obraz kondycji cyberbezpieczeństwa w Polsce w 2025 roku, potwierdzając, że to czynnik ludzki, a nie technologiczny, pozostaje najsłabszym ogniwem w systemie ochrony bankowości elektronicznej. Luki w wiedzy oraz obawy przed zwiększeniem ryzyka cyberprzestępczości jednoznacznie podkreślają potrzebę kontynuacji, a nawet wzmocnienia działań edukacyjnych oraz transparentnej komunikacji instytucji bankowych z klientami, aby ukształtować ich cyfrowe kompetencje i wykorzystać wszelkie możliwe sposoby skutecznego oporu przeciwko stale rozwijającemu się światu cyberprzestępczości. Technologia bowiem powinna przede wszystkim wspierać użytkowników, budując poczucie bezpieczeństwa i kontroli, nie zaś wzbudzać lęk czy niepewność wobec potencjalnych zagrożeń — do tego jednak potrzebne jest ukształtowanie świadomej, aktywnej postawy wobec wszelkich zagrożeń, opartej na wiedzy i umiejętności bezpiecznego korzystania z przestrzeni cyfrowej.

5. Podsumowanie

Z analizy przeprowadzonej w niniejszym artykule wynikają następujące wnioski:

- oszustwa popełniane na szkodę osób fizycznych charakteryzują się nawiązaniem bezpośredniej relacji z osobą pokrzywdzoną i wykorzystaniem technik manipulacji i wywierania wpływu, co sprawia, że skuteczna obrona przed nimi wymaga od ofiary podstawowej wiedzy o mechanizmach działania cyberprzestępców;
- duża część nadużyć cyfrowych mogła zostać udaremniona, gdyby ich ofiary w porę dostrzegły niepokojące sygnały i wykazały się odpowiednią reakcją na ich wystąpienie — nawet najbardziej zaawansowane zabezpieczenia bankowe mogą okazać się nieskuteczne w starciu z socjotechnikami, którymi posługują się przestępcy;
- najczęściej spotykanymi rodzajami cybernetycznych zagrożeń, z którymi mierzą się polscy użytkownicy, są fałszywe okazje inwestycyjne, oszustwa

ankietowe, kurierskie i pocztowe, podszywanie się pod instytucje bankowe oraz złośliwe oprogramowanie;

- niemal 94% badanych korzysta z bankowości internetowej lub mobilnej, co uwypukla potrzebę kładzenia szczególnego nacisku na ten kanał komunikacji i wymusza jego uwzględnienie w ramach projektowania strategii bezpieczeństwa;
- przeprowadzone badanie nie pozwoliło jednoznacznie potwierdzić postawionych hipotez. W przypadku pierwszej z nich, zakładającej negatywny wpływ doświadczenia próby oszustwa na poczucie bezpieczeństwa, wyniki okazały się przeciwne — mimo tego, że niemal połowa ankietowanych zetknęła się z próbą oszustwa cybernetycznego, najczęściej w formie różnych postaci phishingu, paradoksalnie nie wpłynęło to negatywnie na ich poczucie bezpieczeństwa, co może być związane z nieskutecznością próby oszustwa, jak również z ogólnym wysokim zaufaniem do instytucji bankowych. Druga hipoteza, dotycząca wpływu stosowania praktyk bezpieczeństwa na ocenę poziomu zabezpieczeń, również nie znalazła pełnego potwierdzenia — przeprowadzone badanie wykazało poważne luki w wiedzy badanych na temat stosowania podstawowych metod zabezpieczeń, pozwalających na minimalizowanie ryzyka cybernetycznego, jak również brak konsekwencji i regularności w ich praktycznym stosowaniu; równocześnie ocena poziomu informacji dostarczanych przez bank oraz ocena stosowanych przez niego zabezpieczeń pozostaje niezwykle wysoka; sugeruje to, iż poziom wiedzy klientów nie odgrywa decydującej roli w kształtowaniu poczucia bezpieczeństwa — może być to związane z tym, iż respondenci nie odczuwają potrzeby stosowania dodatkowych zabezpieczeń, uznając rozwiązania zapewniane przez bank za wystarczające, bądź też nie są świadomi istnienia dodatkowych metod ochrony, które mogliby samodzielnie stosować;
- zdecydowana większość badanych obawia się zwiększenia ryzyka cyberprzestępczości w kontekście rozwoju technologii cyfrowych, co wskazuje na potrzebę intensyfikacji działań edukacyjnych oraz transparentnej komunikacji z klientami w celu ukształtowania ich cyfrowych kompetencji oraz zwiększenia zarówno obiektywnego, jak i subiektywnego poczucia bezpieczeństwa.

Z uwagi na ograniczoną liczebność próby przedstawione badania należy traktować jako wstępne, mające na celu przede wszystkim zasygnalizowanie problemu bezpieczeństwa cyfrowego w dobie rosnących zagrożeń ze strony cyberprzestępców; ich wyniki mogą stanowić punkt wyjścia do dalszych, pogłębionych analiz,

pozwalających lepiej zrozumieć relację między świadomością zagrożeń a zaufaniem do sektora bankowego.

Bibliografia

Biometria w bankowości elektronicznej — rynek, technologia, klient. (2022). Program Analityczno-Badawczy przy Fundacji WIB. https://pabwib.pl/produkt/biometria-w-bankowosci-elektronicznej-rynek-technologia-klient/

Ciszewska, N. (2016). Przestępstwa gospodarcze — istota i rodzaje. *Studia nad bezpieczeństwem, 1*, 169–170.

Fabisiak, I., Michnik, M. (2016). Wykroczenia jako jeden z obszarów nadużyć w przedsiębiorstwie. W: M. Wójcik-Jurkiewicz (red.), *Ryzyko nadużyć w rachunkowości i finansach* (wyd. 1, s. 107–108). Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.

Gratkowska, A. (2024, 5 czerwca). *Sztuczna inteligencja w bankowości, czyli jak AI rewolucjonizuje proces zwalczania oszustw bankowych*. Altkomsoftware. https://www.altkomsoftware.com/pl/blog/sztuczna-inteligencja-w-bankowosci-a-oszustwa-bankowe/

Haertle, A. (2015, 8 czerwca). *Poważne włamanie do polskiego banku, skradzione dane i hasła klientów*. Zaufana trzecia strona. https://zaufanatrzeciastrona.pl/post/powazne-wlamanie-do-polskiego-banku-skradzione-dane-i-hasla-klientow/

Jasiński, W. (2013). *Nadużycia w przedsiębiorstwie — przeciwdziałanie i wykrywanie* (wyd. 1). Wydawnictwo Poltext.

Kisiel, M. (2024, 24 maja). *Blokada PESEL rusza lada moment. Nie zdziw się w banku, jeśli zastrzegłeś numer*. Bankier. https://www.bankier.pl/wiadomosc/Zastrzezony-PESEL-w-banku-kredyty-konta-limity-wyplaty-gotowki-8751648.html

Król, P. (2024). Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej. *Bezpieczny bank, 1*(94), 26.

Kubisa-Ślipko, A. (2000). *Słownik języka polskiego* (wyd. 1). Wydawnictwo Językowe Aneks.

Kutera, M. (2010). Ryzyko nadużyć finansowych w warunkach kryzysu gospodarczego. W: P. Urbanek (red.), *Nadzór korporacyjny w warunkach kryzysu gospodarczego* (wyd. 1, s. 116). Wydawnictwo Uniwersytetu Łódzkiego.

Majka, D. (2024, 9 stycznia). *Wewnątrzsektorowa wymiana informacji i edukacja klientów to najskuteczniejsze działania antyfraudowe*. Vsoft. https://www.vsoft.pl/blog/wewnatrzsektorowa-wymiana-informacji-i-edukacja-klientow-to-najskuteczniejsze-dzialania-antyfraudowe/

Postawy Polaków wobec cyberbezpieczeństwa. (2025). *SW Research na zlecenie Warszawskiego Instytutu Bankowości i Związku Banków Polskich*. https://bs.net.pl/wp-content/uploads/2025/10/Raport-z-badania-Postawy-Polakow-wobec-cyberbezpieczenstwa-2025.pdf

Rajewski, K. (2020). 2.4.1. Nadużycia finansowe. W: B. Jagura, B. Makowicz (red.), *Systemy zarządzania zgodnością. Compliance w praktyce*. Wolters Kluwer Polska.

Ransomware w Banku Spółdzielczym w Zambrowie. (2024, 22 stycznia). Krajowy Instytut Cyberbezpieczeństwa. https://kicb.pl/ransomware-w-banku-spoldzielczym-w-zambrowie/

Raport 2024: Bezpieczeństwo cyfrowe Polaków. (2024). SMSAPI. https://www.smsapi.pl/raport2024-bezpieczenstwo

Raport Roczny CSIRT KNF 2024. (2024). KNF. https://www.knf.gov.pl/?articleId=93227&p_id=18

Wieprow, J. (2022, 26 maja). *Wystarczy jedno spojrzenie, czyli o bankowości biometrycznej*. Merito. https://www.merito.pl/blog/wystarczy-jedno-spojrzenie-czyli-o-bankowosci-biometrycznej

Zawłocki, R., Gałęski, M. (2024). Komentarz do art. 296 k.k. W: M. Królikowski, R. Zawłocki (red.), *Kodeks karny. Część szczególna. Tom III. Komentarz do artykułów 222–316* (wyd. 5). C.H. Beck.

Cyberthreats and Sense of Security and Awareness Level Among Bank Customers in Poland, in Light of Own Research

Abstract. This article aims to analyze cyber threats in the Polish banking sector in the context of the growing importance of digital banking and the resulting risk of fraud. The study was conducted using an anonymous survey completed by 152 participants. It focused on assessing the sense of security among bank customers in Poland and their level of knowledge regarding fraud prevention measures. The results indicate a very high sense of security, even though nearly half of them have experienced attempted fraud. The study also revealed a strong level of trust in the banking sector, despite respondents' limited knowledge of cybersecurity. The findings underscore the need for intensified educational efforts from the banking sector and transparent communication aimed at enhancing user security.

Keywords: cybersecurity, financial fraud, banking frauds