Wojciech Wodo
Damian Stygar
Klaudia Winiarska

BEZPIECZEŃSTWO SYSTEMÓW BANKOWOŚCI ELEKTRONICZNEJ I MOBILNEJ W POLSCE

Badania użytkowników 2019

WOJCIECH WODO
DAMIAN STYGAR
KLAUDIA WINIARSKA

Bezpieczeństwo systemów bankowości elektronicznej i mobilnej w Polsce

Badania użytkowników 2019

Oficyna Wydawnicza Politechniki Wrocławskiej
Wrocław 2019

Partnerzy

Patronat

ZWIĄZEK BANKÓW POLSKICH

Recenzent

Lucjan Hanzlik, Stanford University

Korekta

Zuzanna Sawicka, Martyna Mokrzecka

Współpraca

Jan Czajkowski, Aleksandra Dobroń, Maciej Górski, Mateusz Jachniak, Agnieszka Rucka, Damian Rybak, Rafał Szymanek, Marek Żytko

DTP

Wojciech Sierżęga

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-367 Wrocław
http://www.oficyna.pwr.edu.pl; e-mail: oficwyd@pwr.edu.pl
zamawianie.ksiazek@pwr.edu.pl

ISBN 978–83–7493–109–0
DOI 10.37190/WSW_BU2019

Spis treści

1. Wprowadzenie

Rok 2019 dla rozwoju usług cyfrowych i cyfryzacji administracji w Polsce był bardzo znaczący, o ile nie przełomowy. Wprowadzono usługi administracji państwowej, gdzie po raz pierwszy został w pełni uruchomiony system rozliczania podatków – Twój e-PIT[1], ponadto zostały wprowadzone nowe dowody osobiste z warstwą elektroniczną[2], dodatkowo udostępniono aplikację mObywatel[3] umożliwiającą potwierdzenie tożsamości. Jednak za najważniejsze należy uznać przygotowanie sektora finansowego do wdrożenia dyrektywy PSD2 [1], uruchomienie i wystawienie przez banki testowego interfejsu API[4] i zbrojenia fintechów, aby przejąć sektor usług finansowych [2].

Podnoszenie standardów administracyjnych buduje pozytywne wizje rozwoju gospodarczego oraz zwiększa płynność w realizacji wielu działań, zarówno prywatnych, jak i biznesowych. Za szybko podążającą cyfryzacją nadchodzi ryzyko związane z: zagrożeniami cyberbezpieczeństwa, brakiem świadomości użytkowników, polem do nadużyć i niedostosowaniem odpowiednio szybko przepisów prawnych. Rząd podjął działania w kierunku zagwarantowania podstaw prawnych dla określonych czynności i usług. Te działania to: ustawa o cyberbezpieczeństwie [3], ustawa zakazująca wytwarzania dokumentów imitujących dokumenty tożsamości i dokumentów uprawniających do wykonywania czynności [4] czy uprzednio ratyfikowana, szeroko omawiana ustawa o ochronie danych osobowych RODO [5].

Czy jednak przeciętni obywatele potrafią funkcjonować w tak zmiennej rzeczywistości postępu technologicznego? Czy potrafią we właściwy sposób użyć oferowanych dóbr i prawidłowo zabezpieczyć się przed zagrożeniami płynącymi z korzystania z usług elektronicznych? To tylko niektóre z zagadnień podejmowanych w niniejszym opracowaniu, którego celem jest nakreślenie postaw i zachowań użytkowników korzystających z usług cyfrowej bankowości.

---

1 https://www.gov.pl/web/finanse/twoj-e-pit-nowa-jakosc-w-rozliczeniu-podatku

2 https://www.gov.pl/web/cyfryzacja/e-dowod-dowod-zwarstwa-elektroniczna

3 https://www.gov.pl/web/mobywatel

4 https://polishapi.org/

1.1. Motywacja

Olbrzymie tempo wdrażania nowych technologii w każdej domenie życia, zarówno prywatnej, jak i biznesowej[5], nie znajduje odzwierciedlenia w kampaniach informacyjno-edukacyjnych, które zapewniłyby bezpieczne i świadome korzystanie z dobrodziejstw usług cyfrowych[6]. Obszar opracowania to finanse elektroniczne, bankowość cyfrowa i usługi finansowe.

Polem badań jest to jak obecni użytkownicy usług finansowych i bankowości elektronicznej postrzegają dostępne rozwiązania, jak zapatrują się na kwestie bezpieczeństwa, jakie mają odczucia podczas korzystania z różnych form płatności, czy są świadomi zagrożeń płynących z różnych rozwiązań technologicznych i zachowań ryzykownych. Celem jest poznanie użytkowników, ich postaw, aby zidentyfikować obszary warte szczególnej uwagi w kontekście edukacji, informacji oraz możliwości zmiany formuły świadczonych usług. Zdobyte informacje chcemy przekuć w cenne wskazówki dla użytkowników, podmiotów świadczących usługi finansowe oraz instytucji bankowych. Opracowane przez nas wytyczne mają na celu wskazanie elementów poprawiających komfort i bezpieczeństwo korzystania z nowych usług. Nasze badania pomogą uchwycić aspekty, które nie zostały uwzględnione przy przygotowywaniu i projektowaniu usług, systemów przez banki czy administrację państwową. Chcemy rzucić nowe światło na środowisko usług finansowych, patrząc z perspektywy ich użytkownika, nie instytucji.

1.2. Dotychczasowe badania

W obszarze bankowości elektronicznej na bieżąco prowadzone są badania monitorujące stan jej rozwoju, dostępności usług, zagrożeń i struktury użytkowników. Dzięki aktywności Związku Banków Polskich[7] są organizowane corocznie konferencje i szkolenia poświęcone poszczególnym obszarom bankowości, w tym technologicznym oraz i bezpieczeństwa. Z inicjatywy ZBP powołane zostało Bankowe Centrum Cyberbezpieczeństwa[8], które monitoruje incydenty i zagrożenia w sieci oraz koordynuje i zarządza trudnymi sytuacjami. ZBP publikuje również regularnie raporty na tematy związane z poziomem „adopcji" usług bankowych w kraju oraz kwestiami bezpieczeństwa. Przykładem jest raport z 2018 roku *Cyberbezpieczny portfel* [8] wskazujący zachowania i preferencje klientów bankowości elektronicznej oraz *PSD2 i Open Banking – Rewolucja czy ewolucja*? [2] biorący pod lupę kwestie open bankingu i dyrektywy PSD2, a także szans i zagrożeń biznesowych dla rynku fintechów.

Dzięki współpracy Konferencji Przedsiębiorstw Finansowych w Polsce i EY powstaje corocznie (od 2009) raport dotyczący nadużyć w sektorze finansowym [2]. Raport prezentuje zmiany na rynku cyfrowych usług bankowych, nowe zagrożenia oraz zmiany polityki insty-

[5] https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up
[6] https://economictimes.indiatimes.com/news/economy/indicators/indias-way-to-1-trillion-digital-economy/articleshow/63561270.cms
[7] https://zbp.pl/
[8] https://zbp.pl/aktualnosci/Archiwalne-wydarzenia/otwarcie-bankowego-centrum-cyberbezpieczenstwa

tucji finansowych. MasterCard w 2019 roku wykonał badania w kontekście postaw polskich konsumentów wobec zakupów online, uwzględniając nadchodzące zmiany w płatnościach w e-commerce. Efektem ich pracy jest raport *Bezpieczne e-zakupy*[9]. Autorzy udowadniają, że biometria stanie się standardem potwierdzania tożsamości w płatnościach. Ponadto, ponad 75% badanych uważa, że silne uwierzytelnienie płatności kartą online, które weszło w życie w połowie września 2019 r., jest potrzebne, co jednoznacznie wyznacza nowy trend w bankowości.

W roku 2016 zajęliśmy się badaniami preferencji użytkowników, ich nastawienia i poziomu świadomości w stosunku do bezpieczeństwa urządzeń mobilnych i biometrii, czego efektem jest raport *Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badania użytkowników 2016* [6]. Opracowanie wyróżniło cztery główne typy użytkowników urządzeń i aplikacji mobilnych, przypisując im charakterystyczne cechy, poglądy i zachowania. Co niepokojące, ponad połowa użytkowników wykazała się nieodpowiedzialnością w podejściu do aspektów bezpieczeństwa, nie zauważając wartości swoich prywatnych danych, takich jak np. dane dotyczące tożsamości. Ponadto większość ankietowanych użytkowników korzysta z domyślnych funkcji zabezpieczeń telefonu i aplikacji, nie zważając na to, by je zmienić i dostosować do swoich potrzeb. Najistotniejszym wnioskiem płynącym z raportu jest stwierdzenie, że niemożliwe jest stworzenie jednego, uniwersalnego rozwiązania odpowiadającego na wszystkie potrzeby bezpieczeństwa użytkowników urządzeń mobilnych. Systemy bezpieczeństwa powinny być projektowane z myślą o określonej grupie odbiorców łączących podobne cechy, poglądy i potrzeby.

Temat bezpieczeństwa bankowości korporacyjnej podjęło z kolei KPMG, przygotowując w 2018 roku raport *Bezpieczeństwo technologii mobilnych* [9]. Z raportu wynika, że przedsiębiorstwa podchodzą z większą uwagą do kwestii bezpieczeństwa niż klienci indywidualni. Ponad połowa badanych firm korzysta z urządzeń mobilnych w swojej praktyce biznesowej, a 76% organizacji nie pozwala przetwarzać danych firmowych na prywatnych urządzeniach mobilnych pracowników. Ponad połowa firm wymusza uwierzytelnienie w celu dostępu do urządzenia mobilnego oraz pozwala instalować jedynie aplikacje mobilne zatwierdzone przez organizacje.

Firma Yubico sponsorowała badania w 2019 roku poświęcone podejściu użytkowników w odniesieniu do haseł i bezpieczeństwa uwierzytelniania tożsamości, czego efektem jest raport *State of Password and Authentication Security Behaviors Report* [10]. Badania zostały przeprowadzone w Stanach Zjednoczonych, Wielkiej Brytanii, Niemczech i Francji na próbie 1761 osób zajmujących się technologiami IT. Co ciekawe, ponad 57% respondentów stwierdziło, że ze względu na fakt, że zarządzanie hasłami jest niewygodne i uciążliwe, chcieliby stosować metody alternatywne do uwierzytelniania swojej tożsamości. 56% badanych opowiedziało się za wykorzystaniem kluczy sprzętowych. Z raportu wynika, że wykorzystanie uwierzytelniania dwuskładnikowego nie jest powszechne, 67% przebadanych osób nie używa 2FA w żadnej formie w swoim życiu prywatnym, a 55% nie używa go nawet w pracy.

[9] https://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-biometria-stanie-sie-nowym-standardem-potwierdzania-tozsamosci-w-platnosciach/

2. Badania użytkowników

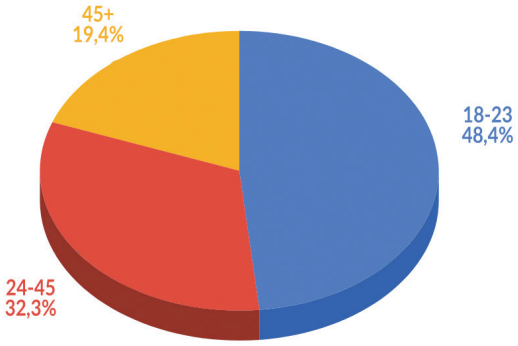
W celu analizy sytuacji w obszarze technologii bezpieczeństwa usług bankowości elektronicznej i mobilnej w Polsce przeprowadzono badania eksploracyjne rynku użytkowników z wykorzystaniem metodyki Design Thinking. Jest to metoda tworzenia innowacyjnych produktów i usług w oparciu o głębokie zrozumienie problemów i potrzeb użytkowników, opracowana na Uniwersytecie Stanforda w Kalifornii [11].

Głównym założeniem tej metody jest koncentracja na użytkowniku, bowiem to właśnie on ma przynieść odpowiedź na najważniejsze pytania związane ze świadomością i podejściem do systemów bezpieczeństwa bankowości elektronicznej.

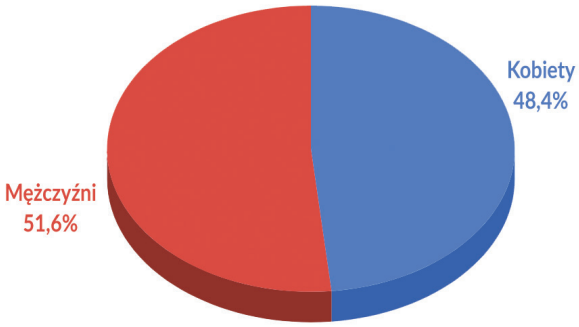
Aby projektowane rozwiązanie osiągnęło dojrzałość, powinno przejść kilka cykli projektowych, podczas których dojdzie do weryfikacji podjętych decyzji i obranych kierunków pracy, a przede wszystkim kiedy stanie twarzą w twarz ze swoim finalnym odbiorcą – użytkownikiem. Etapy procesu Design Thinking ilustruje rysunek 1.

Rys. 1. Etapy procesu Design Thinking. Źródło: http://designthinking.pl

W badaniu wzięły udział 62 osoby stanowiące próbę badawczą, w tym 32 mężczyzn oraz 30 kobiet w wieku od 18 do 78 lat. Należy podkreślić, że przeprowadzone badania mają charakter badań jakościowych, w których pojedynczy wywiad z respondentem trwa ok. godziny i jest nastawiony na dogłębne zrozumienie postaw, myśli i zachowań badanego. Grupa badawcza (n = 62) została tak dobrana, aby była zróżnicowana zarówno pod względem płci i wieku, jak i wykształcenia oraz wykonywanej profesji, dzięki czemu uzyskane informacje mają większą wartość poznawczą. Przy czym uwzględniono większy udział grupy osób w wieku 18–23 lata, czyli grupy uczącej się/studiującej, ze względu na jej podatność oraz najczęstsze korzystanie z nowych technologii. Ponadto będą stanowić znaczącą grupę na rynku pracy. Staną się oni nowym segmentem klientów usług finansowych.



Rys. 2. Rozkład wieku badanych (n = 62)



Rys. 3. Rozkład płci badanych (n = 62)

2.1. Budowa kwestionariusza i jego podstawowe cechy

Zgodnie z przyjętą metodyką prace rozpoczęły się od powołania interdyscyplinarnego zespołu badawczego, który ze względu na różnorodne doświadczenie członków mógł spojrzeć na zagadnienie z wielu perspektyw. Budowa kwestionariusza jest efektem zróżnicowanej wiedzy i doświadczenia zespołu, który opracował go tak, by w jak największym stopniu otrzymać od użytkowników odpowiedzi na najistotniejsze pytania.

W pierwszej fazie procesu Design Thinking (empatyzacji) skonstruowano ramowy kwestionariusz wywiadu. Uwzględniono reguły i wskazówki sugerowane przez amerykańskich twórców procesu, pamiętając przy tym o kontekście badania. Jako że zdecydowano się na stosowanie wywiadu pogłębionego, podkreślono istotność eksploracji potrzeb i obaw badanego. Zwrócono również uwagę na aspekty behawioralne – czyli zachowania, gestykulację podczas udzielanych odpowiedzi oraz wiążące się z tym nierozerwalnie wyrażanie emocji chociażby poprzez ton głosu, prędkość mówienia, czy mimikę twarzy. Zdecydowano, że powyższe aspekty powinny stanowić ramę wywiadu, a kwestionariusz, jako punkt początkowy rozmowy, o której kierunku decydować będzie pytający. Przed przystąpieniem do fazy wywiadów zespół badawczy, składający się z dziesięciu osób, został przeszkolony pod względem prawidłowego i jednolitego prowadzenia badań, celem zapewnienia spójności i jakości uzyskanych danych.

Kwestionariusz poruszał 13 obszarów i składał się z pytań otwartych, których celem była eksploracja obszaru użytkowania bankowości elektronicznej i mobilnej. Badano również towarzyszące odpowiedziom tło emocjonalne, wyrażające się w zachowaniu respondentów czy motywację podejmowania przez nich decyzji. Wywiad poruszał też kwestie poglądów dotyczących kwestii cyberbezpieczeństwa. Głównym celem kwestionariusza była weryfikacja potrzeb oraz obaw użytkowników związanych z różnymi aspektami korzystania z bankowości elektronicznej i usług powiązanych.

Obszary poruszane w wywiadzie dotyczyły:

- wykorzystania płatności elektronicznych i mobilnych, sposobów ich przeprowadzania i uwierzytelniania;
- poczucia bezpieczeństwa wynikającego z korzystania z płatności online i mobilnych;
- wykorzystania aplikacji mobilnych do płatności elektronicznych i ich aktualizacji;
- doświadczeń i emocji (osobistych lub osób bliskich) związanych z cyberatakami;
- higieny korzystania z bankowości elektronicznej i mobilnej, znajomości zasad bezpieczeństwa i ich przestrzegania;
- znajomości zagadnień dotyczących cyberataków na finanse elektroniczne i źródeł informacji na ich temat;
- wykorzystania kart płatniczych i płatności zbliżeniowych, stosowanych limitach i zasadach bezpieczeństwa;
- znajomości mechanizmów podwójnej weryfikacji (2FA), systemu ePUAP, usług weryfikujących tożsamość jak „zaloguj się przez bank" i nastawienia do nich oraz stopnia ich wykorzystania;
- wizji idealnego systemu zabezpieczeń dla usług bankowości elektronicznej i mobilnej.

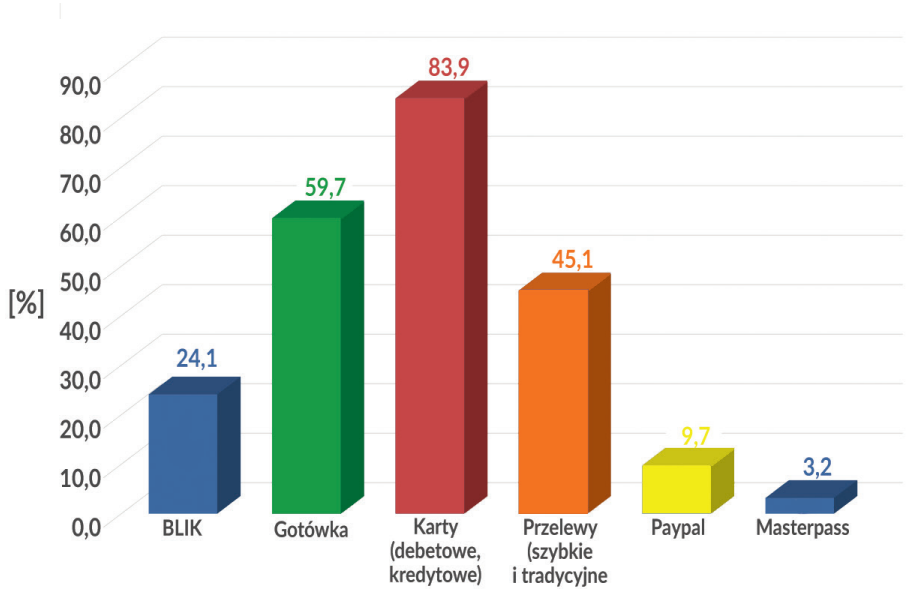
2.2. Ujęcie zebranych danych, interpretacja i dyskusja

W tej części opracowania zostaną zaprezentowane dane uzyskane z wywiadów w ujęciu ilościowym oraz ich omówienie w podziale na poszczególne zagadnienia. Obszary badawcze zostaną opatrzone wypowiedziami użytkowników (persony ubrane w cytaty), co pozwoli na dokładne zilustrowanie nastawienia, opinii i podejścia do omawianych kwestii. Taka forma pozwala na łatwiejsze utożsamienie swoich (czytelnika) poglądów i zachowań z personami, bowiem postacie stają się nam bliższe poprzez odwołania do sytuacji, faktów i zachowań znanych nam z własnego życia.

Przedstawione zestawienia stanowią jedynie część wywiadu – nie sposób bowiem ująć wszystkich zależności w postaci graficznej.

2.2.1. Płatności

2.2.1.1. Jak dokonujesz płatności za usługi i produkty? Dlaczego?



Rys. 4. Jak dokonujesz płatności za usługi i produkty? (n = 62)

Przeważająca liczba osób – 83,9% ankietowanych na co dzień płaci kartą (debetową, kredytową itd.). Komentarzem do wybranej formy płatności jest poniższa wypowiedź:

> [Wybieram] płatność kartą zbliżeniowo ze względu na wygodę, historię płatności na stronie banku i brak potrzeby noszenia przy sobie gotówki.

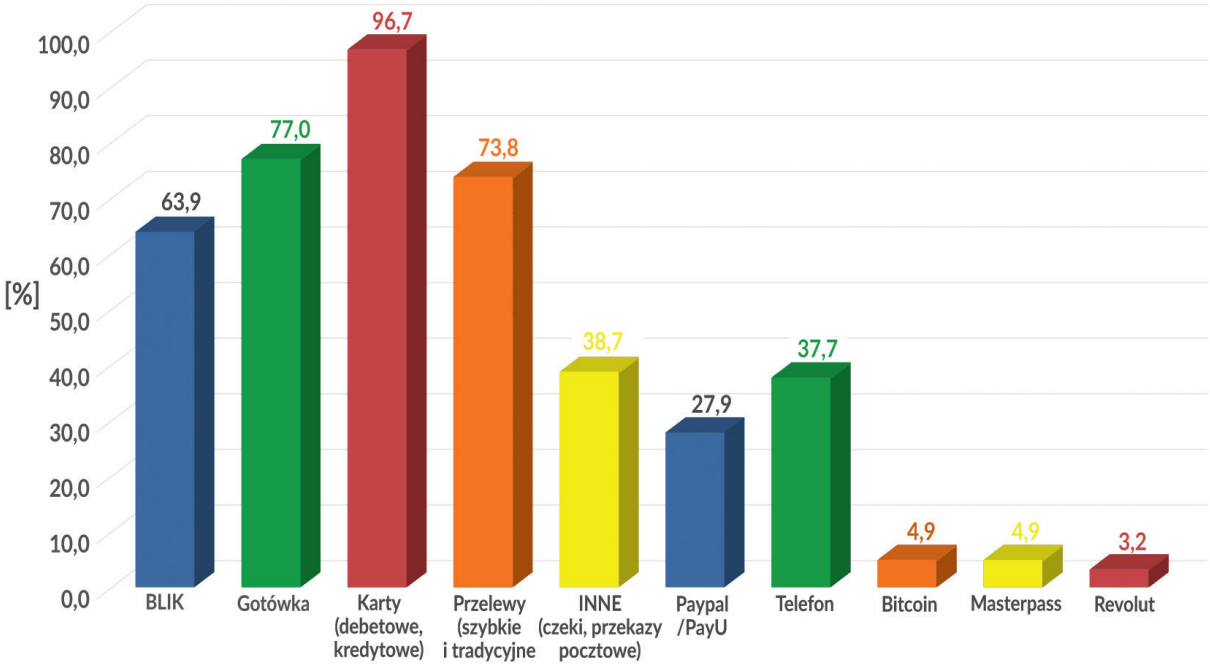
Ta oraz wiele innych, zbliżonych odpowiedzi pokazuje, że użytkownicy bankowości mobilnej lubią „cieszyć się swobodą" – dla wielu płacenie kartą jest szybkie, a brak potrzeby posiadania przy sobie portfela pełnego gotówki to udogodnienie, które wielokrotnie pojawiło się w wypowiedziach ankietowanych.

> [O szybkich przelewach] ...ponieważ umiem je dobrze obsłużyć i budzą moje zaufanie, lubię je.

Nie tylko szybkość decyduje jednak o tym, jak płacą badani.

Komentarz autorów: *Ludzie chętniej wybierają te metody, które znają, wzbudzają większe zaufanie. Dzięki takim odpowiedziom można wywnioskować, że popularyzacja danego sposobu płatności i jego reklama wpływa na liczbę ludzi, która z niego skorzysta.*

2.2.1.2. Jakie znasz metody płatności?



Rys. 5. Jakie metody płatności znasz? (n = 62)

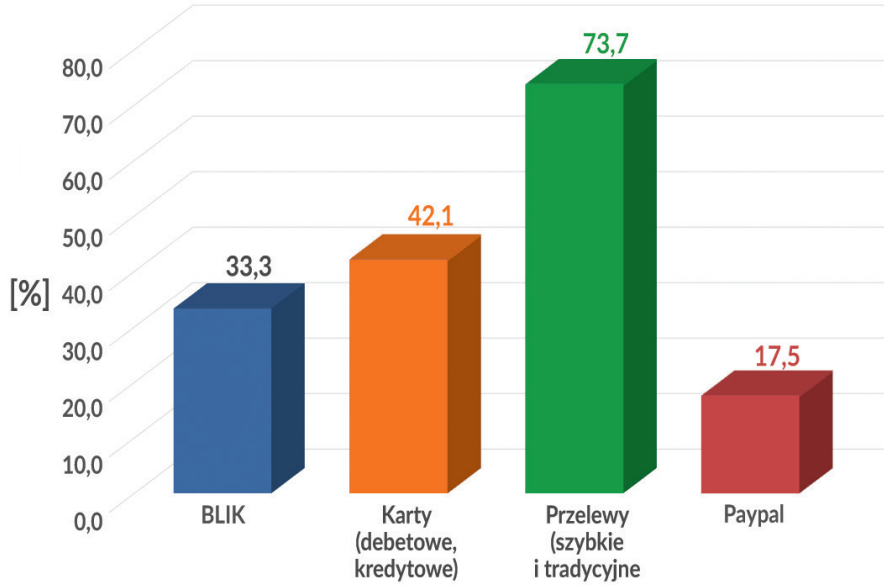
Na podstawie danych z tego oraz poprzedniego pytania wysuwa się jasny wniosek – płatność kartą to zdecydowanie najpopularniejsza metoda płatności wśród ankietowanych. Ciekawe jednak jest to, że wiele osób wymienia poszczególne nazwy serwisów płatności elektronicznych, jako metody, które znają. Dostawcy, którzy się pojawiają najczęściej to PayPal/ /PayU/Revolut/Masterpass. Dzięki swojej popularności i dostępności na rynku, są one rozpoznawane przez wielu ankietowanych. Świadczy to o bardzo dużej sile marek, mimo że same rozwiązania zawierają się w poprzednio wymienionych kategoriach.

Coraz więcej osób w Polsce wie także o bitcoinie, który pojawił się w odpowiedziach ankietowanych (4,9%).

Kategoria „telefon" jest bardzo interesującą odpowiedzią. Ankietowani nie precyzowali, w jaki sposób wykorzystują urządzenie mobilne do płatności, zaznaczali jedynie, że taka możliwość istnieje.

Wciąż jeszcze pamiętane są stare sposoby płatności, co odzwierciedla kategoria „INNE". W niej właśnie zawarte są odpowiedzi typu czeki i przekazy pocztowe.

2.2.1.3. Jak płacisz za zakupy online? Dlaczego?



Rys. 6. Jakie metody płatności znasz? (n = 62)

Spośród wszystkich ankietowanych 92% płaci za zakupy online. Pozostałe 8% albo nie robi zakupów online wcale, albo prosi kogoś bliskiego o zakup, albo korzysta tylko z płatności za pobraniem.

> Płacę najczęściej przelewem z tych szybkich płatności, czasami kartą lub paypalem. Głównie robię to dla wygody i dla szybkości potwierdzenia transakcji. Jeśli sklep wymaga tradycyjnego przelewu to jeśli mogę to rezygnuję z kupna i kupuję gdzie indziej.

Dla jednej z ankietowanych szybkość i łatwość obsługi BLIKA stała się problematyczna:

> Kiedyś płaciłam BLIKIEM, ale w pewnym momencie zrezygnowałam bo nie do końca kontrolowałam wszystkie transakcje. Wtedy zdecydowanie za szybko ubywały mi pieniądze na koncie.

Obawy jednak towarzyszą niejednemu użytkownikowi bankowości elektronicznej.

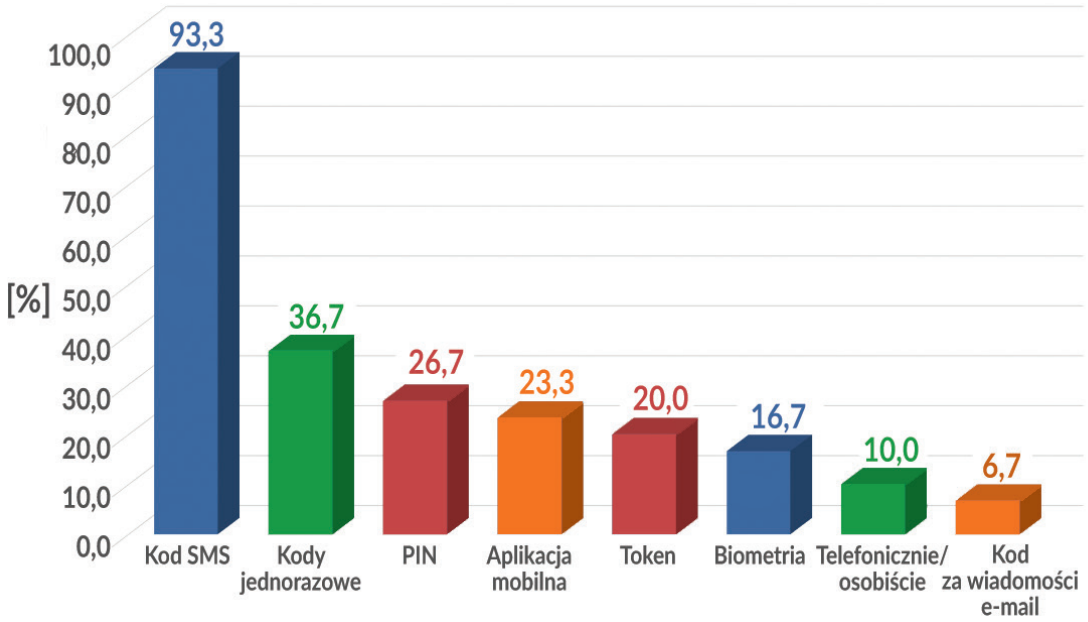
> Boję się [płacić] kartą, że zostanie ona w jakiś sposób w internecie przechwycona. Do takich płatności [internetowych] posiadam subkonto.

Po raz kolejny w odpowiedziach ankietowanych głównymi powodami korzystania z wybranych płatności są szybkość i wygoda, co podkreśla jeden z pytanych:

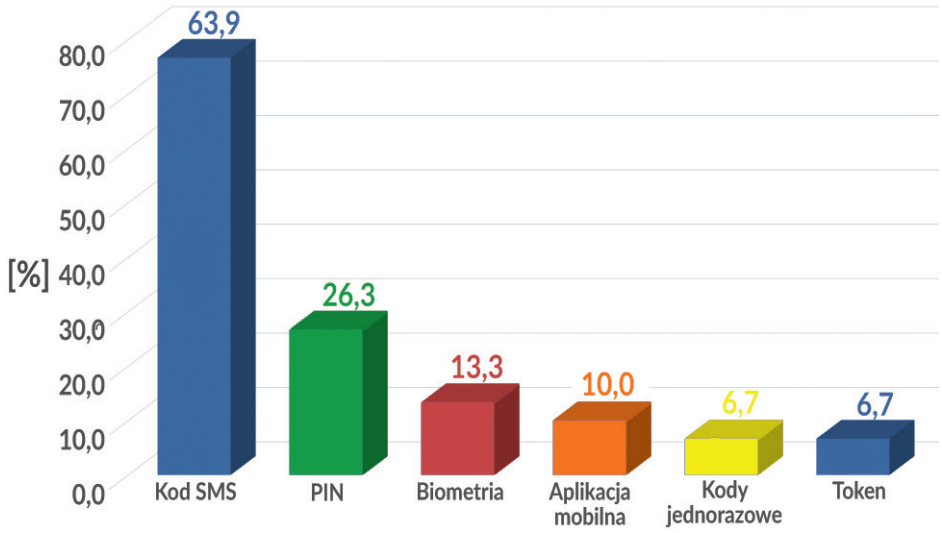
I I Kartą, tak jest najprościej.

Komentarz autorów: *Z odpowiedzi ankietowanych wynika, że nie rozpatrują korzystania z określonych metod płatności pod względem bezpieczeństwa. Przykładowo, transakcja płatnicza kartą to rozsądny wybór przy płatnościach online. Podczas gdy ankietowani wspominają o prostocie i szybkości tego rozwiązania, warto dodać, że płatność kartą jest również bezpieczna, na przykład ze względu na obciążenie zwrotne (ang.* chargeback*). Dzięki niemu, w określonych przypadkach, właściciel karty płatniczej może wystąpić o zwrot kwoty z transakcji.*

2.2.1.4. Jakie znasz sposoby potwierdzenia transakcji i z których korzystasz?



Rys. 7. Jakie znasz sposoby potwierdzenia transakcji? (n = 30)



Rys. 8. Jakie metody potwierdzenia transakcji stosujesz? (n = 30)

W obu przypadkach wielu ankietowanych błędnie zrozumiało pytanie. Dotyczyło ono potwierdzeń transakcji, takich jak kod jednorazowy, które umożliwiają rozpoczęcie procesu płatności. W interpretacji niektórych ankietowanych potwierdzenia transakcji to powiadomienia SMS oraz maile, które mówią o dokonaniu procesu płatności. Ze względu na ten błąd interpretacyjny próba statystyczna dla tych pytań to połowa ankietowanych.

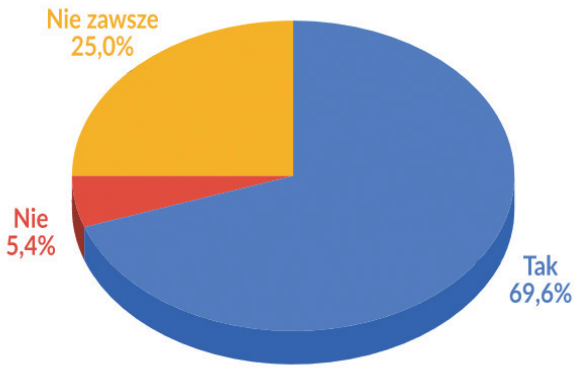
Najlepiej znaną metodą potwierdzania transakcji jest jednorazowy kod SMS. Wynikać to może przede wszystkim z ich dużej popularności w polskiej bankowości.

Banki zachęcają do korzystania z kodów SMS, wycofują inne metody autoryzacji transakcji[10], a kilku ankietowanych zwróciło uwagę na to, że w ich banku kody SMS były jedyną możliwą opcją do wyboru.

Komentarz autorów: *Kody SMS mogą nie być bezpiecznym sposobem potwierdzania transakcji, istnieje bowiem opcja dodania zaufanego odbiorcy. Po tej akcji kod SMS nie jest wymagany do wykonania transakcji. Możliwe jest również zduplikowanie karty SIM i przejęcie numeru ofiary[11]. Implementacja mechanizmu kodu SMS także bywa wadliwa. Kod może nie być powiązany w żaden sposób z wykonywaną przez użytkownika transakcją, więc istnieje możliwość wykorzystania go w tym samym czasie do innej transakcji (np. podmiany danych transakcji).*

[10] https://www.zadluzenia.com/pekao-rezygnacja-z-kart-kodow-jednorazowych/
[11] https://niebezpiecznik.pl/post/duplikat-karty-sim-kradziez-bank-mbank-bzwbk/

2.2.1.5. Czy podczas płatności online czujesz się bezpiecznie, komfortowo? Dlaczego?



Rys. 9. Czy podczas płatności online czujesz się bezpiecznie/komfortowo? (n = 56)

Przeważająca liczba osób twierdzi, że czuje się bezpiecznie podczas korzystania z płatności online. Częstym uzasadnieniem wśród ankietowanych był brak przykrych doświadczeń. Wyodrębniona została dodatkowa odpowiedź — „nie zawsze". Kategoria ta skupia odpowiedzi zbliżone do poniższych komentarzy:

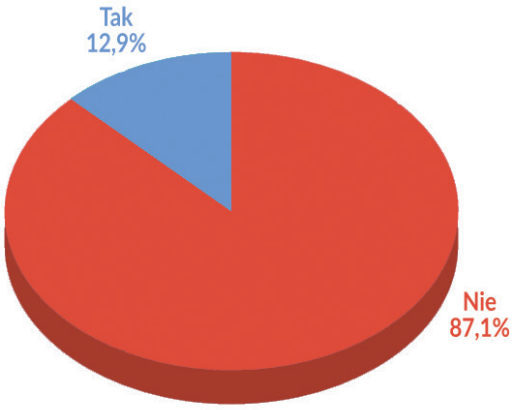
> Czuję się bezpiecznie, ale to taka ślepa wiara, wierzę że informatycy to dobrze zaprogramowali.

> Tak, czuję się bezpiecznie, może dlatego, że dużo pieniędzy nie używam.

Komentarz autorów: *Przy wzięciu pod uwagę odpowiedzi i wniosków z poprzednich pytań, można zauważyć, że ankietowani w życiu codziennym nie martwią się bezpieczeństwem. Liczy się, aby usługa działała dobrze, dlatego też wielokrotne podkreślanie szybkości i wygody danego rozwiązania. Bezpieczeństwo systemów bankowych nie pozostaje na długo w świadomości użytkowników. Większość z nich nie zdaje sobie sprawy z czyhających zagrożeń lub przykrych konsekwencji. Wielu ankietowanych osobiście nie doświadczyło żadnych przykrych incydentów. Stąd może wynikać przeświadczenie, że nie mogą być oni obiektami ataku, co przekłada się na (fałszywe) poczucie bezpieczeństwa.*

2.2.2. Aplikacje do płatności

2.2.2.1. Czy korzystasz z aplikacji mobilnej do płatności (np. GooglePay/ApplePay)? Dlaczego?



Rys. 10. Czy korzystasz z aplikacji mobilnej do płatności? [np. GooglePay/ApplePay]? (n = 62)

Przeważająca liczba ankietowanych (87,1%) nie korzysta z aplikacji mobilnych do płatności. Może to wynikać z niewiedzy o takich aplikacjach jak np. GooglePay czy ApplePay. Przykładem może być przytoczona wypowiedź jednego z ankietowanych:

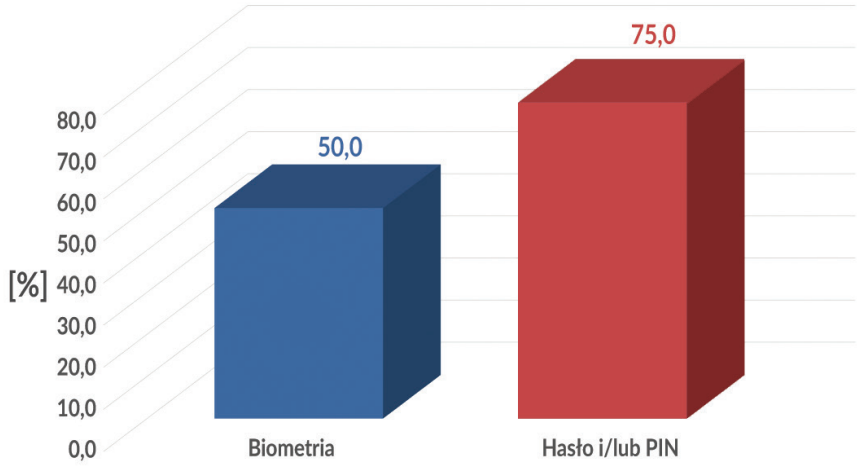
> Nie. Nie do końca o nich wiem i przez niewiedzę się boję.

Jedna z pytanych osób korzystała z GooglePay do płatności zbliżeniowych, ale obecnie nie używa tej funkcji, ponieważ nie odczuła większej różnicy płacąc w ten sposób niż płacąc kartą.

Podobnego zdania było kilka pozostałych osób, które także wspominały o tym, że szybkość i wygoda płacenia aplikacją mobilną nie różniły się znacząco od płacenia kartą.

Komentarz autorów: *Ze względu na szeroki wybór metod płatności w Polsce [12], nie ma krytycznej potrzeby szukania nowych metod realizacji transakcji, więc popularność na rynku usług płacenia aplikacjami mobilnymi nie jest wysoka.*

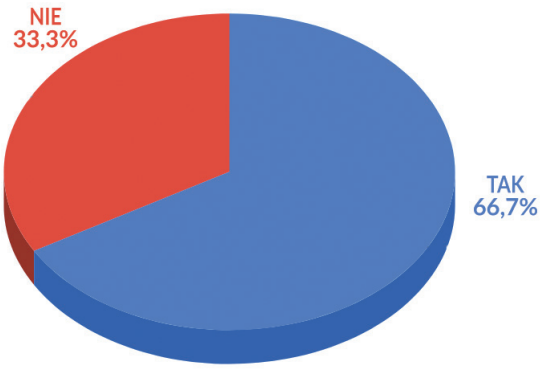
2.2.2.2. Czy płatność działa przy zablokowanym telefonie?



Rys. 11. Czy płatność działa przy zablokowanym telefonie? (n = 17)

71% badanych odpowiedziało, że płatność aplikacją mobilną jest niemożliwa, jeśli telefon jest zablokowany. Niepewność miało 18% osób, które nie wiedziały czy w ich przypadku taka płatność jest możliwa. Jest to sytuacja niebezpieczna ze względu na to, że część aplikacji bankowych domyślnie umożliwia płatność zbliżeniową, nawet jeśli telefon jest zablokowany.

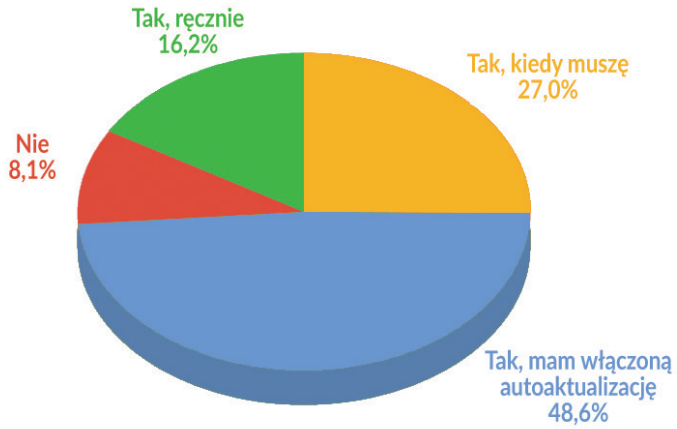
2.2.2.3. Czy płatność działa bez zalogowania do aplikacji bankowej?



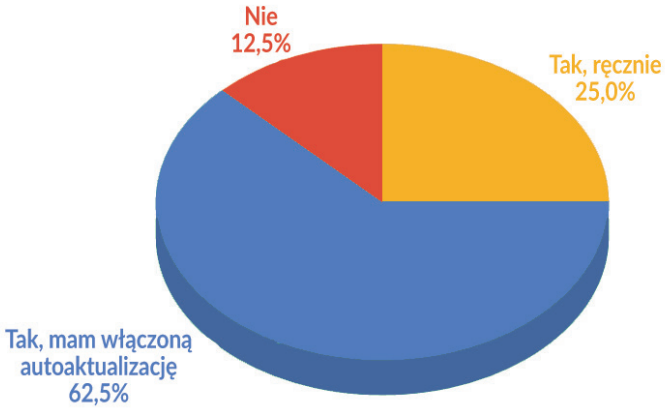
Rys. 12. Czy płatność działa bez zalogowania do aplikacji bankowej? (n = 12)

W przypadku 67% osób, które udzieliły odpowiedzi na to pytanie, płatność jest możliwa do zrealizowania bez zalogowania do aplikacji bankowej. Jeżeli osoby te nie korzystają z możliwości silnego zablokowania telefonu, np. za pomocą biometrii, to jest to podobnie niebezpieczny przypadek jak w poprzednim pytaniu.

2.2.2.4. Czy aktualizujesz aplikacje mobilne, w tym te do płatności elektronicznych?



Rys. 13. Czy aktualizujesz aplikacje mobilne? (n = 37)



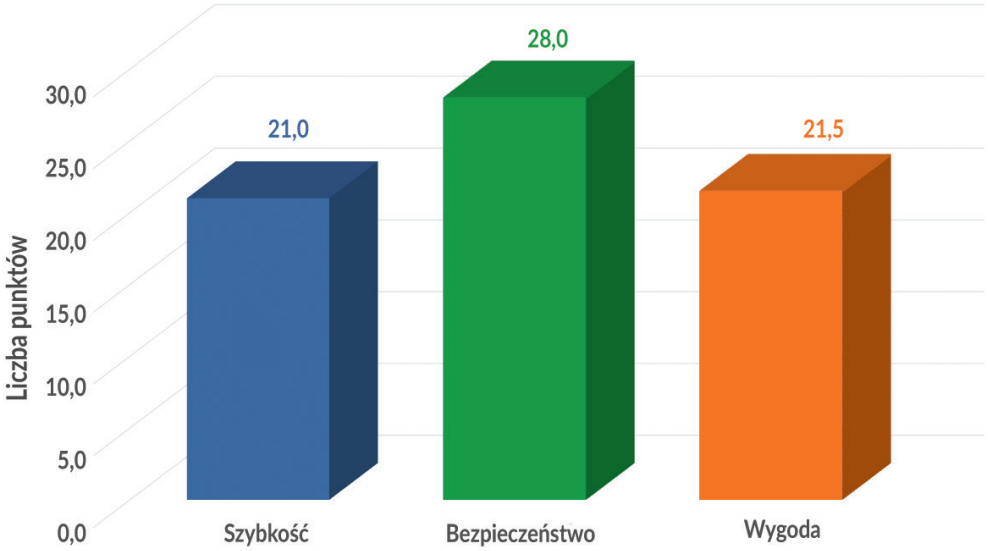
Rys. 14. Czy aktualizujesz aplikację mobilną do płatności? (n = 8)

Po analizie zebranych danych można zauważyć jak istotną rolę odgrywają automatyczne aktualizacje. Niestety nie wszystkim użytkownikom aplikacji mobilnych aktualizacje kojarzą się pozytywnie. Jedna z ankietowanych mówi tak:

> Jestem sceptycznie nastawiona do nowych aktualizacji bo miałam tak kilka razy, że aplikacja nie działała poprawnie po aktualizacji.

Komentarz autorów: *Zdecydowanie zbyt często zdarza się, że aktualizacja oprogramowania pogarsza jakość korzystania z aplikacji i programów. Może to zbudować obraz aktualizacji jako niepotrzebnej, przez co użytkownik może zniechęcić się do aktualizowania oprogramowania.*

2.2.3. Co jest dla Ciebie ważne przy korzystaniu z płatności elektronicznej/mobilnej?



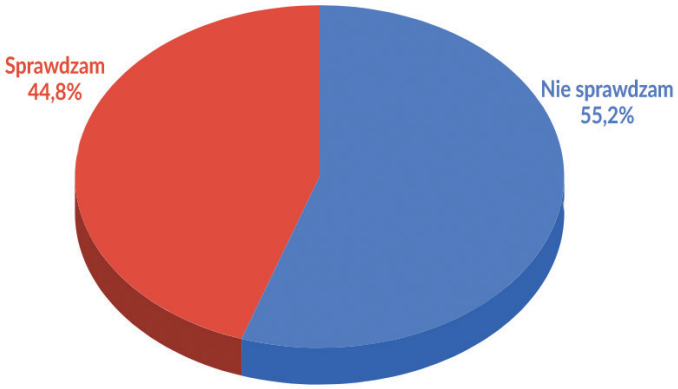
Rys. 15. Co jest dla ciebie ważne przy korzystaniu z płatności elektronicznej/mobilnej? (n = 62)

Najpopularniejszymi odpowiedziami były cechy, które można pogrupować w 3 kategorie: szybkość, wygoda i bezpieczeństwo. W celu wyłonienia najistotniejszej kategorii, dokonaliśmy oceny danej kategorii na podstawie jej wystąpienia, a w przypadku wystąpienia kilku kategorii, oceniana była kolejność wymienienia. Przyznawana była punktacja: 1 pkt za najważniejsze w wypowiedzi, 0,5 pkt za kolejne miejsce i 0,25 pkt za ostatnie. Jak widać na wykresie bezpieczeństwo wydaje się być najistotniejszym elementem w korzystaniu z płatności mobilnych/elektronicznych.

Dotychczas bezpieczeństwo było pomijane przez ankietowanych przy opisie sposobów płatności, których zazwyczaj używają. Po dłuższej refleksji ankietowani jednak decydowali się na bezpieczeństwo, jako na czynnik znacząco poprawiający komfort dokonywanych płatności.

Komentarz autorów: *Odpowiedzi w tym pytaniu pokazują sprzeczność pomiędzy tym, co jest wybrane jako najistotniejsze – bezpieczeństwo, a co tak naprawdę cenią sobie ankietowani – szybkość i wygoda.*

2.2.4. Czy sprawdzasz konto bankowe w miejscach publicznych (np. kawiarnia, tramwaj)?

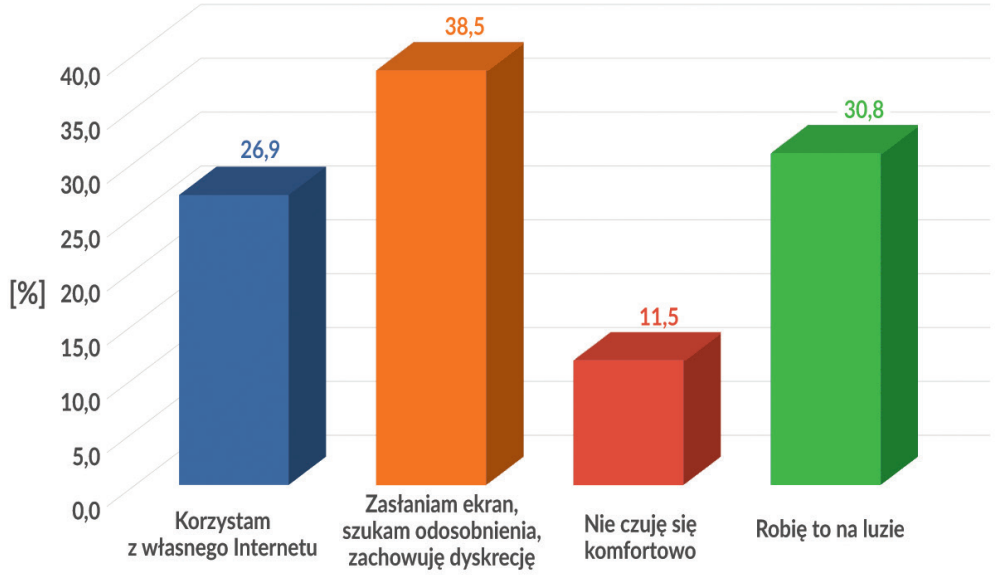


Rys. 16. Czy sprawdzasz konto bankowe w miejscach publicznych? (np. kawiarnia, tramwaj)? (n = 58)

Wśród badanych dominuje opinia, że dom i praca to bezpieczne miejsca do operacji finansowych. Czasami jednak pojawia się konieczność przeprowadzenia operacji finansowej w miejscu publicznym i wtedy badani decydują się na to (44,8% respondentów), z zastrzeżeniem, że używają swojego urządzenia (25% sprawdzających), starają się znaleźć miejsce odosobnione albo przynajmniej zakryć ekran podczas wprowadzania danych logowania bądź danych transakcji (35,7% sprawdzających). Ponadto 11,5% badanych, którzy sprawdzają konto, deklaruje, że towarzyszy im poczucie dyskomfortu.

Powyższe dane pokazują obawy ankietowanych, związane z naruszeniem sfery prywatności czy potencjalnym zagrożeniem finansów. Tylko niespełna 31% badanych wykonuje czynności finansowe w miejscach publicznych bez obaw i poczucia dyskomfortu.

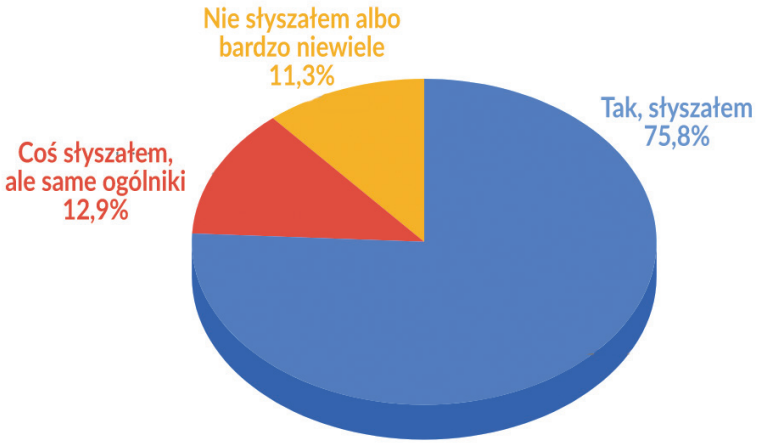
Część badanych osób wypracowała metody, które pozwalają z większą dozą bezpieczeństwa korzystać z finansów elektronicznych w miejscach publicznych, a mianowicie stosują suwak procentowy w aplikacji bankowej, który odzwierciedla stan konta w stosunku do ustalonej kwoty.



Rys. 17. Zachowanbia i emocje wśród osób sprawdzających konto bankowe w miejscach publicznych (n = 26)

2.2.5. Cyberataki

2.2.5.1. Czy słyszałeś o cyberatakach na finanse elektroniczne?



Rys. 18. Czy słyszałeś o cyberatakach na finanse elektroniczne? (n = 62)

Ponad 88% ankietowanych słyszało o cyberatakch na finanse elektroniczne, jednakże po analizie cytatów opisujących te informacje można odnieść wrażenie, że są to informacje szczątkowe, nieprecyzyjne, nieniosące ze sobą solidnej wiedzy, co należałoby zrobić, żeby uniknąć takiego ataku w przyszłości. Zaledwie 12,9% ankietowanych odpowiedziało szczątkowo na temat takich incydentów:

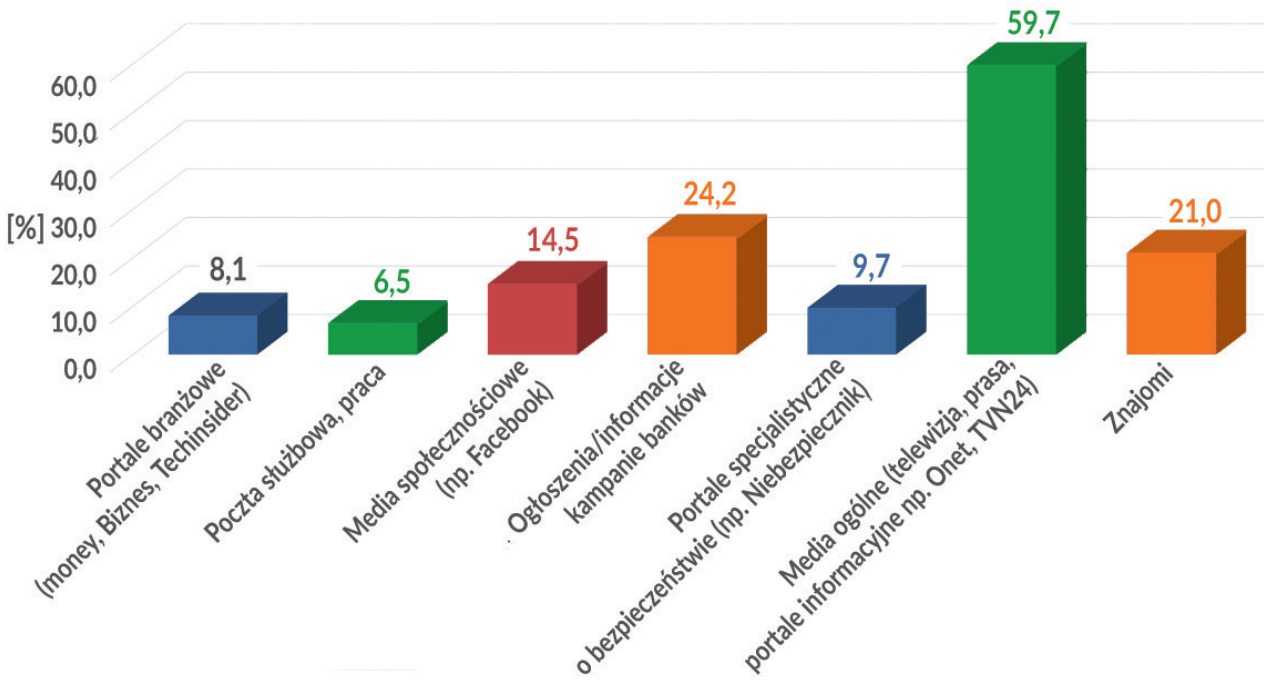
> Słyszałem o Sony, na Playstation wykradano numery kont.

> Czy wiesz z czego wynikają cyberataki na finanse? Z głupoty ludzi!!!
> Wyjmują 200 zł na ladę sklepową i liczą, że może się uda.

> Słyszałam z rodzinnej firmy, że przychodzi sms czasem do kogoś
> o treści „wyślij szybko 30 tysięcy na podane konto".
> Kilka razy się zdarzało.

> Oszustwa na OLX z podrobioną stronę banku, boję się również
> podmiany numeru konta podczas wykonywania przelewów.

2.2.5.2. Skąd czerpiesz wiedzę na temat bezpieczeństwa?



Rys. 19. Czy słyszałeś o cyberatakach na finanse elektroniczne? (n = 62)

Przeważającym źródłem informacji o cyberbezpieczeństwie są wśród badanych media ogólne(ok. 60%), takie jak internet (portale informacyjne) czy telewizja i prasa.

> A dowiedziałem się... Jakby to Ci powiedzieć, w wiadomościach czasem można to usłyszeć, że kody hakerzy łamią i z chmur znikają pieniądze.

Około 25% badanych deklaruje, że czyta ogłoszenia i informacje bankowe, wskazywałoby to na istotny kanał edukacyjny i informacyjny.

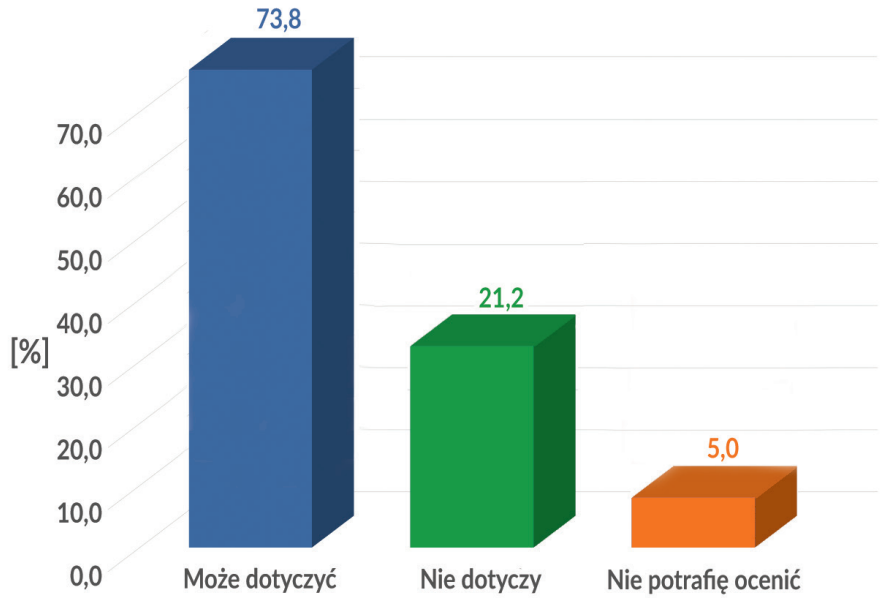
> Nie zwracam uwagi na bezpieczeństwo, chyba, że reklama banku zwraca na to uwagę, wtedy poświęcam trochę uwagi na zgłębianie tematu. Sama nie sprawdzam kanałów informacyjnych dotyczących bezpieczeństwa.

Ponad 20% badanych radzi się znajomych w kwestiach bezpieczeństwa, na ten kanał informacji nie można mieć bezpośredniego wpływu. Za to na media społecznościowe, które dla prawie 15% ankietowanych stanowią źródło informacji o bezpieczeństwie już tak. Adresując wymienione kanały komunikacyjne, można dotrzeć do większości różnych użytkowników, są to, zatem wyśmienite miejsca dla kampanii edukacyjnych i ostrzegających.

Komentarz autorów: *Są to nośniki informacji nieprofesjonalnej, ale ewidentnie należy je wykorzystywać, aby docierać do dużej grupy odbiorców, stąd banki powinny poświęcić im więcej uwagi prowadząc kampanie informacyjno-edukacyjne.*

Komentarz autorów: *Należy popracować nad formą wiadomości bankowych, ponieważ dla przeciętnego odbiorcy przekazywane tam treści są nieatrakcyjne i niezrozumiałe, przez co szybko traci uwagę i nie odnoszą one właściwego skutku.*

2.2.5.3. Czy uważasz, że cyberataki dotyczą również Ciebie?



Rys. 20. Czy uważasz, że cyberataki na finanse elektroniczne dotyczą również Ciebie? (n = 62)

Jak pokazano na powyższym wykresie ok. 74% osób uważa, że cyberataki mogą ich dotyczyć, dodatkową informacją są poniższe wypowiedzi:

> Tak, bo skoro ktoś (bank) autoryzuje czasem telefonicznie transakcje, to znaczy że dzieje się podejrzany ruch i bank chce przerzucić odpowiedzialność na klienta, więc pośrednio wierzę, że może to mnie dotyczyć.

> W tym momencie jakbym zostawiła gdzieś swoje dane, to nie czułabym się komfortowo. Ktoś mógłby chwilówkę na mnie wziąć.

> Ostatnio próbowali wyłudzić ode mnie okup na mailu, w zamian za nie upublicznienie informacji i nagrań, które podobno uzyskali hakując mnie, więc tak.

W pierwszej chwili wynik ten wygląda obiecująco, pokazuje, bowiem, że istnieje świadomość zagrożenia płynącego ze świata cyberprzestępczości. Niestety część z tych osób natychmiast bagatelizuje realność takich ataków poprzez stwierdzenia: „nie będę obiektem ataku, bo nie mam pieniędzy" (~11%) czy „nie obawiam się, bo dobrze się zabezpieczyłem" (~6,5%). Odzwierciedlają to odpowiedzi na następne pytanie wywiadu.

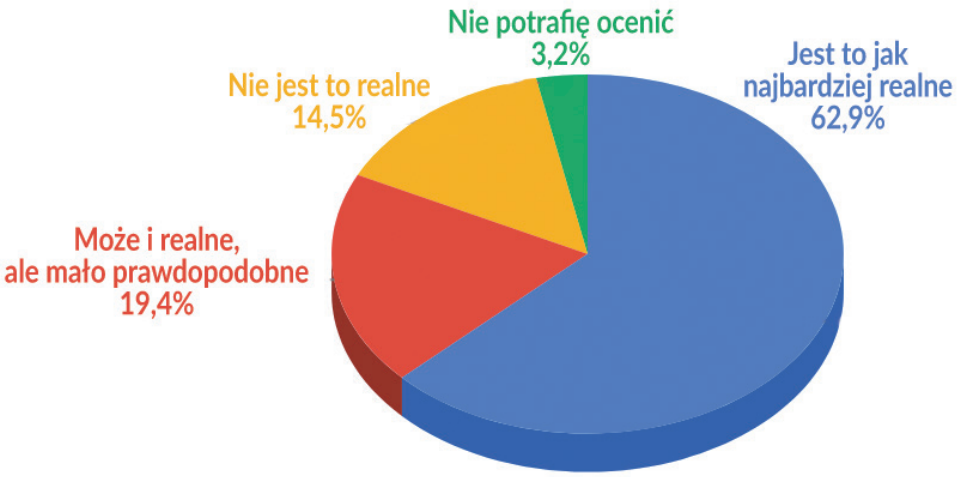
Spora część ankietowanych (ok. 21%) nie wierzy, że cyberataki ich dotyczą, argumentując swoją opinie zawartością kont bankowych:

> Nie – jestem za wielkim biedakiem, żeby mnie „cyberakakować", jak ktoś może takie rzeczy, to okradnie kogoś, komu można z konta ściągnąć 2 miliony.

> Nie, nie dotyczą, bo mam tak mało na koncie, ze nikt nie chce się włamywać. Raczej nie jestem dobrym celem. Nie kopie się leżącego.

Komentarz autorów: *Wnioski płynące z tych wyników są zatrważające, ponieważ spora grupa osób ewidentnie nie zdaje sobie sprawy, że mogą stać się obiektem ataku cyberprzestępców i że wcale nie trzeba mieć dużych pieniędzy ani być kimś ważnym. Ewidentnie brakuje im świadomości jak takie ataki przebiegają i że w większości przypadków nie są targetowane, a zautomatyzowane, oparte o phishing i instalację malware na urządzeniach ofiar.*

2.2.5.4. Czy uważasz, że zagrożenie cyberatakami na Twoje finanse elektroniczne jest realne?



Rys. 21. Czy uważasz, że zagrożenie cyberatakami na Twoje finanse elektroniczne jest realne? (n = 62)

Jak obrazują odpowiedzi na to pytanie, przeważająca grupa badanych (ok. 63%) uważa, że zagrożenie cyberatakami na ich prywatne finanse jest jak najbardziej realne. W porównaniu z poprzednim pytaniem dotyczącym cyberataków (ok. 74% pozytywnych odpowiedzi) obserwujemy spadek pewności odpowiedzi. Badani uzasadniają swoje obawy w stwierdzeniach:

> Tak, mogę być celem takich ataków i są one realne, w końcu korzystam z internetu, a dodatkowo na pewno są metody ataku o których nie wiem.

> Jak najbardziej są one realne. Chociaż tak się kojarzą bardziej w Stanach, ale w Polsce nie ma tak, w Polsce podobno ma najlepsze zabezpieczenia bankowe. Tam chyba sie podpisuje paragon w USA. Dziwne to.

> Tak, przecież ludzie na tym zarabiają, opowiem historię jak to ktoś dostał telefon niby za wieloletnie uznanie w pracy, a to przez złodziei, telefon przesyłał wszystkie dane.

> One się cały czas dzieje, więc jak najbardziej tak. Mam przyjaciela który, mimo że studiuje IT, to i tak nie wierzy w te rzeczy, co jest dla mnie totalna głupota. Interesuje się bezpieczeństwem i wiem, że takie ataki są bardzo realne. Opowiadałem mu różne nawet nie IT sposoby wyłudzania pieniędzy, a on się trochę śmiał, co dla mnie było bardzo głupie. Tak jak mówiła mi jedna osoba, potwierdza się teza, że nawet jeśli ktoś dobrze się zna na informatyce, to może kompletnie nic nie wiedzieć o bezpieczeństwie.

Komentarz autorów: *Wynik ten jest obiecujący, ponieważ ilustruje obecność wśród ankietowanych obawy związanej z realnością ataków płynących z cyberprzestrzeni, jednakże w istocie jest dalece odbiegający od percepcji prawdziwego poziomu zagrożenia, który może dotyczyć właściwie każdego, kto istnieje w przestrzeni internetu i korzysta z jakichkolwiek usług.*

Niestety, wciąż spora grupa osób (ok. 34%) uważa realność wymienionych ataków za znikomą, bądź wręcz wykluczoną, uzasadniając to wypowiedziami:

> Jestem płotką, nie jestem atrakcyjną ofiarą ataku, taki atak musiałby być targetowany.

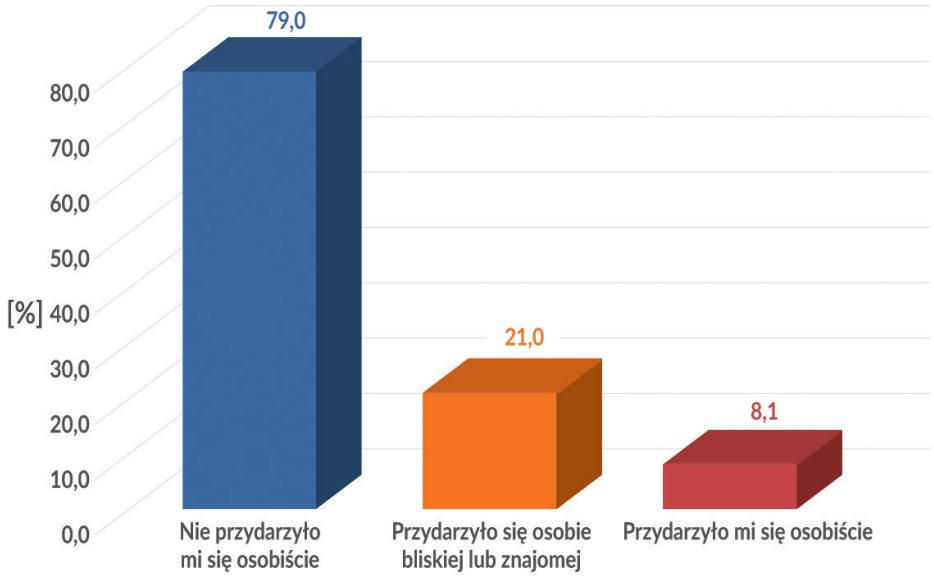
> Jak z rozpędu kliknę w link albo ściągnę keygen, ale mam podejrzenia co do maili jak zaczynają się od „I am the prince" albo „Publish with us".

> Realny, ale mało prawdopodobny, ufam swojemu bankowi.

> Nie mam pojęcia, raczej nie są to ataki sprecyzowane na konkretnej osobie, chyba, że są to osoby majętne.

Komentarz autorów: *Po przeanalizowaniu odpowiedzi badanych nasuwa się wniosek, że użytkownicy nie zastanawiają się na co dzień nad kwestiami bezpieczeństwa, więc ich ocena zagrożenia jest zbyt optymistyczna. Wiąże się to również z brakiem osobistego doświadczenia krzywdy, co ilustruje wynik badania w następnym pytaniu. Badani żyją w przeświadczeniu, że jeśli coś jest nienamacalne i ich nie dotknęło, to tak będzie dalej. Ewidentnie w odpowiedziach badanych widać brak ich świadomości w kwestiach zagrożeń cyberprzestrzeni i mechanizmów ich działania.*

2.2.6. Czy stałeś się osobiście, bądź ktoś bliski z Twojego otoczenia ofiarą cyberataku na finanse? Co czułeś? Co czuła ta osoba?



Rys. 22. Czy stałeś się osobiście, bądź ktoś bliski z Twojego otoczenia, ofiarą cyberataku na finanse? (n = 62)

Odpowiedzi na to pytanie są niezwykle istotną wskazówką, pokazują bowiem, że prawie 80% respondentów nie doświadczyło krzywdy i nie stało się ofiarą cyberataku na swoje finanse.

Ponad 21% badanych deklaruje, że przykre incydenty związane z cyberatakami wystąpiły w ich rodzinach lub u znajomych, te doświadczenie powinny ich uczulić na kwestie bezpieczeństwa, nie są to jednak ich własne doświadczenia, zatem oddziaływanie takich sytuacji jest znacznie mniejsze. Opisy tych sytuacji możemy przeczytać poniżej:

> Aaaa, właśnie, wczoraj na grillu znajoma znajomej opowiadała, ze jej koleżanka, miala sytuacje, że ukradli jej konto na fejsie, a następnie prosiła (tzn. atakujący) o hajs, aby wysłać blikiem, i to były kwoty 600–1000 zł. 2 osoby tak uczyniły, ale co w tym wszystkim jest najśmieszniejsze, to były osoby z którymi ona nie miała prawie kontaktu.

> Nie mnie, ale znajomej zhackowali kompa, podszyli się pod helpdesk i wyłudzili hasła do zdalnego dostępu oraz wykradli poufne informacje, bardzo źle się czuła, że tak dała się podejść.

Komentarz autorów: *Brak takiego bezpośredniego i silnego doświadczenia sprawia, że ich percepcja zagrożenia jest mniej realna, trudno im sobie wyobrazić jak miałaby wyglądać ich sytuacja i jakie emocje by im towarzyszyły. Jest to również powiązane z brakiem zastanawiania się nad kwestiami bezpieczeństwa cyberprzestrzeni w codziennym życiu. Łatwo sobie wyobrazić, co stanie się, gdy nie zamkniemy mieszkania i stracimy dobytek życia, zdecydowanie trudniej myśleć o wirtualnych pieniądzach i kontach bankowych, które są nienamacalne i dalekie.*

8,1% badanych doświadczyło krzywdy w wyniku cyberataku, ich nastawienie oraz podejście do kwestii bezpieczeństwa zmieniło się diametralnie. Przykłady związane z wyłudzeniami i stratami finansowymi ilustrują poniższe przypadki:

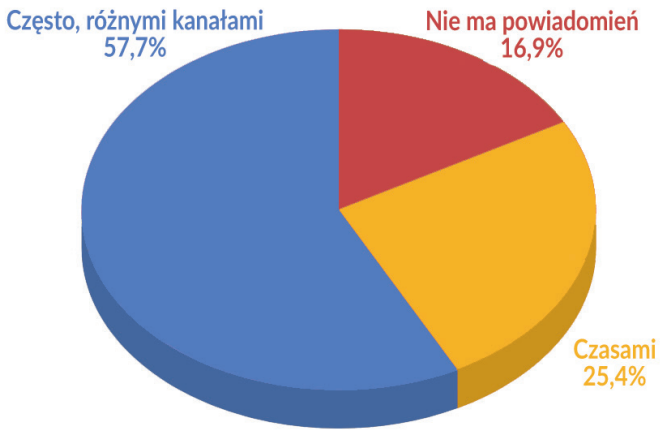
> Cyberatak nie, ale fałszywy bankomat tak. Miał podkładkę i co miesiąc ktoś pobierał sobie 5 zł. Zdenerwowana byłam, niby 5 zł miesięcznie, ale to przez rok było. Tam sporo ludzi mogło zostać oszukanych, to tylko 5 zł.

> Tak – po płatności kartą w jakimś sklepie. Potem ktoś płacił tymi danymi z karty za jakieś zakupy na chińskiej stronie.Bank potem oddał pieniądze. Czułam się potem zagrożona, otworzyło mi to bardzo oczy. Potem dużo lepiej się starałam zabezpieczyć.

> Finanse nie, ale dałam sobie wyłudzić dane podczas próby naciągnięcia na prywatne usługi medyczne – w ostatniej chwili powstrzymałam się przed podpisaniem umowy, ale naciągacz odszedł z kartką wypełnioną moimi danymi osobowymi, dziwnie się z tym czułam, ale nic z tym nie zrobiłam.

2.2.7. Zasady bezpieczeństwa

2.2.7.1. Czy Twój bank ostrzega Cię przed cyberatakami?



Rys. 23. Czy Twój bank ostrzega Cię przed cyberatakami? (n = 59)

Bardzo ważną rzeczą jest, aby dbać o świadomość użytkowników bankowości elektronicznej. Powinni być oni na bieżąco informowani o atakach, na które mogą być narażeni. W przeciwnym razie w prosty sposób mogą stać się ofiarami. Na pytanie „Czy Twój bank ostrzega Cię przed cyberatakami?" Aż ~83% badanych stwierdziło, że tak. Jest to pozytywna informacja, jednak należy zadbać, aby ten wskaźnik cały czas wzrastał, ponieważ to oznacza, że do pozostałej części ~17% powiadomienia nie są wysyłane lub są one publikowane w formie, która pozostaje niezauważona przez użytkowników.

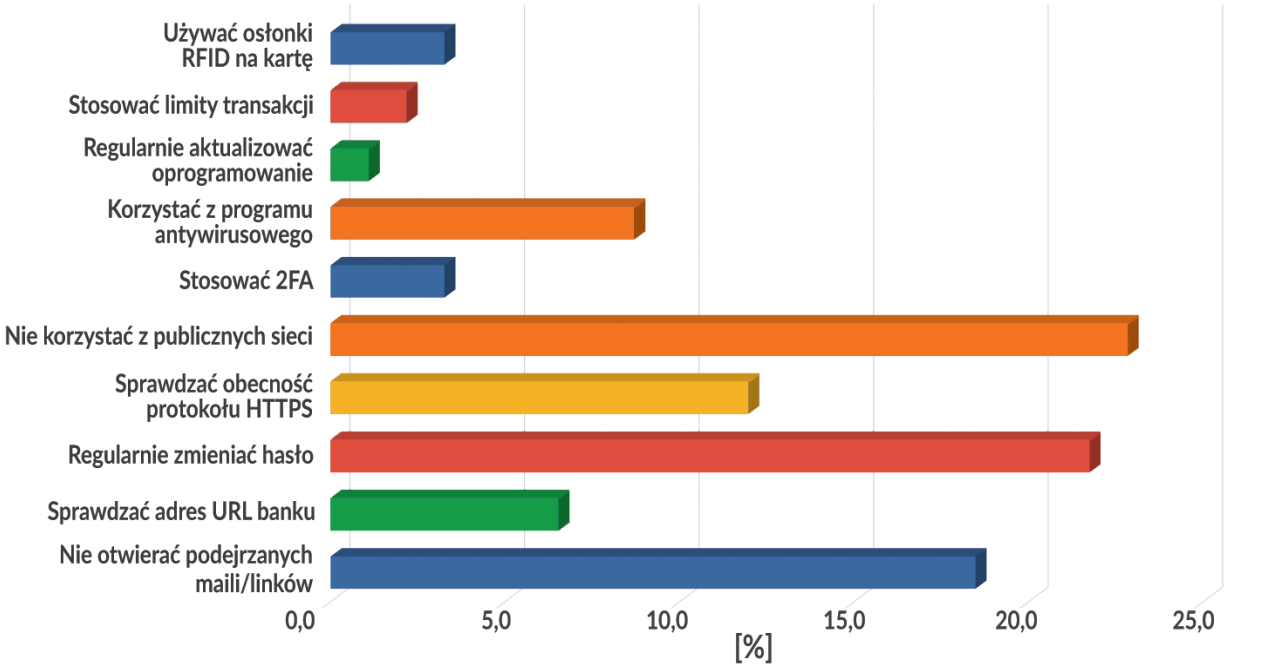
Podczas odpowiedzi na pytanie została zauważona przypadłość, na którą trzeba zwrócić szczególną uwagę. Około 22% badanych użytkowników, którzy stwierdzili, że otrzymują powiadomienia otwarcie przyznaje, że nie czyta tych informacji. Potwierdzają to poniżej uzyskane odpowiedzi podczas przeprowadzonych wywiadów:

> Tak informuje. Za często nawet. Denerwuje mnie juz to i przestałem to czytać.

> Coś tam jakieś informacje wysyłają, ale tego i tak się nie czyta.
> Jakieś powiadomienia sa w aplikacji od konta.

> Zapewne umieszcza informacje o zasadach bezpieczeństwa na swojej stronie, jednak nigdy nie mam czasu tam zajrzeć.

2.2.7.2. Jakie znasz zasady bezpieczeństwa?



Rys. 24. Jakie znasz zasady bezpieczeństwa?

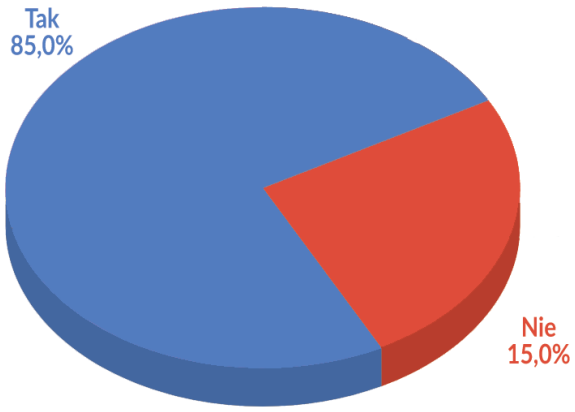
Z uzyskanych odpowiedzi wynika, że duża część respondentów jest świadoma, aby stosować silne hasła oraz regularnie je zmieniać.

> Dobrze mieć niepowtarzalne hasło, raczej inne niż do domofonu.

Równie popularne wskazania dotyczyły tego, aby unikać otwierania podejrzanych maili oraz linków. Pozwala to m.in. uniknąć wprowadzenia danych logowania na spreparowanej stronie. Przebadane osoby nie korzystają z publicznych sieci podczas korzystania z bankowości elektronicznej obawiając się przechwycenia wrażliwych danych. Zdecydowanie najmniej wskazań uzyskała opcja „Regularnie aktualizowanego oprogramowania", jednak wyni-

ka to z tego, że zdecydowana część badanych korzysta z automatycznych aktualizacji i na co dzień nie musi o tym pamiętać. Dość małą popularnością cieszyła się zasada, aby sprawdzać adres URL strony banku. Część badanych wykorzystuje zakładki w przeglądarce, dzięki czemu nie musi wpisywać samodzielnie adresu. Natomiast częstym zachowaniem jest wpisywanie nazwy banku w wyszukiwarce Google i wybranie linku, który znajduje się na pierwszym miejscu z wyszukanych pozycji. Takie zachowanie w połączeniu z brakiem weryfikacji adresu może prowadzić do niebezpiecznych sytuacji.

2.2.7.3. Czy kojarzysz jakieś formy wyłudzania danych?

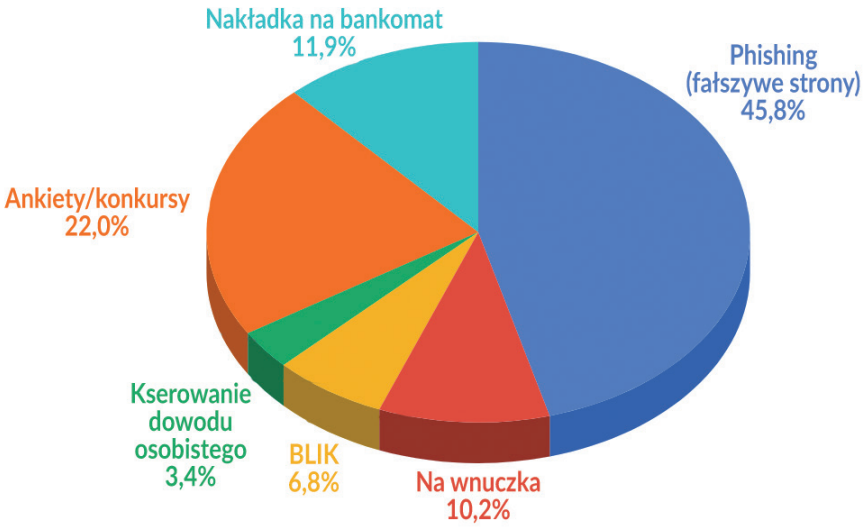


Rys. 25. Czy kojarzysz jakieś formy wyłudzania danych? (n = 60)

Około 15% osób otwarcie przyznało, że nie zna żadnych form wyłudzenia danych.

> Jak w Starbucksie się pytają o imię... A tak to nie.

> Tak coś tam kojarzę, ale nic konkretnego. Chyba chodzi o to, że ktoś posługuje się twoimi danymi i bierze kredyt na Twoje nazwisko.



Rys. 26. Jakie formy wyłudzenia danych kojarzysz?

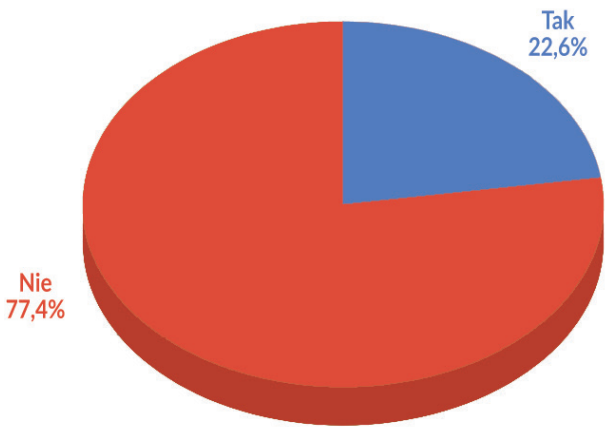
Wśród wymienionych form wyłudzeń danych znalazły się zarówno fizyczne, jak i wirtualne metody. Do fizycznych, które według odpowiedzi stanowią łącznie ok. 1/4 wskazań, można przypisać metodę „na wnuczka", kserowanie dowodu osobistego i stosowanie skimmerów w bankomatach. Jednak zdecydowanie najpopularniejszą formą wśród badanych jest phishing, który uzyskał prawie 46%.

> Kradzież danych ze stron, to coś z czego się boję. Za czasów studenckich wszędzie brali mój PESEL, od kontrolerów do dziekanatu. Źle się czułam podając publicznie takie dane.

> Nie wiem jak do końca nazywa się to przestępstwo, ale teraz dużo ludzi podszywa się pod znajomych na facebooku i prosi o szybki przelew BLIKIEM.

Niepokojąco rzadko została wymieniona możliwość kserowania dowodu osobistego, jako formy wyłudzenia danych. Problem z tego typu zachowaniem miała rozwiązać „Ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych" [4], jednak kserowanie dokumentu dalej będzie możliwe.

2.2.7.4. Czy doświadczyłeś wyłudzenia danych? Co wtedy zrobiłeś?



Rys. 27. Czy doświadczyłeś wyłudzenia danych? (n = 53)

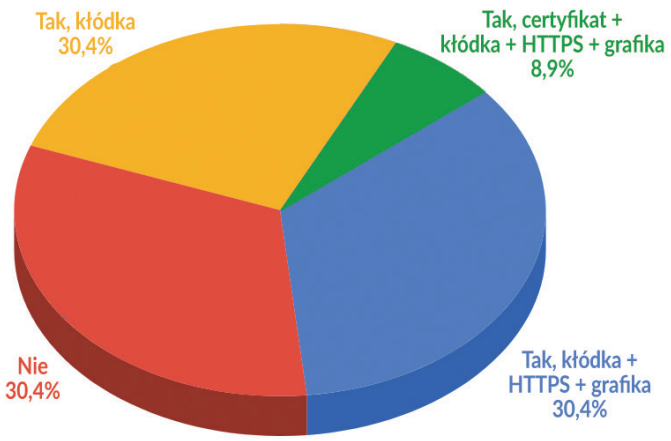
Ponad 77% przebadanych osób nie doświadczyło wyłudzenia danych. Jednak przy odpowiedziach pojawiały się również wątpliwości, że mogli paść ofiarami tylko nie odczuli jeszcze skutków tego zdarzenia. Badani mają małą świadomość, że oszust chętnie wykorzysta dane osobowe innej osoby, aby osiągnąć korzyść, np. w postaci w złożenia wniosku o kredyt.

> Skąd mam wiedzieć. Może ktoś to zrobił, ale o tym nie wiem.

Jednak znalazły się również takie osoby, które padły ofiarami wyłudzeń danych i doświadczyły skutków tego zdarzenia.

> Tak, zarejestrowałem się do przychodni medycznej, a po 3 dniach dzwoni do mnie Fabryka Zdrowia z ofertami dot. mojego stanu zdrowia, nic nie zrobiłam, bo wiem, że jest to narzędzie sprzedaży, którego sama używam.

2.2.7.5. Jak weryfikujesz stronę banku?



Rys. 28. Czy weryfikujesz stronę banku? (n = 56)

Około 30% przebadanych użytkowników stwierdziła, że w ogóle nie weryfikuje strony swojego banku. Osoby, które przeprowadzają weryfikacje głównie sprawdzają obecność „kłódki" przy adresie strony bankowej oraz szatę graficzną, a jedynie 9% osób sprawdza dodatkowo certyfikat.

Niepokojącym zjawiskiem jest to, że osoby, które przeprowadzają weryfikację nie mają odpowiedniej wiedzy czy jest to wystarczający zabieg. W związku z tym odczuwają niepokój przy korzystaniu z elektronicznych rozwiązań, ponieważ nie są pewni czy to gwarantuje im bezpieczeństwo.

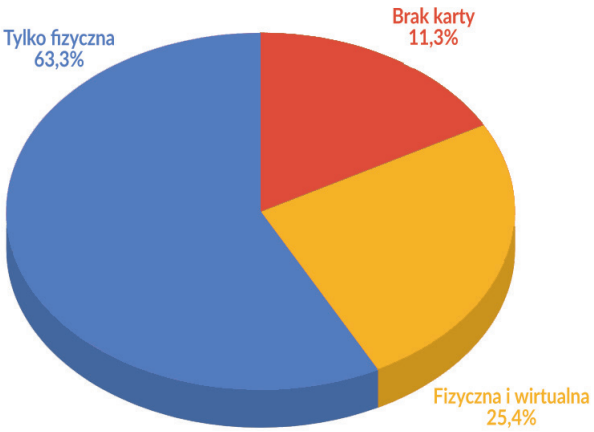
> Mam zapisaną zakładkę z bankiem, więc chyba nie da się, żeby ktoś mi to podmienił.

> Jeśli wygląda jak strona banku to wchodzę, raczej sprawdzam zieloną kłódkę. Gdyby nie było kłódki, może bym się zalogowała, ale nie wiem czy bym zrobiła jakąś płatność.

> Zawsze wpisuję pełny adres i sprawdzam czy jest ta kłódka. Aczkolwiek nie wiem na ile to gwarantuje mi bezpieczeństwo.

2.2.8. Karty płatnicze

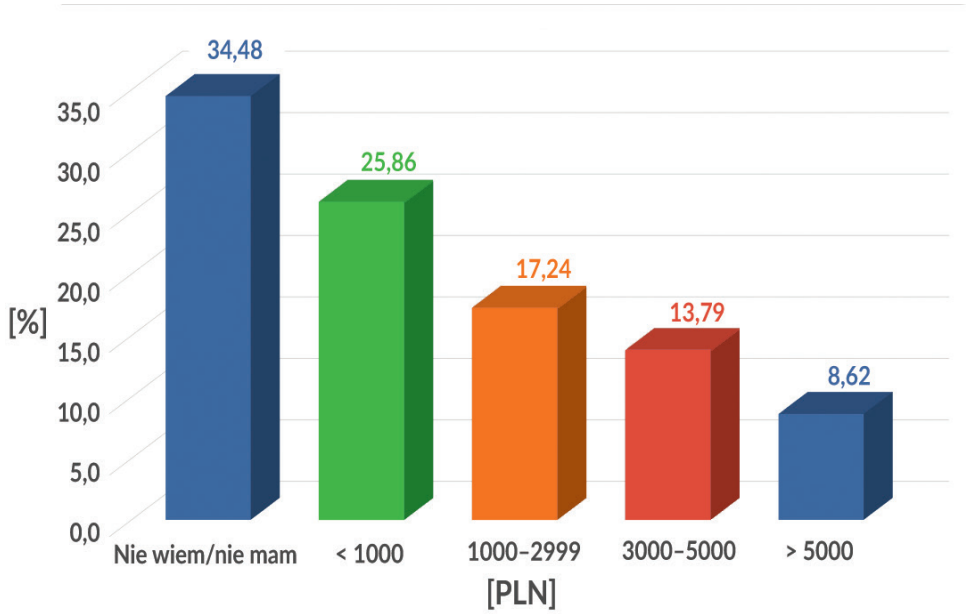
2.2.8.1. Jakie masz karty płatnicze (fizyczne i wirtualne)?



Rys. 29. Jakie karty płatnicze posiadasz? (n = 49)

63% osób spośród badanych wskazuje, że posiada jedynie fizyczne karty płatnicze. Ok. 25% ankietowanych używa zarówno kart fizycznych, jak i wirtualnych, ale wśród badanych są także osoby, które nie posiadają żadnej karty.

2.2.8.2. Jakie masz ustawione limity płatności/transakcji?



Rys. 30. Jakie masz limity? (n = 58)

Prawie 1/3 osób odpowiedziała, że nie korzysta lub nie wie czy ma ustawiony jakikolwiek limit płatności. Powodem, dla którego tak znaczna część nie jest w stanie wskazać konkretnych wartości jest to, że ustawione limity są zbyt wysokie, a to powoduje, że nigdy nie spotkali się z tym mechanizmem.

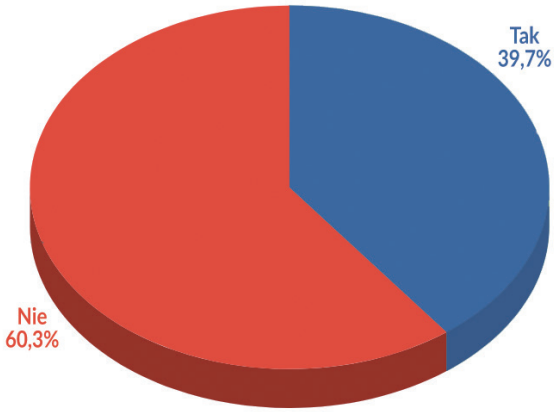
> Oj nie pamiętam, ale chyba dosyć spore.

> Bardzo wysokie, gdyż mi to przeszkadzało. Jednak trzymam tam niewielkie środki.

> Nie używam limitów płatności lub są bardzo wysokie (żeby płacić ile chce). Raz korzystałem, ale trzeba było odblokowywać, aby korzystać, więc je wyłączyłem, żeby było szybciej.

Komentarz autorów: *Częstym przypadkiem jest sytuacja, w której użytkownik potrzebuje jednorazowo zrealizować płatność lub wypłatę gotówki, której kwota znacznie przekracza ustawiony limit i w takim przypadku zwiększa go, aby móc zrealizować swoje żądanie. Niestety po zakończonej płatności użytkownik najczęściej nie pamięta lub nie chce ponownie ustawić niższego limitu, ponieważ w przyszłości chce uniknąć potrzeby modyfikowania ustawień w celu zwiększenia wygody.*

2.2.8.3. Czy korzystasz z płatności zbliżeniowych (NFC)?

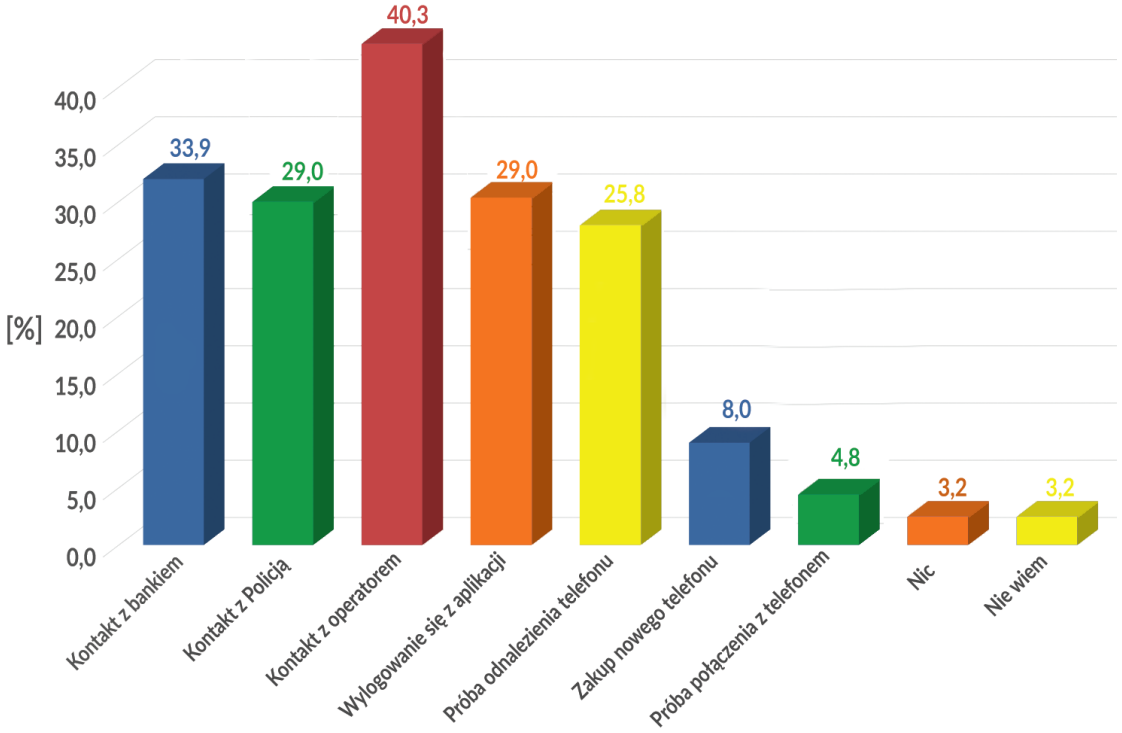


Rys. 31. Czy korzystasz z płatności zbliżeniowych (NFC)? (n = 58)

60% osób, które udzieliły odpowiedzi, korzysta z płatności zbliżeniowych NFC.

Komentarz autorów: *Niestety znaczna część badanych nie rozumie czym jest płatność NFC oraz, że do takiego modelu należy płatność zbliżeniowa kartą płatniczą, ale także zegarkiem. Według badanych płatność NFC utożsamiana jest jedynie z płatnością telefonem.*

2.2.9. Co byś zrobił/zrobiła w przypadku zgubienia telefonu?



Rys. 32. Co byś zrobił/zrobiła w przypadku zgubienia telefonu? (n = 62)

Pierwszą myślą, która przychodziła do głowy ankietowanym był kontakt z operatorem (40.3%), tuż po tym był kontakt z bankiem (33.9%). Odpowiedzi te sugerują, że telefon komórkowy staje się coraz częściej tożsamy z narzędziem płatniczym, dlatego ankietowani w tak dużej części opowiedzieli się za poinformowaniem swojego banku o zgubieniu telefonu. W ramach tego pytania jedna osoba wspomniała o jednej z obaw związanych z utratą telefonu:

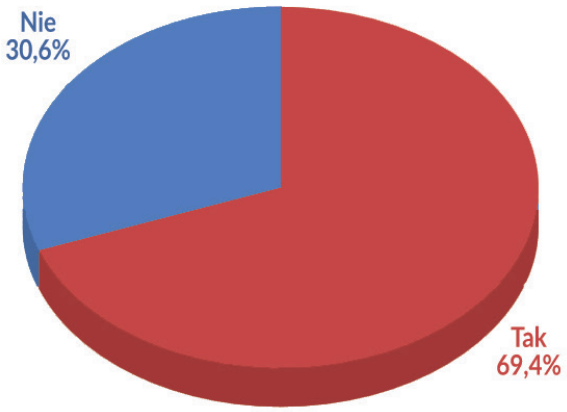
> Może mi grozić kradzież tożsamości, ktoś mógłby zobaczyć moje prywatne rzeczy, boję się „fałszywego porno" – doklejenie twarzy z mojego normalnego zdjęcia do czegoś erotycznego i puszczenie w sieć...

> Ten, co posiadam obecnie, nie przechowuje wrażliwych danych. Gdybym zgubił tablet musiałbym zmienić aplikację, która generowałaby token. Jedyne co ma zapisane to pin do karty, ale w taki sposób że nikt się nie zorientuje. Pin jest zapisany w postaci numeru telefonu pod jakimś wymyślonym nazwiskiem, tylko ja wiem, które cyfry są pinem do karty.

> Jest też możliwość zlokalizowania telefonu za pomocą różnych aplikacji jednak nie korzystam z takiej możliwości, nie przekonuje mnie to za bardzo, chociaż i tak nas wszędzie śledzą.

2.2.10. Autoryzacja dwuskładnikowa

2.2.10.1. Czy słyszałeś o autoryzacji dwuskładnikowej (2FA)?



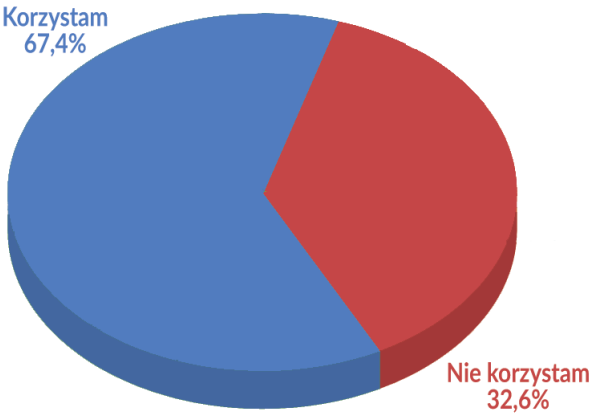
Rys. 33. Czy słyszałeś o autoryzacji dwuskładnikowej (2FA)? (n = 62)

Jak się okazało, spośród osób, które słyszały o 2FA (69% os.), 24% badanych nie miało wiedzy na temat 2FA. Dopiero po wyjaśnieniu ankietujących, badani często uświadamiali sobie, że jednak znają i nawet korzystają z tego rozwiązania.

Niektórzy użytkownicy nie są zaznajomieni z nazwami rozwiązań, z których korzystają. Powodem takiego stanu rzeczy może być stosowanie przez banki zbyt powierzchownych – opisowych nazw rozwiązań, jak również fakt, że wielu badanych użytkowników bankowości elektronicznej nie poszerza swojej wiedzy w dziedzinie bezpieczeństwa.

Komentarz autorów: *Istotne jest, by instytucje bankowe nie tylko w sposób jasny, ale także niestrywializowany informowały użytkownika o wykorzystywanych rozwiązaniach. Krótkie, ale rzetelne wyjaśnienie mogłoby zachęcić do dokładniejszego poznania jak dany system, dana metoda (np. uwierzytelnienia) działa.*

2.2.10.2. Czy korzystasz z autoryzacji dwuskładnikowej (2FA)?



Rys. 34. Czy korzystasz z autoryzacji dwuskładnikowej (2FA)? (n = 43)

Większość ankietowanych korzysta z 2FA:

> Tak ciągle, bo warto, nawet jeśli czasem jest to irytujące.

Zdarzają się jednak sceptyczne głosy:

> Raczej nie, z lenistwa nie chce mi się tego konfigurować i dodawać sobie dodatkowych zadań.

Komentarz autorów: *Pytanie zostało zadane grupie ankietowanych, którzy w poprzednim pytaniu zadeklarowali znajomość autoryzacji dwuskładnikowej. Analizując odpowiedzi na powyższe pytanie, można zauważyć pewien brak konsekwencji badanych. Wiele osób chce korzystać z dodatkowych zabezpieczeń, mimo że mogą być one mniej wygodne niż, np. jednoskładnikowa autoryzacja. Znajdą się oczywiście osoby, które nie chcą korzystać z dodatkowych zabezpieczeń, ponieważ kojarzy im się to z problemem, a nie zabezpieczeniem. Potrzeba zatem popularyzacji autoryzacji takich jak biometria, która jest wygodnym i skutecznym sposobem potwierdzania tożsamości. Podobne wnioski wysunięto w wynikach badań przeprowadzonych przez firmę MasterCard*[12].

[12] https://newsroom.mastercard.com/eu/pl/press-releases/badanie-mastercard-biometria-stanie-sie-nowym-standardem-potwierdzania-tozsamosci-w-platnosciach/

2.2.10.3. Czy korzystałbyś/korzystałabyś z autoryzacji dwuskładnikowej, gdyby była ona bardziej dostępna?

Rys. 35. Czy korzystałbyś/korzystałabyś z autoryzacji dwuskładnikowej, gdyby była ona bardziej dostępna? (n = 62)

> Odkąd zacząłem używać tego, nie wyobrażam sobie nie używać tego w znaczących i dotkliwych dla mnie serwisach.

> Wiem, że można, ale to chyba zbyt duże zabezpieczenie w stosunku do środków, jakimi obracam.

> Chyba nie, bo to zajmuje chwile czasu. Chociaż w sumie do logowania do banku ze względów bezpieczeństwa byłaby taka funkcja wskazana.

> Raczej nie, mam porządne hasła.

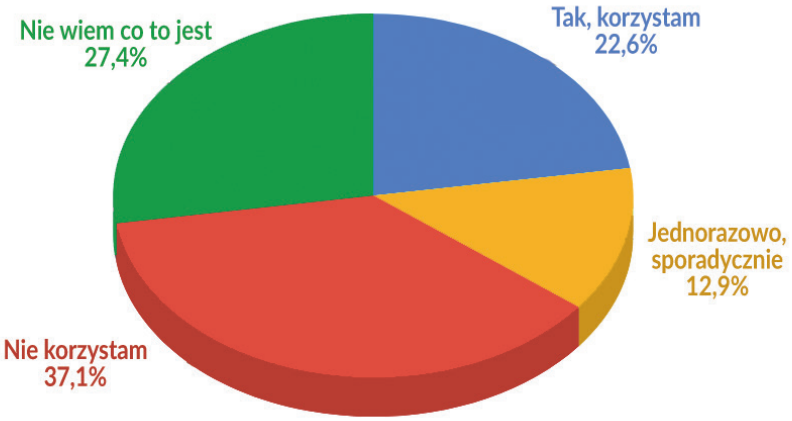
Komentarz autorów: *Rozwiązania bezpieczeństwa są tworzone uniwersalnie, ponieważ bezpieczeństwo każdego użytkownika bankowości jest ważne, niezależnie od ilości pieniędzy, którymi dysponuje. Nie ma niestety idealnych systemów, więc trzeba czasem znaleźć równowagę pomiędzy różnymi czynnikami. Przykładowo, trzeba poświęcić dodatkową minutę lub dwie na wykonanie kolejnego kroku uwierzytelnienia, by znacznie zwiększyć swoje bezpieczeństwo.*

Przeważająca część ankietowanych (61,3%) mówi, że skorzystałaby z autoryzacji dwuskładnikowej, gdyby była bardziej dostępna. To może wskazywać na fakt, iż większość użytkowników jest skłonna do zwiększania swojego bezpieczeństwa.

Jednak 27,4% ankietowanych deklaruje przeciwnie. Jest to uwarunkowane różnymi przekonaniami. Jedni uważają, że dodatkowe zabezpieczenie jest działaniem zbyt intensywnym w stosunku do środków, które posiadają, inni natomiast traktują je jako rzecz uciążliwą i niekoniecznie potrzebną.

2.2.11. Platforma ePUAP

2.2.11.1. Czy korzystasz z usługi ePUAP?



Rys. 36. Czy korzystasz z usługi ePUAP? (n = 62)

Badani w przeważającej większości nie korzystają z usługi platformy ePUAP (64,5%), z czego prawie połowa tych osób (27,4% ogółu) nie wie, co to jest za platforma i do czego służy. Wynik ten świadczy o małej penetracji rynku wykorzystania usług cyfrowych przez obywateli na rzecz administracji publicznej. Z informacji Ministerstwa Cyfryzacji wynika, że 4 mln Polaków ma założony Profil Zaufany[13]. Ich przyczyny to przede wszystkim niewystarczająca edukacja obywatela w tym zakresie oraz przeciętna jakość wykonania platformy i problemy z jej działaniem[14], a także brak zaufania do rozwiązania rządowego. Można je zilustrować następującymi stwierdzeniami:

> Tak, ale błędy błędy, np. przy składaniu wniosków o nowe dowody osobiste, już 3 razy do mnie dzwonili i kazali nowe dokumenty składać.

> „Nie nie korzystam, to jest jakiś (myśli patrząc się w około) pewnie urzędowa platforma, ale nie wiem dokładnie, co to jest." - Jak dowiedział się o opcji logowania przez bank, to się skrzywił i powiedział, że na pewno by tego nie zrobił.

> Korzystałam z tego. PIT rozliczałem, inne sprawy też załatwiam.

Komentarz autorów:
Podobny efekt spowodowała konieczność składania sprawozdań do KRS-u przez system elektroniczny wymagający albo podpisu kwalifikowanego, albo podpisu profilem zaufanym członków zarządu[15].

[13] https://www.gov.pl/web/cyfryzacja/4-miliony-polakow-ma-juz-profil-zaufany
[14] https://www.computerworld.pl/news/Nie-uzywam-profilu-zaufanego-na-ePUAP,382785.html
[15] https://www.michalin.pl/jak-podpisac-sprawozdanie-finansowe-profilem-zaufanym-epuap/

W wyniku badań stwierdzono jednoznacznie, że uruchomienie rozliczania zeznania rocznego PIT w formie elektronicznej w roku 2019, spowodowało zwiększenie wykorzystania profilu zaufanego i tym samym przyczyniło się do skorzystania z usługi ePUAPu. Z 12,9% badanych, którzy deklarowali użytkowanie sporadyczne bądź jednorazowo, ponad trzy czwarte wykorzystało platformę do rozliczenia się z urzędem skarbowym.

2.2.11.2. Czy masz włączone potwierdzanie logowania SMS/ kodem w ePUAP?

Rys. 37. Czy masz włączone potwierdzanie logowania SMS kodem w ePUAP? (n = 22)

Podczas weryfikacji poziomu użycia weryfikacji dwuskładnikowej (2FA) wśród użytkowników platformy, okazało się, że zaledwie 18,2% badanych świadomie z niej korzysta, 31,8% nie wie lub nie pamięta, co najprawdopodobniej przekłada się na brak użycia (ponieważ standardowo jest ona wyłączona). Tak duża frakcja badanych (prawie jedna trzecia użytkowników platformy) nie jest świadoma istotności zabezpieczania swojego profilu obywatela dodatkowym mechanizmem. Jeśli przyjrzymy się grupie sporadycznych użytkowników ten procent gwałtownie wzrośnie – aż do 50% użytkowników.

Rys. 38. Czy masz włączone potwierdzanie logowania SMS kodem w ePUAP? (osoby korzystające sporadycznie)

2.2.11.3. Czy korzystasz z opcji „zaloguj przez bank” w ePUAP?

Rys. 39. Czy korzystasz z opcji “zaloguj przez bank” w ePUAP? (n = 22)

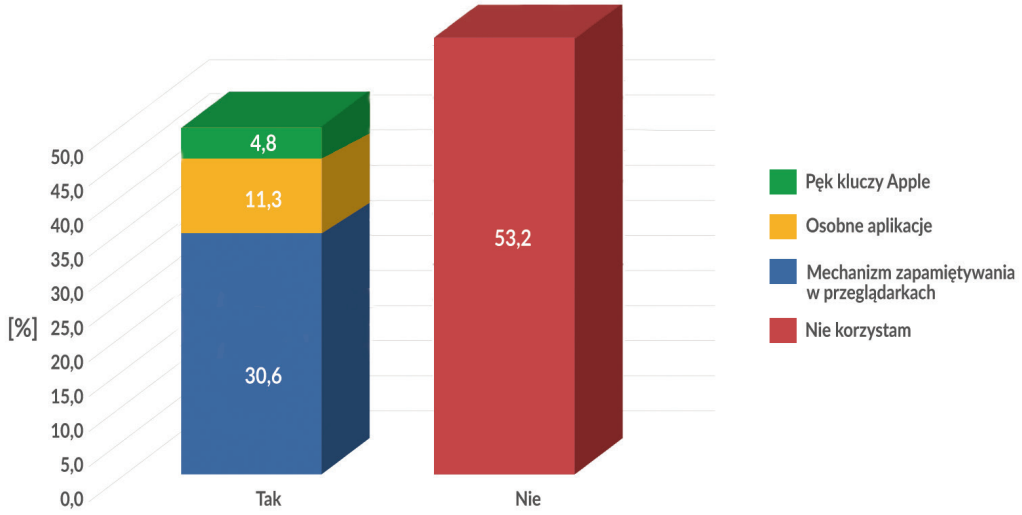
Jak można zauważyć ponad połowa użytkowników usługi ePUAP (54,5%) wykorzystuje możliwość zalogowania się do niej przez swojego dostawcę usług bankowych. Jako zalety tego rozwiązania wymieniają przede wszystkim wygodę i szybkość oraz zaufanie do swojego banku. Poniższe stwierdzenia opisują nastawienie użytkowników:

> Tak, najprościej oraz wierzę w bezpieczeństwo zapewnione przez bank.

> Tak, korzystam z „zaloguj się przez Bank”, taki gdzie nie mam $, a mam kredyt, dlaczego? Bo dobrze działa w Pekao SA.

Komentarz autorów: *Powyższa obserwacja nasuwa wniosek, że wykorzystanie instytucji bankowych do zarządzaniem tożsamością oraz jej weryfikacją może być skutecznym i społecznie akceptowalnym rozwiązaniem.*

2.2.12. Czy korzystasz z aplikacji (na telefonie/komputerze) do przechowywania haseł/PIN-ów do logowania/ uwierzytelniania?



Rys. 40. Czy korzystasz z aplikacji (na telefonie/komputerze) do przechowywania haseł/PIN-ów do logowania/uwierzytelniania? (n = 62)

Badani prawie w równym stopniu korzystają i nie korzystają z mechanizmów do przechowywania i zarządzania hasłami do usług uwierzytelniania. Pośród osób, które deklarują wykorzystanie takich mechanizmów (46,7%), największą popularnością cieszy się zapamiętywania haseł w przeglądarce (ponad 66% przypadków użycia). Pula użytkowników rozwiązań firmy Apple stosuje pęk kluczy (10% przypadków użycia). Ponadto, osoby które używają wspomnianych rozwiązań zaznaczają, że nie do zastosowań bankowych! Nastawienie badanych do mechanizmów i narzędzi wspomagających proces zapamiętywania haseł i kluczy do usług uwierzytelniania opisuję m.in. poniższe stwierdzenia:

> Nie, nie wiedziałam, że takie istnieje.

> Nie, wierzę w swoją pamięć i kartki papieru, rozłożonych w różnych miejscach (rozproszenie jest złe), niewidoczne na pierwszy rzut oka. Ponadto kartki są wygodniejsze dla niego, przyzwyczajenie.

> Nie korzystam, i nie uważam żeby było to bezpieczne. Ktoś wymyślił tę aplikację, w jakiś sposób łączy się to z internetem i może w jakiś sposób te dane nie mogą wypłynąć.

> Nie mam żadnego programu do zarządzania hasłami, ponieważ raczej takim aplikacją nie ufam tak szczerze, bo zawsze istnieje możliwość żeby jakoś wyciągnąć te hasła. Do maili mam raczej podobne hasła, mail który jest podany w banku ma inne hasło, zupełnie inne mam do konta w banku. Ważniejsze hasła mam spisanie, leżą bezpiecznie u mnie w domu. Raczej nie zdarzyło mi się żebym zapomniał jakiegoś hasła.

> Korzystam. W Chromie przechowuje sobie hasło, Staram sie tego unikać, ale to jest bardzo wygodne. Na dużej ilości stron trzeba mieć konto i nie idzie z tego zapamiętać.

2.2.13. Jak wyglądałby Twoim zdaniem idealny system zabezpieczeń do płatności elektronicznej/mobilnej?

Z udzielonych odpowiedzi można wywnioskować, że użytkownicy czują potrzebę zwiększenia poziomu zabezpieczeń. Najczęściej pojawiają się wskazania w kierunku większego wykorzystania biometrii, np. odcisk palca, skan tęczówki. Takie rozwiązania budzą zaufanie badanych, niezależnie od ich wieku czy doświadczeń w bankowości elektronicznej . Wskazywały na to zarówno osoby młodsze jak i starsze.

Na podstawie niektórych wywiadów powstaje również obraz osoby, dla której wygoda jest zdecydowanie ważniejsza niż bezpieczeństwo. Taka osoba chętnie zrezygnowałaby na przykład: z potwierdzania czynności poprzez używanie kodów SMS. To otwiera właśnie drogę do popularyzacji rozwiązań biometrycznych:

> Korzystałby z moich danych biometrycznych, które w sposób jednoznaczny identyfikował by moją osobę sprawdzając żywotność moich cech, ale nie wymagałby ode mnie żadnej aktywności.

> Akceptacje głosowe, moze cos takiego. Potwierdzenie przyciskiem palca. Nie wiem no, nie mam pojęcia.

> Nie da się wprost odpowiedzieć. Może oprócz karty zbliżeniowej jeszcze warstwa zabezpieczeń np. na odcisk palca, skanowanie tęczówki. Coś wieloetapowego, niepodrabialnego.

Ponadto, zwrócono uwagę na problem mnogości danych do logowania do różnych serwisów. Badani wierzą w bezpieczeństwo rozwiązań bankowych i chętnie korzystaliby szerzej z możliwości uwierzytelnienia poprzez serwis bankowy, tak jak ma to miejsce w serwisie ePUAP. To stwarza szansę na wprowadzanie rozwiązań takich jak moje ID[16].

> Dobrze by było, gdybym mógł np.. Wszystko robić przez bank, jak z epuapem, żebym nie musiał podawać wszędzie swoich danych. Ewentualnie, żebym wykorzystywali odcisk palca, skoro i tak coraz więcej telefonów i laptopów to ma.

[16] https://www.mojeid.pl/

2.3. Persony

Przeprowadzone badania pozwoliły pogłębić wiedzę na temat użytkowników bankowości elektronicznej i mobilnej. Na podstawie analizy udzielonych przez użytkowników odpowiedzi i towarzyszącym im emocji wyszczególniono trzy główne persony, łączące zbliżone cechy zachowań, potrzeby i obawy.

Persona 1 – Nieświadoma Nadia

Osoba ta w małym stopniu zna się na obecnych systemach bankowości. Zwykle jest zaznajomiona z bardzo podstawowymi zasadami korzystania z płatności elektronicznych lub mobilnych, a jej wiedza na temat ataków na bankowość elektroniczną jest często niewielka lub znikoma. Skutkuje to przeświadczeniem Nadii, że nie może być ona celem ataku hakerskiego, ponieważ jest mało atrakcyjnym celem, gdyż nie posiada dużej ilości środków finansowych i nie jest ważną osobą.

W bankowości ceni sobie przede wszystkim szybkość i wygodę. Nie zastanawia się nad bezpieczeństwem systemów, z których korzysta, dlatego też nie czuje potrzeby zgłębiania swojej wiedzy w tym kierunku, uważa, że ktoś inny zadba o jej bezpieczeństwo. Nadia niejednokrotnie nie ma potrzeby wykorzystywania nowinek technicznych i wystarczają jej podstawowe mechanizmy płatności, do których jest przyzwyczajona, nie widzi korzyści dla siebie ze stosowania ich.

W mediach nie poszukuje nowych informacji o bezpieczeństwie. Nieświadomej Nadii w niektórych przypadkach towarzyszy przekonanie „nie znam się, więc mnie to nie interesuje", co jest niebezpieczne dla jej finansów. Mimo korzystania z bankowości elektronicznej i mobilnej, nie interesuje ją to, czy dane rozwiązanie jest bezpieczne. Często elementy takie jak metody płatności i uwierzytelniania wybiera tylko na podstawie rekomendacji banku i używa ustawień fabrycznych.

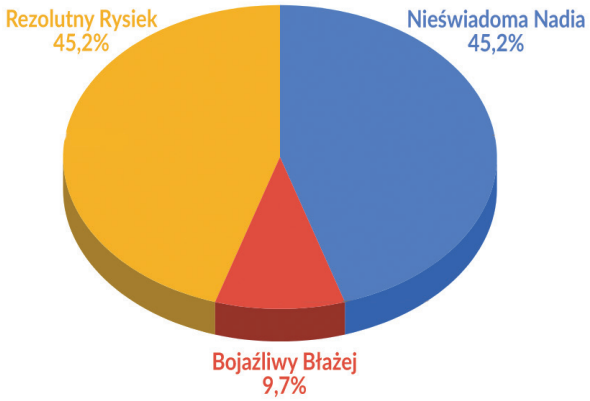
Persona 2 – Bojaźliwy Błażej

Osoba, która ma pewne obawy względem bankowości elektronicznej i mobilnej. Pomimo swoich obaw, korzysta jednak z nowoczesnych rozwiązań, ale z ograniczonym zaufaniem. Błażej posiada pewną wiedzę związaną z bankowością, ale zwykle nie jest ona kompletna, co może prowadzić do różnych nieścisłości. Osoba ta czerpie informacje głównie z internetu, ale nie z profesjonalnych źródeł, stąd często operuje na „półprawdach" o jakimś ataku czy systemie. Dodatkowo Błażej może przejawiać dużą nieufność do systemów finansowych, obawiać się szpiegostwa, spisku, co wynika z braku jego gruntownej wiedzy i braku chęci jej pogłębienia. Jego postawa często reprezentowana jest przez takie stwierdzenia jak: „oni i tak wiedzą", „wszystko jest monitorowane", "nie ufam swojemu telefonowi".

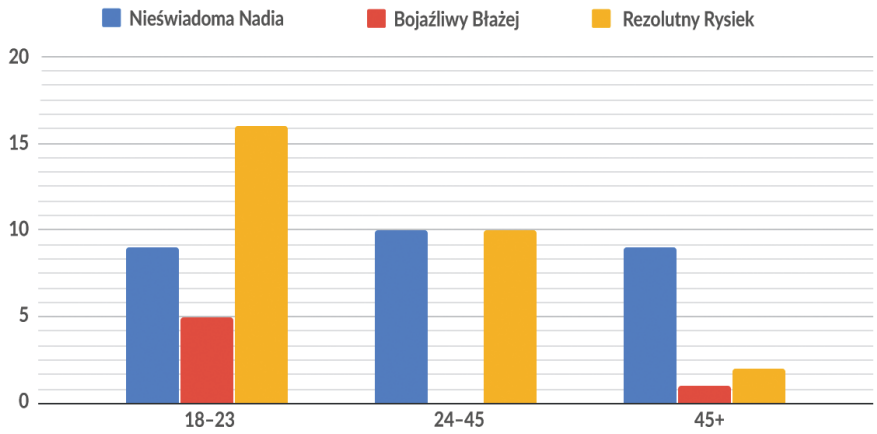
Błażej czuje się spokojniejszy, gdy jest świadomy tego, jak działają rozwiązania, z których korzysta. Jeśli w jego odczuciu aplikacja jest prosta i przejrzysta, a jego dane nie są nigdzie zapisywane, wtedy nie obawia się utraty środków ani ataków. To, co dla niego najważniejsze w bankowości, może podsumować stwierdzenie: „Pewność, że dana transakcja zostanie wykonana, że nikt nic w niej nie będzie mieszał i pieniądze trafią do właściwego odbiorcy."

Persona 3 – Rezolutny Rysiek

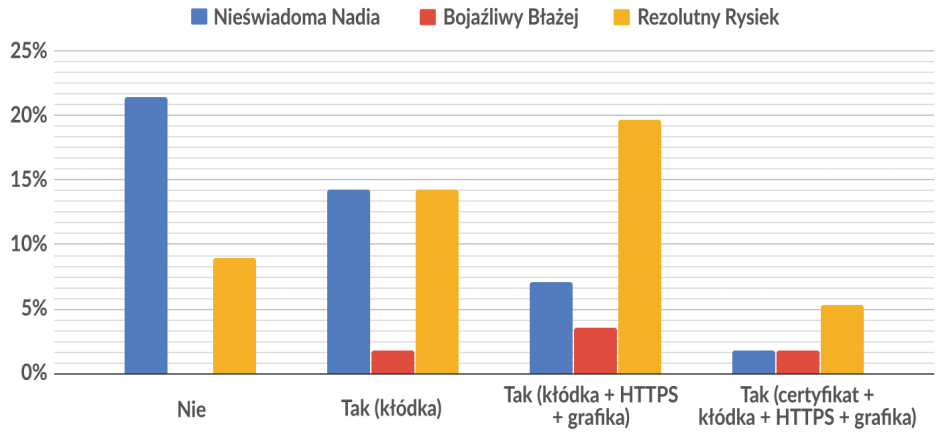
Osoba dobrze zorientowana w temacie bankowości oraz nowych technologii, świadoma ryzyka związanego z cyberatakami na finanse elektroniczne. Rysiek zna i stosuje różne mechanizmy zabezpieczeń oraz zasadniczo przestrzega zasad bezpieczeństwa. Osoba ta czerpie wiedzę z różnych źródeł, często są one rzetelne i sprawdzone. Rysiek czasami nawet odwiedza portale branżowe, aby doczytać jakieś szczegóły. Oprócz szybkości lub wygody często nadmienia, że bezpieczeństwo jest istotną cechą systemu bankowego. Może się zdarzyć, że Rysiek przecenia swoją wiedzę i jego pewność siebie jest zbyt duża, co wyraża się w przekonaniach typu „komunikaty z banku są zbyt proste, ja to już wszystko wiem” i przez to pomija alerty bankowe czy naraża się na nowe zagrożenia.



Rys. 41. Rozkład badanych z uwzględnieniem person. (n = 62)

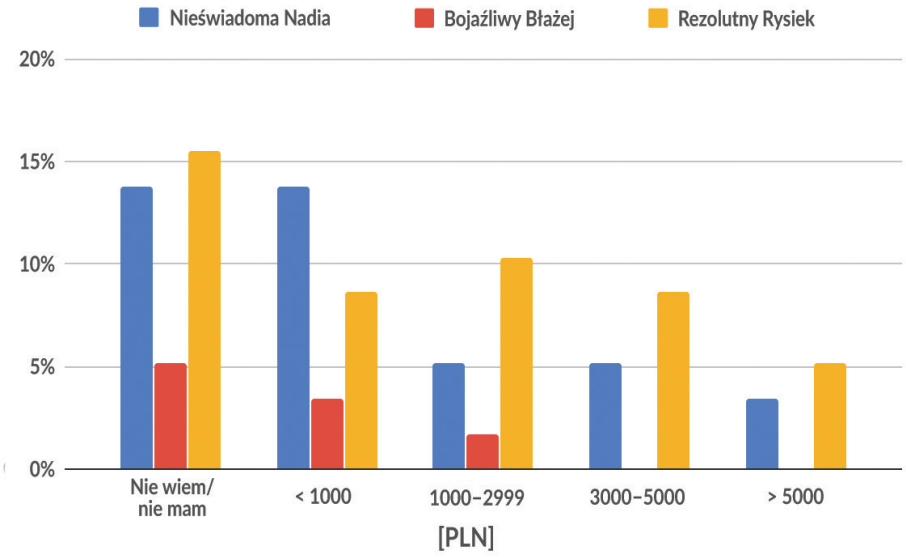


Rys. 42. Rozkład na persony z uwzględnieniem wieku badanych. (n = 62)



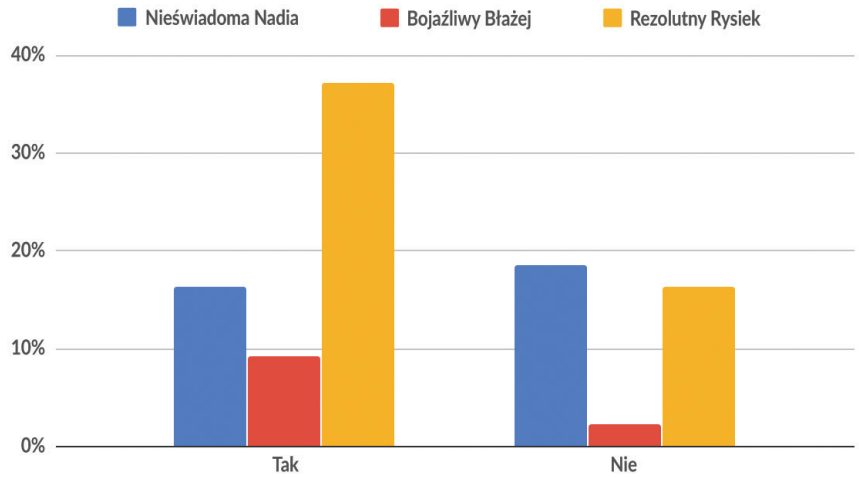
Rys. 43. Czy weryfikujesz stronę banku? (z uwzględnieniem person, n = 56)

Wśród osób, które nie weryfikują strony banku przeważają te z cechami Nieświadomej Nadii. Świadczy to o tym, że to przede wszystkim braki w wiedzy oraz stawianie wygody nad bezpieczeństwem są przyczyną narażania się na potencjalne ataki. Można zauważyć, że wraz ze wzrostem świadomości użytkowników rośnie również liczba składników, które są weryfikowane podczas odwiedzania strony banku. Ilustruje to zwiększony udział osób z cechami Rezolutnego Ryśka w kolejnych odpowiedziach na to pytanie.



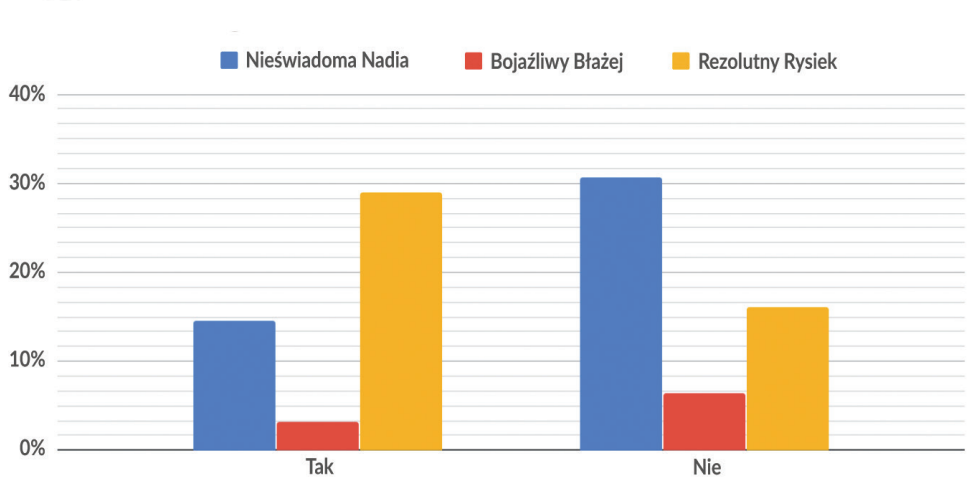
Rys. 44. Jakie masz limity? (z uwzględnieniem person, n = 58)

Na podstawie odpowiedzi oraz wyróżnionych person podczas badania można wysnuć wniosek, że osoby o cechach Rezolutnego Ryśka ustawiają zdecydowanie wyższe limity niż pozostałe persony. Może to mieć związek z tym, że osoby te czują się bezpieczne, bo podejmują więcej wysiłku podczas weryfikacji pozostałych mechanizmów bezpieczeństwa. Adekwatnie do swojego wzorca zachowania, reprezentanci Bojaźliwego Błażeja mają ustawione niskie wartości limitów.



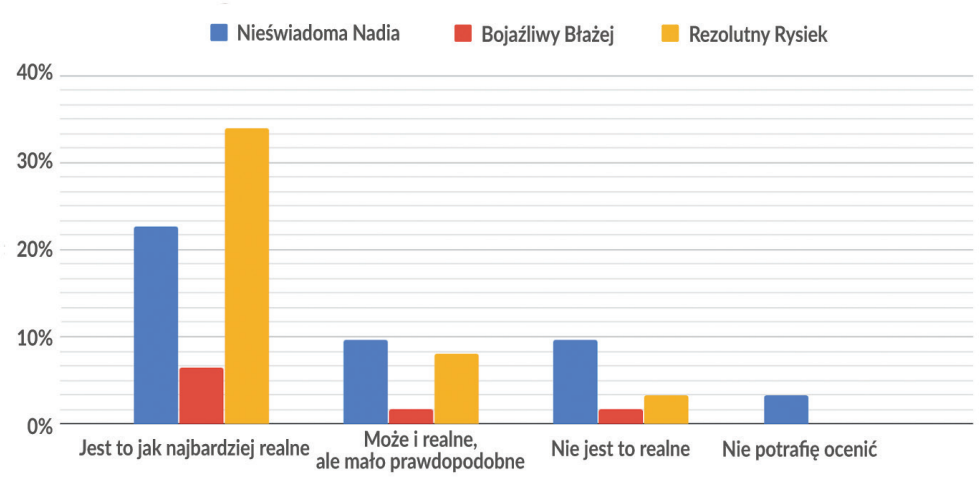
Rys. 45. Czy korzystasz z autoryzacji dwuskładnikowej? (n = 43)

W obszarze użytkowania autoryzacji dwuskładnikowej możemy zaobserwować, że w grupie, która korzysta z rozwiązań 2FA, prawie 60% użytkowników to Rezolutni Ryśkowie, osoby te stanowią prawie 40% spośród wszystkich badanych w tym pytaniu. Znowu potwierdza się zachowanie charakterystyczne dla Bojaźliwego Błażeja, w przeważającej większości osoby reprezentujące tę personę używają drugiego składnika uwierzytelniania.



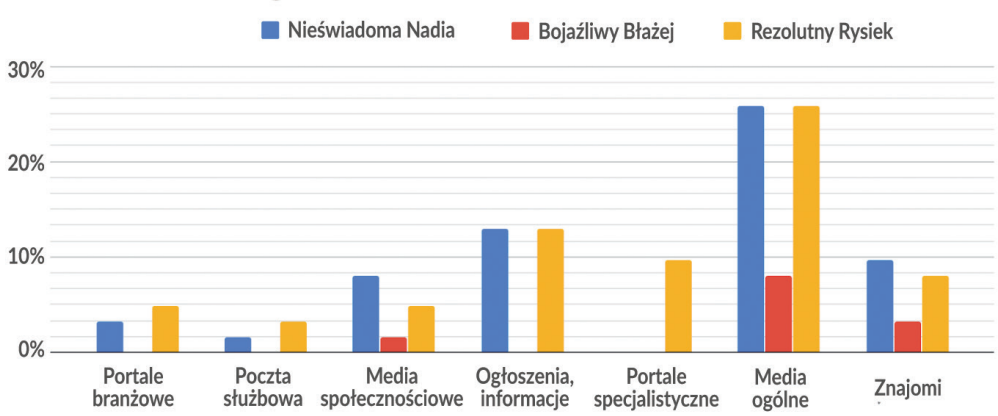
Rys. 46. Czy korzystasz z aplikacji (na telefonie/komputerze) do przechowywania haseł/PIN-ów do logowania/uwierzytelniania? (z uwzględnieniem person, n = 62)

Jeśli chodzi o wykorzystanie mechanizmów do zapamiętywania haseł, to zdecydowana przewaga występuje w grupie Rezolutnych Ryśków (prawie 30% wszystkich badanych i ponad 60% w grupie osób korzystających). Do tej grupy należą także wszyscy, którzy wymieniają specjalistyczne narzędzia, takie jak menadżer haseł czy pęk kluczy Apple'a, co świadczy o wysokim poziomie świadomości. Około 2/3 spośród osób o charakterze Bojaźliwego Błażeja nie korzysta z mechanizmów zapamiętywania haseł, co jest spójne z ich obawami.



Rys. 47. Czy uważasz, że zagrożenie cyberatakami na Twoje finanse elektroniczne jest realne? (z uwzględnieniem person, n = 62)

Świadomość zagrożeń płynąca ze świata cybernetycznego jest w największym stopniu posiadana przez przedstawicieli persony Rezolutny Rysiek, obserwujemy prawie 35% reprezentację tej grupy jako silnie przekonanych o realności zagrożenia. Również Bojaźliwi Błażeje w zdecydowanej większości wyrażają zadanie o realności zagrożeń cyberataków na finanse elektroniczne. W przypadku osób należących do archetypu Nieświadomej Nadii mamy dużą rozbieżność opinii i występują wśród nich wszystkie odpowiedzi, przy czym ponad 20% również uważa, że zagrożenie jest wysoce realne.



Rys. 48. Skąd czerpiesz wiedzę na temat bezpieczeństwa? (z uwzględnieniem person, n = 62)

Wśród osób, które czerpią wiedzę o bezpieczeństwie ze źródeł specjalistycznych, portali branżowych oraz poczty służbowej mają przewagę przedstawiciele persony Rezolutny Rysiek. W przypadku portali poświęconych stricte bezpieczeństwu stanowią jedyną grupę, która wykorzystuje to źródło i to w dość licznym gronie – prawie 10% wszystkich badanych. Media społecznościowe i znajomi to domena Nieświadomej Nadii. W tych rodzajach źródeł przeważają jej reprezentanci nad innymi i w każdym z przypadków jest to ok. 10% osób badanych.

3. Wnioski i rekomendacje

W tej części opracowania zostaną podsumowane przeprowadzone badania i sformułowane główne wnioski z nich wynikające. Wypracowane zostaną ponadto rekomendacje, zarówno dla użytkowników, jak i instytucji finansowych.

3.1. Główne wnioski

- Użytkownicy często wymieniają jako daną usługę z której korzystają, konkretną markę firmy świadczącą tę usługę. Mówi to o sile rozpoznawalności tej marki i jej oddziaływaniu na odbiorcę.
- Badani zaczynają rozumieć potrzebę wykorzystania biometrii, darzą ją większym zaufaniem i doceniają zalety, jakie ze sobą niesie.
- Użytkownicy korzystają z nowych, cyfrowych usług, jeśli doświadczą korzyści dla siebie. Doskonałym przykładem stała się możliwość rozliczania podatku PIT w 2019 roku, kiedy zalogować można było się z pomocą zaufanego profilu bądź banku. Wielu ankietowanych po raz pierwszy skorzystało wtedy z usługi platformy ePUAP.
- Badani wykazują zaufanie do instytucji bankowych i chętnie korzystają z mechanizmów uwierzytelniania się za ich pośrednictwem (m.in. do usługi *Profil Zaufany*). Wskazuje to na obiecujący kierunek rozwoju usług zarządzania tożsamością i jej weryfikacją przez instytucje finansowe.
- 60% badanych wskazuje telewizję, prasę oraz zwykłe, pozabranżowe portale informacyjne jako główne źródło informacji o bezpieczeństwie. Wykorzystanie tych miejsc podczas kampanii społeczno-edukacyjnych może znacząco przyczynić się do podniesienia świadomości użytkowników.
- Stosowanie na rynku rozwiązania 2FA jest coraz bardziej popularne. Ok. 70% badanych deklaruje wykorzystanie podwójnego mechanizmu autoryzacji. Wdrożenie dyrektywy PSD2 przez sektor bankowy w jeszcze większym stopniu spopularyzuje użycie i świadomość istnienia tych rozwiązań.

- Jedynie 3,8% osób wskazało kserowanie dowodu osobistego jako formę wyłudzenia danych. To pokazuje brak świadomości konsekwencji takiego zachowania wśród badanych. Rozwiązaniem tego problemu miała być ustawa z dnia 22 listopada 2018 r. o dokumentach publicznych [4], jednak interpretacja jej zapisów dalej nie jest jasna. Instytucje finansowe są uprawnione do sporządzania kserokopii dokumentów, o ile kserokopia ta nie będzie spełniała ustawowych przesłanek definicji „repliki". Prawo to wynika z ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu [13].
- 1/3 ankietowanych nie potrafi odpowiedzieć na jakim poziomie ma ustawione limity, np. wypłat gotówki lub wysokości przelewu. 22% badanych korzysta z limitów na poziomie ponad 3000 zł, w tym 9% ustawiło kwotę ponad 5000 zł. Biorąc pod uwagę średnią zarobków w Polsce na rok 2019, która wynosi 3600 zł netto, te osoby ryzykują utratą prawie całych swoich zarobków.
- Ponad 60% badanych weryfikuje stronę banku, sprawdzając „zieloną kłódkę", podobieństwo grafiki serwisu i protokół HTTPS w pasku adresu, ale wciąż nie mają pewności czy to jest wystarczające. Tylko ok. 9% ankietowanych sprawdza certyfikat witryny.
- Ponad połowa ankietowanych (ok. 63%) zdaje sobie sprawę z realności zagrożenia cyberatakiem na ich finanse. Wnioskując – z jednej strony należy propagować informacje na temat bezpieczeństwa użytkowników usług w sektorze finansowym, a z drugiej można zauważyć, że tendencja jest rosnąca – z roku na rok rośnie świadomość zagrożeń płynących z cyberprzestrzeni [7].
- Tylko niewielka liczba badanych osób (ok. 8%) doświadczyła bezpośrednio cyberataku na swoje finanse lub dane, dlatego większość badanych nie potrafi sobie wyobrazić jak taka sytuacja wygląda i jakie towarzyszą jej emocje. Jest to doświadczenie dla nich obce i odległe.
- Popularność aplikacji do płatności elektronicznych typu GooglePay czy ApplePay nie jest duża, niespełna 13% użytkowników deklaruje ich użycie. Wynika to najprawdopodobniej z dużej dostępności w Polsce różnych mechanizmów płatności mobilnych i elektronicznych [12].

3.2. Rekomendacje

W ramach analiz przeprowadzonych badań i interpretacji ich wyników wypracowany został szereg rekomendacji, które podzielone zostały na dwie kategorie. Jedne dotyczą prawidłowych zachowań i dobrych praktyk dla użytkowników, drugie zaś aktywności, które powinny zostać podjęte przez instytucje finansowe.

Rekomendacje dla użytkowników

- Podstawowa wiedza na temat działania systemów bankowości elektronicznej i mobilnej może być bardzo przydatna w walce z cyberatakami, warto czytać komunikaty banku i się do nich stosować. Istotne jest również, aby korzystać z różnych źródeł informacji o bezpieczeństwie i możliwie je weryfikować.

- Limity transakcyjne na kontach bankowych czy kartach płatniczych to jedne z fundamentalnych mechanizmów bezpieczeństwa. Jest to często ostatnia linia obrony, po przełamaniu innych zabezpieczeń, która pozwala ograniczyć straty. Należy bezwzględnie ograniczyć limity do wartości dopasowanych do codziennych potrzeb danego użytkownika.
- Nowa dyrektywa UE PSD2 wymusiła na bankach zastosowanie mechanizmów podwójnej weryfikacji (2FA). Większość z nich standardowo proponuje zastosowanie kodów SMS, które niestety nie są najlepszym rozwiązaniem. Należy sprawdzić czy bank ma w swojej ofercie inne mechanizmy potwierdzania transakcji jak tokeny softwarowe czy aplikacje mobilne.
- Aby chronić swoje dane osobowe i kontrolować wszelką aktywność kredytową zaleca się założenie konta w BIK[17] i wykupienie monitoringu zapytań o zdolność kredytową.

Rekomendacje dla instytucji finansowych

- Dokładne przeanalizowanie implementacji swoich rozwiązań bezpieczeństwa pod kątem ich skuteczności i odporności na cyberataki. Przykładem jest powiązanie kodu/tokena potwierdzającego daną transakcję z danymi tej transakcji (przynajmniej z kwotą i nr konta odbiorcy). Innym krytycznym obszarem jest mechanizm przyłączania nowego urządzenia mobilnego poprzez aplikację bankową do konta.
- Nieustająca kampania informacyjno-edukacyjna na temat bezpieczeństwa, zagrożeń i odpowiednich zachowań jest konieczna. Komunikaty powinny adresować większą niż dotychczas grupę użytkowników. Aby to osiągnąć musi zmienić się ich formalny i techniczny charakter. Informacje w pierwszej warstwie komunikacyjnej powinny być przyjazne w odbiorze i zrozumiałe dla przeciętnego użytkownika, zaś, aby utrzymać uwagę użytkownika zaawansowanego należy umieścić na końcu wiadomości odnośniki do konkretnych danych technicznych i/lub poszerzone wyjaśnienie merytoryczne. Istotnym elementem jest również wybór kanałów komunikacyjnych, bezwzględnie należy wyjść poza system notyfikacji wewnętrznych i korzystać z mediów ogólnych (choćby portale informacyjne) i społecznościowych.
- Celem zwiększenia procentu użytkowników, którzy będą czytać komunikaty banku można zastosować mechanizm zachęty – poprzez zaproponowanie lepszych warunki instrumentów finansowych w stosunku do oferty podstawowej, jeśli użytkownik przeczyta informacje i odpowie prawidłowo na zestaw pytań czy rozwiąże quiz.
- Zaleca się wprowadzenie przez banki nowej usługi w postaci czasowej zmiany limitu płatności/wypłaty gotówki. Po określonym czasie, np. 15 minutach limit zostanie ustawiony na poprzednią wartość, dzięki czemu użytkownik, w przypadku jednorazowej potrzeby zrealizowania transakcji przekraczającej limit, dalej będzie chroniony przez ten mechanizm.
- Konieczne jest, aby istotne komunikaty były przez bank rozsyłane wszystkimi dostępnymi kanałami do użytkownika, e-mail, SMS, informacje w serwisach transakcyjnym i inne. Do takich sytuacji należy zaliczyć m.in. zmianę hasła, mechanizmu potwierdzania transakcji, przyłączenie/odłączenie urządzenia mobilnego czy znaczącą zmianę limitów transakcji.

[17] https://www.bik.pl/

- Można wykorzystać fakt istnienia silnie rozpoznawalnych marek wśród użytkowników (m.in. wymienione przez badanych PayPal czy PayU) i próbować współpracować przy organizacji wspólnych kampanii społecznych i edukacyjnych. Dzięki takiemu podejściu kampanie te będą bardziej wiarygodne w odbiorze użytkowników.

3.3. Podsumowanie

Przeprowadzone badania pokazały, że nie można traktować użytkowników bankowości elektronicznej jako jednolitej grupy i próbować zaspokoić wszystkich ich potrzeb zunifikowanymi rozwiązaniami. Zarówno w obszarze kanałów informacyjnych, zakresu usług finansowych, jak i świadomości oraz potrzeb związanych z cyberbezpieczeństwem występują znaczące różnice wśród badanych. Dzięki przedstawieniu użytkowników w formie trzech archetypów klientów można lepiej zrozumieć i precyzyjniej dotrzeć do szerszego grona odbiorców usług, a także zapewnić wyższy poziom satysfakcji z ich wykorzystania.

Jednocześnie zaobserwowaliśmy, że technologie takie jak biometria, usługi e-tożsamości czy płatności bezgotówkowe nie są dla ankietowanych czymś nadzwyczajnym, a raczej pożądanym kierunkiem rozwoju i zapewnieniem większej wygody oraz użyteczności systemów bankowości cyfrowej. Wobec instytucji finansowych badani wykazują duże zaufanie i powierzają im swoje dane oraz pieniądze, zatem to po ich stronie leży zapewnienie najwyższej możliwej ochrony tożsamości i zgromadzonych aktywów. Rozwiązań bezpieczeństwa nie można szukać najmniejszym kosztem czy w oderwaniu od realiów cyberprzestępczości. To właśnie sektor finansowy powinien być motorem i dostawcą nowoczesnych mechanizmów bezpieczeństwa cyfrowego zorientowanych na użytkownika.

4. Bibliografia

1. Parlament Europejski (2015). Dyrektywa (EU) 2015/2366 z 25 listopada 2015 o usługach płatniczych na rynku wewnętrznym. Dziennik Urzędowy Unii Europejskiej. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN
2. Związek Banków Polskich (2019). *PSD2 i Open Banking - Rewolucja czy ewolucja?* https://assets.kpmg/content/dam/kpmg/pl/pdf/2019/03/pl-raport-kpmg0-zbp-psd2-i-open-banking-rewolucja-czy-ewolucja.pdf
3. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018 poz. 1560. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/O/D20181560.pdf
4. Ustawa z dnia 11 stycznia 2019 r. o dokumentach publicznych. Dz.U. 2018 poz. 53. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20190000053/O/D20190053.pdf
5. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018 poz. 1000. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf
6. Wojciech Wodo i Hanna Ławniczak (2016). *Bezpieczeństwo i biometria urządzeń mobilnych w Polsce. Badania użytkowników 2016.* Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław. https://www.dbc.wroc.pl/dlibra/publication/39839/edition/36335
7. Konferencja Przedsiębiorstw Finansowych w Polsce (KPF) i EY (2018). *Nadużycia w sektorze finansowym. Raport z badania. Edycja 2018*. https://www.kpf.pl/pliki/raporty/raport_naduzycia_2018.pdf
8. Związek Banków Polskich (2018). *Cyberbezpieczny portfel*. https://www.zbp.pl/getmedia/5f90b612-ac57-43fc-bc98-49870e34d555/Raport_ZBP_-_Cyberbezpieczny_Portfel
9. KPMG (2018). *Bezpieczeństwo technologii mobilnych*. https://assets.kpmg/content/dam/kpmg/pl/pdf/2018/11/pl-raport_kpmg_bezpieczenstwo_technologii_mobilnych.pdf
10. Ponemon Institute LLC (2019). *State of Password and Authentication Security Behaviors Report. Ponemon Institute Research Report*. https://www.yubico.com/wp-content/uploads/2019/01/Ponemon-Authentication-Report.pdf

11. Tim Brown (2009). *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation*, HarperBusiness.
12. Shoper (2019). *Płatności. Raport 2019*. https://www.shoper.pl/static/raporty/Shoper_Raport_Platnosci_2019.pdf
13. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Dz.U. 2018 poz. 723. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180000723/U/D20180723Lj.pdf

Wydawnictwa Politechniki Wrocławskiej są do nabycia w księgarni
ul. C.K. Norwida 9, 50-374 Wrocław, tel. 71 328 08 95
Prowadzimy sprzedaż wysyłkową: zamawianie.ksiazek@pwr.edu.pl

ISBN 978-83-7493-109-0
DOI 10.37190/WSW_BU2019