ZESZYTY NAUKOWE
WYŻSZEJ SZKOŁY BANKOWEJ W POZNANIU
2024, T. 105, NR 2

MAJA LOTKO
Uniwersytet WSB Merito w Poznaniu
Wydział Zamiejscowy w Chorzowie
https://orcid.org/0009-0007-4223-0495
e-mail: majusslot@gmail.com

Bezpieczeństwo płatności w erze cyfrowej

Streszczenie. Artykuł dotyczy bezpieczeństwa płatności internetowych w erze cyfrowej. Celem przedstawionego badania było zidentyfikowanie czynników wpływających na poczucie bezpieczeństwa użytkowników oraz ich obaw związanych z płatnościami elektronicznymi. Analiza zagadnienia opiera się na danych zebranych za pośrednictwem ankiety przeprowadzonej wśród 103 studentów Uniwersytetu WSB Merito. Okazuje się, że większość respondentów regularnie korzysta z płatności internetowych, a ich główną obawą są nieuprawnione obciążenia wynikające z kradzieży danych dostępowych do kont bankowych. Zdaniem respondentów kluczową rolę w ochronie transakcji odgrywają zaawansowane środki bezpieczeństwa, takie jak dwuetapowa weryfikacja. Wyniki badania sugerują, że poprzez edukację na temat standardów bezpieczeństwa bankowego oraz dzięki regularnej zmianie haseł można zwiększyć zaufanie użytkowników do płatności cyfrowych oraz poziom bezpieczeństwa transakcji.

Słowa kluczowe: cyberbezpieczeństwo, płatności online, kradzież danych, środki bezpieczeństwa, zaufanie użytkowników

https://doi.org/10.58683/dnswsb.1999

1. Wstęp

W czasie dynamicznego rozwoju technologii cyfrowych codzienne czynności, takie jak dokonywanie płatności, uległy znaczącej transformacji. Przechodzimy do świata online, co sprawia, że coraz większa liczba ludzi reguluje swoje zobowiązania drogą elektroniczną. Korzyści wynikające z tego przejścia są liczne — od wygody i szybkości po dostępność usług z dowolnego miejsca na świecie. Niemniej jednak wraz z tymi korzyściami pojawia się szereg zagrożeń, związanych głównie z bezpieczeństwem transakcji i ochroną danych osobowych użytkowników. Postępująca digitalizacja i rosnąca popularność płatności cyfrowych, takich jak płatności mobilne, wyznaczają nowy kierunek w gospodarce światowej. Te innowacje rewolucjonizują sposób, w jaki dokonujemy transakcji, eliminując tradycyjne bariery i otwierając nowe możliwości. Jednak wzrost liczby oszustw

internetowych oraz ataków cybernetycznych stawia przed użytkownikami i instytucjami finansowymi nowe wyzwania w zakresie ochrony danych i środków finansowych.

Zrozumienie i analiza tych zagrożeń oraz sposobów ich minimalizacji są istotne dla budowania zaufania do nowoczesnych metod płatności. Wraz z tym rośnie także znaczenie regulacji i standardów bezpieczeństwa w sektorze finansowym, które wymagają ciągłej analizy ich skuteczności oraz wpływu na użytkowników.

Problem cyberbezpieczeństwa w bankowości online jest licznie opisywany w publikacjach. Poruszają ten temat między innymi: I. Dąbrowska-Antoniak (2019), K. Dmowska (2022), R. Pitera (2017), M. Czyżak (2016). Cele teoretyczne artykułu koncentrują się na identyfikacji, charakterystyce oraz redukcji zagrożeń wynikających z korzystania z nowoczesnych metod płatności. Celem praktycznym artykułu jest wyznaczona hipoteza: „Im większe doświadczenie w płatnościach online, tym większe poczucie bezpieczeństwa". Wpisując się w ten nurt, podjęty zostanie problem związany z cyberbezpieczeństwem w bankowości online.

2. Podstawowe aspekty cyberbezpieczeństwa w bankowości

Postęp technologii finansowych umożliwia szybkie i wygodne transakcje, ale jednocześnie zwiększa złożoność zagrożeń ze strony oszustów. Banki, które przetwarzają dane finansowe, są coraz bardziej narażone na zaawansowane ataki cybernetyczne. Analiza oszustw w sektorze bankowym koncentruje się na transakcjach bezgotówkowych. Rzecznik Finansowy codziennie otrzymuje co najmniej jeden wniosek o interwencję w sprawie nieautoryzowanych transakcji płatniczych, które można podzielić na trzy kategorie: rachunki bankowe, karty debetowe i karty kredytowe.

Cyberbezpieczeństwo obejmuje praktyki, technologie, procesy i środki służące ochronie systemów komputerowych, sieci, danych i infrastruktury przed atakami, nieautoryzowanym dostępem, uszkodzeniami i kradzieżą (Chałubińska-Jentkiewicz, 2019). Zagrożenia cybernetyczne to potencjalne niebezpieczeństwa i ataki w cyberprzestrzeni, takie jak wirusy, złośliwe oprogramowania i ataki hakerskie (Grzelak, Liedel, 2022; Raport Cyfrowa Polska, 2019; Wodo, Stygar Winiarska, 2019).

Narodowy Bank Polski (NBP) stosuje ogólne kryteria w nadzorze systemowym, koncentrując się na sprawności, bezpieczeństwie i zgodności z prawem. W ramach kryterium bezpieczeństwa ocenia się cyberbezpieczeństwo. Zgodnie z definicją z Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku: „Cyberbezpieczeństwo to zdolność systemów informacyjnych do odporno-

ści na działania naruszające poufność, integralność, dostępność i autentyczność danych oraz związanych z nimi usług. Oznacza to, że systemy te są zdolne do skutecznego przeciwdziałania zagrożeniom, zapewniając jednocześnie ochronę danych" (Ustawa, 2018).

Banki są atrakcyjnym celem dla cyberprzestępców ze względu na potencjalne zyski finansowe. Główne powody to: dostęp do wartościowych danych finansowych, pieniądze elektroniczne oraz wpływ na gospodarkę.

Wraz z rozwojem bankowości internetowej rośnie liczba ataków na użytkowników, a nowe metody wyłudzania środków ciągle się pojawiają. Najczęstsze ataki obejmują: nieautoryzowany dostęp do systemów bankowych w celu oszustw lub kradzieży danych, podszywanie się pod oficjalne strony firm w celu pozyskiwania haseł, loginów i kodów, ataki typu ransomware, malware, phishing i spear phishing, wysyłanie złośliwych plików przez e-mail, wirusy w aplikacjach mobilnych i przeglądarkach internetowych w celu uzyskania danych do logowania oraz ataki hybrydowe łączące różne techniki.

3. Rodzaje cyberzagrożeń w sektorze bankowym

W ciągu ostatnich dekad sektor bankowy przeszedł znaczną transformację, dostosowując się do rosnących zagrożeń cybernetycznych i postępu technologii informatycznych. Początkowo zagrożenia koncentrowały się na wirusach komputerowych i złośliwym oprogramowaniu, mającym na celu kradzież danych. Obecnie ataki stały się bardziej zaawansowane i złożone, z wykorzystaniem różnych technik do zdobywania informacji o klientach i przenikania do systemów bankowych. Takie zagrożenia stwarzają poważne konsekwencje ekonomiczne, reputacyjne i społeczne dla sektora bankowego.

Jedną z metod ataków w sektorze bankowym są ataki na systemy informatyczne banków, a ich celem jest uzyskanie dostępu do środków finansowych lub przechwycenie poufnych informacji. Polskie banki regularnie inwestują znaczne środki w cyberbezpieczeństwo, aby zapewnić kompleksową ochronę swoim klientom.

Inny sposób ataku stosowany przez hakerów koncentruje się na użytkownikach usług bankowych. Przestępcy fałszują strony internetowe, aby uzyskać poufne informacje od klientów, którzy mogą nie zauważyć, że odwiedzają fałszywą stronę internetową zamiast oryginalnej strony banku. Klienci, wpisując swoje dane do logowania i hasła na sfałszowanej stronie, nieumyślnie przekazują je przestępcom, co często prowadzi do nieuprawnionego dostępu do ich kont bankowych. Dodatkowo, podczas przeprowadzania operacji na fałszywej stronie

klienci mogą nieświadomie używać kodów SMS do autoryzacji operacji, które są w rzeczywistości próbą wyłudzenia pieniędzy. Najczęściej ofiarami takich ataków są osoby prywatne.

Phishing to metoda oszustwa internetowego, w której przestępcy podszywają się pod zaufane strony internetowe lub instytucje, aby wyłudzić poufne dane od użytkowników, takie jak hasła, numery kart kredytowych czy informacje logowania. Ataki phishingowe opierają się na socjotechnice, wykorzystując psychologię i manipulację emocjonalną, by skłonić ofiary do niebezpiecznych działań. Cyberprzestępcy mogą udawać firmy kurierskie, urzędy, operatorów telekomunikacyjnych lub znajomych, aby zdobyć dane do kont bankowych, społecznościowych czy systemów biznesowych (Narodowe Standardy Cyberbezpieczeństwa, b.d.; Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, b.d.).

Kolejną z metod ataków w sektorze bankowym jest malware, czyli złośliwe oprogramowanie stworzone w celu wyrządzania szkód lub uzyskania nieautoryzowanego dostępu do systemów komputerowych. Ataki z użyciem malware mogą prowadzić do kradzieży danych logowania, numerów kart kredytowych, numerów kont bankowych i innych poufnych informacji, a także do wyłudzenia środków finansowych lub zdobycia informacji umożliwiających dostęp do kont bankowych. Złośliwe oprogramowanie może również umożliwiać zdalną kontrolę nad komputerem ofiary.

4. Formalnoprawne regulacje cyberbezpieczeństwa w sektorze bankowym

CSIRT KNF (Computer Security Incident Response Team Komisji Nadzoru Finansowego) to zespół reagowania na incydenty bezpieczeństwa komputerowego, działający przy Komisji Nadzoru Finansowego (KNF). Jego głównym zadaniem jest ochrona polskiego sektora finansowego przed zagrożeniami cybernetycznymi. Zespół CSIRT KNF nieustannie śledzi i analizuje nowe trendy oraz zagrożenia w dziedzinie cyberbezpieczeństwa, które są skierowane do klientów rynku finansowego. Zgromadzona wiedza jest wykorzystywana do działań mających na celu zmniejszenie ryzyka oraz do edukacji — zwiększania świadomości klientów bankowości elektronicznej w zakresie cyberbezpieczeństwa. Prowadzone są analizy, aby wcześniej wykrywać oszukańcze strony i ograniczać dostęp do nich. W przypadku wykrycia podszywania się pod instytucje finansowe podejmowane są działania mające na celu usunięcie fałszywej strony lub ograniczenie do niej

dostępu. W 2023 roku zespół CSIRT KNF zidentyfikował i zgłosił do zablokowania 30140 fałszywych domen.

Należy zwrócić uwagę na działania KNF w kontekście bezpieczeństwa systemów teleinformatycznych używanych w sektorze bankowym. Zgodnie z przepisami Ustawy z dnia 29 sierpnia 1997 roku Prawo bankowe (Ustawa, 1997) KNF posiada uprawnienie do wydawania rekomendacji dotyczących praktyk ostrożnego i stabilnego zarządzania przez banki. W ramach tych działań rekomendacja KNF skupia się na kwestiach związanych z zarządzaniem technologią informacyjną i bezpieczeństwem środowiska teleinformatycznego w bankach. Szczegółowa rekomendacja nr 16 zawarta w ramach tej inicjatywy odnosi się do obszaru „Zarządzanie elektronicznymi kanałami dostępu". Zgodnie z jej postanowieniami banki świadczące usługi przy użyciu elektronicznych kanałów dostępu są zobowiązane do posiadania skutecznych rozwiązań technicznych i organizacyjnych, które gwarantują weryfikację tożsamości oraz bezpieczeństwo danych i aktywów klientów.

Współpracując w ramach Związku Banków Polskich (ZBP), banki wzmocniły współpracę w zakresie cyberbezpieczeństwa. Oprócz wewnętrznych środków bezpieczeństwa aktywnie wymieniają doświadczenia w obszarach transakcji internetowych, mobilnych i kart płatniczych. Regularnie publikują na swoich stronach internetowych ogłoszenia dotyczące zasad bezpieczeństwa oraz komunikaty reagujące na konkretne zagrożenia. Współpraca między bankami minimalizuje ryzyko ataków cybernetycznych, oszustw finansowych i innych zagrożeń operacyjnych, przyczyniając się do stabilności systemu finansowego. Wymiana informacji o zagrożeniach pozwala na szybkie reagowanie i wprowadzenie środków zaradczych, a w przypadku poważnych zagrożeń umożliwia szybkie opracowanie planów zarządzania kryzysowego.

W sektorze bankowym obowiązują liczne regulacje mające na celu zabezpieczenie danych klientów, utrzymanie stabilności systemu finansowego oraz zapobieganie zagrożeniom cybernetycznym. Jedną z nich jest Rozporządzenie o ochronie danych osobowych (RODO, 2016), które zapewnia większą kontrolę nad danymi osobowymi i zwiększa ochronę prywatności obywateli UE. Dyrektywa o usługach płatniczych (PSD2) (Dyrektywa, 2015) reguluje bezpieczeństwo transakcji online i wspiera innowacje w sektorze płatności, tworząc jednolity rynek płatniczy w UE. Dyrektywa ta wymaga silnego uwierzytelniania, które obejmuje potwierdzenie tożsamości klienta za pomocą dwóch niezależnych elementów uwierzytelniających. Aktualizuje ona przepisy unijne w celu zwiększenia odporności na incydenty cybernetyczne i gotowości państw członkowskich do reagowania na takie incydenty poprzez odpowiednie zespoły.

5. Metodyka badań

Celem badania było zidentyfikowanie czynników wpływających na poczucie bezpieczeństwa użytkowników podczas płatności online, określenie ich głównych obaw związanych z płatnościami elektronicznymi oraz analiza działań podejmowanych przez użytkowników w celu zwiększenia bezpieczeństwa transakcji cyfrowych. Analiza wyników umożliwi lepsze zrozumienie postaw użytkowników wobec płatności online oraz wskazanie kierunku dalszych działań na rzecz poprawy bezpieczeństwa tych transakcji.

Badanie przeprowadzono w 2024 roku, przy użyciu metod ilościowych, wykorzystując technikę ankiety. Wzięło w nim udział 103 respondentów, w tym 74 kobiety oraz 29 mężczyzn. Wszyscy uczestnicy są studentami Uniwersytetu WSB Merito. Największą grupę wiekową wśród respondentów stanowią osoby w wieku 18–25 lat, które reprezentują 61% wszystkich badanych. Następnie 15% uczestników to osoby w wieku 26–35 lat. Kolejną grupę wiekową obejmującą 12% respondentów tworzą osoby w wieku 36–45 lat. Grupa w wieku 46–55 lat to 11% badanych, natomiast osoby powyżej 56. roku życia stanowią 1% respondentów.

6. Wyniki badań i dyskusja

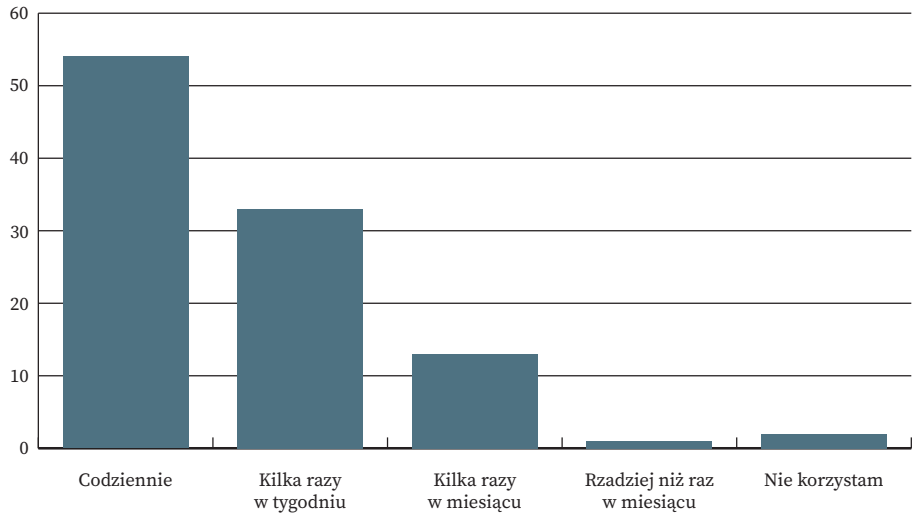
W tej części zawarto odpowiedzi na pytania dotyczące cyberbezpieczeństwa płatności online.

Respondenci zostali zapytani o częstotliwość dokonywania płatności online. Rys. 1 przedstawia ich odpowiedzi.

Rys. 1 przedstawia szczegółową analizę częstotliwości dokonywania płatności online. Analiza danych pokazuje, że większość respondentów (54) codziennie dokonuje płatności online, a 33 kilka razy w tygodniu. Ponadto 13 respondentów korzysta z płatności online kilka razy w miesiącu, 1 osoba rzadziej niż raz w miesiącu, a 2 osoby w ogóle nie korzystają z płatności online.

Kolejne pytanie dotyczyło obaw respondentów związanych z korzystaniem z płatności elektronicznych. W tabeli 1 przedstawiono główne obawy respondentów dotyczące korzystania z płatności elektronicznych.

Najwięcej respondentów, 56 osób, obawia się nieuprawnionych obciążeń wynikających z kradzieży danych finansowych. Kradzież danych osobowych stanowi znaczącą obawę dla 17 respondentów, podobnie jak problemy techniczne, które mogą uniemożliwić dokonanie transakcji. Grupa licząca 4 osoby wyraziła obawy związane z brakiem zaufania do nowoczesnych technologii płatniczych, natomiast 9 osób stwierdziło, że nie posiada żadnych z wymienionych obaw.



Rys. 1. Częstotliwość dokonywania płatności online
Źródło: Opracowanie własne na podstawie wyników badań

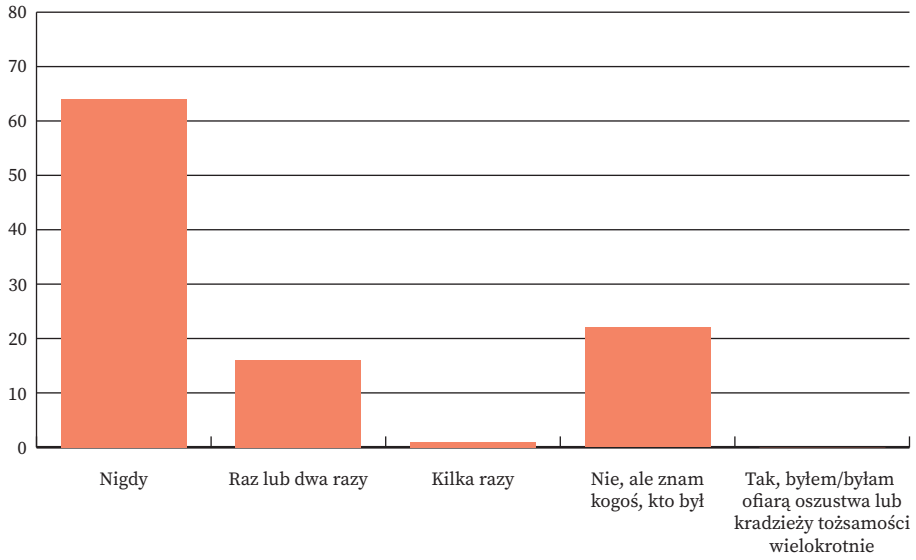
Tabela 1. Obawy związane z korzystaniem z płatności elektronicznych według respondentów

Obawy związane z korzystaniem z płatności elektronicznych	Odsetek respondentów, którzy wyrażają daną obawę
Kradzież danych osobowych	16,5%
Nieuprawnione obciążenia związane z kradzieżą danych finansowych	54%
Problemy techniczne uniemożliwiające dokonanie transakcji	16,5%
Brak zaufania do nowoczesnych technologii płatniczych	4%
Żadna z powyższych	9%

Źródło: Opracowanie własne na podstawie wyników badań

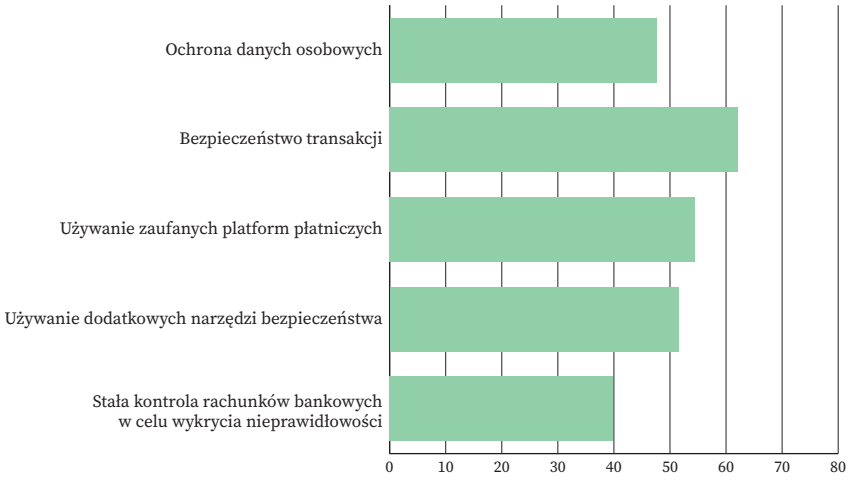
Następne pytanie dotyczyło tego, czy zdarzyło się respondentom być ofiarą oszustwa finansowego lub kradzieży tożsamości w kontekście płatności online. Rys. 2 ilustruje doświadczenia respondentów w tym zakresie.

Zdecydowana większość ankietowanych (64 osoby) nigdy nie miała do czynienia z żadną formą oszustwa finansowego lub kradzieży tożsamości przy płatnościach online. Jednakże 22 respondentów stwierdziło, że choć sami nie byli ofiarami, to znają osoby, które padły ofiarą takich przestępstw. 16 osób przyznało, że doświadczyło oszustwa finansowego lub kradzieży tożsamości raz lub dwa razy, a jedna osoba przyznała, że spotkało ją to kilka razy. Żaden z respondentów nie był ofiarą oszustwa finansowego lub kradzieży tożsamości wielokrotnie.



Rys. 2. Doświadczenie respondentów związane z oszustwami finansowymi lub kradzieżą tożsamości w kontekście płatności online
Źródło: Opracowanie własne na podstawie wyników badań

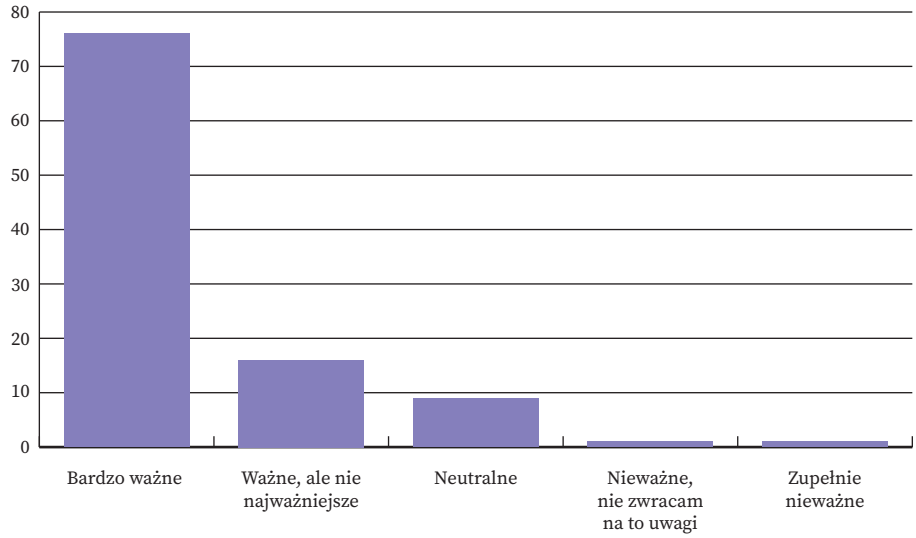
W dobie rosnącej popularności płatności online, bezpieczeństwo transakcji staje się priorytetem dla użytkowników. Respondenci mieli możliwość wskazania wielu czynników, które uważają za najważniejsze dla ochrony swoich finansów i danych osobowych w trakcie dokonywania płatności internetowych.



Rys. 3. Czynniki wpływające na poczucie bezpieczeństwa podczas płatności online według respondentów
Źródło: Opracowanie własne na podstawie wyników badań

Wśród najczęściej wymienianych przez respondentów czynników znalazły się bezpieczeństwo transakcji (64 osoby) oraz korzystanie z zaufanych platform płatniczych (56 osób). Kolejne istotne elementy to ochrona danych osobowych (49 osób) oraz stosowanie dodatkowych narzędzi bezpieczeństwa (53 osoby). Stała kontrola rachunków bankowych w celu wykrycia nieprawidłowości została wskazana przez 41 respondentów. Analiza według płci wykazała, że kobiety najczęściej zaznaczały ochronę danych osobowych, bezpieczeństwo transakcji oraz używanie dodatkowych narzędzi bezpieczeństwa. Natomiast mężczyźni częściej wskazywali na używanie zaufanych platform płatniczych oraz ochronę danych osobowych. Osoby deklarujące codzienne korzystanie z płatności online najczęściej zaznaczały ochronę danych osobowych jako najważniejszy czynnik wpływający na ich poczucie bezpieczeństwa.

Kolejnym aspektem badania było określenie, jak ważne dla respondentów dokonujących płatności online są zaawansowane środki bezpieczeństwa, takie jak dwuetapowa weryfikacja czy biometryczne uwierzytelnianie. Respondenci zostali poproszeni o ocenę znaczenia tych mechanizmów bezpieczeństwa stosowanych przez platformy płatnicze.

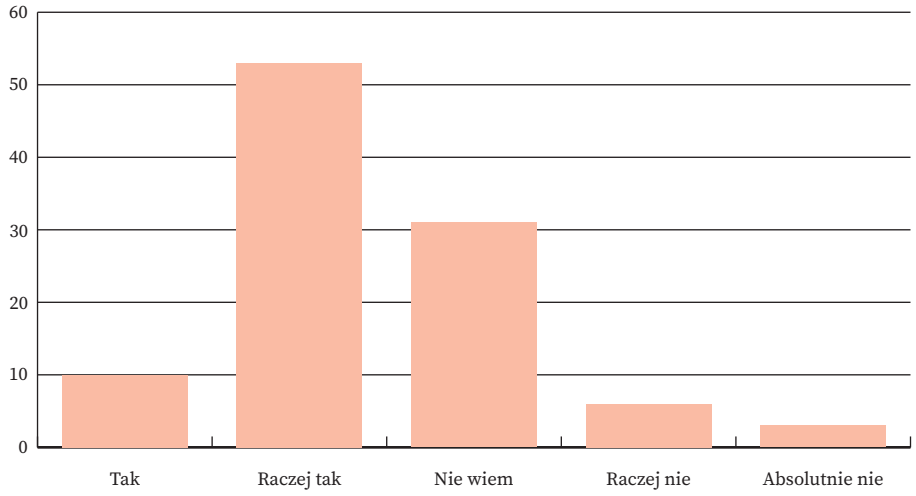


Rys. 4. Znaczenie zaawansowanych środków bezpieczeństwa w płatnościach online według respondentów
Źródło: Opracowanie własne na podstawie wyników badań

Z badania wynika, że zdecydowana większość respondentów (76) uważa, iż zaawansowane środki bezpieczeństwa są bardzo istotne. Mniejsza grupa (16) oceniła je jako ważne, lecz nie najważniejsze. Nieliczna liczba respondentów była neutralna w tej kwestii (9), a dwie osoby uznały, że te środki nie mają dla nich

znaczenia. Analiza według płci nie wykazała istotnych różnic — zarówno kobiety, jak i mężczyźni najczęściej zaznaczali, że jest to bardzo ważne. Podobnie osoby deklarujące codzienne korzystanie z płatności online przeważnie uważały to za bardzo ważny czynnik. Wynik ten wskazuje na powszechne zapotrzebowanie na zaawansowane środki bezpieczeństwa w płatnościach online, które mogą znacząco wpłynąć na poczucie bezpieczeństwa respondentów.

Następne pytanie miało na celu ocenę poziomu zaufania respondentów do obowiązujących regulacji i standardów dotyczących płatności cyfrowych, a także ich wpływu na poczucie bezpieczeństwa transakcji online. Respondenci byli pytani, czy uważają, że obecne regulacje są wystarczające, aby zapewnić bezpieczeństwo transakcji dla użytkowników.



Rys. 5. Ocena regulacji i standardów dotyczących płatności cyfrowych a poczucie bezpieczeństwa transakcji przez respondentów
Źródło: Opracowanie własne na podstawie wyników badań

Z analizy wynika, że większość respondentów (53) uważa, że regulacje i standardy są raczej wystarczające, aby zapewnić bezpieczeństwo transakcji. Mniejsza grupa respondentów (10) odpowiedziała, że tak jest. Natomiast znaczna liczba ankietowanych (31) wskazała, że nie jest pewna, czy obecne regulacje są wystarczające. Niewielka liczba respondentów (łącznie 9) wyraziła negatywne opinie na ten temat, przy czym 6 osób odpowiedziało, że raczej nie są wystarczające, a 3 osoby stwierdziły, że absolutnie nie. Analiza odpowiedzi w podziale na płeć wykazała, że kobiety najczęściej wybierały odpowiedź „raczej tak" (40), ale także często zgłaszały wątpliwości, zaznaczając odpowiedź „nie wiem" (22). Natomiast mężczyźni zdecydowanie częściej skłaniali się ku odpowiedzi „raczej tak". Osoby

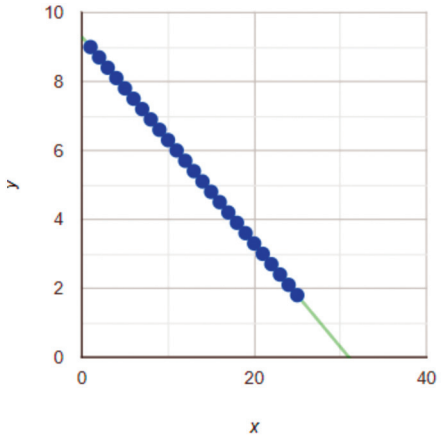
korzystające z płatności online codziennie najczęściej zgłaszały raczej pozytywne opinie, podobnie osoby korzystające z płatności mobilnych kilka razy w miesiącu lub rzadziej. Wynik ten sugeruje, że częstsze korzystanie z płatności online może wpływać na większe zaufanie do obecnych regulacji i standardów w zakresie bezpieczeństwa transakcji.

Aby sprawdzić poprawność stwierdzenia: „Im większe doświadczenie w płatnościach online, tym większe poczucie bezpieczeństwa", została przeprowadzona korelacja Spearmana dwóch zmiennych — pomiędzy częstotliwością dokonywania płatności online a poczuciem bezpieczeństwa przez respondentów.

Po przeliczeniu otrzymujemy wynik korelacji Spearmana:

$$r(x, y) = 0{,}99995$$

Wynik korelacji może wahać się od −1 do 1: wartość bliska 1 wskazuje na silną dodatnią korelację, wartość bliska −1 oznacza silną ujemną korelację, a wartość bliska zeru wskazuje na brak lub bardzo słabą korelację między zmiennymi. Poniższy wykres (rys. 6) przedstawia kształtowanie się tych dwóch zmiennych.

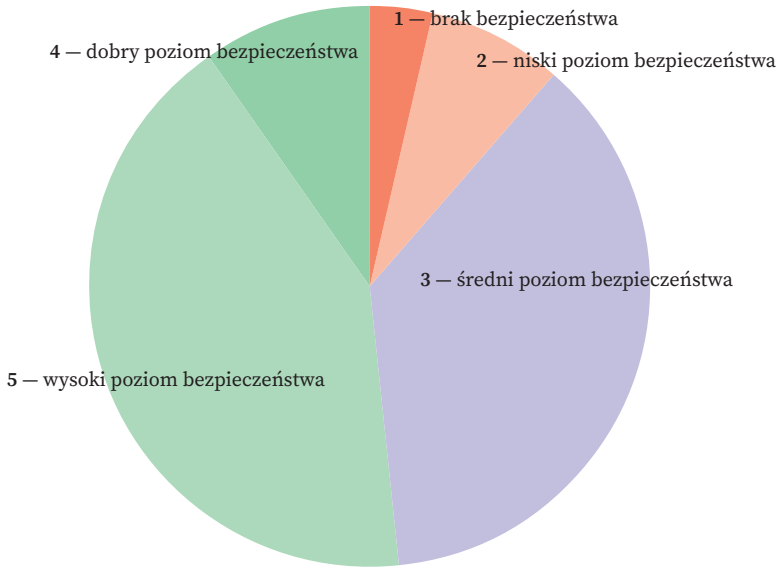


Rys. 6. Wykres prostej regresji dwóch zmiennych — doświadczenie a poczucie bezpieczeństwa w płatnościach online
Źródło: Opracowanie własne na podstawie wyników badań

Wartość korelacji rangowej Spearmana wynosi około 0,99995. Oznacza to, że istnieje silna dodatnia zależność między doświadczeniem w płatnościach online a poczuciem bezpieczeństwa. Zatem stwierdzenie: „Im większe doświadczenie w płatnościach online, tym większe poczucie bezpieczeństwa" jest prawdziwe. Analizując — im większe doświadczenie w płatnościach online, tym większe po-

czucie bezpieczeństwa, a im mniejsze doświadczenie w płatnościach online, tym mniejsze poczucie bezpieczeństwa.

Następne pytanie miało na celu zrozumienie, w jakim stopniu respondenci postrzegają płatności online jako bezpieczne oraz jakie czynniki mogą wpływać na to postrzeganie. Respondenci byli poproszeni o ocenę bezpieczeństwa płatności online na skali od 1 do 5, gdzie 1 oznaczało brak bezpieczeństwa, a 5 oznaczało bardzo wysoki poziom bezpieczeństwa.



Rys. 7. Postrzeganie bezpieczeństwa płatności online przez respondentów
Źródło: Opracowanie własne na podstawie wyników badań

Z analizy wynika, że większość respondentów (43) oceniła płatności online na poziomie 4, co sugeruje, że uważają je za względnie bezpieczne. Kolejna grupa respondentów (38) oceniła bezpieczeństwo na poziomie 3. Natomiast mniejsza liczba respondentów wyraziła skrajne opinie. 10 osób oceniło płatności online na najwyższym poziomie bezpieczeństwa (poziom 5), podczas gdy tylko 4 osoby oceniły je na poziomie 1.

Następne pytanie miało na celu zrozumienie, w jakim stopniu respondenci podejmują działania w celu podniesienia poziomu bezpieczeństwa płatności cyfrowych, poprzez regularną zmianę hasła do swojego konta bankowego w serwisie internetowym lub aplikacji mobilnej.

Tabela 2. Zwyczaje zmiany haseł do kont bankowych w serwisach internetowych i aplikacjach mobilnych respondentów

Częstotliwość zmiany haseł	Odsetek respondentów dokonujących zmian
Co miesiąc lub częściej	5%
Co kilka miesięcy	10%
Raz na pół roku	10%
Raz do roku	13%
Rzadziej niż raz do roku lub nigdy	62%

Źródło: Opracowanie własne na podstawie wyników badań

Z analizy wynika, że większość respondentów (65) rzadziej niż raz do roku lub w ogóle nie zmienia swojego hasła do konta bankowego, jednakże 13 respondentów zmienia hasło raz do roku, a kolejne 10 respondentów co kilka miesięcy. Mniejsza grupa respondentów (5) regularnie zmienia hasło co miesiąc lub częściej. Analiza odpowiedzi według płci pokazała, że kobiety (48 osób) rzadziej niż raz do roku lub w ogóle nie zmieniają hasła do konta bankowego. Natomiast mężczyźni zgłaszali, że rzadziej niż raz do roku lub w ogóle nie zmieniają hasła (17 osób), ale także (6 osób) zmienia hasło co kilka miesięcy. Osoby deklarujące codzienne korzystanie z płatności online (55) zgłosiły, że rzadziej niż raz do roku lub w ogóle nie zmieniają swojego hasła. Osoby korzystające z płatności mobilnych kilka razy w miesiącu lub rzadziej zgłosiły podobne nawyki w zmianie haseł, co osoby korzystające codziennie z płatności online.

Kolejne pytanie ankiety miało na celu zrozumienie, w jakim stopniu respondenci podejmują działania w celu podniesienia poziomu bezpieczeństwa płatności cyfrowych poprzez regularne monitorowanie i sprawdzanie swoich transakcji oraz konta bankowego w celu wykrycia nieautoryzowanych operacji.

Tabela 3. Nawyki monitorowania transakcji i konta bankowego w celu wykrycia nieautoryzowanych operacji przez respondentów

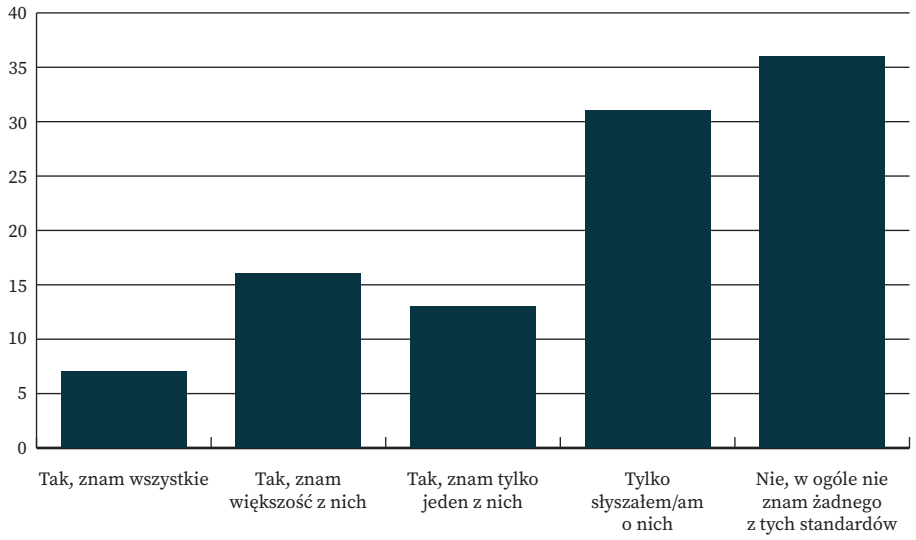
Nawyki monitorowania transakcji i konta bankowego	Odsetek respondentów dokonujących monitorowania
Zawsze, to ważne dla mnie	27%
Często, staram się to robić regularnie	48%
Czasami, ale nie zawsze pamiętam	13%
Rzadko, nie uważam tego za konieczne	8%
Nigdy, nie przypuszczam, że mogłoby mi się to przytrafić	4%

Źródło: Opracowanie własne na podstawie wyników badań

Z analizy wynika, że większość respondentów (49) często stara się regularnie monitorować swoje transakcje i konto bankowe w celu wykrycia nieautoryzowanych operacji. Kolejna duża grupa respondentów (28) zawsze — uznaje to za ważne i regularnie to robi. Mniejsza liczba respondentów (13) czasami to robi, ale nie zawsze pamięta. Natomiast mniejsza liczba respondentów (8) rzadko, nie uważa to za konieczne, a tylko 5 respondentów nigdy nie przypuszczało, że mogłoby im się to przytrafić.

Następne pytanie zadane ankietowanym miało na celu zrozumienie, w jakim stopniu znają oni i są świadomi różnych standardów bezpieczeństwa bankowości elektronicznej. Respondenci byli poproszeni o wskazanie, czy znają poszczególne standardy i w jakim stopniu. Poniżej przedstawiono standardy, o które zostali zapytani respondenci.

- PCI DSS: Standard bezpieczeństwa danych branży kart płatniczych.
- ISO 27001: Międzynarodowy standard zarządzania bezpieczeństwem informacji.
- TLS: Protokół warstwy transportowej zapewniający bezpieczne połączenia internetowe.
- EMV: Standard płatności kartami z chipem, który zwiększa bezpieczeństwo transakcji.
- 3D Secure: Protokół zapewniający dodatkową autoryzację dla transakcji kartami płatniczymi online.



Rys. 8. Znajomość standardów bezpieczeństwa bankowości elektronicznej przez respondentów
Źródło: Opracowanie własne na podstawie wyników badań

Z analizy wynika, że większość respondentów (36) nie zna żadnego z tych standardów bezpieczeństwa bankowości elektronicznej. Kolejna duża grupa respondentów (31) słyszała jedynie o tych standardach, ale ich szczegółowa znajomość jest ograniczona. Natomiast 13 respondentów zna tylko jeden z tych standardów, a 16 respondentów zna większość z nich. Zaledwie 7 respondentów zna wszystkie wymienione standardy.

7. Podsumowanie

Wyniki badań zestawiające ze sobą częstotliwość korzystania z płatności online z poczuciem bezpieczeństwa tych transakcji potwierdziły się poprzez współczynnik korelacji, który sugeruje, iż częstsze korzystanie z płatności online może wpływać na większe zaufanie do obecnych regulacji i standardów w zakresie bezpieczeństwa transakcji.

Niemniej jednak istnieje potrzeba zwiększenia edukacji konsumentów na temat bezpiecznego korzystania z płatności elektronicznych, ponieważ większość respondentów nie wykazała konkretnej wiedzy na temat standardów bezpieczeństwa bankowości elektronicznej. Dodatkowo obawy związane z nieuprawnionymi obciążeniami i kradzieżą danych finansowych stanowią główne wyzwanie dla rozwoju płatności cyfrowych. Jest to obszar, który wymaga większej uwagi i działań mających na celu poprawę świadomości i bezpieczeństwa konsumentów w zakresie korzystania z płatności online.

Podsumowując, wyniki badania sugerują rosnącą akceptację i zaufanie do płatności online, choć dają się zauważyć pewne różnice w postrzeganiu między grupami respondentów. Jednakże istnieją pewne wyzwania związane z bezpieczeństwem i edukacją konsumentów, które należy uwzględnić w dalszych działaniach mających na celu promowanie płatności cyfrowych. Istotne jest kontynuowanie działań edukacyjnych, w tym promowanie regularnej zmiany haseł oraz monitorowania transakcji, w celu zwiększenia świadomości klientów na temat bezpieczeństwa płatności online. Należy również zwiększyć świadomość konsumentów w obszarze standardów bezpieczeństwa bankowości elektronicznej, co może przyczynić się do wzrostu zaufania do systemów płatniczych.

Organizacje rządowe, instytucje finansowe oraz firmy zajmujące się płatnościami online powinny wspólnie prowadzić kampanie edukacyjne, informując o zagrożeniach związanych z oszustwami finansowymi i kradzieżą danych oraz prezentować metody ochrony przed nimi. Warto również inwestować w zaawansowane metody bezpieczeństwa, takie jak dwuetapowa weryfikacja, biometryczne uwierzytelnianie czy szyfrowanie danych, aby zapewnić użytkownikom maksy-

malne bezpieczeństwo podczas dokonywania transakcji (Siemieniuk, Zalewska-Bochenko, 2017).

Niestety, badania wykazują, iż ankietowani niewystarczająco dbają o cyberbezpieczeństwo we własnym zakresie, w związku z tym można powiedzieć o subiektywnym poczuciu bezpieczeństwa. Rodzi to potrzebę ciągłego doskonalenia wiedzy użytkowników na temat bezpieczeństwa płatności online oraz konieczność podjęcia działań przez banki i instytucje finansowe w celu zabezpieczenia tych transakcji. Równie ważne jest, aby sami użytkownicy podejmowali aktywne kroki w kierunku zwiększenia swojego bezpieczeństwa w sektorze płatności online.

Bibliografia

Chałubińska-Jentkiewicz, K. (2019). Cyberbezpieczeństwo — zagadnienia definicyjne. *Cybersecurity and Law*, *2*(2), 7–23.

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y? (n.d.). Baza wiedzy. Serwis Rzeczypospolitej Polskiej. https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y

Dąbrowska-Antoniak, I. (2019). *Nieautoryzowane transakcje — zasady i główne problemy*. Rzecznik Finansowy. https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf

Dmowska, K. (2022). Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego. *Bank i Kredyt, 53*(4), 357–374.

Dyrektywa. (2015). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

Grzelak, M., Liedel, K. (2022). Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski — zarys problemu. *Studia Bezpieczeństwa Narodowego, 12*(25), 11–23.

Narodowe Standardy Cyberbezpieczeństwa. (b.d.). Baza wiedzy. Serwis Rzeczypospolitej Polskiej. https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

Pitera, R. (2017). Współczesne problemy i zagrożenia cyberbezpieczeństwa w sektorze usług bankowości elektronicznej. *Przegląd Nauk o Obronności, 2*(4), 181–192.

Raport CSIRT KNF. (2023). *Cyberzagrożenia w sektorze finansowym*. CSIRT KNF.

Czyżak, M. (2016). Cyberprzestępczość bankowa i środki jej zwalczania. *Ekonomiczne Problemy Usług,* 123, 203–211.

Raport Cyfrowa Polska. (2019). Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań. https://cyfrowapolska.org/pl/raporty/

RODO. (2016). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Siemieniuk, N., Zalewska-Bochenko, A. (2017). Bezpieczeństwo systemów informatycznych w instytucjach bankowych. *Roczniki Kolegium Analiz Ekonomicznych / Szkoła Główna Handlowa*, 44, 55–67.

Ustawa. (1997). Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe Dz.U. 2015 poz. 128, z późniejszymi zmianami.
Ustawa. (2018). Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku. Dz.U. 2024 poz. 1077.
Wodo, W., Stygar, D., & Winiarska, K. (2019). *Bezpieczeństwo systemów bankowości elektronicznej i mobilnej w Polsce*. Oficyna Wydawnicza Politechniki Wrocławskiej.

Payment Security in the Digital Age

Abstract. The article deals with the security of online payments in the digital age. The aim of the study was to identify factors influencing users' sense of security and their concerns related to electronic payments. The analysis of the problem is based on data collected in a questionnaire survey involving 103 students of WSB Merito University. As it turns out, most respondents regularly use online payments and are mainly concerned about unauthorized charges resulting from the theft of login credentials to their bank accounts. According to respondents, advanced security measures, such as two-factor authentication, play a key role in protecting transactions. The results of the study suggest that by educating users about banking security standards and encouraging them to regularly change passwords, their level of trust towards digital payments and the level of transaction security can be increased.

Keywords: cyber security, online payments, data theft, security measures, user confidence