EDUKACJA KLIENTÓW BANKÓW W ZAKRESIE USŁUG PŁATNICZYCH Z UWZGLĘDNIENIEM KWESTII CYBERBEZPIECZEŃSTWA

Anna Warchlewska

SYGN. PAB/WIB 9/2026

ISBN 978-83-910226-2-7

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY

O raporcie

Raport **„Edukacja klientów banków w zakresie usług płatniczych z uwzględnieniem kwestii cyberbezpieczeństwa”** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorka raportu

dr Anna Warchlewska – doktor nauk ekonomicznych, adiunkt w Katedrze Pieniądza i Bankowości Uniwersytetu Ekonomicznego w Poznaniu. Specjalizuje się w tematyce finansów osobistych, wykluczenia finansowego i nowoczesnych technologii w procesie zarządzania finansami osobistymi. Autorka publikacji o zasięgu krajowym i międzynarodowym, w tym monografii „Wykluczenie finansowe. Od finansów tradycyjnych do cyfrowych”; „Determinanty zachowań finansowych konsumentów. Ujęcie pokoleniowe” oraz „Modern technologies in financial advice and personal financial planning” (współautorka). Realizowała projekty badawcze w tematyce sektora LendTech oraz użyteczności aplikacji PFM i robo-doradztwa. W ramach ogólnopolskiej inicjatywy edukacyjnej realizowanej we współpracy z Warszawskim Instytutem Bankowości uczestniczyła w przygotowaniu kompleksowych materiałów edukacyjnych z zakresu finansów osobistych i bezpieczeństwa cyfrowego, skierowanych do uczniów klas IV–VIII szkół podstawowych oraz wspierających nauczycieli w kształtowaniu praktycznych kompetencji finansowych młodego pokolenia.

Konsultacja naukowa

dr Marcin Bielicki – doktor nauk ekonomicznych, adiunkt w Katedrze Inwestycji i Rynków Finansowych Uniwersytetu Ekonomicznego w Poznaniu. Rozdział 2.2 powstał przy jego udziale merytorycznym. Specjalizuje się on w projektowaniu i wdrażaniu innowacyjnych, interaktywnych form oraz narzędzi edukacyjnych.

O programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 r. jako odpowiedź na potrzeby sektora bankowego w zakresie wysokiej jakości analiz i badań z obszaru cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz – w ostateczności – kreowania wartości dla klientów – końcowych użytkowników bankowości.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie w sektorze bankowym, cyberbezpieczeństwo banków i systemy płatnicze**
- **Ekonomiczna analiza rozwoju sektora bankowego, stabilności banków, otoczenia makroekonomicznego**
- **Prawno-regulacyjne i legislacyjne uwarunkowania działalności sektora bankowego oraz wyzwania wynikające z orzecznictwa sądów krajowych i europejskich**
- **ESG i sustainable finance**
- **Prace analityczno-badawcze w zakresie poszczególnych obszarów funkcjonowania banków oraz w zakresie funkcjonowania wskaźników referencyjnych**

Więcej na temat działalności programu na stronie www.pabwib.pl

Kontakt

dr Tomasz Pawlonka
Dyrektor Programu
m: 505 917 778
e: tpawlonka@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

Warszawski Instytut Bankowości
00-380 Warszawa, ul. Kruczkowskiego 8
t: (22) 182 31 70
e: pab@wib.org.pl

dr Radosław Ciukaj
m: 784 680 685
e: radoslaw.ciukaj@zbp.pl

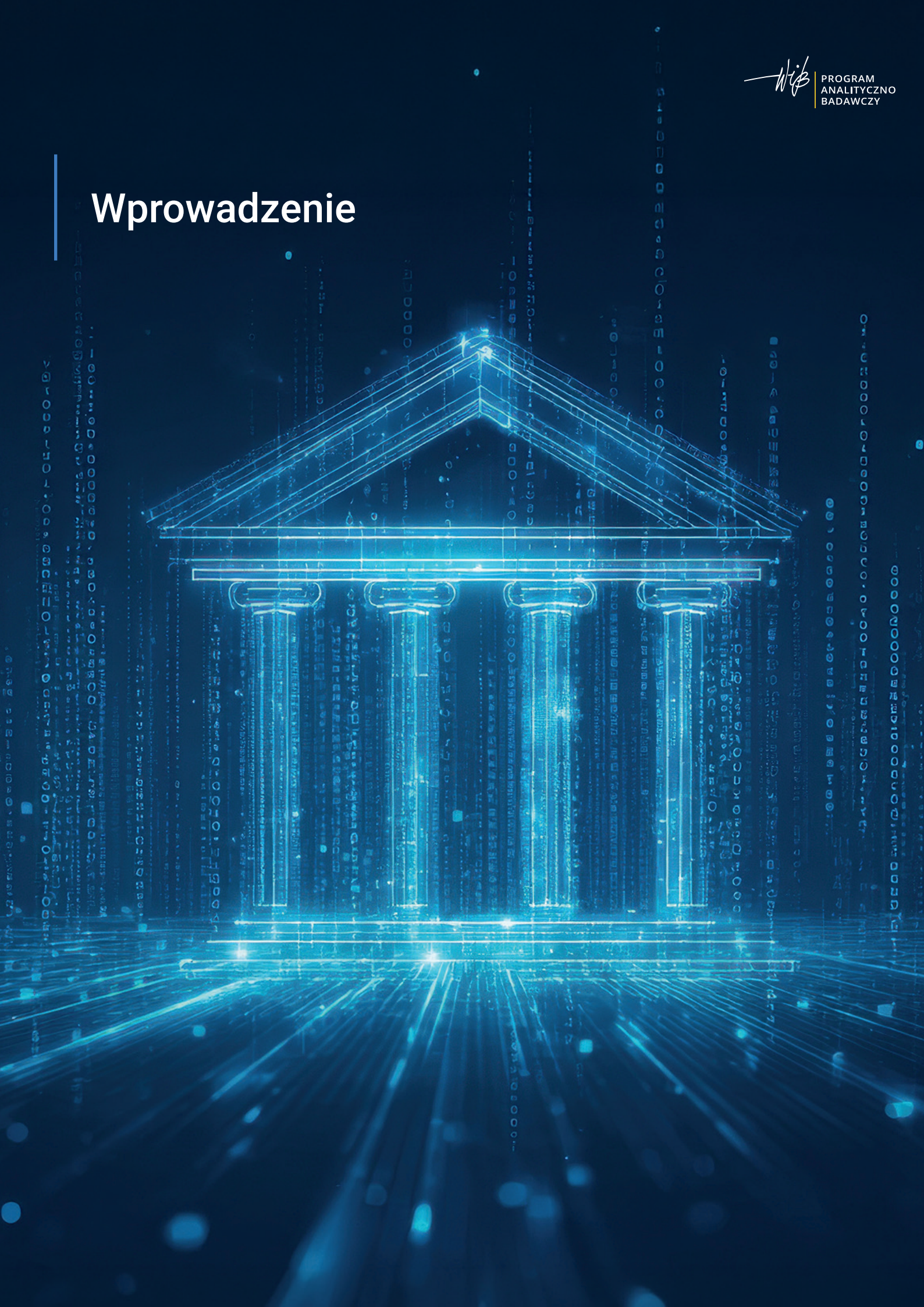
dr Agnieszka Wicha
m: 661 646 474
e: agnieszka.wicha@zbp.pl

Bartosz Przyborowski
m: 795 933 104
e: bartosz.przyborowski@zbp.pl

Spis treści

PROGRAM ANALITYCZNO BADAWCZY

Wprowadzenie



Współczesny rynek usług płatniczych dynamicznie się rozwija, a kluczowym trendem jest cyfryzacja i digitalizacja. Ta zmiana przynosi niezwykłe korzyści – wygodę, szybkość i szeroki dostęp do finansów – ale jednocześnie niesie za sobą poważne wyzwania związane z bezpieczeństwem dla użytkowników usług płatniczych, instytucji finansowych, regulatorów oraz podmiotów prowadzących działania edukacyjne. Wraz ze wzrostem popularności usług bankowości internetowej i mobilnej rośnie również aktywność cyberprzestępców, którzy wykorzystują coraz bardziej wyrafinowane metody ataków.

Analiza koncentruje się na rynku usług płatniczych w Polsce, uwzględniając najważniejsze zmiany zachodzące w ostatnich latach w obszarze cyfryzacji finansów, ewolucji zagrożeń oraz sposobów podnoszenia świadomości użytkowników. Celem raportu jest zdiagnozowanie zagrożeń towarzyszących rozwojowi i cyfryzacji usług płatniczych, identyfikacja ryzyk dla ich użytkowników oraz analiza roli edukacji finansowej i odpowiednio projektowanej komunikacji instytucji finansowych w zwiększaniu świadomości i bezpieczeństwa korzystania z usług płatniczych. Raport ma charakter przekrojowy i interdyscyplinarny – łączy analizę cyfryzacji usług płatniczych i zagrożeń dla ich użytkowników z problematyką edukacji finansowej oraz projektowania komunikacji wspierającej bezpieczne korzystanie z tych usług. Koncentruje się on na analizie współczesnych zagrożeń dla klientów usług płatniczych w środowisku cyfrowym oraz na znaczeniu edukacji jako mechanizmu prewencyjnego i obronnego przed tymi zagrożeniami. Ważnym elementem opracowania jest także przedstawienie zasad podziału odpowiedzialności pomiędzy klientami a instytucjami finansowymi w przypadku incydentów związanych z płatnościami elektronicznymi, w tym mobilnymi. Jest to zagadnienie często niedostatecznie rozumiane przez użytkowników, a jednocześnie kluczowe dla budowania zaufania do bankowości cyfrowej oraz świadomego korzystania z usług płatniczych.

Pomimo dynamicznego rozwoju zabezpieczeń technologicznych oraz coraz bardziej rozbudowanych regulacji prawnych, skala oszustw i incydentów w obszarze usług płatniczych nie maleje. Wskazuje to na istnienie luki, która nie ma charakteru *stricte* technologicznego, lecz kompetencyjny i edukacyjny. Problemem nie jest wyłącznie dostępność narzędzi ochrony, lecz sposób, w jaki są one rozumiane i wykorzystywane przez użytkowników końcowych. Nie pomijając znanych już zagrożeń, takich jak skimming czy phishing, coraz większym wyzwaniem stają się nowoczesne formy ataków, w tym m.in. smishing (fałszywe wiadomości SMS), vishing (podszywanie się pod instytucje, najczęściej finansowe, przez telefon), instalacja złośliwego oprogramowania mobilnego czy ataki typu MiTM (man-in-the-middle – przechwytywanie komunikacji pomiędzy użytkownikiem a systemem, np. bankiem). Coraz częściej cyberprzestępcy wykorzystują także deepfake'i (fałszywe materiały audio lub wideo generowane z wykorzystaniem sztucznej inteligencji, które imitują wizerunek lub głos konkretnej osoby) oraz zaawansowane techniki inżynierii społecznej, szczególnie w ramach oszustw typu BEC (Business Email Compromise – podszywanie się pod zaufaną osobę lub instytucję w korespondencji e-mail w celu wyłudzenia pieniędzy lub danych). Szczególnie niebezpieczną kategorią zagrożeń pozostaje ransomware – złośliwe oprogramowanie, które szyfruje dane lub całe systemy IT i żąda okupu za ich odblokowanie.

Dodatkowo, wraz z rozwojem sztucznej inteligencji, pojawiają się nowe, trudniejsze do wykrycia metody ataków. Modele AI umożliwiają m.in. generowanie przekonujących wiadomości phishingowych dopasowanych do profilu ofiary, automatyczne prowadzenie rozmów podszywających się pod pracowników instytucji finansowych, czy tworzenie hiperrealistycznych deepfake'ów głosu i wideo, które ułatwiają przeprowadzanie oszustw finansowych. AI pozwala także na automatyzację rekonesansu i analizę dużych zbiorów danych, co dodatkowo zwiększa skuteczność cyberprzestępców. Tego rodzaju ataki mogą oddziaływać nie tylko osoby prywatne, ale całe przedsiębiorstwa, w tym także instytucje finansowe i usługodawców płatniczych. W efekcie może dojść do utraty danych klientów przez różne przedsiębiorstwa, przestojów operacyjnych i znaczących strat finansowych oraz reputacyjnych. Wśród innych rozwijających się zagrożeń warto wymienić także: keyloggery – programy szpiegujące rejestrujące naciskane klawisze, służące do wykradania loginów i haseł; fałszywe strony płatnicze i sklepy internetowe – profesjonalnie przygotowane serwisy, które mają na celu wyłudzanie danych karty płatniczej; ataki DDoS – ukierunkowane na unieruchomienie serwisów płatniczych, czasem stosowane jako odwrócenie uwagi od innego ataku; QR-code phishing (quishing) – oszustwa polegające na podmianie lub rozpowszechnianiu złośliwych kodów QR, które prowadzą do fałszywych stron płatności lub pobierają złośliwe aplikacje.

Skala, złożoność oraz dynamiczny charakter opisanych zagrożeń jednoznacznie wskazują, że ochrona

użytkowników usług płatniczych nie może opierać się wyłącznie na rozwiązaniach technologicznych i regulacyjnych. Nawet najbardziej zaawansowane systemy bezpieczeństwa okazują się niewystarczające w sytuacji, gdy użytkownicy nie posiadają odpowiedniej wiedzy i umiejętności pozwalających rozpoznawać próby oszustw oraz właściwie reagować na incydenty. W tym kontekście kluczowego znaczenia nabiera edukacja finansowa i cyfrowa, rozumiana jako proces długofalowego budowania świadomości zagrożeń oraz odpowiedzialnych postaw wobec korzystania z usług płatniczych w środowisku cyfrowym.

Skala i złożoność współczesnych zagrożeń pokazują jednak, że skuteczna ochrona nie może opierać się wyłącznie na rozwoju technologii bezpieczeństwa, lecz wymaga również systematycznego podnoszenia świadomości użytkowników. W Polsce istotną rolę w podnoszeniu kompetencji cyfrowych użytkowników usług finansowych odgrywają instytucje sektora finansowego, które od lat realizują liczne programy edukacyjne. Ogłoszenie Roku Edukacji Ekonomicznej 2024 stworzyło ramy do pogłębionej refleksji nad rolą edukacji ekonomicznej, w tym także finansowej w warunkach postępującej cyfryzacji, ze szczególnym uwzględnieniem bezpieczeństwa korzystania z usług płatniczych – jednego z obszarów najbardziej narażonych na działania cyberprzestępcze. W ramach inicjatyw podejmowanych w Roku Edukacji Ekonomicznej 2024 szczególny nacisk położono na kształtowanie świadomego i krytycznie myślącego klienta, który potrafi nie tylko korzystać z nowoczesnych rozwiązań płatniczych, lecz także rozumie zasady bezpiecznego ich używania. Skuteczna edukacja w tym zakresie powinna mieć charakter praktyczny, być dostosowana do zróżnicowanych grup odbiorców oraz realizowana w sposób długofalowy i angażujący. Tylko takie podejście pozwala realnie ograniczać skuteczność cyberoszustw oraz wzmacniać zaufanie do cyfrowych narzędzi płatniczych i bankowości elektronicznej.

W ramach prac nad raportem wykorzystano zarówno dane wtórne – w tym publicznie dostępne statystyki, raporty branżowe oraz analizy eksperckie – jak i wyniki badania własnego. Badanie zostało przeprowadzone metodą ankiety internetowej (CAWI) wśród przedstawicieli różnych grup użytkowników usług płatniczych, takich jak studenci, osoby pracujące, seniorzy oraz przedsiębiorcy. Zebrane informacje pozwoliły zdiagnozować poziom świadomości zagrożeń, dotychczasowe doświadczenia z cyberincydentami oraz preferencje dotyczące form edukacji.

Opracowanie składa się z trzech głównych części, z których każda analizuje inny wymiar wyzwań i możliwości związanych z bezpieczeństwem usług płatniczych oraz rolą edukacji w ich ochronie. W pierwszej części przedstawiono charakterystykę współczesnych usług płatniczych, ich potencjał rozwojowy oraz kluczowe zagrożenia występujące w środowisku cyfrowym – od technik ataku po konsekwencje incydentów i dostępne mechanizmy zabezpieczeń. Druga część koncentruje się na edukacji finansowej jako cyfrowej tarczy ochronnej, prezentując zarówno klasyczne, jak i nowoczesne formy działań edukacyjnych, w tym rozwiązania interaktywne, oparte na doświadczeniu oraz perspektywy rozwoju edukacji finansowej wspieranej sztuczną inteligencją. Część trzecia stanowi podsumowanie wniosków z Roku Edukacji Ekonomicznej 2024, obejmując analizę dobrych praktyk oraz rekomendacje dotyczące skutecznego wzmacniania świadomości cyfrowej użytkowników usług płatniczych.

Raport jest skierowany do szerokiego grona odbiorców korzystających lub współtworzących cyfrowy ekosystem płatniczy. Obejmuje on zarówno klientów indywidualnych – w tym osoby aktywnie korzystające z bankowości elektronicznej, seniorów oraz młodzieży – jak i małe i średnie przedsiębiorstwa, które wymagają wsparcia w bezpiecznym korzystaniu z usług finansowych online. Grupa ta narażona jest na różnorodne cyberzagrożenia, dlatego raport dostarcza im praktycznych wskazówek, narzędzi edukacyjnych oraz rozwiązań wspierających świadome i bezpieczne korzystanie z cyfrowych usług płatniczych. Jednocześnie raport jest adresowany do instytucji i podmiotów odpowiedzialnych za bezpieczeństwo oraz rozwój rynku finansowego, takich jak sektor bankowy i fintech, instytucje nadzorcze, administracja publiczna, sektor edukacji, media oraz firmy oferujące usługi pozabankowe. To właśnie te podmioty – poprzez regulacje, nadzór, działania edukacyjne i projektowanie usług – kształtują standardy bezpieczeństwa oraz wpływają na poziom świadomości użytkowników. Opracowanie to ma na celu wspieranie ich w budowaniu spójnego, bezpiecznego środowiska płatniczego opartego na nowoczesnych technologiach, odpowiedzialnych praktykach i świadomych użytkownikach.

Raport ma charakter nie tylko diagnostyczny, lecz także aplikacyjny – jego celem jest dostarczenie wniosków i rekomendacji, które mogą stanowić podstawę do projektowania skutecznych działań edukacyjnych oraz komunikacyjnych w sektorze finansowym.

PROGRAM ANALITYCZNO BADAWCZY

Rozdział 1. Usługi płatnicze – możliwości i pułapki

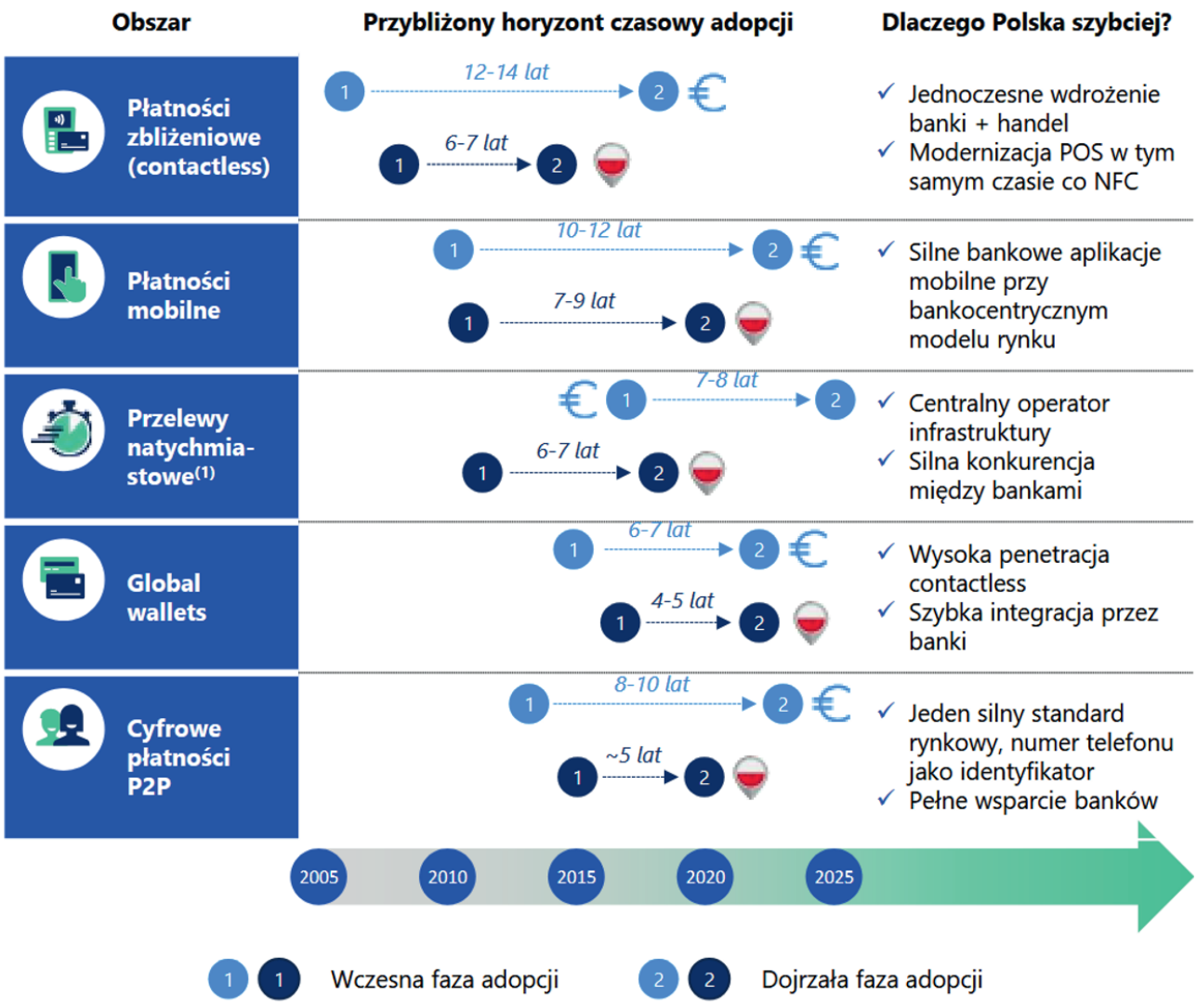
1.1. Rozwój rynku płatności w Polsce

Rynek usług płatniczych stanowi jeden z kluczowych elementów infrastruktury współczesnej gospodarki. Obejmuje on instytucje, instrumenty oraz systemy umożliwiające realizację transferów pieniężnych pomiędzy uczestnikami obrotu gospodarczego, zarówno w relacjach między konsumentami, przedsiębiorstwami, jak i instytucjami publicznymi. Sprawne funkcjonowanie systemów płatniczych ma fundamentalne znaczenie dla stabilności systemu finansowego oraz efektywności procesów gospodarczych, ponieważ umożliwia bezpieczny i szybki przepływ środków pieniężnych w gospodarce (KNF, 2024).

W ostatnich dwóch dekadach rynek płatności przeszedł dynamiczną transformację związaną z rozwojem technologii cyfrowych oraz zmianą zachowań użytkowników usług finansowych. Tradycyjne formy rozliczeń, oparte głównie na gotówce i przelewach bankowych, zostały uzupełnione przez szeroki wachlarz instrumentów płatniczych, takich jak płatności kartowe, mobilne, internetowe czy płatności natychmiastowe. Rozwój ten jest związany zarówno z postępem technologicznym, jak i z rosnącymi oczekiwaniami użytkowników dotyczącymi szybkości, wygody i dostępności usług finansowych (Iwańczuk-Kaliska i in., 2021).

Współczesny rynek usług płatniczych charakteryzuje się wysokim poziomem innowacyjności oraz silną konkurencją pomiędzy różnymi kategoriami dostawców usług. Oprócz banków coraz większą rolę odgrywają instytucje płatnicze, fintechy oraz globalne

Rysunek 1. Tempo adopcji rozwiązań płatniczych w Polsce i strefie euro



Źródło: (Fundacja Polska Bezgotówkowa, 2025, s. 31).

organizacje płatnicze oferujące nowoczesne rozwiązania technologiczne. W efekcie powstaje złożony ekosystem obejmujący zarówno instytucje finansowe, operatorów infrastruktury płatniczej, dostawców technologii, jak i regulatorów odpowiedzialnych za stabilność i bezpieczeństwo rynku. Polska stanowi przykład kraju, w którym transformacja rynku płatności dokonała się w relatywnie krótkim czasie. Jeszcze na początku XXI wieku udział płatności bezgotówkowych w transakcjach detalicznych pozostawał stosunkowo niski, jednak w kolejnych latach nastąpił dynamiczny wzrost zarówno liczby, jak i wartości transakcji elektronicznych (rysunek 1). W rezultacie polski system płatniczy należy obecnie do jednych z najbardziej dynamicznie rozwijających się w Europie, a użytkownicy usług finansowych szybko adaptują nowe rozwiązania technologiczne w obszarze płatności. Jedną z charakterystycznych cech polskiego rynku płatności jest wysoka intensywność korzystania z nowoczesnych instrumentów płatniczych (Fundacja Polska Bezgotówkowa, 2024).

Rozwój rynku płatności w Polsce znajduje odzwierciedlenie w danych dotyczących liczby instrumentów płatniczych, skali transakcji oraz infrastruktury akceptacji płatności (NBP, 2025). Na koniec września 2025 r. w obiegu znajdowało się 46,8 mln kart płatniczych, z czego zdecydowaną większość stanowiły karty debetowe (86,4%), natomiast karty kredytowe odpowiadały za 10,8% rynku. Charakterystyczną cechą polskiego systemu płatniczego jest bardzo wysoki poziom wykorzystania technologii zbliżeniowej – udział kart zbliżeniowych wyniósł 98,2% wszystkich wydanych kart. W III kwartale 2025 r. zrealizowano 2,9 mld transakcji kartami płatniczymi o łącznej wartości 364,8 mld zł, przy czym transakcje bezgotówkowe stanowiły 95,9% ich liczby. Płatności bezgotówkowe w zdecydowanej większości miały charakter zbliżeniowy, odpowiadając za 98% wszystkich transakcji bezgotówkowych. Dynamiczny rozwój rynku widoczny jest również w rozbudowie infrastruktury płatniczej. Na koniec września 2025 r. w Polsce funkcjonowało około 1,39 mln terminali płatniczych oraz 657 tys. akceptantów, co sprzyja dalszemu wzrostowi znaczenia płatności elektronicznych w gospodarce.

Jednocześnie rynek usług płatniczych funkcjonuje w silnie uregulowanym otoczeniu instytucjonalnym. Regulacje prawne dotyczące świadczenia usług płatniczych mają na celu zapewnienie stabilności systemu finansowego, ochrony użytkowników usług płatniczych oraz zapewnienie uczciwej konkurencji pomiędzy dostawcami usług. W Unii Europejskiej kluczową rolę odgrywają regulacje dotyczące usług płatniczych, w tym m.in. dyrektywa PSD2[1], która wprowadziła koncepcję otwartej bankowości oraz umożliwiła powstanie nowych modeli usług finansowych opartych na dostępie do danych rachunków bankowych za zgodą użytkownika. Znaczenie regulacji w obszarze usług płatniczych wynika również z konieczności zapewnienia bezpieczeństwa systemów finansowych oraz ochrony środków użytkowników usług płatniczych. Organy nadzorcze, w tym instytucje krajowe i europejskie, monitorują funkcjonowanie rynku oraz identyfikują potencjalne zagrożenia związane z rozwojem nowych technologii i nowych modeli biznesowych w sektorze finansowym. Wśród istotnych wyzwań wskazuje się m.in. rosnącą skalę cyberzagrożeń, konieczność zapewnienia odporności cyfrowej systemów finansowych oraz ochronę danych użytkowników usług finansowych (UKNF, 2026).

Dynamiczny rozwój rynku płatności powoduje również zmianę roli płatności w gospodarce. Coraz częściej płatność przestaje być odrębnym etapem procesu zakupowego i staje się integralnym elementem doświadczenia użytkownika, realizowanym automatycznie w ramach różnych usług cyfrowych. Rozwój technologii takich jak sztuczna inteligencja, IoF (Internet of Things) czy rozwiązania mobilne sprawia, że płatności coraz częściej są zintegrowane z innymi usługami cyfrowymi i realizowane w sposób niemal niewidoczny dla użytkownika. Wraz z postępującą cyfryzacją usług finansowych rośnie jednak również skala wyzwań związanych z bezpieczeństwem oraz poziomem kompetencji użytkowników. Badania międzynarodowe wskazują, że pomimo powszechnego korzystania z płatności cyfrowych znaczna część konsumentów nie posiada wystarczających kompetencji cyfrowych i finansowych pozwalających na bezpieczne korzystanie z tych usług, co zwiększa podatność na oszustwa oraz inne formy nadużyć w środowisku cyfrowym. W tym kontekście szczególnego znaczenia nabiera edukacja finansowa i cyfrowa użytkowników usług płatniczych, która stanowi jeden z kluczowych elementów budowania bezpiecznego ekosystemu płatniczego.

1 Obecnie na poziomie Unii Europejskiej prowadzone są prace legislacyjne nad nowymi regulacjami dotyczącymi rynku usług płatniczych – dyrektywą PSD3 (Payment Services Directive 3) oraz rozporządzeniem PSR (Payment Services Regulation), których celem jest dalsze wzmocnienie bezpieczeństwa płatności, ograniczenie oszustw oraz rozwój otwartej bankowości w Europie.

1.2. Rodzaje usług płatniczych

Współczesny rynek płatności charakteryzuje się dużą różnorodnością świadczonych usług – od tradycyjnych przelewów i operacji gotówkowych, po nowoczesne, zautomatyzowane formy płatności elektronicznych, portfele cyfrowe i usługi świadczone przez instytucje niebankowe. W niniejszym podrozdziale dokonana zostanie systematyczna klasyfikacja dostępnych na polskim rynku usług płatniczych, w oparciu o obowiązujące regulacje prawne.

Podstawę regulacji europejskiego rynku usług płatniczych stanowi obecnie dyrektywa w sprawie usług płatniczych - 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 (PSD2).[2] Celem unijnych regulacji w zakresie usług płatniczych jest przede wszystkim otwarcie rynku finansowego na możliwość świadczenia usług płatniczych przez podmioty inne niż banki, tj. instytucje płatnicze i podmioty prowadzące działalność w niewielkim zakresie (w Polsce – małe instytucje płatnicze i biura usług płatniczych). W Polsce, kluczową regulacją w zakresie świadczenia usług płatniczych jest Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (u.u.p.).

Przepisy u.u.p. wprowadziły zasadę, że usługi płatnicze mogą być wykonywane jedynie przez określoną grupę podmiotów - dostawców usług płatniczych. Do grupy tej należą, oprócz banków, m.in. instytucje płatnicze, instytucje pieniądza elektronicznego, małe instytucje płatnicze, biura usług płatniczych oraz dostawcy świadczący wyłącznie usługę dostępu do informacji o rachunku płatniczym. Prowadzenie działalności w charakterze krajowej instytucji płatniczej albo krajowej instytucji pieniądza elektronicznego wymaga uzyskania zezwolenia KNF (postępowanie licencyjne). W przypadku małej instytucji płatniczej, biura usług płatniczych lub dostawcy świadczącego wyłącznie usługę dostępu do informacji o rachunku wymagany jest jedynie wpis do rejestru usług płatniczych i wydawców pieniądza elektronicznego (postępowanie rejestrowe).

W przepisach u.u.p. brak jest odrębnej definicji usług płatniczych. Ustawa wskazuje jednak zamknięty katalog czynności, które uznaje się za świadczenie takich usług. W praktyce obejmują one m.in. prowadzenie rachunków płatniczych, realizację przelewów i poleceń zapłaty, obsługę płatności kartowych, wydawanie instrumentów płatniczych, przyjmowanie i dokonywanie wpłat oraz wypłat gotówki, świadczenie usługi przekazu pieniężnego, a także nowsze rozwiązania, takie jak inicjowanie transakcji płatniczej (PIS - Payment Initiation Service) czy dostęp do informacji o rachunku (AIS - Account Information Service) funkcjonujący w modelu otwartej bankowości. Szerszy, precyzyjny katalog rodzajów działalności uznawanych za usługi płatnicze został ujęty w art. 3 ustawy o usługach płatniczych i to do niego należy odwoływać się przy kwalifikowaniu danej aktywności jako regulowanej usługi płatniczej.

Dokonując oceny, czy dana działalność kwalifikuje się jako świadczenie usług płatniczych należy więc w pierwszej kolejności sprawdzić, czy mamy do czynienia z wchodzeniem w posiadanie środków pieniężnych będących przedmiotem transakcji płatniczej (nie dotyczy –usługi inicjowania transakcji płatniczej i usługi dostępu do informacji o rachunku), następnie czy nie zachodzą wyłączenia z art. 6 u.u.p. Obejmują one m.in. transakcje płatnicze dokonywane wyłącznie w gotówce między płatnikiem a odbiorcą, określone usługi o charakterze technicznym wspierające świadczenie usług płatniczych (jeżeli podmiot nie wchodzi w posiadanie środków pieniężnych), transakcje realizowane w ramach systemów płatności lub rozrachunku papierów wartościowych, a także instrumenty płatnicze o ograniczonym zastosowaniu. W takich przypadkach dana działalność nie podlega regulacjom ustawy o usługach płatniczych. Dopiero w przypadku braku zastosowania wyłączeń przewidzianych w art. 6 u.u.p. możliwe jest dokonanie kwalifikacji zamierzonej działalności do poszczególnych rodzajów usług płatniczych (KNF, 2023).

Na potrzeby niniejszego raportu skoncentrowano uwagę na usługach płatniczych wykorzystywanych w codziennych rozliczeniach klientów indywidualnych oraz małych i średnich przedsiębiorstw, realizowanych przede wszystkim w kanałach cyfrowych. Obejmują one w szczególności: płatności kartą w punktach handlowo-usługowych i w internecie, płatności mobilne (w tym BLIK i portfele cyfrowe), przelewy internetowe, zlecenia stałe i płatności cykliczne, a także wybrane usługi towarzyszące, takie

2 Szersza analiza uwarunkowań regulacyjnych oraz ryzyk związanych z usługami opartymi na otwartych interfejsach programistycznych (API) w kontekście implementacji Dyrektywy PSD2 została przedstawiona w raporcie *Bezpieczeństwo usług opartych o otwarte interfejsy programistyczne (API) w kontekście implementacji Dyrektywy PSD2* (Kostro i in., 2020).

jak szybkie płatności online czy usługi typu „pay-by--link". Poza zakresem analizy pozostają transakcje hurtowe rynku międzybankowego, rozliczenia skomplikowanych instrumentów finansowych oraz płatności realizowane wyłącznie w gotówce. Taki wybór obszaru badawczego jest uzasadniony specyfiką współczesnych zagrożeń cybernetycznych. To właśnie usługi płatnicze wykorzystywane na co dzień przez szerokie grono użytkowników – a zwłaszcza ich cyfrowe kanały obsługi – stanowią obecnie najczęstszy cel działań przestępczych. Ataki takie jak phishing, smishing, przejęcia kont, manipulacje socjotechniczne, malware mobilny, fałszywe bramki płatnicze czy oszustwa z wykorzystaniem deepfake'ów uderzają głównie w użytkowników dokonujących prostych, rutynowych transakcji. To w tych obszarach obserwuje się największą liczbę incydentów, straty finansowe oraz potrzebę intensywnej edukacji klientów. Skupienie analizy na usługach płatniczych powszechnie stosowanych w środowisku cyfrowym pozwala więc adekwatnie ocenić zarówno dynamikę zagrożeń, jak i skuteczność działań edukacyjnych oraz prewencyjnych.

1.3. Kategorie zagrożeń w usługach płatniczych

Zagrożenia w obszarze usług płatniczych można klasyfikować według różnych kryteriów – m.in. ze względu na zastosowaną technikę ataku, wykorzystywany kanał (bankowość internetowa, mobilna, płatności kartowe, BLIK) czy główny cel przestępców (kradzież danych, środków finansowych, tożsamości). Przyjęta w raporcie klasyfikacja pozostaje spójna z podejściem stosowanym m.in. w raportach ENISA, European Payments Council (2024) oraz w statystykach CERT Polska (2024), CSIRT NASK (2024) i CSIRT KNF (2024), które wyróżniają przede wszystkim zagrożenia oparte na socjotechnice, złośliwym oprogramowaniu, atakach na infrastrukturę, nadużyciach danych oraz czynniku ludzkim.

Na potrzeby niniejszego opracowania kategorie te uporządkowano w pięć głównych grup: (1) socjotechnika i wyłudzanie danych, (2) złośliwe oprogramowanie (malware), (3) ataki na kanały komunikacji i infrastrukturę usług płatniczych, (4) nadużycia danych osobowych i tożsamości oraz (5) błędy i nawyki użytkowników – które zostały syntetycznie zaprezentowane na rysunku 1, a następnie omówione poniżej (rysunek 2). Techniki ataku w poszczególnych kategoriach zostaną szczegółowo omówione w części 1.3.

a. Socjotechnika i wyłudzanie danych – obejmuje ataki oparte na manipulacji zachowaniem użytkownika, takie jak phishing (fałszywe e-maile), smishing (fałszywe SMS-y), vishing (oszustwa telefoniczne), spoofing numeru (podszywanie się pod inny numer telefonu lub nadawcę komunikatu) czy bardziej złożone scenariusze „na pracownika banku" oraz oszustwa typu BEC (Business Email Compromise – podszywanie się pod zaufanego nadawcę w korespondencji e-mail w celu wyłudzenia danych lub środków finansowych). Ich celem jest skłonienie ofiary do ujawnienia danych logowania, podania kodów autoryzacyjnych lub samodzielnego wykonania przelewu.

b. Złośliwe oprogramowanie (malware) – ta kategoria dotyczy m.in. trojanów bankowych, keyloggerów, fałszywych aplikacji mobilnych oraz ransomware. Po zainfekowaniu urządzenia użytkownika (telefonu lub komputera) złośliwe oprogramowanie może zostać wykorzystane przez przestępców do przechwytywania danych logowania, podmiany numeru rachunku odbiorcy, przejmowania sesji bankowości elektronicznej lub blokowania dostępu do danych.

c. Ataki na kanały i infrastrukturę – zagrożenia te obejmują m.in. ataki typu man-in-the-middle (MitM – przechwytywanie komunikacji między użytkownikiem a systemem, np. bankiem), przechwytywanie ruchu w publicznych sieciach Wi-Fi, fałszywe strony i bramki płatnicze, quishing (wykorzystanie złośliwych kodów QR prowadzących do fałszywych stron lub instalacji szkodliwego oprogramowania) oraz ataki DDoS na serwisy płatnicze (Distributed Denial of Service – przeciążenie serwera dużą liczbą zapytań w celu uniemożliwienia dostępu do usługi). Ataki te mogą prowadzić zarówno do kradzieży danych, jak i czasowego unieruchomienia usług płatniczych.

d. Nadużycia danych osobowych i tożsamości – chodzi o sytuacje, w których przejęte lub wykradzione dane osobowe są wykorzystywane do zakładania rachunków, zaciągania kredytów czy dokonywania transakcji w imieniu ofiary. Skutki takich zdarzeń są często długotrwałe i wykraczają poza pojedynczą transakcję, wpływając na wiarygodność klienta i zaufanie do instytucji finansowych.

e. Błędy i nawyki użytkowników – ta kategoria przenika wszystkie pozostałe obszary. Obejmuje m.in. używanie tych samych haseł

Rysunek 2. Kategorie zagrożeń w usługach płatniczych

Źródło: opracowanie własne.

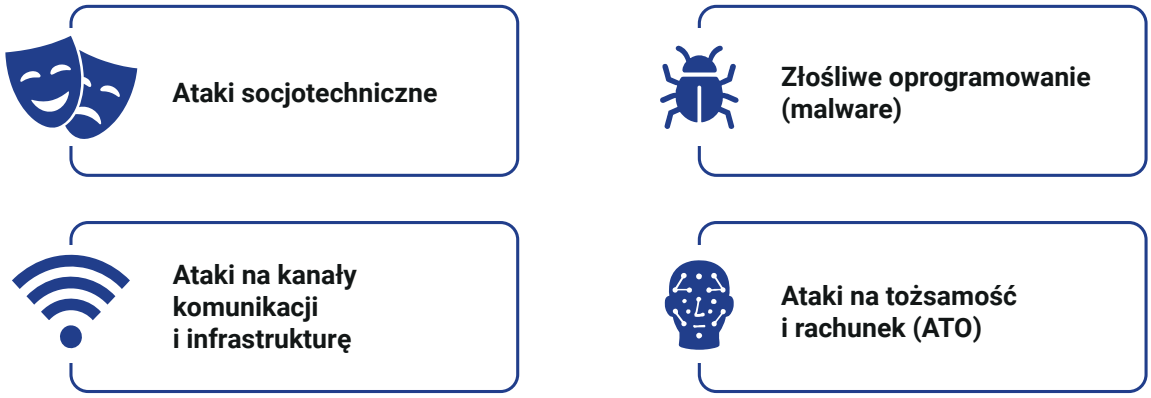
w wielu serwisach, brak aktualizacji systemów, instalowanie aplikacji z nieznanych źródeł, ignorowanie ostrzeżeń zabezpieczeń czy udostępnianie danych logowania osobom trzecim. Niska świadomość i brak podstawowej „higieny cyfrowej" znacząco zwiększają skuteczność większości ataków.

Poszczególne kategorie nie są od siebie całkowicie odseparowane – w wielu incydentach występują łącznie. Przykładowo, atak socjotechniczny (phishing lub smishing) może prowadzić do instalacji złośliwego oprogramowania na urządzeniu ofiary, a następnie umożliwić przejęcie sesji bankowości elektronicznej. Analiza wzmiankowanych raportów krajowych i europejskich pokazuje jednocześnie kilka istotnych tendencji. Po pierwsze, ciężar zagrożeń coraz wyraźniej przesuwa się z typowo technicznych ataków na infrastrukturę w stronę działań ukierunkowanych na użytkownika – w szczególności socjotechniki oraz złośliwego oprogramowania wymierzonego w urządzenia wykorzystywane do bankowości internetowej i mobilnej. Po drugie, rośnie znaczenie kanałów zdalnych i mobilnych, w których transakcje są realizowane szybko, często automatycznie oraz przy wysokim poziomie wygody, co zwiększa ryzyko popełnienia błędu lub pochopnego potwierdzenia operacji. Po trzecie, wiele incydentów ma obecnie charakter złożony – łączy elementy socjotechniki, nadużyć danych, błędów użytkownika oraz wykorzystania luk technicznych, co utrudnia ich jednoznaczną klasyfikację i wzmacnia potrzebę holistycznego podejścia do edukacji w zakresie bezpieczeństwa przy korzystaniu z cyfrowych kanałów płatniczych.

1.4. Przegląd technik ataku

Współczesne zagrożenia cybernetyczne w sektorze finansowym cechuje wysoki stopień złożoności i hybrydyzacji technik ataku. W praktyce wiele kampanii łączy różne elementy – np. phishing z malware, socjotechnikę z atakiem systemowym czy przejęcie konta z inżynierią QR. Przedstawiona w niniejszym podrozdziale typologia zagrożeń ma zatem charakter umowny i porządkujący, a nie ścisły technicznie

Rysunek 3. Wybrane techniki ataku na usługi płatnicze



Źródło: opracowanie własne.

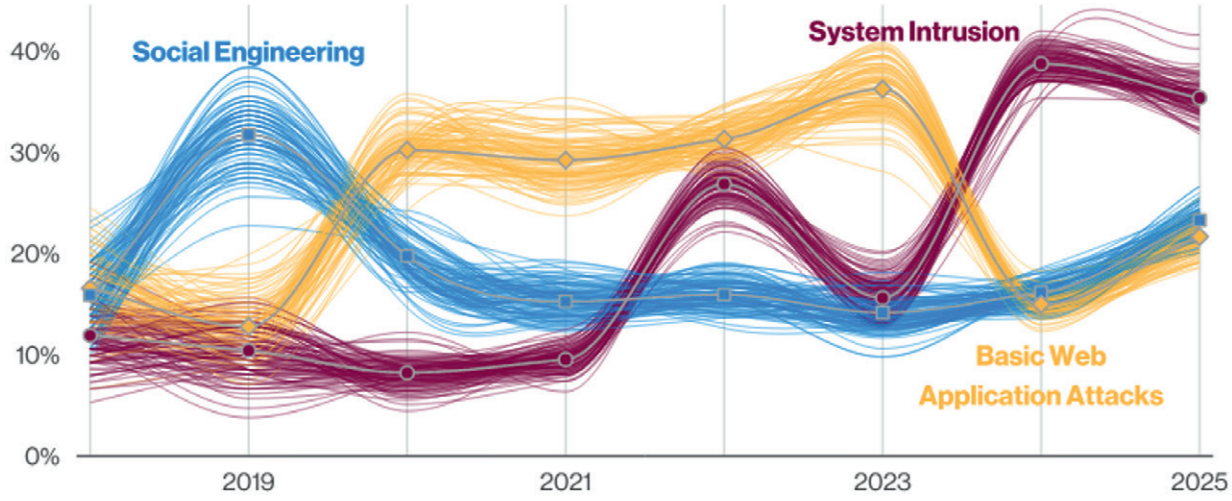
(rysunek 3). Jej celem jest wyodrębnienie kluczowych wektorów ataku i mechanizmów działania, które – choć często wzajemnie się przenikają – stanowią podstawę analizy ryzyka i budowania strategii obronnych. Przykładowo, quishing to technika należąca do szerokiej kategorii phishingu, jednak została opisana oddzielnie ze względu na rosnącą specyfikę i częstotliwość występowania w kontekście płatności mobilnych.

Na przestrzeni analizowanych lat (rysunek 4) widoczne są okresowe zmiany dominacji poszczególnych typów zagrożeń. W 2021 r. to ataki socjotechniczne osiągnęły najwyższy udział procentowy (powyżej 35%), natomiast w 2023-2025 dominującym wzorcem stały się ataki systemowe. Mimo to, udział ataków socjotechnicznych utrzymuje się na stabilnym poziomie i pozostaje istotnym wektorem naruszeń. Dane te podkreślają rosnącą złożoność i ewolucję zagrożeń w sektorze, a także konieczność kompleksowego podejścia do ochrony przed różnymi formami cyberataków.

1.4.1. Ataki socjotechniczne (social engineering)

Ataki socjotechniczne koncentrują się nie na łamaniu zabezpieczeń technicznych, lecz na manipulowaniu człowiekiem – jego emocjami, zaufaniem, stresem czy brakiem wiedzy. W praktyce są one dziś najsku-

Rysunek 4. Zmiany dominujących wzorców ataków w sektorze finansowym i ubezpieczeniowym w latach 2018–2025.



Źródło: Verizon Data Breach Investigations Report 2024, s. 12.

Notatka: Raport objął analizą 22 052 rzeczywistych incydentów bezpieczeństwa informacji, spośród których 12 195 zostało potwierdzonych jako naruszenia danych. Zdarzenia analizowane w okresie od 1 listopada 2023 r. do 31 października 2024 r. i dotyczyły organizacji różnej wielkości w 139 krajach świata.

teczniejszą formą cyberataków, co potwierdzają dane w Polsce i na świecie (CERT Polska, NASK, 2025).

Do najczęściej spotykanych form oszustw opartych na socjotechnice (social engineering) należą w szczególności:

- phishing – fałszywe wiadomości e-mail nakłaniające do ujawnienia danych lub kliknięcia w złośliwy link,
- spear-phishing – spersonalizowana forma phishingu skierowana do konkretnej osoby lub organizacji,
- smishing – wyłudzenia realizowane za pomocą fałszywych wiadomości SMS,
- vishing – oszustwa telefoniczne polegające na podszywaniu się pod instytucje lub zaufane osoby,
- spoofing – podszywanie się pod inny numer telefonu, adres e-mail lub nadawcę komunikatu,
- BEC (Business Email Compromise) – podszywanie się pod zaufanego nadawcę w korespondencji e-mail w celu wyłudzenia danych lub środków finansowych.

Do ataków opartych na komunikacji elektronicznej (masowe i ukierunkowane) należą ataki wykorzystujące e-mail, SMS-y oraz komunikatory internetowe. Ich celem jest nakłonienie ofiary do wykonania określonej czynności – kliknięcia w link, podania danych uwierzytelniających lub autoryzacji transakcji (Król, 2024; ENISA, 2024):

a. phishing polega na masowym rozsyłaniu wiadomości (e-mail, SMS, komunikatory), które podszywają się pod zaufane instytucje – banki, operatorów płatności, platformy e-commerce czy administrację publiczną. Celem jest skłonienie ofiary do: kliknięcia w złośliwy link, podania danych logowania, autoryzacji płatności.

b. spear-phishing to ukierunkowana odmiana phishingu polegająca na przygotowaniu spersonalizowanej wiadomości skierowanej do konkretnej osoby lub organizacji, z wykorzystaniem wcześniej pozyskanych informacji (np. o stanowisku, projektach czy relacjach służbowych). Whaling stanowi szczególną formę spear-phishingu, wymierzoną w członków najwyższej kadry zarządzającej (CEO, CFO), gdzie potencjalna wartość wyłudzonych środków jest zazwyczaj bardzo wysoka.

Ataki wykorzystujące telefonię i SMS (inżynieria głosu i numeru). Ta grupa obejmuje ataki, w których kluczową rolę odgrywa bezpośredni kontakt głosowy lub tekstowy oraz podszywanie się pod numer telefonu instytucji (KNF, CSIRT, 2024):

a. smishing wykorzystuje wiadomości SMS, często informujące o rzekomej blokadzie konta, dopłacie do paczki lub nieudanej transakcji.

b. vishing to analogiczny atak prowadzony przez rozmowy telefoniczne, w których przestępcy podszywają się np. pod konsultantów banku.

c. spoofing numerów telefonicznych (CLI spoofing) – ofiara widzi na ekranie numer banku, infolinii lub instytucji publicznej, co znacząco zwiększa wiarygodność oszustwa.

d. ataki wykorzystujące autorytet i relacje społeczne. Ataki te bazują na zaufaniu do instytucji publicznych lub więziach rodzinnych oraz na wywieraniu presji czasu. Oszustwa „na pracownika banku / policjanta / kuriera / członka rodziny" bazują na autorytecie i presji czasu. Przestępcy: podają się za pracowników banku lub policji, informują o „zagrożonych środkach" lub „tajnej akcji", nakłaniają do szybkiego przelewu, wypłaty gotówki lub przekazania kodów BLIK. Wariant „na członka rodziny" wykorzystuje silne emocje (strach, empatię), np. historię o wypadku lub nagłej potrzebie finansowej. Ataki te często łączą kilka kanałów jednocześnie (telefon + SMS + e-mail).

Ataki wymierzone w organizacje i procesy biznesowe. Do tej grupy należą ataki skierowane głównie przeciwko przedsiębiorstwom i instytucjom. BEC (ang. Business Email Compromise) to oszustwa wymierzone w firmy i instytucje. Atakujący: przejmują lub podszywają się pod skrzynkę e-mail pracownika, obserwują korespondencję biznesową, w odpowiednim momencie wysyłają fałszywą dyspozycję zmiany numeru rachunku lub pilnego przelewu. Straty z tytułu BEC należą do najwyższych w cyberprzestępczości, ponieważ pojedyncze transakcje mogą opiewać na miliony złotych.

Coraz powszechniejsze są fałszywe oferty inwestycji: w akcje znanych spółek, w kryptowaluty, w „gwarantowane" projekty finansowe. Reklamy prowadzą do profesjonalnie wyglądających stron, a kontakt z „doradcą" odbywa się telefonicznie lub przez komunikatory. Ofiary są często nakłaniane do użycia szybkich form płatności (BLIK, przelewy natychmiastowe), co utrudnia odzyskanie środków.

Dynamicznie rozwijającym się zagrożeniem są deepfake'i – syntetyczny głos prezesa lub dyrektora finansowego, spreparowane nagrania wideo czy fałszywe wideokonferencje. Technologia ta umożliwia bardzo realistyczne podszywanie się pod konkretne osoby, co znacząco zwiększa skuteczność wyłudzeń przelewów lub autoryzacji. Problem ten został podkreślony m.in. w raporcie *European Payments Council (2024), Payment Threats and Fraud Trends*, w którym techniki socjotechniczne (social engineering) wskazywane są jako jedno z kluczowych i rosnących ryzyk dla systemów płatniczych w Europie, zwłaszcza w kontekście coraz bardziej zaawansowanych metod manipulacji i inżynierii psychologicznej.

1.4.2. Techniki oparte na złośliwym oprogramowaniu

Złośliwe oprogramowanie (malware) pozostaje jednym z najważniejszych wektorów zagrożeń dla instytucji finansowych i ich klientów. Narzędzia tego typu, wykorzystywane przez cyberprzestępców do ataków na sektor finansowy i jego klientów, stają się coraz bardziej zautomatyzowane, modularne i trudne do wykrycia. Współczesne kampanie cyberprzestępcze wykorzystują zaawansowane, zróżnicowane typy malware'u, często łącząc je z socjotechniką i atakami wieloetapowymi (ENISA, 2024; CERT Polska, 2024; EPC, 2024):

a. trojany bankowe, zarówno desktopowe, jak i mobilne, stanowią podstawowe narzędzie służące do kradzieży danych uwierzytelniających oraz przejmowania kontroli nad kontami bankowymi użytkowników. Zagrożenie ze strony banking trojans utrzymuje się na wysokim poziomie w całym sektorze finansowym, przy czym ich szczególną odmianą są trojany dostosowane do systemów mobilnych, takich jak Anubis czy FluBot, ukierunkowane na klientów indywidualnych (Lookout, 2021).

b. keyloggery i infostealery to zaawansowane klasy złośliwego oprogramowania, których podstawowym celem jest rejestrowanie i przechwytywanie danych wprowadzanych przez użytkownika oraz kradzież wrażliwych informacji. Keyloggery działają na poziomie systemu, monitorując i zapisując naciśnięcia klawiszy – dzięki temu mogą pozyskiwać dane logowania do kont bankowych, hasła, tokeny uwierzytelniające czy dane kart płatniczych bez wiedzy użytkownika. Infostealery natomiast są modułami, które aktywnie wyszukują i wysyłają na serwery kontrolowane przez atakujących określone typy danych, takie jak pliki konfiguracyjne przeglądarek, ciasteczka sesji, klucze API, dane finansowe lub inne poufne informacje zgromadzone na urządzeniu ofiary.

c. fałszywe aplikacje mobilne, które podszywają się pod legalne aplikacje bankowe lub bramki płatnicze. Użytkownik zostaje nakłoniony do ich pobrania np. poprzez fałszywe strony www, reklamy, komunikatory czy wiadomości SMS. CERT Polska (2025) regularnie odnotowuje kampanie tego typu, w których złośliwe aplikacje są dystrybuowane z wykorzystaniem SMS phishingu (smishingu) – zawierającego link do rzekomej „aktualizacji aplikacji bankowej".

d. ransomware stanowi jedno z najpoważniejszych zagrożeń dla sektora finansowego, ponieważ może prowadzić do paraliżu kluczowych usług, czasowego wstrzymania operacji bankowych, a nawet trwałych strat operacyjnych i reputacyjnych. Szczególnie niebezpieczne są kampanie prowadzone przez grupy typu APT (ang. Advanced Persistent Threats), które łączą klasyczne techniki infekcji z zaawansowanym rozpoznaniem środowiska sieciowego oraz eskalacją uprawnień wewnątrz systemów. Tego rodzaju złożone ataki charakteryzują się długofalowym i ukierunkowanym działaniem, obejmującym m.in. identyfikację kluczowych zasobów, lateralne poruszanie się w sieci oraz precyzyjne wdrażanie ransomware w newralgicznych punktach infrastruktury. Efektem może być pełne unieruchomienie działalności instytucji finansowej, wymuszenie okupu, a w niektórych przypadkach – również wyciek danych wrażliwych. Współczesne kampanie ransomware coraz częściej wykorzystują model double extortion, czyli połączenie szyfrowania danych z groźbą ich ujawnienia (KNF, CSIRT, 2024b).

1.4.3. Ataki na kanały komunikacji i infrastrukturę płatniczą

Wraz z postępującą cyfryzacją usług finansowych rośnie liczba zagrożeń ukierunkowanych na infrastrukturę komunikacyjną i technologiczną, która pośredniczy w realizacji transakcji płatniczych. Atakujący wykorzystują luki w zabezpieczeniach sieciowych, błędy konfiguracji oraz nieuwagę użytkowników końcowych, by przechwycić dane, zakłócić działanie systemów lub przejąć kontrolę nad procesami autoryzacyjnymi (DFP, 2025):

a. ataki typu Man-in-the-Middle (MitM) polegają na przechwyceniu komunikacji pomiędzy użytkownikiem a instytucją finansową – często w niezabezpieczonych sieciach Wi-Fi (np. publicznych hotspotach). Przestępca może w ten sposób uzyskać dostęp do danych logowania, sesji płatniczych czy numerów kart. Zabezpieczenie kanałów transmisji danych (np. poprzez szyfrowanie, stosowanie TLS, SCA i monitoring behawioralny) jest kluczowe w zapobieganiu tego rodzaju incydentom.

b. fałszywe strony logowania i bramki płatnicze (np. podszywające się pod pay-by-link, komunikaty operatorów płatności lub banków) służą do phishingu danych logowania, kodów SMS czy danych kart płatniczych. Użytkownikowi prezentowany jest interfejs identyczny z prawdziwym, często w ramach fałszywego komunikatu SMS, e-maila lub reklamy w wyszukiwarce. Zagrożenie to jest stale obecne i wysoce skuteczne, szczególnie gdy towarzyszy mu presja czasu lub kontekst finansowy (np. „dopłata do przesyłki").

c. quishing, czyli phishing za pomocą kodów QR, to technika coraz częściej wykorzystywana do przekierowywania użytkowników na złośliwe strony płatnicze lub autoryzacyjne. Przestępcy podmieniają kody QR w przestrzeni publicznej (np. na parkometrach, plakatach, automatów płatniczych), przekierowując użytkowników na fałszywe strony przejęcia danych. Technika ta zyskuje popularność z uwagi na łatwość wdrożenia i rosnącą powszechność skanowania kodów QR w usługach płatniczych.

d. ataki DDoS (ang. Distributed Denial of Service – polegające na przeciążeniu serwera lub usługi online dużą liczbą zapytań w celu zablokowania działania strony internetowej lub systemu) na serwisy bankowości internetowej lub operatorów płatności nie służą jedynie zakłóceniu działania usług. W niektórych przypadkach są one stosowane jako element szantażu, rozpraszania uwagi zespołów bezpieczeństwa lub maskowania innych ataków, np. transferu środków w tle. Skoordynowane kampanie DDoS coraz częściej angażują botnety (sieci przejętych i zainfekowanych urządzeń, takich jak komputery lub urządzenia IoT – (Internet of Things – czyli urządzenia podłączone do internetu) oraz techniki ataku warstwowego (np. jednoczesne przeciążenie API – Application Programming Interface, interfejs programowania aplikacji, DNS – Domain Name System, systemu tłumaczącego nazwy domen na adresy IP, oraz aplikacji webowej).ataki na API i systemy otwartej bankowości (open banking) stanowią szczególne zagrożenie ze względu na strukturę współdzielonych danych i autoryzacji między różnymi podmiotami. Cyberprzestępcy mogą próbować wykorzystać niedoskonałości w implementacji, błędy uprawnień lub niewystarczającą walidację żądań, by uzyskać dostęp do kont użytkowników lub manipulować transakcjami. Chociaż poziom zabezpieczeń tych interfejsów systematycznie rośnie, wskazuje się, że są one celem zaawansowanych ataków z użyciem botów, automatyzacji i testowania słabych punktów w czasie rzeczywistym.

1.4.4. Ataki na tożsamość i rachunek (account takeover)

Ataki na tożsamość cyfrową i przejęcia kont użytkowników (tzw. *account takeover*, ATO) należą do jednej z najgroźniejszych i jednocześnie najbardziej rosnących kategorii zagrożeń w usługach płatniczych. W przeciwieństwie do incydentów jednorazowych, takich jak kliknięcie w fałszywy link czy instalacja malware, skutki przejęcia tożsamości lub konta są często długofalowe i trudne do odwrócenia – mogą prowadzić do utraty środków, zaciągnięcia zobowiązań, a nawet naruszenia wiarygodności finansowej ofiary. Do najczęściej wykorzystywanych technik przejęcia tożsamości i kont należą (EPC, 2024):

a. przejęcia kont z wykorzystaniem wycieków danych (ATO + credential stuffing). Cyberprzestępcy masowo korzystają z danych uwierzytelniających wykradzionych w wyniku wcześniejszych wycieków – m.in. loginów, haseł,

tokenów. Zastosowanie techniki *credential stuffing* polega na automatycznym testowaniu tych danych w różnych serwisach (np. bankowość internetowa, aplikacje mobilne), licząc na to, że użytkownik stosuje te same dane logowania w wielu miejscach. Ze względu na powszechność tego zjawiska, ATO należy dziś do najczęstszych źródeł fraudów płatniczych w Europie.

b. nadużycia związane z dokumentami tożsamości i zdalną identyfikacją. Coraz więcej instytucji finansowych umożliwia zdalne zakładanie kont i korzystanie z usług przy użyciu skanów dowodów osobistych, selfie, podpisów elektronicznych. Przestępcy wykorzystują skradzione lub spreparowane dokumenty (np. z dark webu) do zakładania nowych rachunków, których następnie używają w działalności przestępczej. Nadużycia te obejmują również rejestrację kont do oszustw inwestycyjnych, kryptowalutowych lub wyłudzania płatności.

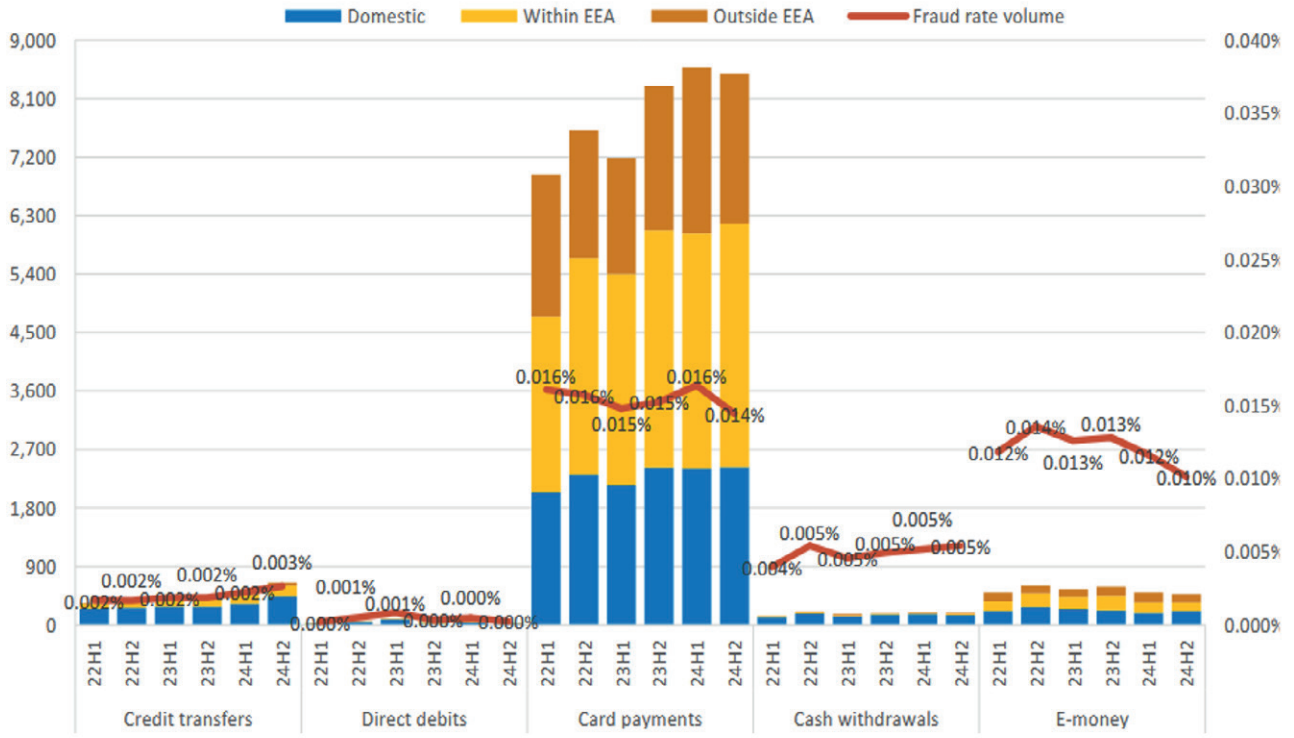
c. fałszywe tożsamości syntetyczne (ang. synthetic identity fraud). Zjawisko to polega na tworzeniu nowej, fikcyjnej tożsamości na bazie fragmentów danych różnych osób (np. PESEL jednej osoby, adres innej, fałszywe dane kontaktowe). Taka „osoba" może skutecznie przejść podstawowe procesy weryfikacyjne i uzyskać dostęp do usług płatniczych – zwłaszcza w przypadkach uproszczonych procedur rejestracji. Fraud syntetyczny stanowi rosnące zagrożenie, ponieważ jest trudniejszy do wykrycia i często ujawnia się dopiero po zaciągnięciu zobowiązań finansowych.

d. zmiany danych odbiorcy i manipulacje na rachunku. W praktyce wielu incydentów przestępcy, po uzyskaniu dostępu do konta, dokonują zmiany numeru rachunku odbiorcy w zapisanych zleceniach cyklicznych lub poleceniach zapłaty. Alternatywnie, podszywają się pod kontrahenta (np. w ramach ataku typu Business Email Compromise) i przesyłają fałszywą fakturę z nowym numerem konta. Techniki te są szczególnie skuteczne w środowisku MŚP oraz wśród użytkowników nieposiadających weryfikacji drugiego poziomu (np. dwuetapowej autoryzacji).

Konsekwencje przejęcia konta mogą być bardzo poważne – obejmują zarówno bezpośrednie straty finansowe (np. nieautoryzowane przelewy), jak i utratę reputacji czy czasowe zablokowanie dostępu do środków w trakcie postępowania wyjaśniającego. W przypadku wykorzystania danych do wyłudzeń kredytów lub założenia rachunku problem może dodatkowo wpływać na historię kredytową klienta w Biurze Informacji Kredytowej (BIK), czyli instytucji gromadzącej dane o zobowiązaniach kredytowych, a jego rozwiązanie często wymaga długotrwałych procedur administracyjno-prawnych. Skuteczna ochrona przed przejęciem kont wymaga zintegrowanego podejścia zarówno po stronie instytucji finansowych, jak i użytkowników usług płatniczych. Po stronie instytucji kluczową rolę odgrywają m.in. silne uwierzytelnianie użytkowników (SCA – Strong Customer Authentication), systemy monitorowania anomalii w zachowaniu użytkowników (*behavioral analytics*), a także współpraca między bankami, instytucjami płatniczymi oraz innymi podmiotami rynku finansowego w zakresie identyfikowania schematów fraudowych. Jednocześnie należy podkreślić, że skuteczna ochrona przed przejęciem kont nie zależy wyłącznie od działań instytucji finansowych. Istotną rolę odgrywają również działania samych użytkowników, takie jak stosowanie silnych i unikalnych haseł, korzystanie z dwuetapowej autoryzacji, ostrożność wobec podejrzanych wiadomości oraz unikanie ponownego używania tych samych danych logowania w różnych serwisach.

Analizy prowadzone na poziomie europejskim (rysunek 5) wskazują na istotne zróżnicowanie skali oraz struktury oszustw w zależności od rodzaju instrumentu płatniczego (EBA, 2025). Dane pokazują, że w ujęciu wartościowym największe straty finansowe generowane są przez oszustwa związane z przelewami, zwłaszcza elektronicznymi. Zjawisko to jest często powiązane z rosnącą skalą ataków opartych na socjotechnice, w tym oszustw typu authorised push payment (APP), polegających na nakłonieniu użytkownika do samodzielnego wykonania przelewu na rachunek kontrolowany przez przestępców, a także z przejęciami tożsamości lub kont użytkowników (account takeover). Jednocześnie dane wskazują, że płatności kartowe – mimo relatywnie niższej średniej wartości pojedynczej transakcji fraudowej – odpowiadają za największą liczbę incydentów. Z analiz EBA wynika również, że szczególnie wysoki poziom nadużyć obserwowany jest w przypadku transakcji zdalnych oraz płatności transgranicznych, zwłaszcza realizowanych poza Europejskim Obszarem Gospodarczym, gdzie wskaźniki fraudów pozostają wyższe niż w transakcjach krajowych i wewnątrzunijnych.

Rysunek 5. Poziom oszustw w ujęciu bezwzględnym i względnym według rodzaju instrumentu płatniczego (wolumen)



Źródło: EBA, 2025, s. 11.

Notatka: lewa oś: łączna liczba przypadków oszustw (w milionach transakcji); prawa oś: udział oszustw w całkowitej liczbie transakcji danego rodzaju.

Zjawisko to potwierdza podatność ekosystemu kartowego na ataki o charakterze masowym, wykorzystujące skradzione dane uwierzytelniające oraz ograniczone zastosowanie silnego uwierzytelniania klienta. Struktura wolumenu i wartości oszustw pokazuje wyraźne zróżnicowanie profilu ryzyka pomiędzy instrumentami płatniczymi. Przelewy charakteryzują się niską liczbą incydentów, lecz wysoką wartością strat jednostkowych, natomiast w przypadku kart płatniczych obserwuje się odwrotną zależność – wysoką częstotliwość zdarzeń przy relatywnie niskich kwotach pojedynczych nadużyć. Wskazuje to na odmienne strategie działania sprawców oraz różne mechanizmy podatności użytkowników końcowych. Zestawione dane potwierdzają, że skuteczność współczesnych ataków nie wynika wyłącznie z zaawansowania technicznego wykorzystywanych narzędzi, lecz w dużej mierze z eksploatacji zachowań, błędów poznawczych oraz zaufania użytkowników usług płatniczych. W tym kontekście czynnik ludzki pozostaje jednym z kluczowych wektorów ryzyka, którego znaczenie nie jest w pełni kompensowane nawet przez rosnący poziom zabezpieczeń technicznych.

Przegląd technik ataku wskazuje, że współczesne zagrożenia w usługach płatniczych nie mają wyłącznie charakteru zewnętrznego i technicznego, lecz bardzo często są ściśle powiązane z zachowaniami użytkowników końcowych. Znajduje to odzwierciedlenie również w klasyfikacji stosowanej na poziomie regulacyjnym, w której wyróżnia się fraud w transakcjach autoryzowanych przez użytkownika oraz fraud w transakcjach nieautoryzowanych (EBA, 2025). W pierwszym przypadku do incydentu dochodzi mimo prawidłowego działania zabezpieczeń technicznych, ponieważ użytkownik – działając pod wpływem socjotechniki, ale także braku wystarczającej wiedzy, ograniczonej świadomości zagrożeń, presji czasu, tempa życia cyfrowego lub zwykłej nieuwagi – samodzielnie zatwierdza transakcję lub ujawnia dane uwierzytelniające. W drugim przypadku naruszenie następuje bez wiedzy i zgody użytkownika, najczęściej w wyniku wykorzystania luk technicznych lub złośliwego oprogramowania. Działania takie jak nieostrożne kliknięcie w link, instalacja niezweryfikowanej aplikacji, ujawnienie danych uwierzytelniających czy stosowanie słabych i powtarzalnych haseł mogą zatem stanowić bezpośrednią przyczynę incydentu bezpieczeństwa, ale jednocześnie – w przypadku przejęcia konta lub tożsamości – stają się jego długofalową konsekwencją, prowadząc do eskalacji strat finansowych i organizacyjnych. W tym

sensie użytkownik usług płatniczych funkcjonuje zarówno jako potencjalny cel ataku, jak i jego istotne ogniwo, którego decyzje wpływają na skuteczność mechanizmów ochronnych. Zależność ta podkreśla potrzebę postrzegania cyberzagrożeń w sposób holistyczny, łączący perspektywę technologiczną, organizacyjną oraz behawioralną, co znajduje odzwierciedlenie w dalszej analizie konsekwencji incydentów oraz roli edukacji jako narzędzia prewencyjnego.

1.5. Konsekwencje incydentów

Naruszenia bezpieczeństwa związane z usługami płatniczymi niosą za sobą wielowymiarowe konsekwencje dla klientów indywidualnych oraz małych i średnich przedsiębiorstw. Ich skutki nie ograniczają się wyłącznie do bezpośrednich strat finansowych, lecz obejmują również konsekwencje organizacyjne, psychologiczne oraz długoterminowe efekty ekonomiczne, wpływające na sposób korzystania z usług finansowych oraz poziom zaufania do instytucji sektora bankowego. Analiza tych konsekwencji została przeprowadzona w oparciu o dane wtórne, obejmujące w szczególności raporty branżowe publikowane w ostatnich latach, a także o wyniki badania własnego przeprowadzonego metodą ankiety internetowej (CAWI) w okresie listopad-grudzień 2025 r.. Wyniki te pozwalają uzupełnić perspektywę makroekonomiczną o doświadczenia, postawy i percepcję zagrożeń po stronie użytkowników usług płatniczych (tabela 1).

Badanie ankietowe zostało w pierwszej kolejności rozpowszechnione wśród osób od 18 do 25 roku życia, którzy stanowili pierwszą, docelową grupę badania. Osoby należące do tzw. pokolenia Z charakteryzują się wysokim poziomem aktywności w środowisku cyfrowym, częstym korzystaniem z płatności elektronicznych oraz intensywną obecnością w sieci, co czyni je istotną grupą z punktu widzenia analizy zagrożeń cyberbezpieczeństwa oraz skuteczności działań edukacyjnych w obszarze usług płatniczych. Jednocześnie dystrybucja ankiety nie została ograniczona wyłącznie do tej kategorii wiekowej. Kwestionariusz udostępniono szerzej, umożliwiając udział respondentom reprezentującym różne grupy wiekowe oraz statusy zawodowe. Takie podejście pozwoliło na uwzględnienie zróżnicowanych doświadczeń użytkowników usług płatniczych, w tym również osób potencjalnie bardziej narażonych na zagrożenia cybernetyczne, np. osób starszych.

Internetowy charakter badania oraz otwarty sposób dystrybucji kwestionariusza umożliwiły pozyskanie opinii i doświadczeń także tych grup, choć ich udział w próbie był zróżnicowany. Uzyskane wyniki należy zatem traktować jako badanie o charakterze eksploracyjnym, ukazujące postawy, doświadczenia oraz subiektywne odczucia respondentów wobec zagrożeń związanych z płatnościami elektronicznymi[3]. Zebrane dane dostarczają wartościowego wglądu w sposób postrzegania ryzyka przez najbardziej aktywnych użytkowników usług płatniczych, a jednocześnie stanowią punkt wyjścia do dalszych, pogłębionych badań obejmujących w większym stopniu starsze grupy wiekowe oraz inne kategorie zawodowe.

1.5.1. Konsekwencje incydentów – informacje z analiz rynkowych i raportów

Incydenty cyberbezpieczeństwa w obszarze usług finansowych generują zróżnicowane i wielowymiarowe konsekwencje, które wykraczają daleko poza jednorazowe straty finansowe. Analiza danych z raportów branżowych wskazuje, że skutki te mają charakter finansowy, operacyjny, psychologiczny oraz długofalowy, a ich intensywność i przebieg zależą zarówno od rodzaju incydentu, jak i od pozycji podmiotu dotkniętego zdarzeniem – w szczególności od tego, czy jest nim klient indywidualny, instytucja finansowa czy przedsiębiorstwo sektora MŚP (rysunek 5).

Najczęściej identyfikowaną i bezpośrednio odczuwaną konsekwencją incydentów cyberbezpieczeństwa są straty finansowe ponoszone przez klientów indywidualnych, wynikające z nieautoryzowanych transakcji, przejęć kont użytkowników oraz oszustw typu authorised push payment (APP). Zgodnie z raportem Związku Przedsiębiorstw Finansowych i EY (2025), to właśnie klienci indywidualni zostali wskazani przez 63% instytucji finansowych jako grupa najbardziej narażona na skutki nadużyć. Jednocześnie instytucje raportują rosnącą liczbę przypadków przejęć kont oraz fraudów opartych na socjotechnice, co potwierdza utrzymującą się asymetrię ryzyka pomiędzy użytkownikami końcowymi a podmiotami profesjonalnymi. Skala strat jest dodatkowo wzmac-

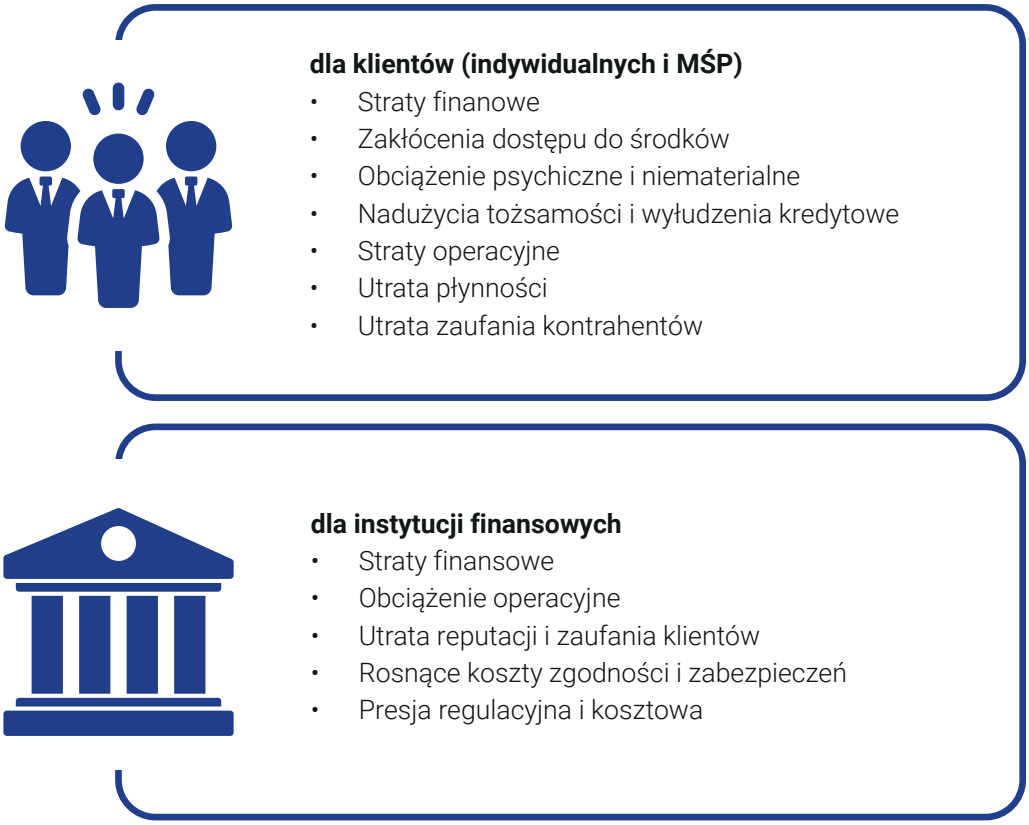
3 Warto dodać, że badania nad zachowaniami płatniczymi Polaków prowadzone są przez instytucje publiczne i branżowe (m.in. KNF, NBP, WIB) które publikują raporty dotyczące korzystania z instrumentów płatniczych, poziomu ubankowienia oraz postaw użytkowników wobec nowych technologii płatniczych.

Tabela 1. Charakterystyka socjodemograficzna respondentów

Zmienna	Kategoria	Liczba respondentów (N)	Udział (%)
Wiek	poniżej 18 lat	63	11.2%
	18–25 lat	393	69.9%
	26–30 lat	17	3%
	31–44 lata	26	4.6%
	45–59 lat	31	5.5%
	60 lat i więcej	32	5.7%
Płeć	kobieta	329	58.5%
	mężczyzna	220	39.1%
	inna / wolę nie podawać	13	2.3%
Status zawodowy*	uczeń / student	430	76.5%
	osoba pracująca	85	15.1%
	przedsiębiorca	11	2%
	emeryt / rencista	30	5.3%
	osoba nieaktywna zawodowo	2	0.4%
	inny	4	0.7%
Miejsce zamieszkania	wieś	120	21.4%
	małe miasto (do 50 tys.)	113	20.1%
	średnie miasto (50–200 tys.)	83	14.8%
	duże miasto (powyżej 200 tys.)	246	43.8%
Σ		562	100%

Źródło: opracowanie własne na podstawie badania własnego.
*Notatka: * w przypadku łączenia kilku ról, respondenci kierowali się główną aktywnością – np. dla pracujących studentów: „uczeń / student", a dla pracujących emerytów: „emeryt / rencista".*

Rysunek 5. Najczęstsze konsekwencje występowania incydentów cyberbezpieczeństwa



Źródło: opracowanie własne na podstawia analizowanych raportów

niana przez rozwój nowych wektorów zagrożeń, takich jak deepfake wykorzystywany w kanałach zdalnych, generatywna sztuczna inteligencja służąca do tworzenia fałszywych tożsamości i dokumentów oraz coraz bardziej zaawansowane techniki manipulacji psychologicznej, które utrudniają wykrywanie nadużyć i zwiększają potencjalne straty zarówno po stronie klientów, jak i instytucji finansowych.

Istotnym, choć często pomijanym skutkiem incydentów cyberbezpieczeństwa są zakłócenia w dostępie do środków finansowych, będące konsekwencją działań ochronnych podejmowanych przez instytucje finansowe. Z danych raportu „Cyberbezpieczny portfel" (WIB, 2024) wynika, że 54% użytkowników postrzega banki jako liderów cyberbezpieczeństwa, co przekłada się na wysokie oczekiwania wobec stosowanych mechanizmów prewencyjnych. W praktyce jednak środki takie jak blokada rachunku, wstrzymanie transakcji czy czasowe ograniczenie dostępu do konta – mimo że mają charakter ochronny – często prowadzą do realnych trudności w codziennym funkcjonowaniu klientów. Procedury wyjaśniające i analizy ryzyka mogą trwać od kilku dni do nawet kilku tygodni, w trakcie których użytkownicy pozbawieni są dostępu do bieżących środków, co utrudnia regulowanie zobowiązań finansowych, dokonywanie płatności czy wypłaty gotówki.

Na podatność klientów na incydenty cyberbezpieczeństwa istotny wpływ mają czynniki behawioralne i kompetencyjne. Badania WIB (2024) wskazują, że mimo rosnącej świadomości zagrożeń to człowiek pozostaje najsłabszym ogniwem systemu bezpieczeństwa cyfrowego. Choć większość respondentów deklaruje posiadanie aktualnego oprogramowania antywirusowego na komputerze, znaczna część użytkowników nie stosuje podstawowych zasad ochrony urządzeń mobilnych i danych uwierzytelniających. Niski poziom wykorzystania uwierzytelniania wieloskładnikowego, menedżerów haseł czy regularnej zmiany danych dostępowych zwiększa podatność na phishing, malware oraz wyłudzenia tożsamości, co w konsekwencji inicjuje incydenty wymagające kosztownych i długotrwałych procedur prewencyjnych po stronie instytucji finansowych.

Konsekwencje incydentów cyberbezpieczeństwa nie ograniczają się jednak wyłącznie do wymiaru finansowego i operacyjnego. Istotną kategorię stanowią

obciążenia psychologiczne i niematerialne, które są trudniejsze do jednoznacznego oszacowania, lecz powszechnie i intensywnie odczuwalne przez osoby dotknięte cyberoszustwami. Doświadczenie naruszenia bezpieczeństwa wiąże się ze stresem, lękiem, poczuciem zagrożenia oraz trwałą utratą zaufania do kanałów cyfrowych i instytucji finansowych. Skutki te często utrzymują się długo po formalnym zakończeniu incydentu, prowadząc do ograniczania korzystania z bankowości elektronicznej, zmniejszenia liczby transakcji online lub rezygnacji z części usług cyfrowych. W wymiarze społecznym incydenty mogą generować także poczucie wstydu lub winy, co ogranicza skłonność poszkodowanych do zgłaszania zdarzeń i poszukiwania wsparcia (WIB, 2024).

Szczególnie dotkliwy charakter mają incydenty cyberbezpieczeństwa w sektorze MŚP, gdzie ich skutki często przybierają formę kaskadową i długotrwałą. Jak wskazuje Barometr cyberbezpieczeństwa KPMG (2024), 66% badanych firm w Polsce doświadczyło w 2023 r. co najmniej jednego incydentu bezpieczeństwa. Dla mniejszych podmiotów zdarzenia te oznaczają przestoje systemów IT, ograniczenie dostępności kluczowych usług, konieczność ręcznego odtwarzania procesów oraz czasowe wyłączenie kanałów sprzedaży i komunikacji z klientami. Przy ograniczonych zasobach finansowych i kadrowych prowadzi to często do przesunięcia priorytetów biznesowych, rezygnacji z planowanych inwestycji oraz wzrostu ryzyka utraty płynności operacyjnej.

Skutki incydentów cyberbezpieczeństwa wykraczają poza poziom pojedynczych klientów i instytucji, oddziałując na cały system finansowy oraz postawy społeczne wobec płatności cyfrowych. Jednym z kluczowych efektów jest osłabienie zaufania do bankowości elektronicznej i nowoczesnych form płatności, co może prowadzić do ograniczania korzystania z kanałów cyfrowych, a w skrajnych przypadkach – do deklarowanego „powrotu do gotówki". Zjawisko to jest szczególnie widoczne wśród osób starszych oraz użytkowników, którzy doświadczyli incydentów lub zetknęli się z nimi pośrednio poprzez przekazy medialne. Spadek zaufania społecznego wpływa także na tempo wdrażania innowacji finansowych. Rozwiązania takie jak otwarta bankowość, portfele cyfrowe czy nowe modele płatności mobilnych wymagają akceptacji i aktywnego udziału użytkowników. Wysoka percepcja ryzyka może skutkować niechęcią do korzystania z nowych usług, co z kolei ogranicza potencjał rozwojowy rynku oraz zmniejsza efektywność inwestycji technologicznych.

Incydenty bezpieczeństwa generują również presję regulacyjną oraz wzrost kosztów funkcjonowania całego ekosystemu płatniczego. Kluczową rolę odgrywają w tym zakresie regulacje unijne, w szczególności dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2) oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w sprawie cyfrowej odporności operacyjnej sektora finansowego (DORA) (European Parliament & Council of the European Union, 2022a, 2022b). Akty te istotnie rozszerzają zakres podmiotowy i przedmiotowy wymagań dotyczących zarządzania ryzykiem ICT, reagowania na incydenty, ich raportowania oraz testowania odporności operacyjnej instytucji finansowych i podmiotów powiązanych (European Parliament & Council of the European Union, 2022a). Wprowadzenie tych regulacji oznacza, że incydenty cyberbezpieczeństwa przestają być postrzegane wyłącznie jako zdarzenia techniczne, a coraz częściej traktowane są jako złożone kryzysy organizacyjne i regulacyjne, niosące konsekwencje finansowe, reputacyjne oraz nadzorcze (European Parliament & Council of the European Union, 2022a, 2022b). W praktyce skutkuje to wzrostem kosztów zgodności regulacyjnej, obciążeń administracyjnych oraz presji na systematyczne inwestowanie w odporność cyfrową. Dla instytucji finansowych oraz podmiotów sektora MŚP oznacza to konieczność trwałego włączenia cyberbezpieczeństwa w struktury zarządzania ryzykiem i ładu korporacyjnego, co w dłuższej perspektywie wpływa na stabilność całego ekosystemu finansowego.

1.5.2. Świadomość klientów w kwestii cyberbezpieczeństwa – wyniki badania własnego

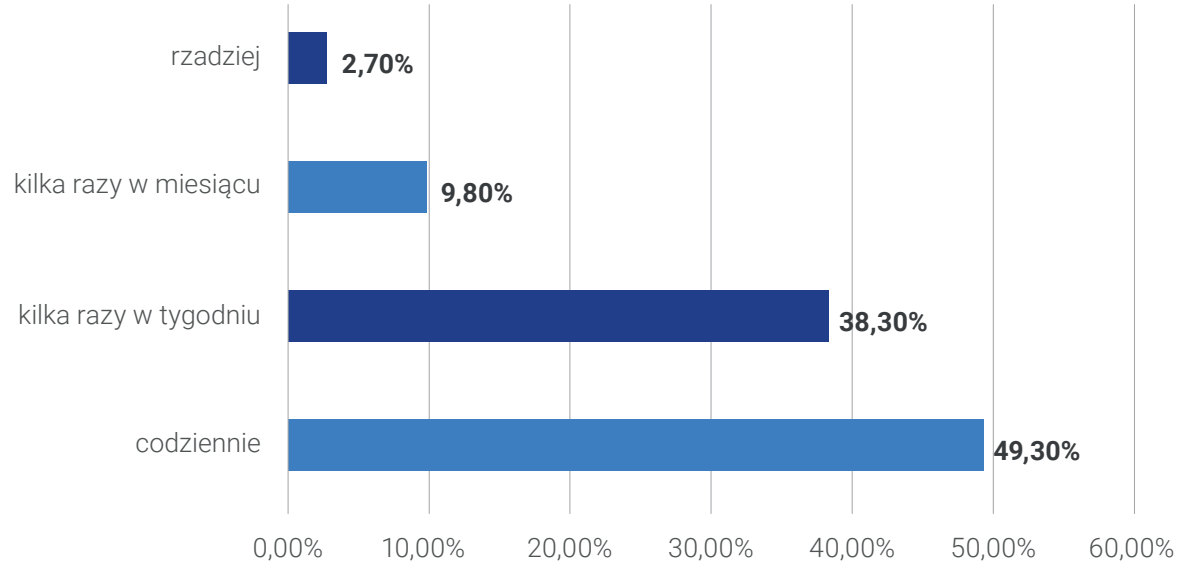
W celu pogłębienia analizy zagadnień związanych z cyberbezpieczeństwem finansowym przeprowadzono badanie własne, którego celem było określenie poziomu świadomości klientów w zakresie zagrożeń występujących podczas korzystania z płatności elektronicznych.

Analiza wyników koncentruje się na ocenie częstotliwości korzystania z płatności elektronicznych, doświadczeń respondentów związanych z próbami oszustw internetowych, a także na subiektywnej ocenie poziomu wiedzy i poczucia poinformowania w zakresie cyberzagrożeń (zestaw pytań znajduje się w Aneksie). Szczególną uwagę poświęcono również postrzeganiu roli edukacji oraz instytucji finansowych w budowaniu bezpieczeństwa użytkowników w środowisku cyfrowym. Uzyskane dane pozwalają na identyfikację zależ-

ności pomiędzy doświadczeniami respondentów a ich postawami i deklarowanym poziomem świadomości w obszarze cyberbezpieczeństwa. Wyniki badania stanowią podstawę do dalszych rozważań dotyczących skuteczności obecnych form edukacji oraz potrzeby wdrażania nowych, bardziej dopasowanych działań informacyjnych i prewencyjnych.

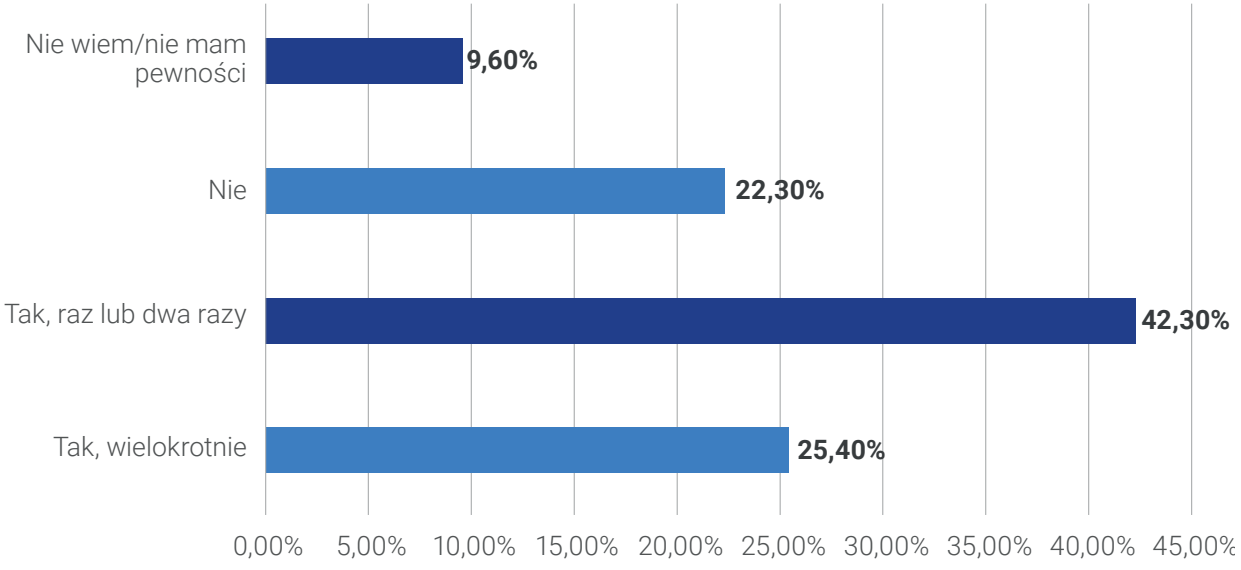
Z danych dotyczących częstotliwości korzystania z płatności elektronicznych (rysunek 7) wynika, że zdecydowana większość respondentów korzysta z nich bardzo intensywnie. Ponad 87% badanych deklaruje używanie płatności cyfrowych codziennie lub kilka razy w tygodniu, co potwierdza wysoki poziom cyfryzacji badanej grupy oraz powszechność tego typu rozwiązań w codziennym funkcjonowaniu użytkowników. Jednocześnie wyniki dotyczące doświadczeń respondentów z próbami oszustw związanych z płatnościami elektronicznymi (rysunek 8) pokazują, że zagrożenia te mają charakter realny

Rysunek 7. Częstotliwość korzystania z płatności elektronicznych (przelewy online, aplikacje mobilne, BLIK)



Źródło: opracowanie własne na podstawie wyników badania

Rysunek 8. Doświadczenie respondentów z próbami oszustw związanych z płatnościami elektronicznymi



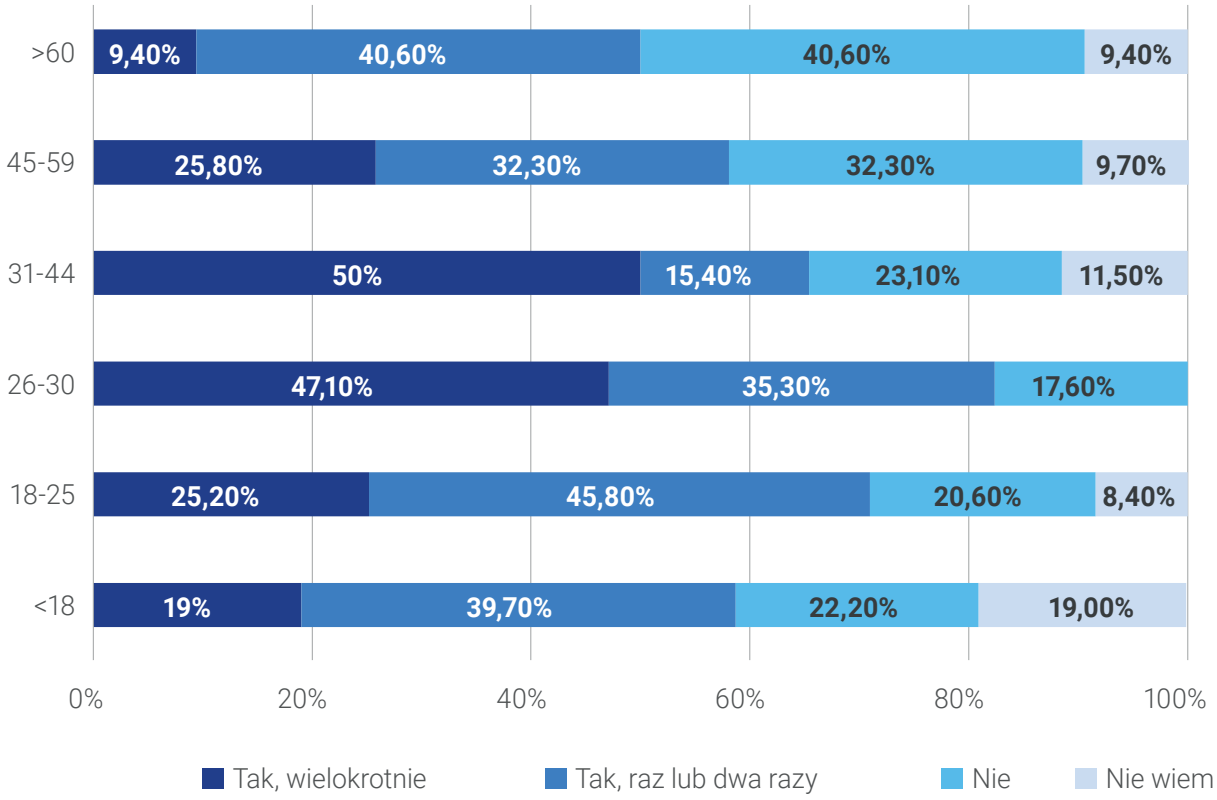
Źródło: opracowanie własne na podstawie wyników badania

i powszechny. Ponad dwie trzecie badanych zetknęło się z próbą oszustwa co najmniej raz, przy czym ponad jedna czwarta respondentów deklaruje, że doświadczała takich sytuacji wielokrotnie. Oznacza to, że dla znacznej części użytkowników ryzyko cyberzagrożeń nie jest zjawiskiem abstrakcyjnym, lecz stanowi bezpośredni element korzystania z usług finansowych online.

Zestawienie obu wyników pozwala zauważyć, że wysoka intensywność korzystania z płatności elektronicznych współwystępuje z częstym kontaktem respondentów z potencjalnymi zagrożeniami cyberbezpieczeństwa (fałszywy e-mail z banku, podejrzany link, nieautoryzowana transakcja). Choć analiza ta ma charakter opisowy i nie wskazuje na zależność przyczynowo-skutkową, wyniki sugerują, że osoby aktywnie korzystające z nowoczesnych form płatności są jednocześnie bardziej narażone na kontakt z próbami oszustw. Powyższe obserwacje uzasadniają potrzebę podejmowania skutecznych i systematycznych działań edukacyjnych w zakresie cyberbezpieczeństwa, szczególnie skierowanych do użytkowników intensywnie korzystających z usług finansowych online.

W dalszej części analizy skoncentrowano się na ocenie związku pomiędzy doświadczeniami respondentów z próbami oszustw a ich subiektywną oceną poziomu wiedzy z zakresu cyberbezpieczeństwa. Ze względu na pilotażowy charakter badania oraz nadreprezentację młodszych respondentów, analizy w podziale na wiek mają charakter eksploracyjny i służą identyfikacji tendencji, a nie formułowaniu wniosków uogólnionych. Najwyższy odsetek respondentów deklarujących wielokrotne doświadczenia z próbami oszustw występuje w grupach wieku 26–30 oraz 31–44 lata (rysunek 9). W młodszych grupach wiekowych dominują doświadczenia jednorazowe lub sporadyczne, natomiast wśród respondentów powyżej 45. roku życia wyraźnie rośnie udział odpowiedzi wskazujących na brak kontaktu z próbami oszustw lub brak pewności co do ich wystąpienia. Może to wynikać z mniejszej intensywności korzystania z płatności elektronicznych przez nieświadomości ich wystąpienia.

Rysunek 9. Doświadczenie respondentów z próbami oszustw związanych z płatnościami elektronicznymi w podziale na grupy wiekowe



Źródło: opracowanie własne na podstawie wyników badania

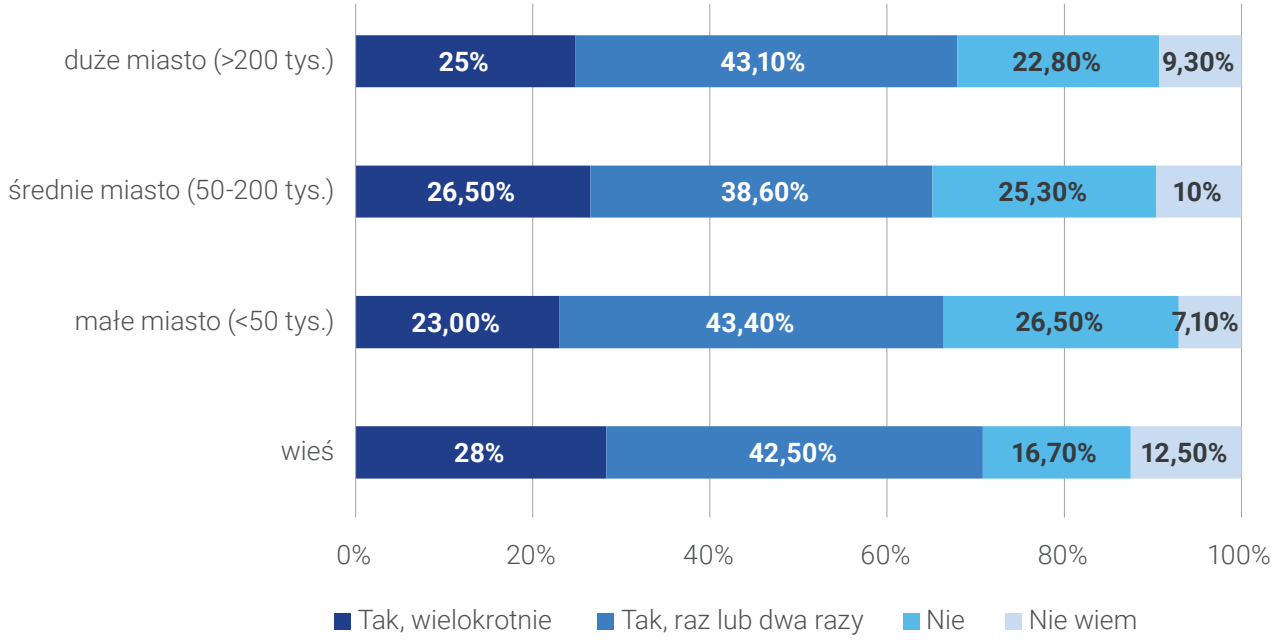
Zestawienie doświadczeń respondentów z próbami oszustw w podziale na miejsce zamieszkania wskazuje, że niezależnie od wielkości miejscowości większość badanych zetknęła się z tego typu zagrożeniami co najmniej raz (rysunek 10). Relatywnie wyższy udział odpowiedzi „tak, wielokrotnie" wśród mieszkańców wsi może świadczyć o mniejszym dostępie do systematycznych działań edukacyjnych w zakresie cyberbezpieczeństwa lub niższym poziomie świadomości dotyczącej mechanizmów ochrony przed oszustwami.

Status zawodowy respondentów został ujęty w formie zagregowanej, co pozwoliło na wyodrębnienie trzech głównych grup: osób aktywnych zawodowo, uczniów i studentów oraz osób biernych zawodowo (rysunek 11). W przypadku łączenia kilku ról zawodowych respondentów przyjęto zasadę klasyfikacji według dominującej aktywności; przykładowo osoby studiujące i jednocześnie pracujące zostały zaklasyfikowane do grupy „uczniowie i studenci", natomiast osoby pracujące będące jednocześnie emerytami lub rencistami – do grupy „emeryci i renciści". Doświadczenia respondentów z próbami oszustw w podziale na status zawodowy wskazują na wyraźne zróżnicowanie poziomu ekspozycji na zagrożenia cyberbezpieczeństwa. Najwyższy odsetek respondentów deklarujących wielokrotne doświadczenia z próbami oszustw występuje wśród osób aktywnych zawodowo (31,3%), co może być związane z częstszym korzystaniem z bankowości elektronicznej oraz płatności online. W grupie uczniów i studentów dominują doświadczenia jednorazowe lub sporadyczne (43,9%), natomiast wśród osób biernych zawodowo najwyższy udział stanowią odpowiedzi wskazujące na brak kontaktu z próbami oszustw (40,6%).

W celu pogłębienia analizy świadomości respondentów w zakresie cyberbezpieczeństwa, w dalszej części badania poddano ocenie zarówno postrzeganie ogólnego poziomu edukacji w tym obszarze w Polsce (rysunek 12), jak i subiektywną ocenę własnego poziomu wiedzy respondentów (rysunek 13). Takie zestawienie pozwala na identyfikację ewentualnych rozbieżności pomiędzy oceną systemową a indywidualnym poczuciem kompetencji, które mogą mieć istotne znaczenie dla skuteczności działań edukacyjnych.

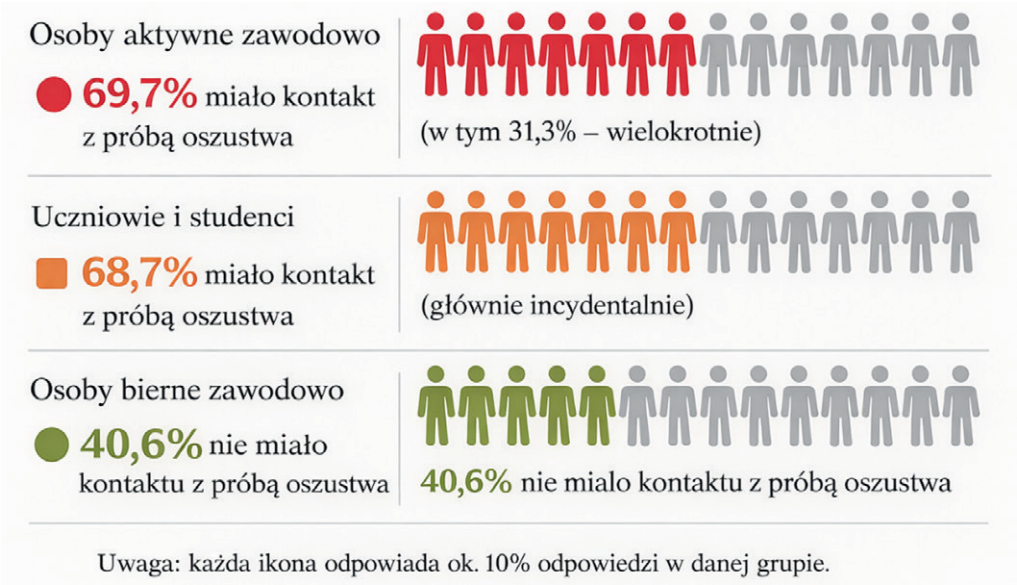
Rozkład ocen ogólnego poziomu edukacji w zakresie cyberbezpieczeństwa w Polsce (rysunek 12) pokazuje, że respondenci postrzegają ją przede wszystkim jako przeciętną. Takiej odpowiedzi udzieliło 45,0% badanych. Dodatkowo niemal co piąty respondent (19,9%) ocenił poziom edukacji jako raczej słaby, a 3,2% jako bardzo słaby. Łącznie zatem ponad jedna piąta respondentów wyraża negatywną

Rysunek 10. Doświadczenie respondentów z próbami oszustw związanych z płatnościami elektronicznymi w podziale na miejsce zamieszkania



Źródło: opracowanie własne na podstawie wyników badania

Rysunek 11. Struktura doświadczeń respondentów z próbami oszustw według statusu zawodowego

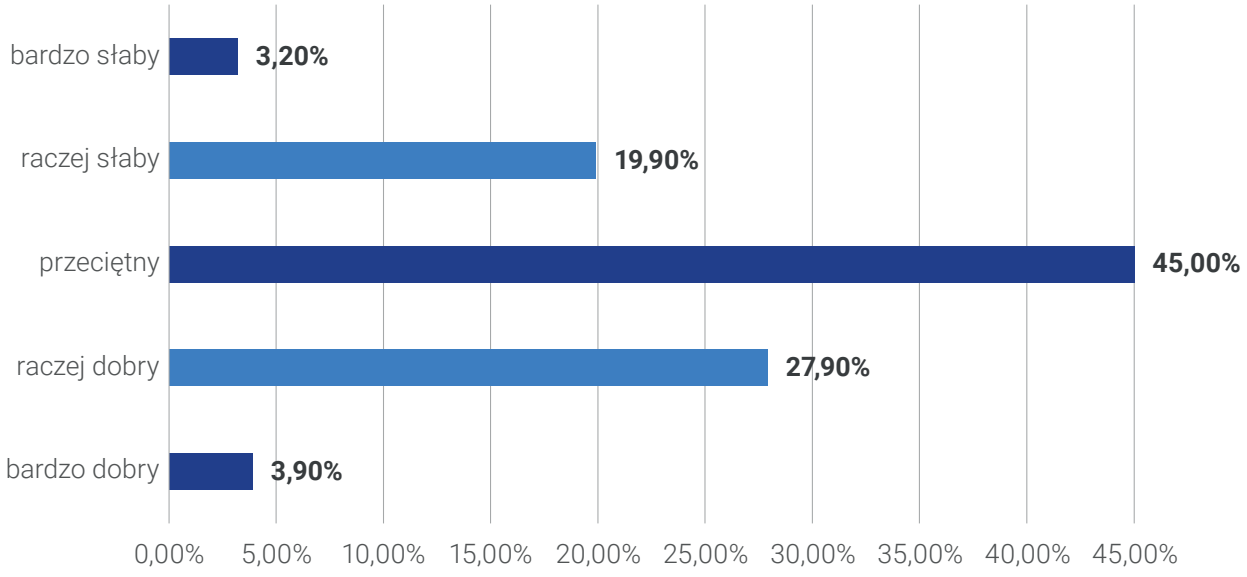


Źródło: opracowanie własne na podstawie wyników badania.

ocenę systemowych działań edukacyjnych w zakresie cyberbezpieczeństwa. Odsetek ocen pozytywnych jest wyraźnie niższy – 27,9% respondentów uznało poziom edukacji za raczej dobry, a jedynie 3,9% za bardzo dobry. Wyniki te sugerują, że w opinii badanych obecne działania edukacyjne w skali kraju są niewystarczające lub nie w pełni odpowiadają na realne potrzeby użytkowników usług cyfrowych. Z kolei samoocena respondentów dotycząca własnego poziomu wiedzy o cyberbezpieczeństwie (rysunek 13) prezentuje odmienny obraz. Zdecydowana większość badanych ocenia swoje kompetencje pozytywnie – 54,8% respondentów określiło swój poziom wiedzy jako raczej dobry, a 22,6% jako bardzo dobry. Jedynie niewielki odsetek badanych wskazał na niski poziom własnej wiedzy (2,7% – raczej słaby, 0,9% – bardzo słaby), natomiast 19,0% respondentów określiło swój poziom wiedzy jako przeciętny. Zestawienie obu ocen ujawnia wyraźną rozbieżność pomiędzy postrzeganiem poziomu edukacji systemowej a subiektywną oceną własnych kompetencji respondentów. O ile ogólny poziom edukacji o cyberbezpieczeństwie w Polsce jest oceniany raczej krytycznie lub co najwyżej przeciętnie, o tyle respondenci znacznie lepiej oceniają własne przygotowanie w tym zakresie. Może to świadczyć o występowaniu zjawiska dysonansu poznawczego, polegającego na przekonaniu o własnej odporności na zagrożenia cybernetyczne mimo jednoczesnej świadomości niedostatków systemowych działań edukacyjnych. Taka rozbieżność może również sprzyjać powstawaniu iluzji bezpieczeństwa, w której subiektywne poczucie kompetencji nie zawsze przekłada się na realną zdolność identyfikowania i unikania zagrożeń w środowisku cyfrowym.

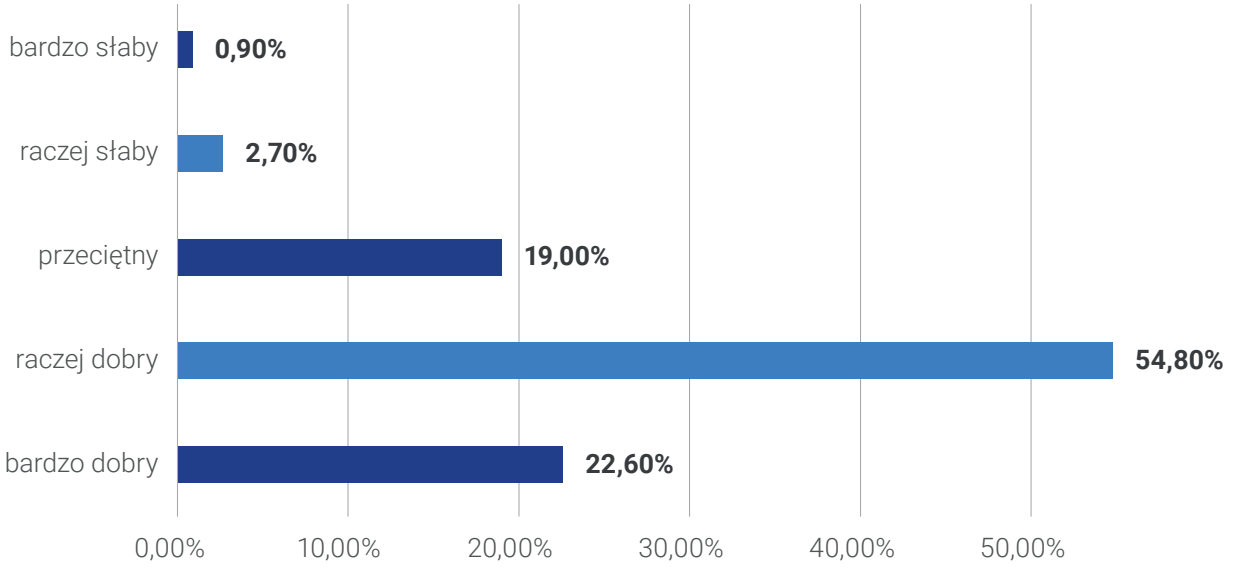
Zestawienie doświadczeń respondentów z próbami oszustw (pytanie 2) z ich subiektywną oceną poziomu wiedzy w zakresie cyberbezpieczeństwa (pytanie 4) ujawnia wyraźną zależność pomiędzy częstością kontaktu z zagrożeniami a poczuciem własnych kompetencji w tym obszarze (rysunek 14). Wśród respondentów, którzy wielokrotnie doświadczyli prób oszustw, aż 83,2% ocenia swój poziom wiedzy jako raczej dobry lub bardzo dobry. Podobnie wysoki odsetek pozytywnej samooceny występuje w grupie osób, które zetknęły się z próbami oszustw raz lub dwa razy (79,4%). Również wśród respondentów deklarujących brak doświadczeń z próbami oszustw dominują pozytywne oceny własnych kompetencji (75,6%). Uzyskane wyniki wskazują, że kontakt z cyberzagrożeniami nie prowadzi do obniżenia subiektywnej oceny własnego poziomu wiedzy, lecz przeciwnie – może sprzyjać wzmacnianiu przekonania o własnej skuteczności w identyfikowaniu i unikaniu zagrożeń. Zjawisko to może świadczyć o występowaniu dysonansu poznawczego, w którym subiektywna ocena kompetencji nie zawsze pozostaje w pełnej zgodności z rzeczywistym poziomem ryzyka funkcjonowania w środowisku cyfrowym. Wyniki badania wskazują, że wysoka samoocena kompetencji w zakresie cyberbezpieczeństwa współwystępuje z częstym kontaktem z próbami oszustw, co podkreśla znaczenie działań edukacyjnych ukie-

Rysunek 12. Ocena ogólnego poziomu edukacji o cyberbezpieczeństwie w Polsce



Źródło: opracowanie własne na podstawie wyników badania.

Rysunek 13. Samoocena respondentów nt. poziomu edukacji o cyberbezpieczeństwie

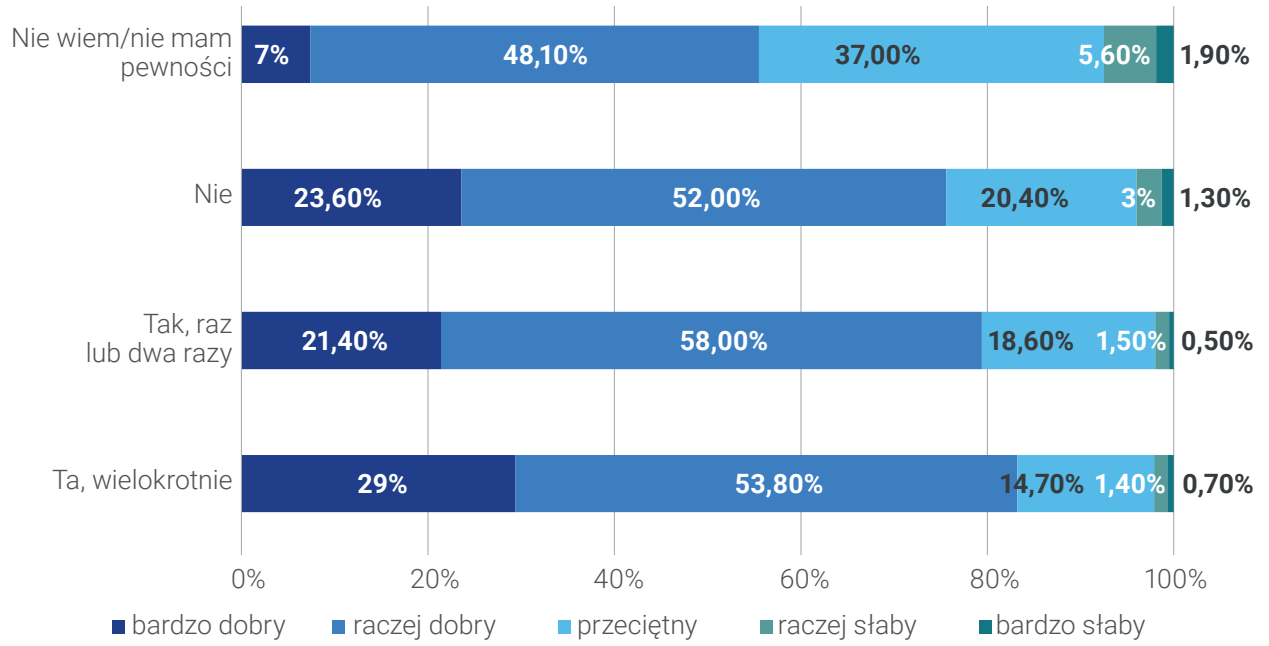


Źródło: opracowanie własne na podstawie wyników badania.

runkowanych nie tylko na przekazywanie informacji, lecz także na kształtowanie realistycznej oceny ryzyka w środowisku cyfrowym.

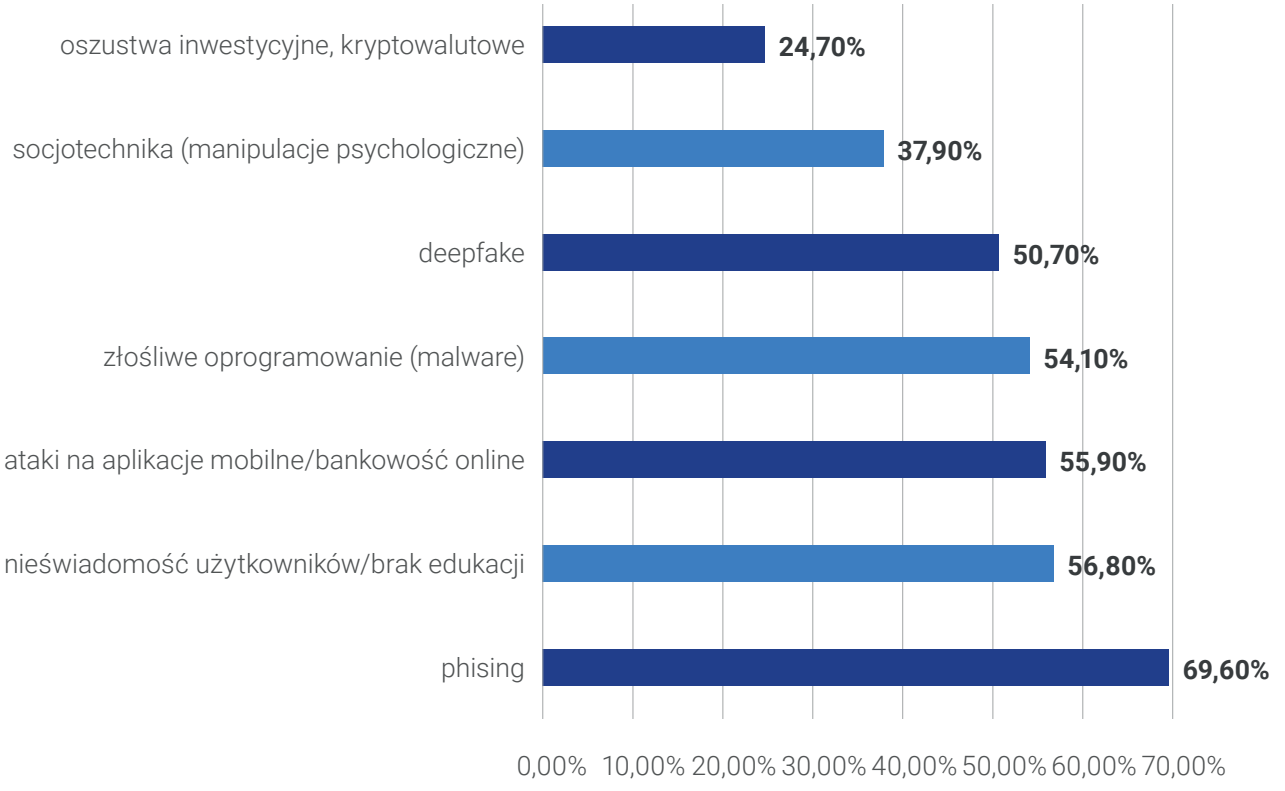
Respondenci wskazali, że największym zagrożeniem dla bezpieczeństwa finansowego w Internecie jest phishing – aż 69,6% badanych uznało go za poważne ryzyko. Pokazuje to, że fałszywe wiadomości i próby wyłudzenia danych są najbardziej rozpoznawalnym i realnym problemem dla użytkowników. Na kolejnych miejscach znalazły się: nieświadomość użytkowników (56,8%), która nie stanowi odrębnego typu ataku, lecz czynnik zwiększający podatność na inne formy oszustw, w szczególności phishing i inne techniki socjotechniczne. Respondenci wskazywali również na ataki na aplikacje mobilne (55,9%) oraz złośliwe oprogramowanie (54,1%), co potwierdza, że zagrożenia techniczne są niemal równie istotne jak zagrożenia socjotechniczne. Ponad połowa ankietowanych (50,7%) wskazała także na deepfake'i, co pokazuje rosnącą świadomość nowych, zaawansowanych form oszustw opartych na sztucz-

Rysunek 14. Samoocena poziomu wiedzy o cyberbezpieczeństwie w zależności od doświadczeń z próbami oszustw (%)



Źródło: opracowanie własne na podstawie wyników badania.
Notatka: wartości procentowe obliczono w obrębie poszczególnych kategorii doświadczeń.

Rysunek 15. Zagrożenia dla bezpieczeństwa finansowego użytkowników Internetu



Źródło: opracowanie własne na podstawie wyników badania.

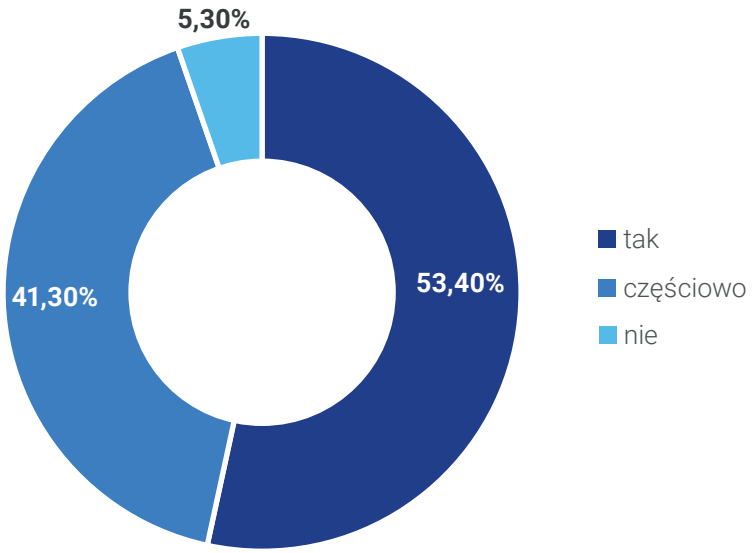
nej inteligencji. Nieco rzadziej, choć nadal istotnie, pojawiały się: socjotechnika (37,9%) oraz oszustwa inwestycyjne i kryptowalutowe (24,7%). Pojedyncze odpowiedzi otwarte (poniżej 1%) miały charakter marginalny i nie wpływają znacząco na ogólny obraz wyników (rysunek 15).

Jeśli chodzi o poziom poinformowania o zagrożeniach, warto zwrócić uwagę na to, czy respondenci mają poczucie, że są odpowiednio informowani (m.in. przez media, instytucje publiczne czy sektor finansowy) o nowych i pojawiających się zagrożeniach związanych z płatnościami w Internecie. W tym kontekście wyniki badania pokazują, że ponad połowa badanych respondentów deklaruje, iż czuje się dobrze poinformowana w zakresie zagrożeń finansowych online, jednak istotna część badanych wskazuje jedynie częściowe poczucie poinformowania (rysunek 16). Może to sugerować, że przekaz informacyjny dociera do użytkowników w różnym stopniu i nie zawsze jest postrzegany jako wystarczający lub kompletny.

Uzyskane wyniki wskazują na wyraźną preferencję respondentów dla bardziej angażujących i interaktywnych form edukacji w zakresie cyberbezpieczeństwa, co sugeruje, że działania edukacyjne nie powinny opierać się wyłącznie na biernym przekazywaniu informacji (tabela 2; zob. również mapa ciepła – rysunek 18). Największy zasięg wśród respondentów mają kampanie informacyjne realizowane w mediach masowych oraz internecie, z których korzystało 66% badanych, a ponad połowa uznała je za użyteczne. Wysokie wskazania dotyczą również materiałów edukacyjnych udostępnianych przez banki, co potwierdza istotną rolę instytucji finansowych jako wiarygodnego źródła wiedzy w zakresie cyberbezpieczeństwa. Jednocześnie formy wymagające większego zaangażowania użytkownika, takie jak szkolenia, webinaria czy quizy, pozostają relatywnie rzadziej wykorzystywane. Choć są one pozytywnie oceniane przez część respondentów, ich zasięg pozostaje ograniczony, co wskazuje na niewykorzystany potencjał bardziej interaktywnych narzędzi edukacyjnych. To właśnie one są postrzegane przez użytkowników jako najbardziej wartościowe, choć pozostają niedostatecznie rozpowszechnione. Wnioski te stanowią punkt wyjścia do dalszej analizy form edukacji finansowej i cyfrowej, przedstawionej w Rozdziale 2.

Uzupełnieniem analizy były odpowiedzi otwarte respondentów, które – choć miały charakter jednostkowy i rozproszony – pozwalają uchwycić bardziej zróżnicowane i nieformalne ścieżki zdobywania wiedzy na temat bezpieczeństwa finansowego i cyfrowego. Wśród wskazań pojawiały się m.in. doświadczenia zawodowe, własne doświadczenia związane z próbami oszustw, rozmowy z rodziną lub znajomymi, zajęcia szkolne i akademickie, a także pojedyncze szkolenia specjalistyczne. Odpowiedzi te pokazują, że istotna część wiedzy kształtowana jest poza formalnymi programami edukacyjnymi, często reaktywnie – w odpowiedzi na realne zagrożenia lub osobiste doświadczenia. Choć skala tych wskazań

Rysunek 16. Odczucia respondentów nt. poziomu poinformowania respondentów na temat zagrożeń związanych z płatnościami w Internecie. *„Czy czujesz się dobrze poinformowany/a o zagrożeniach związanych z płatnościami w Internecie (np. phishing, fałszywe SMS-y, oszustwa)?"*



Źródło: opracowanie własne na podstawie wyników badania.

Tabela 2. Formy edukacji w zakresie bezpieczeństwa finansowego i cyfrowego – korzystanie oraz postrzegana użytecznośćForma edukacji / źródło informacji

	Korzystają	Uznają za użyteczne	Wniosek
Kampanie informacyjne (TV, internet, media)	371 osób (66,0%)	298 osób (53,0%)	największy zasięg i jednocześnie wysoka postrzegana skuteczność
Materiały edukacyjne banków (poradniki, serwisy)	285 osób (50,7%)	166 osób (29,5%)	wysoka wiarygodność, umiarkowana atrakcyjność formy
Artykuły i poradniki online	255 osób (45,4%)	151 osób (26,9%)	wysoka dostępność, lecz ograniczone zaangażowanie odbiorców
Szkolenia, webinaria, warsztaty	177 osób (31,5%)	133 osoby (23,7%)	relatywnie rzadziej wykorzystywane, ale wysoko oceniane
Podcasty	88 osób (15,7%)	59 osób (10,5%)	niszowa, lecz pozytywnie oceniana forma edukacji
Quizy / testy wiedzy	44 osoby (7,8%)	36 osób (6,4%)	niski poziom wykorzystania, potencjał interaktywności
Gry, symulacje, escape roomy	33 osoby (5,9%)	25 osób (4,4%)	marginalne wykorzystanie, potencjał angażujący

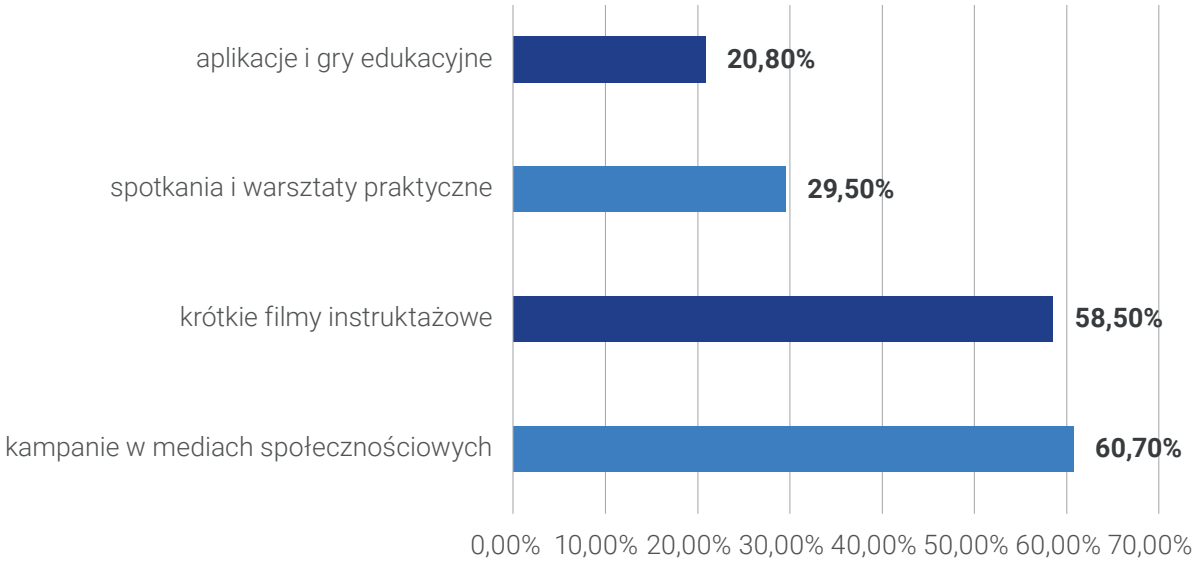
Źródło: opracowanie własne na podstawie wyników badania.
Notatka: Pytania wielokrotnego wyboru (pyt. 7 – dowolna liczba wskazań, pyt. 8 – max. 2 wskazania)

jest niewielka i nie pozwala na ich uogólnienie, stanowią one istotne tło interpretacyjne dla wyników badania, potwierdzając, że edukacja w obszarze cyberbezpieczeństwa ma charakter fragmentaryczny, rozproszony i silnie zależny od indywidualnych doświadczeń użytkowników.

Najczęściej wskazywanymi formami przyszłej edukacji okazały się kampanie prowadzone w mediach społecznościowych, które wybrało 60,7% respondentów, oraz krótkie filmy instruktażowe, wskazane przez 58,5% badanych (rysunek 17). Wyniki te potwierdzają preferencję użytkowników wobec krótkich, wizualnych i łatwo dostępnych treści, dostosowanych do tempa korzystania z mediów cyfrowych. Relatywnie wysokie wskazania uzyskały również spotkania i warsztaty praktyczne (29,5%), co sugeruje zapotrzebowanie na bardziej pogłębione formy edukacji, umożliwiające bezpośredni kontakt z ekspertem oraz omawianie realistycznych scenariuszy zagrożeń. Aplikacje i gry edukacyjne zostały wskazane przez 20,8% respondentów, co – mimo niższego wyniku – potwierdza istnienie potencjału dla narzędzi interaktywnych, szczególnie wśród młodszych użytkowników. Uzyskane wyniki wskazują, że skuteczna edukacja w przyszłości powinna łączyć szeroki zasięg kampanii cyfrowych z konkretnymi, praktycznymi formami przekazu, pozwalającymi na szybkie przyswojenie wiedzy i jej zastosowanie w codziennych sytuacjach.

Zestawienie aktualnie (w momencie badania) wykorzystywanych form edukacji z deklarowanymi

Rysunek 17. Preferowane formy edukacji wspierające bezpieczne korzystanie z płatności cyfrowych



Źródło: opracowanie własne na podstawie wyników badania.
Notatka: możliwy wielokrotny wybór odpowiedzi.

potrzebami na przyszłość ujawnia wyraźny trend ewolucji sposobów zdobywania wiedzy w zakresie cyberbezpieczeństwa (tabela 3). W przypadku form o charakterze statycznym i biernym, takich jak artykuły i poradniki online oraz materiały edukacyjne banków, obserwowany jest spadek oczekiwań dotyczących ich przyszłej skuteczności, mimo ich wysokiego dotychczasowego wykorzystania. Jednocześnie formy oparte na krótkim, wizualnym przekazie oraz elementach interaktywnych utrzymują stabilne lub relatywnie wysokie zainteresowanie respondentów. Wyniki te wskazują na stopniowe przesuwanie się preferencji edukacyjnych od tradycyjnych kanałów informacyjnych w kierunku form bardziej dynamicznych, dostosowanych do codziennych nawyków użytkowników oraz realnych scenariuszy zagrożeń. Trend ten sugeruje, że skuteczna edukacja w zakresie cyberbezpieczeństwa powinna w coraz większym stopniu wykorzystywać formaty umożliwiające szybkie przyswajanie wiedzy oraz jej bezpośrednie zastosowanie w praktyce.

Zbiorcza mapa ciepła prezentująca preferowane formy edukacji w zakresie cyberbezpieczeństwa (rysunek 18) umożliwia syntetyczne ujęcie zróżnicowania oczekiwań respondentów w zależności od wieku, miejsca zamieszkania oraz statusu zawodowego. Najwyższe natężenie wskazań obserwowane jest wśród uczniów i studentów oraz respondentów w wieku 18–25 lat, szczególnie w odniesieniu do kampanii online oraz krótkich filmów instruktażowych. Wynik ten potwierdza silną orientację młodszych użytkowników na szybkie, wizualne i cyfrowe formy przekazu edukacyjnego. Relatywnie wysokie wartości widoczne są również w grupie mieszkańców dużych miast, co może świadczyć o większej dostępności działań edukacyjnych oraz wyższym poziomie ekspozycji na inicjatywy informacyjne w środowisku miejskim. Jednocześnie należy zauważyć, że mimo nadreprezentacji młodszych grup respondentów w próbie badawczej, nie wszystkie formy edukacji cieszą się wysokim poziomem zainteresowania – szczególnie aplikacje i gry edukacyjne, które pozostają marginalnie wybierane także przez najmłodszych uczestników badania. Wraz ze wzrostem wieku respondentów, a także wśród osób aktywnych i biernych zawodowo, natężenie wskazań większości form edukacji wyraźnie maleje, przy jednoczesnym umiarkowanym wzroście zainteresowania szkoleniami i warsztatami w starszych grupach wiekowych. Najniższe wartości odnotowano w przypadku aplikacji i gier edukacyjnych, które pozostają formą niszową we wszystkich analizowanych segmentach. Uzyskane wyniki potwierdzają, że preferencje edukacyjne w obszarze cyberbezpieczeństwa są silnie zróżnicowane demograficznie, co wskazuje na konieczność projektowania działań edukacyjnych w sposób segmentowany, z uwzględnieniem zarówno cech odbiorców, jak i kontekstu ich funkcjonowania społeczno-zawodowego.

Wyniki przedstawione na mapie ciepła wskazują na ogólne preferencje respondentów dotyczące form edukacji w zakresie cyberbezpieczeństwa. Warto

Tabela 3. Formy edukacji w zakresie cyberbezpieczeństwa – obecne wykorzystanie i przyszłe oczekiwania respondentów

Forma edukacji	Aktualnie wykorzystywane
Kampanie informacyjne (TV, internet, media społecznościowe)	371 (66%)
Materiały edukacyjne banków (poradniki, serwisy)	285 (50,7%)
Artykuły i poradniki online	255 (45,4%)
Szkolenia / webinaria / warsztaty	177 (31,5%)
Podcasty	88 (15,7%)
Quizy / testy wiedzy	44 (7,8%)
Gry, symulacje, escape roomy	33 (5,9%)
Forma edukacji	**Preferowane w przyszłości**
Kampanie informacyjne (TV, internet, media społecznościowe)	341 (60,7%)
Krótkie filmy instruktażowe	329 (58,5%)
Spotkania i warsztaty praktyczne	166 (29,5%)
Aplikacje i gry edukacyjne	117 (20,8%)

Źródło: opracowanie własne na podstawie wyników badania.
Notatka: możliwy wielokrotny wybór odpowiedzi.

jednak zwrócić uwagę, że wśród uczestników badania znalazły się również osoby prowadzące działalność gospodarczą. W kontekście projektowania działań edukacyjnych istotne jest zatem uwzględnienie specyfiki sektora małych i średnich przedsiębiorstw. Dodatkowa analiza odpowiedzi respondentów deklarujących prowadzenie działalności gospodarczej (n = 11) wskazuje, że w tej grupie relatywnie częściej wskazywano szkolenia, warsztaty oraz materiały eksperckie jako preferowane formy zdobywania wiedzy w zakresie cyberbezpieczeństwa. Z perspektywy przedsiębiorstw szczególne znaczenie mogą mieć rozwiązania umożliwiające jednoczesne podnoszenie kompetencji większej liczby pracowników, co potencjalnie ogranicza ryzyko wystąpienia incydentów cyberbezpieczeństwa w organizacji. Jednocześnie część respondentów zwracała uwagę na rosnącą rolę krótkich, praktycznych materiałów edukacyjnych dostępnych online, które mogą wspierać bieżące podnoszenie kompetencji cyfrowych pracowników.

Najczęściej wskazywaną rolą banków było przesyłanie ostrzeżeń i informacji o aktualnych zagrożeniach,

Rysunek 18. Mapa ciepła: preferowane formy edukacji przyszłości w zakresie cyberbezpieczeństwa a profil demograficzny

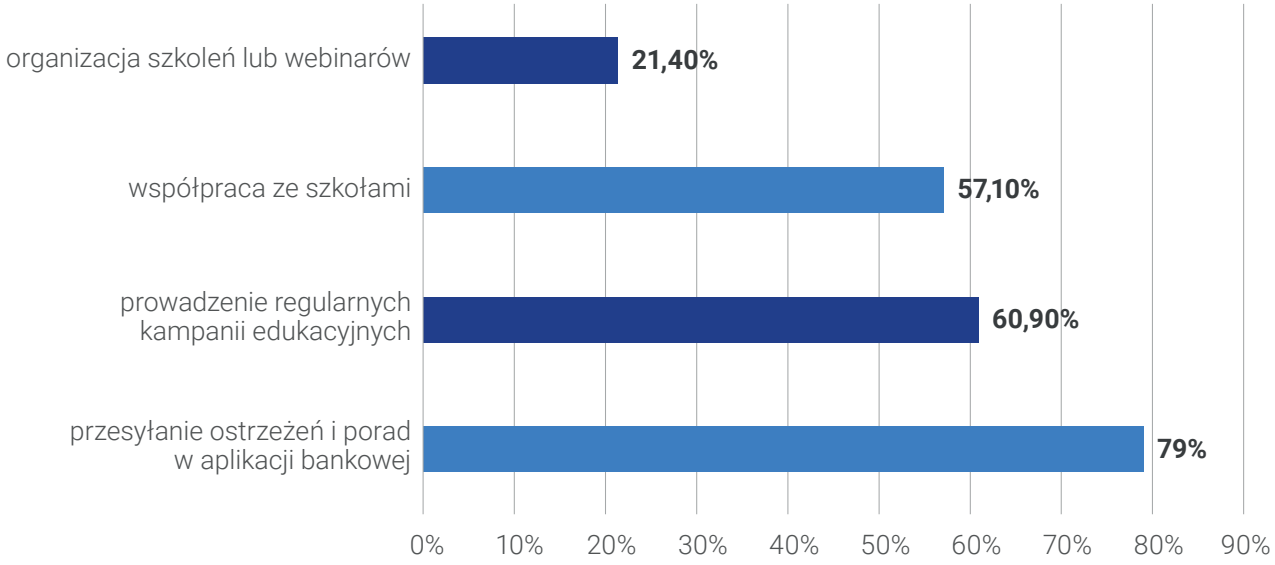
Segment	Kampanie w mediach (w %)	Krótkie filmy (w %)	Spotkania/ warsztaty (w %)	Aplikacje / gry edukacyjne (w %)
18–25	25,3	22,8	10,0	8,2
26–30	12,0	12,0	6,0	3,0
31–44	19,0	17,0	6,0	5,0
45+	20,0	22,0	11,0	6,0
Wieś	6,9	6,4	3,0	3,1
Małe miasto <50 tys.	7,0	6,7	4,0	2,8
Średnie miasto 50–200 tys.	4,5	4,8	2,2	2,1
Duże miasto >200 tys.	15,7	15,0	7,4	3,7
Uczniowie / studenci	25,9	24,4	12,8	10,1
Aktywni zawodowo	6,2	5,4	1,7	0,9
Bierni zawodowo	2,0	3,1	2,1	0,7

Źródło: opracowanie własne na podstawie wyników badania.
Notatka: wartości procentowe obliczono w obrębie poszczególnych grup respondentów. Pytanie miało charakter wielokrotnego wyboru. Przedstawione wartości odzwierciedlają odsetek respondentów z danej grupy demograficznej, którzy wskazali określoną formę edukacji.

na co wskazało 79% respondentów (rysunek 19). Wynik ten podkreśla znaczenie bieżącej, operacyjnej komunikacji – realizowanej m.in. za pośrednictwem aplikacji mobilnych, bankowości internetowej, wiadomości SMS czy e-mail – jako podstawowego narzędzia zwiększania bezpieczeństwa użytkowników. Respondenci oczekują, że banki będą szybko reagować na nowe schematy oszustw oraz przekazywać informacje w sposób zrozumiały i praktyczny.

Drugim istotnym obszarem działań wskazywanych przez badanych jest prowadzenie regularnych kampanii edukacyjnych, co zadeklarowało 60,9% ankietowanych. Odpowiedzi te potwierdzają, że jednorazowe komunikaty ostrzegawcze są postrzegane jako niewystarczające, a edukacja w zakresie cyberbezpieczeństwa powinna mieć charakter długofalowy i systematyczny. Respondenci dostrzegają potrzebę budowania wiedzy i świadomości zagrożeń w sposób ciągły, a nie wyłącznie reaktywny. Istotnym elementem wskazywanym przez badanych jest również współpraca banków ze szkołami i instytucjami edukacyjnymi, którą jako pożądaną formę działań wskazało 57,1% respondentów. Wynik ten świadczy o społecznym oczekiwaniu rozszerzenia roli banków poza bezpośrednią relację

Rysunek 19. Rola banków w edukowaniu klientów o cyberbezpieczeństwie



Źródło: opracowanie własne na podstawie wyników badania.

z klientem oraz o potrzebie ich aktywnego udziału w systemowej edukacji finansowej i cyfrowej, szczególnie w odniesieniu do młodszych użytkowników usług płatniczych. Zdecydowanie rzadziej respondenci wskazywali organizowanie szkoleń lub warsztatów edukacyjnych (21,4%). Może to sugerować, że tradycyjne, bardziej sformalizowane formy edukacji są postrzegane jako mniej dostępne lub gorzej dopasowane do potrzeb użytkowników niż krótkie komunikaty ostrzegawcze i kampanie informacyjne realizowane w kanałach cyfrowych. Wśród odpowiedzi pojawiły się również pojedyncze, rozproszone sugestie dotyczące m.in. wychodzenia przez banki z własną inicjatywą edukacyjną, przejmowania większej odpowiedzialności za skutki oszustw, dalszego doskonalenia zabezpieczeń technicznych, intensyfikacji działań skierowanych do osób starszych, a także organizowania warsztatów i obowiązkowych szkoleń z zakresu cyberbezpieczeństwa. Ich marginalny udział procentowy (poniżej 1% wskazań każdej z kategorii) wskazuje jednak, że w percepcji respondentów rola banków w obszarze cyberbezpieczeństwa jest definiowana przede wszystkim przez komunikację, ostrzeganie oraz edukację prewencyjną, a nie przez działania o charakterze incydentalnym, stricte technologicznym lub formalno-prawnym.

Wyniki badania potwierdzają, że klienci oczekują od banków aktywnej i widocznej roli w budowaniu świadomości cyberzagrożeń. Banki są postrzegane nie tylko jako dostawcy bezpiecznej infrastruktury płatniczej, lecz także jako wiarygodne źródło wiedzy oraz kluczowy partner w procesie edukacji finansowej i cyfrowej. Oczekiwania te wpisują się w szerszy trend przesuwania ciężaru ochrony użytkowników z wyłącznie rozwiązań technicznych na połączenie technologii, komunikacji i edukacji.

Zaprezentowane wyniki pozostają spójne z wnioskami formułowanymi m.in. w opracowaniu Warszawskiego Instytutu Bankowości, „Postawy Polaków wobec cyberbezpieczeństwa 2025" (zgodnie ze stanem na moment tworzenia raportu), które wskazują na utrzymujące się znaczenie phishingu jako kluczowego zagrożenia w przestrzeni cyfrowej. Pomimo rozwoju zabezpieczeń technologicznych oraz powszechności płatności elektronicznych, ataki oparte na socjotechnice – w szczególności phishing, smishing i vishing – nadal cechują się wysoką skutecznością, co wynika przede wszystkim z podatności użytkowników na manipulację oraz presję sytuacyjną. Istotne jest również to, że poziom wiedzy i kompetencji w zakresie cyberbezpieczeństwa pozostaje zróżnicowany i nie zawsze wystarczający, a obserwowane luki nie mają charakteru wyłącznie pokoleniowego. W dużej mierze wynikają one z odmiennych doświadczeń użytkowników, różnych kanałów pozyskiwania informacji oraz zróżnicowanych form dotychczasowej edukacji. Oznacza to, że skuteczna edukacja w zakresie cyberbezpieczeństwa nie może być jednorodna ani jednorazowa, lecz powinna mieć charakter systematyczny, segmentowany i oparty na realistycznych scenariu-

szach zagrożeń. W tym ujęciu edukacja przestaje być dodatkiem do systemu bezpieczeństwa, a staje się jego integralnym elementem – swoistą „cyfrową tarczą", której formy oraz skuteczność wymagają dalszej pogłębionej analizy. Ponadto, wyniki badania własnego korespondują z danymi z raportu „Poziom wiedzy finansowej Polaków 2024" (KEFiP, 2024), w którym respondenci jako główne źródła wiedzy wskazują przede wszystkim kanały internetowe (blogi i portale) oraz media, a także banki i inne instytucje sektora finansowego. Analogicznie, w badaniu własnym najwyższy zasięg osiągają kampanie informacyjne (media/Internet) oraz materiały edukacyjne banków, natomiast formy bardziej angażujące (np. quizy, gry i symulacje) pozostają niszowe. Zbieżność ta sugeruje, że zarówno w obszarze edukacji finansowej ogółem, jak i w edukacji dot. cyberbezpieczeństwa, kluczową rolę odgrywają kanały łatwo dostępne i „niskoprogowe", podczas gdy narzędzia interaktywne – mimo potencjału – wymagają dodatkowych bodźców wdrożeniowych i promocyjnych.

1.6. Praktyki ochrony i najważniejsze mechanizmy zabezpieczeń

Praktyki ochrony stosowane w usługach płatniczych mają charakter wielowarstwowy i obejmują zarówno zabezpieczenia techniczne wdrażane przez dostawców usług płatniczych, rozwiązania organizacyjne i procesowe funkcjonujące po stronie instytucji finansowych, jak i działania edukacyjne skierowane do użytkowników końcowych. Skuteczność systemu bezpieczeństwa zależy od współdziałania wszystkich tych elementów, a także od jasno określonego podziału odpowiedzialności pomiędzy bankami a klientami. W praktyce użytkownicy często zakładają, że za każdy incydent skutkujący utratą środków odpowiada instytucja finansowa, podczas gdy obowiązujące regulacje różnicują zakres odpowiedzialności stron w zależności od charakteru zdarzenia oraz zachowania klienta. Zagadnienie to stanowi istotny kontekst dla analizy mechanizmów ochrony oraz punkt wyjścia do rozważań nad rolą edukacji w ograniczaniu ryzyka nadużyć.

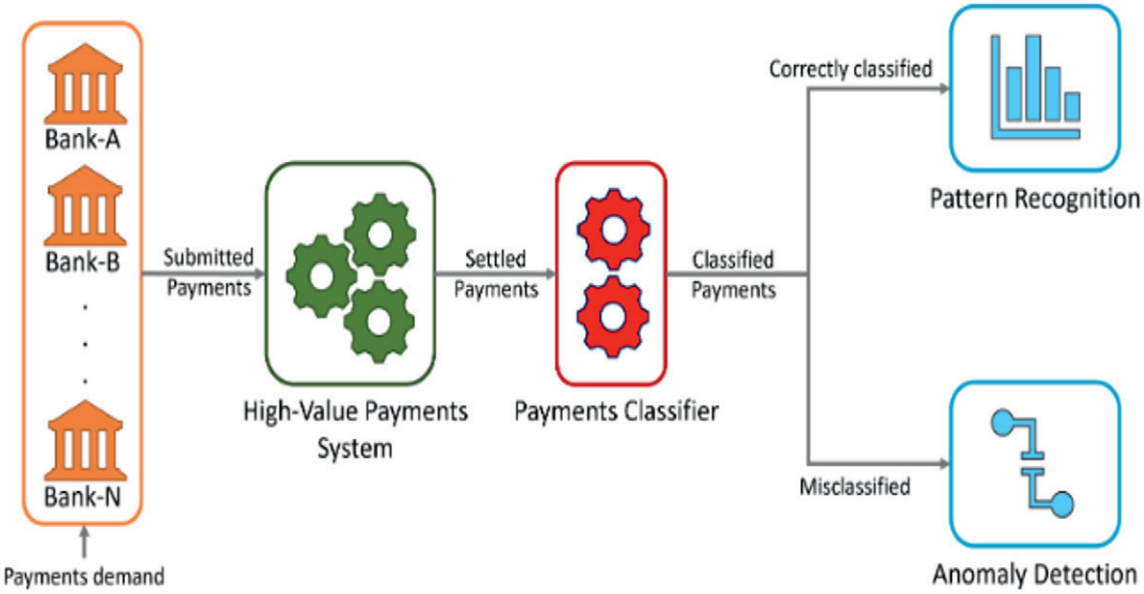
Powyższe wnioski wskazują, że sama świadomość zagrożeń i działania edukacyjne, choć niezbędne (opisane w rozdziale 2), nie są wystarczające do skutecznego ograniczania ryzyka nadużyć w obszarze płatności elektronicznych, co uzasadnia konieczność analizy praktyk ochrony oraz mechanizmów zabezpieczeń stosowanych w usługach płatniczych.

1.6.1. Zabezpieczenia techniczne po stronie dostawców usług płatniczych

Podstawowym filarem ochrony w usługach płatniczych pozostają zabezpieczenia techniczne wdrażane przez banki oraz innych dostawców usług płatniczych. Kluczowe znaczenie ma w tym zakresie silne uwierzytelnianie klienta (ang. Strong Customer Authentication, SCA), wprowadzone na mocy dyrektywy PSD2 (Dyrektywa 2015/2366/UE). Mechanizm ten opiera się na wieloskładnikowym uwierzytelnianiu, łączącym co najmniej dwa elementy z kategorii wiedzy, posiadania lub cech klienta, a także na zasadzie dynamicznego powiązania transakcji z jej kwotą i odbiorcą. Dane publikowane przez EBC (2025) potwierdzają, że stosowanie SCA skutecznie ograniczyło skalę nieautoryzowanych transakcji, w szczególności w obszarze płatności kartowych. Wraz z rozwojem zabezpieczeń technicznych ewoluują również metody działania oszustów, coraz częściej polegające na manipulowaniu użytkownikami w celu skłonienia ich do autoryzowania transakcji oszukańczych, co wymaga dalszego dostosowywania środków ochrony.

Istotnym elementem ochrony infrastruktury płatniczej są mechanizmy kryptograficzne i sieciowe, w tym szyfrowanie komunikacji z wykorzystaniem protokołu Transport Layer Security (TLS), stosowanie polityk HTTP Strict Transport Security (HSTS) oraz zabezpieczenia przed atakami typu man-in-the-middle, których celem jest przechwycenie lub modyfikacja danych przesyłanych pomiędzy uczestnikami systemu płatniczego (rysunek 20). Rozwiązania te zapewniają poufność, integralność oraz uwierzytelnienie komunikacji pomiędzy klientami, instytucjami finansowymi i systemami rozliczeniowymi. Uzupełnieniem zabezpieczeń na poziomie komunikacyjnym jest stały monitoring transakcji w czasie zbliżonym do rzeczywistego, realizowany przez systemy antyfraudowe wykorzystujące zaawansowane metody analityczne. Zgodnie z podejściem warstwowym stosowanym w nowoczesnych systemach płatniczych, pierwsza warstwa monitoringu opiera się na modelach uczenia maszynowego nadzorowanego (supervised machine learning), które klasyfikują transakcje jako typowe lub potencjalnie nietypowe na podstawie zdefiniowanych cech i zmiennych docelowych (Desai i in., 2024). Pozwala to na szybkie odfiltrowanie dużej liczby standardowych operacji i koncentrację dalszej analizy na ograniczonym podzbiorze transakcji budzących wątpliwości. W drugiej warstwie wykorzystywane są metody uczenia maszynowego nienadzorowanego (unsupervised

Rysunek 20. Dwuwarstwowy model monitoringu transakcji oparty na klasyfikacji i detekcji anomalii



Źródło: (Desai i in., 2024, s. 7)

machine learning), w szczególności analiza anomalii oraz modele scoringowe, które umożliwiają identyfikację nietypowych wzorców zachowań odbiegających od historycznych profili uczestników systemu. Takie podejście pozwala na skuteczniejsze wykrywanie rzadkich i wcześniej nieznanych form nadużyć, a także na wczesne reagowanie na potencjalne próby oszustwa, nawet w środowiskach o bardzo dużym wolumenie i złożoności transakcji.

Dodatkową warstwę ochrony w usługach płatniczych stanowią limity transakcyjne, konfigurowane zarówno na poziomie aplikacji mobilnych, kart płatniczych, jak i systemów płatności natychmiastowych, takich jak BLIK. Mechanizmy te pozwalają na ograniczenie maksymalnej wartości pojedynczych transakcji oraz dziennych lub miesięcznych wolumenów płatności, co znacząco redukuje potencjalne straty w przypadku przejęcia kontroli nad rachunkiem lub instrumentem płatniczym. Limity te mogą być dynamicznie modyfikowane przez użytkownika lub dostawcę usług płatniczych, a ich przekroczenie często wymaga zastosowania dodatkowych form uwierzytelnienia.

Coraz większe znaczenie ma również bezpieczeństwo aplikacji mobilnych, które stały się podstawowym kanałem dostępu do usług bankowych i przetwarzania wrażliwych danych finansowych użytkowników. Ochrona ta obejmuje m.in. mechanizmy wykrywania urządzeń z naruszonym środowiskiem systemowym (rooting lub jailbreak), które istotnie zwiększają podatność na ataki oraz umożliwiają omijanie zabezpieczeń aplikacyjnych, prowadząc do ryzyka nieuprawnionego dostępu do danych bankowych (ENISA, 2025; Ministerstwo Cyfryzacji, b.d.). Stosowane są także techniki przeciwdziałania złośliwemu oprogramowaniu typu *overlay*, polegającemu na nakładaniu fałszywych interfejsów użytkownika w celu wyłudzania danych uwierzytelniających i informacji transakcyjnych. Uzupełnieniem tych działań są zabezpieczenia utrudniające analizę i modyfikację aplikacji, takie jak obfuskacja kodu, mechanizmy wykrywania debugowania oraz ochrona integralności aplikacji, które ograniczają możliwość ingerencji w logikę przetwarzania danych finansowych.

W kontekście rozwoju otwartej bankowości istotną rolę odgrywa również bezpieczeństwo interfejsów programistycznych API, które umożliwiają podmiotom trzecim dostęp do danych rachunków i inicjowanie płatności w imieniu użytkownika. Kluczowe znaczenie ma tu certyfikacja podmiotów trzecich (Third Party Providers, TPP), realizowana przez właściwe organy nadzorcze, a także stosowanie silnego uwierzytelniania klienta oraz precyzyjnych ograniczeń dostępowych i transakcyjnych. Rozwiązania te mają na celu minimalizację ryzyka nadużyć, nieautoryzowanego dostępu do danych oraz eskalacji uprawnień w środowiskach opartych na architekturze API (Dyrektywa 2015/2366/UE).

1.6.2. Rozwiązania organizacyjne i procesowe

Oprócz zabezpieczeń technicznych kluczowe znaczenie dla odporności instytucji finansowych na cyberzagrożenia mają rozwiązania organizacyjne i procesowe. Obejmują one m.in. polityki bezpieczeństwa informacji, systemowe zarządzanie ryzykiem ICT, plany ciągłości działania oraz procedury reagowania na incydenty. Istotnym elementem tych działań jest także obowiązek raportowania incydentów do właściwych organów nadzorczych oraz zespołów reagowania, takich jak Komisja Nadzoru Finansowego, Narodowy Bank Polski czy krajowe zespoły CSIRT.

Praktycznym sprawdzianem skuteczności rozwiązań organizacyjnych są ćwiczenia symulacyjne oraz testy odporności operacyjnej. W styczniu 2025 r. polskie banki i instytucje finansowe uczestniczyły w ćwiczeniach Cyber-EXE Polska 2024, organizowanych przez Fundację Bezpieczna Cyberprzestrzeń we współpracy m.in. z EY Polska. Celem tych działań było przetestowanie gotowości operacyjnej sektora na realistyczne scenariusze cyberataków, w tym zdarzenia inspirowane działaniami zaawansowanych grup APT, a także weryfikacja zdolności reagowania w kontekście nowych regulacji unijnych, w szczególności rozporządzenia DORA oraz nadchodzącej implementacji dyrektywy NIS2. Ćwiczenia obejmowały zarówno projektowanie i utrzymanie środowisk obronnych, jak i testowanie procesów monitorowania, klasyfikacji oraz raportowania incydentów. Szczególną uwagę poświęcono współpracy międzyinstytucjonalnej oraz komunikacji z organami administracji publicznej i zespołami CSIRT. Wnioski z ćwiczeń wskazują, że polskie instytucje finansowe są w dużej mierze dobrze przygotowane technicznie i organizacyjnie do reagowania na znane wektory ataków, jednak jednocześnie podkreślają znaczenie bieżącej wymiany informacji oraz koordynacji działań, które istotnie skracają czas wykrywania i raportowania incydentów oraz zwiększają skuteczność reakcji.

1.6.3. Edukacja użytkowników i rola komunikacji instytucji finansowych

Nawet najbardziej zaawansowane mechanizmy techniczne i organizacyjne nie są w stanie całkowicie wyeliminować ryzyka nadużyć, jeżeli użytkownicy nie posiadają podstawowej wiedzy na temat bezpiecznego korzystania z usług płatniczych. W praktyce wiele incydentów inicjowanych jest przez błędy po stronie użytkownika, takie jak udostępnianie danych uwierzytelniających, nieostrożne korzystanie z linków i załączników czy brak aktualizacji systemów i aplikacji. Do podstawowych zasad bezpieczeństwa należą m.in. stosowanie unikalnych haseł, weryfikacja adresów stron internetowych, nieprzekazywanie danych przez telefon lub SMS, korzystanie z aktualnego oprogramowania oraz zabezpieczanie urządzeń mobilnych.

Istotną rolę w kształtowaniu bezpiecznych postaw odgrywają również działania edukacyjne prowadzone przez instytucje finansowe. Komunikaty prezentowane w aplikacjach bankowych, kampanie informacyjne, newslettery oraz materiały edukacyjne publikowane przez sektor bankowy i organizacje branżowe przyczyniają się do podnoszenia świadomości zagrożeń oraz ograniczania skuteczności ataków opartych na socjotechnice. Rekomendacje Komisja Nadzoru Finansowego oraz wytyczne Europejskiej Agencji Bankowej podkreślają znaczenie edukacji klientów jako integralnego elementu systemu zarządzania ryzykiem operacyjnym.

W tym kontekście edukacja użytkowników stanowi kluczowe uzupełnienie zabezpieczeń technicznych i procesowych oraz jeden z najważniejszych czynników ograniczających skalę nadużyć w długim okresie. Zagadnienie to, ze względu na swoją wagę i bezpośredni wpływ na bezpieczeństwo usług płatniczych, stanowi przedmiot szczegółowej analizy w kolejnym rozdziale niniejszego opracowania.

PROGRAM ANALITYCZNO BADAWCZY

Rozdział 2. Edukacja finansowa jako cyfrowa tarcza

Przedstawienie problematyki edukacji finansowej w sposób pełny i rzetelny wymaga odwołania się do konkretnych przykładów działań oraz inicjatyw podejmowanych w tym obszarze. To właśnie praktyczne rozwiązania, programy edukacyjne i projekty realizowane przez różne podmioty pozwalają ukazać, w jaki sposób założenia teoretyczne przekładają się na rzeczywiste działania oraz realny wpływ na odbiorców. Warto przy tym podkreślić, że już wcześniej w historii edukacji finansowej pojawiały się inicjatywy o szerokim i kompleksowym charakterze, m.in. *Mapa edukacji finansowej* ed. VI, cz. 2 (Jurek i in., 2019), która porządkowała i systematyzowała działania edukacyjne realizowane przez różne instytucje. Należy dodać, że syntetyczne zestawienia działań edukacyjnych powstawały również w toku prac nad Krajową Strategią Edukacji Finansowej, stanowiąc próbę całościowego ujęcia i koordynacji inicjatyw realizowanych w tym obszarze.

Podobne podejście zastosowano także w ramach Roku Edukacji Ekonomicznej 2024 (REE, 2024), w którym prowadzono systematyczne gromadzenie i prezentację inicjatyw edukacyjnych realizowanych na poziomie ogólnopolskim, regionalnym i lokalnym. Zestawienie to, obejmujące działania zgłaszane przez różnorodne podmioty z poszczególnych województw, pozwalało na uchwycenie skali, zróżnicowania tematycznego oraz terytorialnego rozkładu aktywności edukacyjnych. W efekcie REE 2024 nie tylko pełnił funkcję inicjatywy promującej edukację ekonomiczną, lecz także dostarczył narzędzia analitycznego umożliwiającego ocenę intensywności i charakteru działań edukacyjnych w skali całego kraju, a tym samym stworzył podstawę do dalszych analiz porównawczych i wniosków systemowych.

Celem takich zestawień jest uporządkowanie działań edukacyjnych pod względem ich formy i charakteru, grup docelowych, stopnia sformalizowania, a także skali, zasięgu oraz cykliczności realizacji. Pozwala to na bardziej przejrzyste ujęcie różnorodnych inicjatyw oraz ułatwia ich analizę porównawczą. W kontekście niniejszego raportu szczególne znaczenie ma identyfikacja tych działań edukacyjnych, które odnoszą się do bezpieczeństwa finansowego w środowisku cyfrowym, w tym w szczególności do zagadnień związanych z bezpiecznym korzystaniem z płatności online. W niniejszym rozdziale szczególna uwaga zostanie zwrócona wyłącznie na wybrane działania, które sprzyjają zwiększaniu świadomości finansowej w przestrzeni online, odpowiadając na współczesne potrzeby odbiorców oraz zmieniające się uwarunkowania technologiczne. W perspektywie bezpieczeństwa płatności elektronicznych i transakcji realizowanych online działania te pełnią dodatkowo funkcję ochronną, wzmacniając zdolność odbiorców do rozpoznawania zagrożeń cyfrowych oraz podejmowania bezpiecznych decyzji finansowych.

Przedstawione przykłady pełnią funkcję analityczną i ilustracyjną i nie mają charakteru promocyjnego wobec banków ani innych instytucji finansowych. Zostały one dobrane z uwzględnieniem ich charakteru edukacyjnego oraz tematyki bezpieczeństwa płatności online. Ich celem jest ukazanie różnorodnych podejść do edukacji finansowej oraz identyfikacja rozwiązań, które mogą stanowić punkt odniesienia do dalszych rozważań, źródło dobrych praktyk oraz inspirację do rozwijania i doskonalenia kolejnych inicjatyw edukacyjnych odpowiadających na zmieniające się potrzeby społeczne i technologiczne. Wymienione inicjatywy nie wyczerpują katalogu działań edukacyjnych prowadzonych w Polsce i zostały dobrane jako przykłady ilustrujące różne modele i podejścia do edukacji w obszarze bezpieczeństwa płatności online.

2.1. Klasyczne formy edukacji – co już działa?

Klasyczne formy edukacji, mimo postępującej cyfryzacji, pozostają istotnym elementem budowania podstawowych kompetencji bezpieczeństwa finansowego, szczególnie w grupach bardziej narażonych na wykluczenie cyfrowe lub oszustwa socjotechniczne. Obejmują one zarówno inicjatywy o charakterze instytucjonalnym, realizowane przez podmioty sektora publicznego i finansowego, jak i działania informacyjne oraz edukacyjne prowadzone w środowisku online. Ich wspólnym celem jest systematyczne przekazywanie wiedzy, kształtowanie bezpiecznych nawyków oraz wzmacnianie kompetencji umożliwiających świadome korzystanie z usług finansowych w warunkach rosnącej cyfryzacji. W rozdziale 2.1 szczególna uwaga zostanie poświęcona inicjatywom, które sprzyjają zwiększaniu świadomości zagrożeń cyfrowych, a jednocześnie odpowiadają na zmieniające się nawyki informacyjne użytkowników. Do tej kategorii należą m.in. spotkania bezpośrednie, kampanie informacyjne, poradniki internetowe, artykuły eksperckie, webinaria, podcasty oraz materiały audiowizualne, które – dzięki łatwej dostępności i możliwości szerokiego dotarcia – odgrywają coraz większą rolę w edukacji finansowej.

2.1.1. Spotkania bezpośrednie – lekcje, wykłady

Spotkania bezpośrednie, takie jak lekcje, wykłady i prelekcje prowadzone stacjonarnie, pozostają jedną z najbardziej klasycznych, a jednocześnie wciąż skutecznych form edukacji finansowej i cyfrowej. Ich istotną zaletą jest możliwość bezpośredniego kontaktu z odbiorcami, prowadzenia dialogu, zadawania pytań oraz omawiania rzeczywistych problemów i scenariuszy zagrożeń związanych z korzystaniem z usług finansowych w środowisku cyfrowym. Warto podkreślić, że inicjatyw o tym charakterze funkcjonuje bardzo wiele, choć nie wszystkie z nich w równym stopniu odnoszą się bezpośrednio do zagadnień omawianych w niniejszym raporcie, takich jak płatności cyfrowe czy cyberbezpieczeństwo.

Program Nowoczesne Zarządzanie Biznesem

Ważną grupę odbiorców spotkań bezpośrednich stanowią uczniowie i młodzież, do których kierowane są inicjatywy realizowane przez ekspertów i praktyków związanych z Biurem Informacji Kredytowej oraz Programem Nowoczesne Zarządzanie Biznesem. Pracownicy NZB prowadzą wykłady oraz spotkania edukacyjne skierowane do uczniów, studentów oraz nauczycieli, obejmujące m.in. zagadnienia bezpiecznego korzystania z płatności elektronicznych, identyfikacji najczęstszych form cyberoszustw, wskazówki dotyczące budowania zdolności kredytowej, a także zasady ochrony danych i odpowiedzialnego zarządzania finansami osobistymi.

Link: https://nzb.pl/

Projekt „klasy akademickie”

Istotnym uzupełnieniem działań edukacyjnych realizowanych w ramach Programu Nowoczesne Zarządzanie Biznesem są inicjatywy prowadzone przez uczelnie wyższe na rzecz szkół ponadpodstawowych, w szczególności w formule tzw. klas akademickich.. W ramach tych projektów nauczyciele akademiccy przygotowują i prowadzą wykłady, prelekcje oraz warsztaty skierowane zarówno do uczniów, jak i nauczycieli, koncentrując się na zagadnieniach związanych z ekonomią, finansami osobistymi, funkcjonowaniem rynku finansowego oraz bezpieczeństwem w środowisku cyfrowym. Tego typu inicjatywy umożliwiają młodym odbiorcom kontakt z wiedzą akademicką już na etapie edukacji szkolnej oraz sprzyjają kształtowaniu świadomych postaw finansowych i cyfrowych.

Link: https://ue.poznan.pl/kandydaci/klasy-akademickie/

Uniwersytety Trzeciego Wieku

Spotkania bezpośrednie odgrywają również istotną rolę w edukacji osób dorosłych i starszych, szczególnie w ramach inicjatyw lokalnych, środowiskowych i wspólnotowych. Przykładem takich działań są spotkania realizowane w ramach Uniwersytetów Trzeciego Wieku, a także spotkania absolwentów uczelni wyższych. W ich trakcie zagadnienia związane z finansami osobistymi, bankowością cyfrową i cyberbezpieczeństwem omawiane są w formule wykładów i dyskusji, często w odniesieniu do realnych doświadczeń życiowych uczestników. Tego typu inicjatywy pełnią nie tylko funkcję edukacyjną, lecz także społeczną i włączającą, sprzyjając aktywizacji osób dorosłych i seniorów oraz przeciwdziałaniu wykluczeniu informacyjnemu i cyfrowemu. Spotkania te tworzą bezpieczną przestrzeń do zadawania pytań, dzielenia się doświadczeniami oraz wzajemnego uczenia się, co ma szczególne znaczenie w przypadku osób, które rzadziej korzystają z kanałów edukacji online. Dzięki temu edukacja finansowa i cyfrowa nabiera charakteru wspólnotowego, wzmacniając poczucie sprawczości, zaufania oraz kompetencji uczestników w codziennym funkcjonowaniu w środowisku finansów cyfrowych. Szczególną wartością spotkań bezpośrednich jest ich wymiar relacyjny, sprzyjający budowaniu zaufania pomiędzy ekspertami a uczestnikami oraz tworzeniu przestrzeni do swobodnej wymiany doświadczeń. Ma to szczególne znaczenie w przypadku osób z starszych grup wiekowych, dla których kontakt bezpośredni bywa jedyną lub preferowaną formą pozyskiwania wiedzy z zakresu finansów i bezpieczeństwa cyfrowego. W przeciwieństwie do kanałów online spotkania stacjonarne pozwalają na spokojniejsze tempo przekazu, indywidualne doprecyzowanie wątpliwości oraz odnoszenie omawianych treści do konkretnych sytuacji życiowych.

Link: https://www.gov.pl/web/nauka/uniwersytet-trzeciego-wieku

Spotkania w domach kultury, bibliotekach, centrach integracji i wsparcia społecznego

Uzupełnieniem działań realizowanych w ramach Uniwersytetów Trzeciego Wieku są spotkania edukacyj-

ne organizowane w innych przestrzeniach lokalnych i środowiskowych, takich jak biblioteki publiczne, domy kultury, osiedlowe centra aktywności, kluby seniora czy kółka zainteresowań funkcjonujące na poziomie społeczności lokalnych. Inicjatywy te mają zazwyczaj charakter kameralny i nieformalny, co sprzyja większej dostępności oraz obniża barierę uczestnictwa, zwłaszcza dla osób, które nie identyfikują się z edukacją instytucjonalną lub akademicką. Spotkania realizowane w tego typu miejscach często koncentrują się na praktycznych aspektach codziennego funkcjonowania w środowisku cyfrowym, w tym na bezpiecznym korzystaniu z bankowości internetowej i mobilnej, ochronie danych osobowych, rozpoznawaniu prób oszustw oraz świadomym korzystaniu z nowoczesnych form płatności. Ich istotną cechą jest silne osadzenie w lokalnym kontekście oraz możliwość bezpośredniego odnoszenia omawianych zagadnień do doświadczeń i potrzeb konkretnej społeczności.

Link: https://bs.katowice.pl/cyberbezpieczenstwo-dla-seniorow-spotkanie/

Centrum Pieniądza NBP

Na pograniczu edukacji formalnej i doświadczeniowej znajdują się także działania realizowane w Centrum Pieniądza NBP. Choć nie mają one charakteru klasycznych wykładów czy lekcji, można je traktować jako formę pośredniego kontaktu z tematyką finansów i pieniądza. Ekspozycje oraz elementy interaktywne odnoszące się do nowoczesnych form płatności, obiegu pieniądza i funkcjonowania systemu finansowego wpływają na kształtowanie świadomości ekonomicznej i cyfrowej odbiorców, również w zakresie współczesnych instrumentów płatniczych.

Link: https://cp.nbp.pl/

W kontekście edukacji cyfrowo-finansowej spotkania bezpośrednie pełnią zatem funkcję komplementarną wobec działań prowadzonych online. Umożliwiają pogłębienie treści znanych z kampanii informacyjnych czy materiałów internetowych poprzez analizę konkretnych przypadków, symulacje sytuacji zagrożeń oraz omawianie realnych incydentów. Dzięki temu uczestnicy zyskują lepsze zrozumienie mechanizmów działania cyberprzestępców oraz konsekwencji nieostrożnych decyzji finansowych podejmowanych w środowisku cyfrowym.

2.1.2. Kampanie informacyjne i materiały edukacyjne

W środowisku edukacji cyfrowej znaczącą rolę odgrywają kampanie informacyjne i szeroko dostępne materiały edukacyjne online. Ich celem jest nie tylko informowanie o ryzykach związanych z korzystaniem z narzędzi cyfrowych i usług finansowych, lecz także dostarczanie praktycznych wskazówek w sposób łatwy do przyswojenia dla szerokiego grona odbiorców oraz możliwość samodzielnego pogłębiania wiedzy. Kampanie tego typu realizowane są przez instytucje nadzorcze, organizacje branżowe, ośrodki badawcze i partnerstwa międzysektorowe.

Kampanie edukacyjne Komisji Nadzoru Finansowego

Ważnym elementem edukacji finansowej realizowanej online są kampanie informacyjne prowadzone przez Komisję Nadzoru Finansowego. KNF, jako organ nadzorczy rynku finansowego, realizuje cykliczne kampanie skierowane do szerokiego grona odbiorców, których celem jest zwiększanie świadomości na temat ryzyk związanych z uczestnictwem w rynku finansowym, w tym działań podejmowanych w środowisku cyfrowym. Jedną z takich inicjatyw jest kampania „Uwaga! Cyberoszust" – akcja edukacyjna koncentrująca się na zagrożeniach związanych z oszustwami finansowymi w sieci. Kampania dostarcza odbiorcom praktycznych wskazówek, jak rozpoznawać sygnały świadczące o próbach wyłudzenia informacji, środków lub tożsamości w internecie. W ramach kampanii publikowane są materiały informacyjne, takie jak krótkie poradniki, grafiki przedstawiające typowe metody działania cyberprzestępców oraz rekomendowane działania zmniejszające ryzyko utraty środków lub danych. Treści kampanii są udostępniane online za pośrednictwem serwisu internetowego KNF oraz mediów społecznościowych, co umożliwia ich dostępność dla odbiorców o różnym profilu i poziomie kompetencji cyfrowych. Poza kampanią „Uwaga! Cyberoszust" KNF prowadzi także inne kampanie informacyjne i materiały edukacyjne dostępne na dedykowanej stronie internetowej instytucji. Obszary tematyczne tych działań obejmują m.in. dobre praktyki i ryzyka związane z nowymi formami inwestowania (np. ryzykowne produkty inwestycyjne, wpływ influencerów finansowych – kampania Finfluencer), bezpieczeństwo uczestnictwa w obrocie finansowym, zwalczanie nadużyć oraz promocję świadomego korzystania z usług finansowych. Publikowane są

w formie artykułów, filmów edukacyjnych, infografik i poradników, które można przeglądać i pobierać bezpłatnie, co sprzyja samodzielnemu pogłębianiu wiedzy przez użytkowników.

Link: https://www.knf.gov.pl/kampanie

Kampanie edukacyjne Narodowego Banku Polskiego

W obszarze edukacji finansowej i cyfrowej istotnym źródłem materiałów online są zasoby przygotowane przez Narodowy Bank Polski, które obejmują treści poświęcone także bezpieczeństwu w środowisku cyfrowym i finansowym. NBP udostępnia szeroki wachlarz materiałów edukacyjnych, które można wykorzystać zarówno w samodzielnej nauce, jak i w prowadzeniu lekcji oraz zajęć online, w tym w ramach programów szkolnych czy kampanii tematycznych. Jednym z przykładów treści o charakterze edukacyjnym są publikacje prezentujące dobre praktyki cyberbezpieczeństwa, zawierające praktyczne wskazówki dotyczące ochrony danych osobowych, bezpiecznego zarządzania danymi oraz rozpoznawania zagrożeń w sieci. Takie materiały, dostępne w formie broszur i poradników do pobrania, mają na celu wspieranie odbiorców w nabywaniu i utrwalaniu bezpiecznych zachowań w codziennym korzystaniu z narzędzi cyfrowych. W ramach ogólnopolskiego programu edukacyjnego „Złote Szkoły NBP" bank centralny udostępnia także dedykowane materiały dotyczące cyberbezpieczeństwa finansowego, przeznaczone przede wszystkim dla środowiska szkolnego, ale mogące być wykorzystywane szerzej w edukacji cyfrowej. Wśród tych zasobów znajdują się plansze i ulotki dotyczące dobrych praktyk bezpieczeństwa, jak również scenariusze lekcji i webinary, które pomagają nauczycielom prowadzić zajęcia związane z bezpieczeństwem finansów w sieci, w tym ochroną haseł, zabezpieczaniem danych oraz bezpiecznymi płatnościami online.

Link: https://nbp.pl/dobre-praktyki-cyberbezpieczenstwa/

„Bezpieczeństwo w Cyberprzestrzeni"

Projekt „Bezpieczeństwo w Cyberprzestrzeni" to ogólnopolska kampania edukacyjna realizowana przez Fundację Warszawski Instytut Bankowości we współpracy z partnerami z sektora publicznego i prywatnego, mająca na celu podnoszenie kompetencji społecznych w zakresie świadomego i bezpiecznego korzystania z internetu oraz narzędzi cyfrowych. Kampania funkcjonuje od kilku lat jako część szerzej zakrojonego programu edukacyjnego „Bankowcy dla Edukacji" i jest realizowana z udziałem instytucji publicznych, a także partnerów technologicznych i firm z sektora finansowego i e-commerce. Kampania ta oferuje planowo i systemowo udostępniane materiały edukacyjne oraz interaktywne działania online, które są dostosowane do potrzeb różnych grup wiekowych i społecznych – od dzieci i młodzieży, przez młodych dorosłych i studentów, po seniorów. W ramach projektu prowadzone są m.in.:

- lekcje i warsztaty online uczące zasad bezpiecznego korzystania z sieci, rozpoznawania cyberzagrożeń, ochrony danych osobowych i odpowiedzialnego uczestnictwa w cyfrowej rzeczywistości;
- konkursy edukacyjne, takie jak „Cyber Geniusz" – interaktywny konkurs grywalizacyjny dla uczniów i studentów, w którym uczestnicy rozwiązują zadania i testy sprawdzające wiedzę o cyberbezpieczeństwie;
- szkolenia dla studentów pierwszego roku w partnerstwie z ponad 100 uczelniami, które wprowadzają młodych ludzi w podstawy bezpiecznego funkcjonowania w sieci;
- materiały do samodzielnej nauki, takie jak raporty, badania, poradniki i podcasty dostępne na dedykowanej platformie kampanii.

Kampania realizowana jest przede wszystkim online, co umożliwia szerokie dotarcie i planowe, regularne udostępnianie treści edukacyjnych w formie dostępnej dla odbiorców w całym kraju. Kombinacja komunikacji internetowej z elementami interakcji i rywalizacji (np. konkursy, webinary, quizy) sprzyja zaangażowaniu uczestników oraz powtarzalnemu wzmacnianiu kluczowych przekazów związanych z bezpieczeństwem cyfrowym

Link: https://cyber.wib.edu.pl/

„Bankowcy dla CyberEdukacji"

Jednym z przykładów tematów poruszanych w ramach ogólnopolskiej kampanii „Bankowcy dla CyberEdukacji" jest inicjatywa edukacyjna poświęcona zagrożeniom związanym z tzw. wyłudzeniami „na znajomego". Kampania ta, realizowana przez Zwią-

zek Banków Polskich we współpracy z Fundacja Warszawski Instytut Bankowości, Bankowe Centrum Cyberbezpieczeństwa, Policją oraz bankami, ma na celu edukowanie użytkowników internetu w zakresie rozpoznawania i przeciwdziałania próbom oszustw finansowych realizowanych poprzez podszywanie się pod znane osoby w mediach społecznościowych. W komunikatach kampanii zwraca się uwagę na mechanizm polegający na tym, że cyberprzestępcy wysyłają wiadomości rzekomo od znajomych, prosząc o pilne przelanie środków, często wraz z linkami do fałszywych stron płatności. Tego typu scenariusze mają na celu wzbudzenie emocji i skłonienie odbiorcy do pochopnej reakcji, bez weryfikacji tożsamości nadawcy. W ramach kampanii publikowane są materiały edukacyjne w formie krótkich filmów i poradników online, które przedstawiają przykłady tych oszustw oraz rekomendowane zasady postępowania w przypadku otrzymania podejrzanej wiadomości. Do kluczowych zaleceń należą m.in. stosowanie dwuskładnikowego uwierzytelniania, weryfikowanie tożsamości osób kontaktujących się w imieniu znajomych, ochrona urządzeń mobilnych oraz rozwaga przy potwierdzaniu transakcji w aplikacjach bankowych. Treści te są udostępniane w kanałach internetowych kampanii, co sprzyja ich szerokiemu rozpowszechnieniu i przypominaniu o zagrożeniach w czasie rzeczywistym. Omawiana odsłona kampanii „Bankowcy dla CyberEdukacji" ilustruje, jak działania edukacyjne oparte na realnych scenariuszach cyberzagrożeń mogą wspierać budowanie kompetencji cyfrowych i finansowych użytkowników poprzez przekaz praktycznych wskazówek, które łatwo zastosować w codziennym korzystaniu z internetu i usług bankowych.

Link: https://www.zbp.pl/Aktualnosci/Wydarzenia/Bankowcy-dla-Cyberedukacji-Wyludzenia-na-znajomego

#Halo! Tu cyberbezpieczny Senior!

Przykładem cyklicznej kampanii jest #Halo! Tu cyberbezpieczny Senior!, realizowana przez Warszawski Instytut Bankowości wraz z Naukową i Akademicką Siecią Komputerową – NASK oraz Centralnym Biurem Zwalczania Cyberprzestępczości. Inicjatywa ta jest adresowana do osób starszych i ma na celu podnoszenie wiedzy na temat zagrożeń internetowych – w szczególności oszustw telefonicznych i internetowych – oraz przedstawianie metod ich rozpoznawania i unikania. Kampania obejmuje szeroki zestaw treści edukacyjnych, takich jak poradniki, infografiki, ulotki oraz webinary, udostępniane w formacie online, co umożliwia dotarcie do osób o różnym stopniu mobilności i kompetencji cyfrowych. Wymieniona kampania jest przykładem działań cyklicznych i wielokanałowych, które wykorzystują internet do ciągłego udostępniania materiałów, organizacji spotkań online, publikacji poradników i artykułów, a także angażowania odbiorców poprzez media społecznościowe oraz interaktywne formy edukacji. Dzięki temu treści są dostępne w dowolnym czasie i miejscu, co sprzyja budowaniu świadomości oraz powtarzalności przekazu, a także umożliwia łatwe aktualizowanie informacji zgodnie z rozwojem technologii i zmianami w sposobach działania cyberprzestępców.

Link: https://www.gov.pl/web/baza-wiedzy/halo-tu-cyberbezpieczny-senior

Kampanie sektora bankowego o charakterze informacyjnym

Uzupełnieniem działań realizowanych przez instytucje nadzorcze i organizacje branżowe są kampanie informacyjne prowadzone bezpośrednio przez banki komercyjne i spółdzielcze. Działania te mają zazwyczaj charakter edukacyjno-informacyjny i koncentrują się na podnoszeniu świadomości klientów w zakresie bezpiecznego korzystania z usług bankowych w środowisku cyfrowym. Kampanie bankowe są w dużej mierze realizowane w kanałach online, takich jak strony internetowe banków, serwisy transakcyjne, bankowość elektroniczna i mobilna, a także media społecznościowe. W ramach tych inicjatyw banki udostępniają m.in. poradniki, artykuły edukacyjne, infografiki oraz krótkie materiały wideo dotyczące bezpieczeństwa płatności elektronicznych, ochrony danych osobowych, rozpoznawania prób phishingu, smishingu i vishingu, a także zasad bezpiecznego korzystania z bankowości mobilnej. Część materiałów ma charakter ostrzegawczy i reaguje na bieżące zagrożenia, inne natomiast pełnią funkcję prewencyjną, wzmacniając długofalowo wiedzę i czujność użytkowników. Charakterystyczną cechą kampanii informacyjnych realizowanych przez banki jest ich planowość oraz powtarzalność. Treści edukacyjne są często aktualizowane w odpowiedzi na zmieniające się metody działania cyberprzestępców, a komunikaty bezpieczeństwa pojawiają się cyklicznie, np. w formie sezonowych kampanii tematycznych lub stałych sekcji edukacyjnych. Dzięki wykorzystaniu kanałów cyfrowych banki mają możliwość szybkiego dotarcia do dużej liczby odbiorców

oraz osadzania przekazu edukacyjnego bezpośrednio w kontekście codziennego korzystania z usług finansowych. Kampanie bankowe wzmacniają spójność przekazu edukacyjnego dotyczącego cyberbezpieczeństwa i płatności cyfrowych, przyczyniając się do kształtowania bezpiecznych nawyków użytkowników oraz zwiększania ich odporności na zagrożenia w środowisku online.

2.1.3. Artykuły, poradniki online

W dobie cyfryzacji edukacja finansowa i bezpieczeństwa w sieci nabiera coraz większego znaczenia, a jednym z najpowszechniej wykorzystywanych sposobów ich upowszechniania są artykuły i poradniki dostępne online. Publikacje tego typu przygotowywane są przez instytucje nadzorcze, organizacje branżowe, instytucje finansowe, ośrodki badawcze oraz ekspertów, a ich celem jest przekazywanie wiedzy w sposób zwięzły, zrozumiały i łatwy do zastosowania w codziennym korzystaniu z płatności elektronicznych.

Artykuły edukacyjne koncentrują się na praktycznych aspektach bezpieczeństwa w sieci – np. rozpoznawaniu metod phishingu i fałszywych wiadomości, zasadach ochrony danych osobowych, korzystaniu z bankowości mobilnej oraz identyfikacji podejrzanych transakcji. Poradniki dostępne w formie tekstowej często są wzbogacone o ilustracje, checklisty i schematy postępowania, co wspiera ich użyteczność jako narzędzi samokształcenia. Takie materiały są powszechnie dystrybuowane na platformach edukacyjnych KNF i NBP, serwisach edukacyjnych WIB, stronach banków komercyjnych, a także w mediach społecznościowych, co zwiększa ich zasięg i dostępność dla szerokiego grona odbiorców. Systematyczne publikowanie artykułów i poradników online stanowi ważny element planowej strategii edukacji cyfrowej, umożliwiając odbiorcom samodzielne pogłębianie wiedzy w dogodnym tempie oraz odniesienie treści do własnych doświadczeń związanych z płatnościami online.

2.1.4. Podcasty edukacyjne, blogi, spoty TV, lekcje online

Formy audio, takie jak podcasty, audycje i blogi audio, zyskują coraz większe znaczenie jako narzędzia edukacji cyfrowej i finansowej, szczególnie w obszarze bezpieczeństwa korzystania z usług finansowych online. Ich rosnąca popularność wynika z możliwości regularnego i długofalowego docierania do odbiorców, elastyczności formatu oraz łatwości konsumpcji treści – zwłaszcza w środowisku mobilnym i w trakcie codziennych czynności, takich jak dojazdy do pracy czy aktywności domowe. W przeciwieństwie do jednorazowych kampanii informacyjnych, format audio sprzyja budowaniu trwałej relacji z odbiorcą oraz systematycznemu utrwalaniu wiedzy.

Podcast „Finanse pod nadzorem”

To oficjalny podcast edukacyjny publikowany przez Komisja Nadzoru Finansowego / Urząd Komisji Nadzoru Finansowego. Jest to cykl nagrań o charakterze edukacyjnym, odnoszących się do zagadnień z zakresu rynku finansowego oraz kwestii, z którymi spotykają się uczestnicy rynku – w szczególności konsumenci i osoby nieprofesjonalne korzystające z usług finansowych. Podcast jest dostępny na platformach streamingowych (np. Spotify) jako seria odcinków poruszających aktualne tematy edukacyjne, w tym również te związane z cyberbezpieczeństwem i zagrożeniami w środowisku online. Format „Finanse pod nadzorem” pozwala na elastyczne słuchanie treści w dowolnym czasie oraz łączy elementy merytorycznej wiedzy regulacyjnej z praktycznymi wskazówkami dotyczącymi bezpieczeństwa – także w kontekście płatności online i zagrożeń cybernetycznych.

Link: https://open.spotify.com/show/5RDdviNW8X1log8VeNDgku

Streamingi Bankowcy dla CyberEdukacji

Szczególnym przykładem takiej inicjatywy jest audycja edukacyjna Bankowcy dla CyberEdukacji, nadawana regularnie co piątek od 2016 r. i dostępna na platformach streamingowych, m.in. Spotify. Audycja liczy już blisko 500 odcinków, co czyni ją jednym z najbardziej długofalowych i systematycznych projektów audio w obszarze edukacji finansowej i cyberbezpieczeństwa w Polsce. Jej tematyka obejmuje zagadnienia związane z finansami osobistymi, bezpieczeństwem w sieci, praktycznymi aspektami wykrywania i unikania zagrożeń w płatnościach cyfrowych, a także analizę aktualnych trendów i mechanizmów wykorzystywanych przez cyberprzestępców. Stała cykliczność emisji, ekspercki charakter treści oraz reagowanie na bieżące zjawiska i nowe formy zagrożeń sprawiają, że audy-

cja pełni funkcję ciągłego narzędzia edukacyjnego, a nie jedynie źródła okazjonalnych informacji. Możliwość odsłuchania odcinków w dowolnym czasie i miejscu sprzyja samodzielnemu pogłębianiu wiedzy oraz powracaniu do omawianych treści w miarę pojawiania się nowych potrzeb lub wątpliwości użytkowników.

Link: https://open.spotify.com/show/4Nq6GNdr6GEqNA1Xe7OTD6?si=696771f7a7ca4e40&nd=1&dlsi=1686e7e675b24f73

Podcast CYBER POD

W ramach podcasu komentowane są najważniejsze wydarzenia ze świata cyberbezpieczeństwa. Audycje mają na celu popularyzowanie wiedzy na temat korzystania z nowoczesnych narzędzi cyfrowych, zwiększanie świadomości dotyczącej cyberzagrożeń oraz kształtowanie właściwych postaw w zakresie bezpieczeństwa w cyberprzestrzeni. Podcast przygotowywany jest w ramach projektu edukacyjnego „Bezpieczeństwo w Cyberprzestrzeni", realizowanego przez Warszawski Instytut Bankowości.

Link: https://open.spotify.com/playlist/0RAfPbbq8gjbpieVYmIM6R?si=9a5cc5a8af974947&nd=1

Blogi eksperckie oraz kanały tematyczne w formie audio

Podobną rolę w ekosystemie edukacji cyfrowej pełnią specjalistyczne blogi eksperckie oraz kanały tematyczne w formie audio, w ramach których publikowane są rozmowy z praktykami sektora finansowego i technologicznego, analizy konkretnych przypadków cyberataków i oszustw, a także komentarze do zmian technologicznych, regulacyjnych i społecznych wpływających na bezpieczeństwo płatności online. Formaty te sprzyjają nie tylko przekazywaniu wiedzy, lecz także budowaniu świadomości zagrożeń, kształtowaniu bezpiecznych postaw oraz integrowaniu społeczności odbiorców zainteresowanych tematyką cyberbezpieczeństwa i finansów cyfrowych. Jednocześnie dynamiczny rozwój kanałów cyfrowych oraz rosnąca popularność roli influencerów finansowych i technologicznych rodzi istotne wyzwania związane z wiarygodnością i rzetelnością prezentowanych treści. W przeciwieństwie do inicjatyw realizowanych przez instytucje publiczne, nadzorcze lub branżowe, część treści publikowanych w formie blogów, vlogów lub podcastów tworzonych przez indywidualnych autorów nie zawsze opiera się na zweryfikowanych źródłach ani aktualnej wiedzy eksperckiej. Zjawisko to może prowadzić do uproszczeń, nadinterpretacji lub rozpowszechniania niepełnych informacji, co w obszarze bezpieczeństwa finansowego i płatności online stanowi szczególne ryzyko. Z tego względu w kontekście edukacji finansowej coraz częściej podkreśla się potrzebę krytycznego odbioru treści publikowanych w mediach cyfrowych oraz wzmacniania kompetencji odbiorców w zakresie oceny źródeł informacji. W raporcie zasadnym jest więc traktowanie blogów i kanałów audio przede wszystkim jako uzupełniającej formy edukacji, której skuteczność i bezpieczeństwo zależą od jakości merytorycznej przekazu oraz odpowiedzialności twórców. W efekcie podcasty, blogi audio i inne formy przekazu eksperckiego mogą stanowić wartościowy element nowoczesnej edukacji finansowej online, pod warunkiem ich osadzenia w szerszym, instytucjonalnym ekosystemie edukacyjnym i uzupełniania treściami pochodzącymi z wiarygodnych źródeł.

Link: https://open.spotify.com/episode/6yTSYfMm9LWm8e6buUkwth

Ogólnopolskie lekcje online dla uczniów i nauczycieli

Jedną z najbardziej dostępnych i jednocześnie efektywnych form edukacji ekonomicznej realizowanych w ramach Roku Edukacji Ekonomicznej 2024 były ogólnopolskie lekcje online skierowane do uczniów oraz nauczycieli szkół podstawowych i ponadpodstawowych. Zajęcia te miały charakter otwarty i były prowadzone w formule zdalnej, co umożliwiło udział szerokiemu gronu odbiorców z różnych regionów kraju, niezależnie od wielkości miejscowości czy zaplecza organizacyjnego szkół. Skala przedsięwzięcia pozwoliła na dotarcie do tysięcy uczniów i nauczycieli, czyniąc tę formę edukacji jednym z kluczowych narzędzi upowszechniania wiedzy ekonomicznej w 2024 roku. Tematyka lekcji obejmowała zarówno zagadnienia historyczne i systemowe, jak i problemy bezpośrednio związane ze współczesnymi wyzwaniami gospodarczymi oraz bezpieczeństwem cyfrowym. Wśród poruszanych tematów znalazły się m.in. reformy gospodarcze Władysława Grabskiego, ewolucja bankowości centralnej w Polsce, rola Unii Europejskiej w kształtowaniu ładu gospo-

darczego, a także kwestie cyberbezpieczeństwa, ochrony danych oraz zagrożeń występujących w środowisku cyfrowym. Tak szeroki zakres tematyczny sprzyjał budowaniu interdyscyplinarnego podejścia do edukacji ekonomicznej, łączącego wiedzę historyczną, instytucjonalną i praktyczną.

Link: https://www.wib.org.pl/2025-rok-w-warszawskim-instytucie-bankowosci/

2.1.5. Szkolenia i webinaria

W kontekście edukacji cyfrowej oraz bezpieczeństwa w płatnościach online szkolenia i webinaria stanowią istotne uzupełnienie treści statycznych i asynchronicznych materiałów edukacyjnych, takich jak artykuły, poradniki czy podcasty. Ich wyróżnikiem jest możliwość bezpośredniego kontaktu z ekspertami, aktualność omawianych zagadnień oraz interaktywny charakter przekazu. Szkolenia tego typu realizowane są zarówno w formule wydarzeń na żywo, jak i w postaci nagrań udostępnianych później na żądanie, co zwiększa ich dostępność i trwałość edukacyjną.

Szkolenia i webinaria online są najczęściej prowadzone przez przedstawicieli instytucji nadzorczych, organizacji branżowych, ośrodków badawczych, uczelni wyższych oraz zespołów odpowiedzialnych za bezpieczeństwo w sektorze bankowym. Zakres tematyczny tych działań koncentruje się na praktycznych aspektach bezpiecznego funkcjonowania w środowisku finansów cyfrowych i obejmuje m.in.: rozpoznawanie zagrożeń w płatnościach elektronicznych i bankowości internetowej; dobre praktyki w zakresie tworzenia haseł i stosowania silnych mechanizmów uwierzytelniania; bezpieczne korzystanie z bankowości mobilnej i aplikacji finansowych; analizę aktualnych trendów i metod działania cyberprzestępców.

Webinaria charakteryzują się wysokim poziomem interaktywności, umożliwiając uczestnikom zadawanie pytań, udział w ankietach, analizę studiów przypadków czy symulacje wybranych scenariuszy zagrożeń. Tego typu forma sprzyja nie tylko przekazywaniu wiedzy, lecz także jej utrwalaniu poprzez aktywne zaangażowanie odbiorców. Istotnym atutem jest również fakt, że wiele webinariów realizowanych jest cyklicznie, co pozwala na planowe i systematyczne budowanie kompetencji cyfrowych i finansowych. W Polsce szkolenia i webinaria dotyczące bezpieczeństwa finansowego online są organizowane m.in. przez następujące instytucje (przykładowe inicjatywy ilustrują zamieszczone odnośniki)[4]:

- Komisję Nadzoru Finansowego: https://www.knf.gov.pl/dla_rynku/edukacja_cedur/seminaria?articleId=95633&p_id=18
- NASK: https://www.nask.pl/aktualnosci/cyberodpornosc-w-praktyce-bezplatny-webinar-nask-i-mrit-dla-firm
- UOKiK: https://finanse.uokik.gov.pl/finanse/zaproszenie-na-webinar-bezpieczne-platnosci-w-internecie-dla-seniorow/
- Ministerstwo Rozwoju i Technologii: https://www.gov.pl/web/rozwoj-technologia/cyberodpornosc-na-start---praktyczny-webinar-dla-przedsiebiorcow
- Krajowe Centrum Kompetencji Cyberbezpieczeństwa: https://www.gov.pl/web/cyber-ncc-pl/cykl-webinarow-dotyczacych-cyberbezpieczenstwa
- Bank Gospodarstwa Krajowego: https://www.bgk.pl/cyberakademia-bgk/webinary/
- Fundacja Warszawski Instytut Bankowości. Program Analityczno-Badawczy: https://pabwib.pl/webinary/
- instytucje płatnicze: https://www.youtube.com/watch?v=f62Vlx3jHtc
- banki komercyjne i spółdzielcze
- uczelnie wyższe

Instytucje te prowadzą działania szkoleniowe skierowane do różnych grup odbiorców – od konsumentów indywidualnych, przez nauczycieli i studentów, po przedstawicieli instytucji publicznych i sektora finansowego i przedsiębiorców. Dostosowanie tematyki szkoleń do bieżących wydarzeń i nowych zagrożeń (np. pojawienia się nowych technik phishingowych lub wykorzystania sztucznej inteligencji w oszustwach finansowych) sprawia, że webinaria i szkolenia online pełnią funkcję aktualnego i elastycznego narzędzia edukacyjnego. Dzięki temu

4 Przytoczone webinary mają w przewadze charakter historyczny.

wspierają one rozwój praktycznych kompetencji użytkowników oraz zwiększają ich odporność na zagrożenia związane z korzystaniem z płatności elektronicznych i usług finansowych w środowisku cyfrowym.

2.2. Interaktywna edukacja finansowa w Polsce

Edukacja finansowa w Polsce zyskuje na znaczeniu, szczególnie w kontekście dynamicznie rozwijającego się sektora usług finansowych oraz wzrastającej potrzeby budowania świadomego społeczeństwa ekonomicznego. Współczesna edukacja finansowa w Polsce realizowana jest poprzez wieloaspektowe podejście obejmujące quizy i konkursy wiedzy, aplikacje mobilne z funkcjami edukacyjnymi oraz gry oparte na mechanizmach grywalizacji. Instytucje takie jak Fundacja Warszawski Instytut Bankowości, Narodowy Bank Polski, banki komercyjne i spółdzielcze tworzą ekosystem edukacyjny docierający rocznie do setek tysięcy Polaków w różnym wieku – zarówno młodzieży, jak i dorosłych użytkowników usług finansowych.

Edukacja ta ma charakter wielopłaszczyznowy: łączy teorię z praktyką, angażuje poprzez grywalizację, a także wykorzystuje nowoczesne technologie, takie jak aplikacje mobilne i platformy online. W tym rozdziale dokonano analizy dostępnych na rynku polskim narzędzi i programów edukacyjnych, kategoryzując je według metodyki nauczania oraz kanałów dotarcia do odbiorcy. Zidentyfikowano sześć kluczowych filarów dydaktycznych: weryfikację wiedzy poprzez quizy i testy, mobilną edukację aplikacyjną, stałą komunikację ekspercką (newslettery), angażującą grywalizację, symulacje procesów rynkowych oraz immersyjne doświadczenia typu escape room. Każdy z tych obszarów został poddany analizie, uwzględniającej nie tylko opis funkcjonalny, ale także status aktywności, grupę docelową oraz mechanizmy psychologiczne stojące za skutecznością danego rozwiązania.

Wdrażanie *Krajowej Strategii Edukacji Finansowej* (KSEF) przyczyniło się do wyznaczenia nowych standardów jakościowych w obszarze edukacji finansowej. Widoczne jest stopniowe odejście od incydentalnych, jednorazowych inicjatyw na rzecz działań o charakterze ciągłym, realizowanych w sposób systematyczny i wspieranych przez zaawansowane rozwiązania technologiczne. Szczególnie istotnym trendem staje się zjawisko określane mianem „bankowości od kołyski", w ramach którego instytucje finansowe – za pośrednictwem aplikacji mobilnych – coraz częściej pełnią rolę pierwszych nauczycieli podstaw ekonomii dla dzieci, wyprzedzając w tym zakresie formalny system edukacji. Równolegle dynamiczny rozwój sektora EdTech (technologii edukacyjnych) sprzyja wprowadzaniu do szkół narzędzi takich jak algorytmiczne symulatory biznesowe, które stopniowo zastępują tradycyjne, statyczne podręczniki, tworząc bardziej interaktywne i realistyczne środowisko rynkowe.

Większość programów edukacji finansowej prowadzonych w Polsce jest skierowana do dzieci i młodzieży. Ma to solidne podstawy naukowe – według badań, nawyki finansowe zaczynają kształtować się już około siódmego roku życia i utrwalają się do trzynastego roku życia (Whitebread i Bingham, 2013). Wczesna edukacja pozwala zatem na wykształcenie odpowiedzialnych postaw wobec pieniędzy, oszczędzania, planowania budżetu i unikania zadłużenia. Programy edukacyjne dla młodych ludzi często łączą teorię z praktyką. Dzieci uczą się nie tylko pojęć finansowych, ale również doświadczają ich znaczenia poprzez korzystanie z kont bankowych, aplikacji mobilnych czy uczestnictwo w konkursach i grach edukacyjnych.

Prezentowane w dalszej części rozdziału inicjatywy edukacyjne różnią się nie tylko formą dydaktyczną i grupą docelową, lecz także stopniem, w jakim uwzględniają zagadnienia cyberbezpieczeństwa w kontekście usług finansowych. Ze względu na centralny temat niniejszego raportu - rolę edukacji finansowej jako „cyfrowej tarczy" chroniącej użytkowników przed zagrożeniami w środowisku płatności cyfrowych – istotne jest wyraźne zidentyfikowanie tych programów, które w szczególny sposób kształtują kompetencje z zakresu bezpieczeństwa cyfrowego.

W tym celu dokonano przekrojowej klasyfikacji wszystkich omawianych inicjatyw według intensywności komponentu cyberbezpieczeństwa, przyjmując następującą typologię:

- Komponent centralny **(●●●)** – inicjatywy, w których cyberbezpieczeństwo stanowi główny lub dominujący temat programu edukacyjnego;
- Komponent rozbudowany **(●●○)** – inicjatywy zawierające rozbudowany moduł cyberbezpieczeństwa w ramach szerszego programu edukacji finansowej;

- Elementy cyberbezpieczeństwa (●○○) – inicjatywy, w których zagadnienia bezpieczeństwa cyfrowego pojawiają się jako jeden z wielu poruszanych tematów, bez wyodrębnionego modułu;

- Brak komponentu (○○○) – inicjatywy skoncentrowane na edukacji finansowej *sensu stricto*, bez wyodrębnionego wątku cyberbezpieczeństwa.

Tabela 3 przedstawia syntetyczne zestawienie analizowanych inicjatyw według czterech wymiarów: formy dydaktycznej (odpowiadającej strukturze podrozdziałów 2.2.1–2.2.3), organizatora, głównej grupy docelowej oraz poziomu intensywności komponentu cyberbezpieczeństwa. Zestawienie to stanowi mapę orientacyjną dla dalszej lektury i umożliwia szybką identyfikację programów najsilniej powiązanych z tematyką bezpieczeństwa cyfrowego.

Jak wynika z powyższego zestawienia, inicjatywy o najwyższej intensywności komponentu cyberbezpieczeństwa (●●●) koncentrują się przede wszystkim w obszarze grywalizacji i interaktywnych konkursów kierowanych do młodzieży szkolnej i stu-

Tabela 3. Inicjatywy interaktywnej edukacji finansowej w Polsce – przekrój według formy, grupy docelowej i komponentu cyberbezpieczeństwa

Inicjatywa	Organizator	Grupa docelowa	Komponent cyberbezpieczeństwa
Europejski Quiz Finansowy (BAKCYL)	WIB / ZBP / EBF	Młodzież (13–15 lat)	●○○ elementy
Olimpiada Wiedzy Ekonomicznej	Polskie Tow. Ekonomiczne	Młodzież (szk. ponadpodst.)	○○○ brak
Mistrzostwa Polski Młodych Ekonomistów (XIX ed.)	SKEF	Młodzież (13–15 lat)	●●● centralny
Test SKO	PKO Bank Polski	Dzieci i młodzież	●○○ elementy
Kapitalni.org	Kapitalni.org / Grupa BIK	Dorośli	●●○ rozbudowany
Test Wiedzy Ekonomicznej Forum Uczelni Ekonomicznych	Forum Uczelni Ekon. / PSRP	Studenci	●○○ elementy
Quiz ekonomiczny InternetowyKantor.pl	InternetowyKantor.pl	Dorośli	○○○ brak
Finansiaki	Santander Bank Polska	Dzieci (3+ lat)	○○○ brak
Nasz Bank Junior	Banki spółdzielcze	Dzieci (<13 lat)	●●○ rozbudowany
PeoPay KIDS	Bank Pekao S.A.	Dzieci (6–13 lat)	○○○ brak
PKO Junior	PKO Bank Polski	Dzieci (<12 lat)	○○○ brak
Moje ING dla dzieci	ING Bank Śląski	Dzieci (6–12 lat)	●●○ rozbudowany

Inicjatywa	Organizator	Grupa docelowa	Komponent cyberbezpieczeństwa
mBank Junior	mBank S.A.	Dzieci (0–13 lat)	●○○ elementy
Score Hunter	BIK / Gamfi	Dorośli, studenci, młodzież 16+	●●○ rozbudowany
Cyber Geniusz	WIB	Młodzież i studenci	●●● centralny
Haki na cyberataki	Stow. Aquila / Santander	Młodzież (szk. podst. i ponadpodst.)	●●● centralny
Gra planszowa Za tydzień impreza!	BPS / Banki spółdzielcze	Dzieci (9+ lat)	○○○ brak
Misja Edukacja	BNP Paribas	Dzieci (6–13 lat)	●○○ elementy
Miasto ING / Akademia Cyberbezpieczeństwa	ING Bank Śląski	Dzieci i młodzież (7–17 lat)	●●○ rozbudowany

Źródło: opracowanie własne na podstawie analizy programów edukacyjnych.

dentów – są to Cyber Geniusz, Haki na cyberataki oraz XIX edycja Mistrzostw Polski Młodych Ekonomistów. W segmencie aplikacji mobilnych dla dzieci, mimo dynamicznego rozwoju funkcjonalności bankowych, komponent cyberbezpieczeństwa pozostaje na ogół ograniczony do podstawowych zasad bezpiecznego korzystania z produktów bankowych, z wyjątkiem Miasta ING, którego Akademia Cyberbezpieczeństwa stanowi rozbudowany moduł obejmujący m.in. rozpoznawanie phishingu i deepfake'ów. Stosunkowo dobrze reprezentowany jest poziom rozbudowany (●●○) – platformy takie jak Score Hunter, Kapitalni.org czy Nasz Bank Junior integrują treści dotyczące ochrony tożsamości, bezpieczeństwa danych i prewencji oszustw z szerszym programem edukacji finansowej. Jednocześnie istotna część analizowanych inicjatyw nie uwzględnia zagadnień cyberbezpieczeństwa w żadnej formie, co - w obliczu rosnącej skali zagrożeń cyfrowych opisanych w rozdziale 1 - stanowi istotną lukę i przesłankę dla rekomendacji formułowanych w dalszej części raportu.

Dalsza część rozdziału zachowuje porządek według formy dydaktycznej - od quizów i testów (2.2.1), przez aplikacje mobilne (2.2.2), po mechanizmy grywalizacji (2.2.3) i ekosystemy instytucjonalne (2.2.4). Wybór ten jest podyktowany trzema przesłankami merytorycznymi. Po pierwsze, forma dydaktyczna determinuje mechanizmy psychologiczne stojące za skutecznością danego rozwiązania – quiz odwołuje się do rywalizacji i natychmiastowej informacji zwrotnej, aplikacja mobilna do uczenia przez doświadczenie, grywalizacja do wewnętrznej motywacji i progresji, a ekosystem instytucjonalny do efektu skali i ciągłości oddziaływania. Uporządkowanie inicjatyw według tych mechanizmów pozwala czytelnikowi nie tylko poznać poszczególne programy, lecz także zrozumieć, dlaczego dana forma sprawdza się w określonym kontekście edukacyjnym i dla określonej grupy odbiorców. Po drugie, tak przyjęta struktura odzwierciedla naturalną ścieżkę intensyfikacji zaangażowania użytkownika – od biernego testowania wiedzy, przez aktywne korzystanie z narzędzi bankowych wbudowanych w aplikacje, po immersyjne doświadczenia grywalizacyjne wymagające wieloetapowego zaangażowania poznawczego. Ten gradient interaktywności stanowi jednocześnie oś porównawczą, wzdłuż której można oceniać potencjał poszczególnych form w budowaniu trwałych kompetencji z zakresu cyberbezpieczeństwa. Po trzecie, podział według formy pozwala uniknąć fragmentaryzacji opisu tych inicjatyw, które łączą edukację finansową z cyberbezpieczeństwem jedynie w wybranych edycjach lub modułach – co

miałoby miejsce w przypadku klasyfikacji opartej wyłącznie na kryterium tematycznym.

Jednocześnie, aby umożliwić lekturę przekrojową – zorientowaną na tematykę cyberbezpieczeństwa niezależnie od formy dydaktycznej – w niniejszym rozdziale wprowadzono przedstawioną powyżej tabelę 3 jako uzupełniające narzędzie nawigacyjne. Czytelnik zainteresowany przede wszystkim aspektem bezpieczeństwa cyfrowego może posłużyć się nią jako mapą orientacyjną, kierując uwagę w pierwszej kolejności na inicjatywy oznaczone najwyższym poziomem komponentu (●●● i ●●○), a następnie oceniając, w jakim stopniu poszczególne formy dydaktyczne sprzyjają kształtowaniu kompetencji cyberodpornościowych. Oba porządki – według formy i według intensywności komponentu cyberbezpieczeństwa – są zatem komplementarne i służą różnym celom analitycznym: pierwszy pozwala zrozumieć „jak" i „dlaczego" uczymy, drugi – „o czym" i „w jakim zakresie".

2.2.1. Quizy i testy – od weryfikacji do kształtowania kompetencji

Współczesne formy testowania wiedzy ekonomicznej w Polsce ewoluowały z prostych sprawdzianów pamięciowych w kierunku skomplikowanych, wieloetapowych procesów analitycznych. Konkursy i quizy wiedzy ekonomicznej stanowią fundamentalny element polskiego systemu edukacji finansowej, łącząc funkcję dydaktyczną z motywacyjną poprzez mechanizmy rywalizacji. Inicjatywy te różnią się skalą, grupą docelową i poziomem zaawansowania, tworząc spójny ekosystem obejmujący uczniów od szkół podstawowych po studentów uczelni wyższych. Stanowią dobrą bazę do wspierania edukacji formalnej.

Europejski Quiz Finansowy – Projekt BAKCYL - jako pomost między edukacją krajową i międzynarodową

Europejski Quiz Finansowy (EQF), znany również jako *European Money Quiz*, stanowi flagową inicjatywę Fundacji Warszawski Instytut Bankowości realizowaną we współpracy ze Związkiem Banków Polskich i Europejską Federacją Bankową. Program funkcjonuje od roku szkolnego 2017/2018, a obecna 8. edycja (2024/2025) realizowana jest pod patronatem Narodowego Banku Polskiego w ramach programu edukacji ekonomicznej. Quiz kierowany jest do uczniów klas VII i VIII szkół podstawowych (wiek 13–15 lat), którzy rywalizują w dwuosobowych zespołach. Format konkursu obejmuje wieloetapową strukturę: etap wojewódzki wyłaniający trzy najlepsze zespoły z każdego regionu, półfinał redukujący 48 drużyn do 10 najlepszych, finał krajowy dla dziesięciu dwuosobowych zespołów oraz prestiżowy finał europejski w Brukseli organizowany przez Europejską Federację Bankową. Rozgrywki odbywają się w formie testów wiedzy online na platformie Kahoot!, gdzie liczy się zarówno poprawność odpowiedzi, jak i czas reakcji. Tematyka konkursu obejmuje wiedzę z zakresu finansów, systemu bankowego w Polsce, bezpieczeństwa w cyberprzestrzeni oraz przedsiębiorczości. Program przyniósł spektakularne sukcesy polskich uczestników – w 2018 roku uczniowie z Głogowa zwyciężyli w finale europejskim, pokonując ponad 41 000 uczniów z 25 krajów. Polacy dwukrotnie stawali na podium finału europejskiego.

Link: https://bakcyl.wib.org.pl/bakcyl/konkursy/europejski-quiz-finansowy/

Olimpiada Wiedzy Ekonomicznej jako najstarsza i najbardziej prestiżowa inicjatywa konkursowa

Olimpiada Wiedzy Ekonomicznej organizowana przez Polskie Towarzystwo Ekonomiczne to najstarsza inicjatywa tego typu w Polsce, działająca nieprzerwanie od roku szkolnego 1987/88. Olimpiada kierowana jest do uczniów szkół ponadpodstawowych kończących się maturą – liceów ogólnokształcących, techników oraz szkół branżowych I i II stopnia. Format zawodów obejmuje trzy stopnie: zawody szkolne (listopad, forma pisemna), zawody okręgowe (styczeń, około 500 najlepszych uczestników) oraz zawody centralne (kwiecień, około 100 uczestników, część pisemna i ustna w siedzibie GPW). W części centralnej uczestnicy odpowiadają na pytanie opisowe nawiązujące do hasła przewodniego, rozwiązują zadanie analityczne i 30 pytań testowych, a do części ustnej kwalifikują się osoby spełniające minimum punktowe. Ostatecznie wyłanianych jest 30 laureatów. Statystyki XXXVII edycji (2023/2024) pokazują skalę przedsięwzięcia: zgłoszonych 6335 uczniów z 526 szkół, do zawodów okręgowych zakwalifikowano 489 uczniów z 204 szkół, do zawodów centralnych 101 uczniów z 65 szkół. Od roku szkolnego 1987/88 uczestniczyło ponad 340 tysięcy uczniów.

Link: https://owe.pte.pl/informacje/program-i-regulamin.html

Mistrzostwa Polski Młodych Ekonomistów

Mistrzostwa Polski Młodych Ekonomistów organizowane przez Stowarzyszenie Krzewienia Edukacji Finansowej (SKEF) z siedzibą w Gdyni funkcjonują od 2006 roku, a ostatnia XIX edycja (2024/2025) prowadzona była pod hasłem „Edukacja finansowa i cyberbezpieczeństwo". W ciągu 19 edycji uczestniczyło ponad 12 000 uczniów. Konkurs kierowany jest do uczniów klas VII i VIII szkół podstawowych (do 18 roku życia) i realizowany jest w formie indywidualnej. Format dwuetapowy obejmuje eliminacje (wypełnienie formularza zgłoszeniowego i rozwiązanie zestawu pytań i zadań, przesłanie prac pocztą, ocena powyżej 70 punktów oznacza pracę kompletną) oraz finał wyjazdowy dla 10–12 najlepszych uczestników. Tematyka XIX edycji koncentrowała się na cyberhigienie, bezpiecznych hasłach, weryfikacji dwuetapowej, phishingu, quishingu, vishingu, spoofingu, socjotechnice, płatnościach BLIK, bankowości elektronicznej, ochronie danych osobowych i atakach z wykorzystaniem AI. Patronat honorowy sprawowali NBP i Krajowa SKOK, a partnerami są m.in. Fundacja im. Franciszka Stefczyka, Saltus Ubezpieczenia i Fundacja Alior Banku. Finał połączony był z konkursem „Żyj Finansowo!" dla młodzieży szkół ponadpodstawowych.

Link: https://www.skef.pl/mistrzostwa-polski-mlodych-ekonomistow/

Test SKO jako element tradycji Szkolnych Kas Oszczędności PKO BP

Test Wiedzy Ekonomicznej (Test SKO) organizowany przez PKO Bank Polski stanowi integralną część programu Szkolnych Kas Oszczędności – inicjatywy o niemal stuletniej tradycji. Historia SKO sięga 1925 roku (okólnik Ministra S. Grabskiego), a w 1935 roku kuratelę przejęła Pocztowa Kasa Oszczędności (dzisiejszy PKO BP). Przed II wojną światową program obejmował blisko 14 000 szkół i ponad milion członków. Współcześnie SKO funkcjonuje w blisko 2000 szkół (1/3 szkół podstawowych), obejmując około 150 000 oszczędzających dzieci, przy czym oferta edukacyjna dociera do ponad 400 000 uczniów. Test SKO, kierowany jest do uczniów szkół podstawowych (klasy 0–6 i wyższe), choć mogą go rozwiązywać wszyscy chętni, w tym dorośli (wersja z 12 pytaniami). Format to test online dostępny na dowolnym urządzeniu z internetem, trwający 30 minut. Uczniowie odpowiadają na 10 pytań, a próg zaliczenia to 7/10 poprawnych odpowiedzi. System losuje nową pulę pytań przy każdym podejściu, co umożliwia wielokrotne przystępowanie. Nagrodą jest elektroniczny dyplom potwierdzający wiedzę. Łącznie rozwiązano ponad 250 000 testów. Tematyka obejmuje szeroko pojęte finanse, nowoczesną bankowość, cyberbezpieczeństwo, ekologię zdrowy styl życia (edycja 2025 związana z Rokiem Edukacji Zdrowotnej i Profilaktyki). Program SKO zdobył liczne nagrody, w tym „Inicjatywa Edukacyjna Roku" (MEN, „Głos Nauczycielski"), Child & Youth Friendly Banking Award (Child and Youth Finance International) oraz Nagrodę Liderów Świata Bankowości.

Link: https://www.pkobp.pl/test-sko/?srsltid=AfmBOooBrX9n-fP6y2Q23rjSv9aZ2zMNRBjwtmhORFBAJkbaX33PjpxP-

Kapitalni.org – platforma edukacji finansowej dla dorosłych z testem osobowości

Platforma Kapitalni.org funkcjonuje od czerwca 2015 roku, pierwotnie stworzona przez Wonga.com, obecnie jako niezależna platforma współpracująca z partnerami takimi jak ZaufanaTrzeciaStrona.pl, Niebezpiecznik.pl, ERIF BIG S.A. i Grupa BIK. Partnerem honorowym jest Związek Przedsiębiorstw Finansowych. Flagowym elementem platformy jest Test Osobowości Finansowej (uruchomiony w maju 2017), który klasyfikuje użytkowników do jednego z czterech typów: „Król życia" (osoby wydające spontanicznie), „Guru Zarządzania Kryzysowego" (specjaliści od radzenia sobie z problemami), „Mistrz Strategii" (planujący długoterminowo) i „Przewodnik Stada" (osoby podążające za trendami). Po wypełnieniu testu użytkownik otrzymuje spersonalizowaną ścieżkę edukacyjną obejmującą materiały wideo, poradniki pisemne i wyzwania praktyczne. Platforma oferuje edukację w obszarach: pożyczanie, oszczędzanie, wychodzenie z długów, pomnażanie oszczędności, psychologia finansów i bezpieczeństwo cyfrowe. Elementy grywalizacji obejmują animowanych przewodników (awatary), system punktowy i rozwój postaci powiązany z nabywaniem wiedzy. Do 2017 roku liczba odtworzeń kursów przekroczyła 174 tysięcy.

Link: https://kapitalni.org/tof

Test Wiedzy Ekonomicznej Forum Uczelni Ekonomicznych – studencka rywalizacja międzyuczelniana

Test Wiedzy Ekonomicznej organizowany przez Forum Uczelni Ekonomicznych (komisję branżową Parlamentu Studentów RP) realizowany jest od 2017/2018 roku, a obecna VII edycja (2024) angażuje studentów pięciu największych uczelni ekonomicznych: Uniwersytetu Ekonomicznego w Katowicach, Szkoły Głównej Handlowej w Warszawie, Uniwersytetu Ekonomicznego w Krakowie, Uniwersytetu Ekonomicznego we Wrocławiu i Uniwersytetu Ekonomicznego w Poznaniu. Struktura konkursu obejmuje etap regionalny (100 studentów na każdej uczelni, łącznie 500 uczestników, format Kahoot) oraz finał ogólnopolski w Warszawie dla 25 finalistów. Tematyka obejmuje finanse i rachunkowość, bankowość i cyberbezpieczeństwo, międzynarodowe stosunki gospodarcze, marketing i zarządzanie, ekonomię sektora publicznego oraz gospodarkę cyfrową. Partnerem merytorycznym jest Warszawski Instytut Bankowości (program „Bankowcy dla Edukacji"), a partnerami biznesowymi Deloitte Kariera i Bank DNB.

Link: https://fue.psrp.org.pl/projekty/test-wiedzy-ekonomicznej/

Quiz ekonomiczny InternetowyKantor.pl – edukacja walutowa dla użytkowników kantoru

Quiz ekonomiczny oferowany przez platformę wymiany walut InternetowyKantor.pl to inicjatywa edukacyjno–marketingowa dostępna publicznie 24/7. Format obejmuje 32 pytania jednokrotnego i wielokrotnego wyboru, z punktacją 1 punkt za poprawną odpowiedź i maksymalnym wynikiem 35 punktów. Tematyka koncentruje się na: kursach walut i rynku FOREX (spread walutowy, bezpieczne waluty, wpływ stóp procentowych), historii finansów (Czarny Czwartek, dot–com boom, kryzys subprime 2008), wiedzy o walutach (symbole, banknoty polskie, denominacja, system SEPA), instytucjach finansowych (Bank Światowy, NBP, FED, RPP) oraz praktycznej wiedzy finansowej (nadpłata kredytu walutowego, dochód pasywny, poduszka bezpieczeństwa).

Link: https://internetowykantor.pl/quiz-ekonomiczny/

Finansiaki – kompleksowy program edukacji ekonomicznej Santander Bank Polska

Program Finansiaki, uruchomiony w grudniu 2016 roku przez Santander Bank Polska przy wsparciu Wydziału Psychologii Uniwersytetu Warszawskiego, stanowi kompleksową inicjatywę edukacyjną dla dzieci od 3. roku życia, rodziców i nauczycieli. Bohaterami programu są postaci z rodziny Finansiaków: Nina (mała mądralińska, odpowiedzialna), Tymon Ancymon (6–letni łobuziak) i oswojony dinozaur Dino. Portal oferuje bogaty zestaw materiałów: 16 scenariuszy lekcji dla nauczycieli (od „Dino, banknoty i monety" przez „Jak powstają pieniądze?" po „Procentowe love"), artykuły dla rodziców o edukacji finansowej dzieci, grę planszową do pobrania, quizy online, animacje edukacyjne i audiobooki. Książka „Finansiaki to my!" (autorzy: dr Agata Trzcińska i Paweł Oksanowicz) osiągnęła nakład ponad 11 600 egzemplarzy (6000 pierwszego nakładu plus 5600 dodruku) i od marca 2020 dostępna jest bezpłatnie online. Tematyka edukacyjna obejmuje wartość pieniądza, oszczędzanie, planowanie zakupów, budżet domowy, rozróżnianie potrzeb i zachcianek, zarabianie, kieszonkowe, bankowość, karty płatnicze i BLIK, podatki i ubezpieczenia oraz procent i odsetki. Wolontariusze Santander Bank Polska prowadzą lekcje w przedszkolach i szkołach – w 2019 roku zajęcia objęły około 1000 dzieci.

Link: https://www.santander.pl/finansiaki

2.2.2. Aplikacje mobile z funkcją edukacyjną jako laboratoria praktycznej nauki finansów

Aplikacje bankowe dla dzieci stanowią innowacyjne połączenie funkcjonalności bankowości mobilnej z elementami edukacji finansowej i grywalizacji. Badania potwierdzają skuteczność takiego podejścia – systematic review Amagir et al. (2018) wskazuje, że „uczenie się poprzez eksperymentowanie" jest „obiecującą metodą nauczania finansów dzieci i młodzieży", a badanie Batty et al. (2020) dotyczące programu „My Classroom Economy" wykazało, że nauka przez doświadczenie przynosi porównywalne efekty do tradycyjnych metod wykładowych, ale „wyłącznie poprzez uczenie się przez działanie zamiast formalnej instrukcji".

Nasz Bank Junior – integracja ze Szkolnymi Kasami Oszczędności w bankach spółdzielczych

Nasz Bank Junior to aplikacja oferowana przez sieć polskich banków spółdzielczych (Banki Spółdzielcze), w tym Bank Spółdzielczy w Nałęczowie, Bank Spółdzielczy w Jutrosinie, BS Pruszcz Pomorski, PBS Września i wiele innych. Aplikacja kierowana

jest do dzieci poniżej 13 lat. Funkcjonalność obejmuje sprawdzanie salda i oszczędności, wirtualne skarbonki, płatności BLIK (za zgodą rodzica), płatności kartą, płatności mobilne zbliżeniowe, doładowania telefonów i personalizację profilu (pseudonim, awatar, tło). Unikalną cechą jest integracja z programem SKO (Szkolne Kasy Oszczędności) – historycznym programem datującym się od 1925 roku. Integracja umożliwia śledzenie oszczędności szkolnych, zaangażowanie nauczycieli w edukację finansową, naukę planowania finansowego w grupie, system rankingowy między klasami/szkołami oraz konkursy z nagrodami dla najbardziej systematycznie oszczędzających. Edukacja koncentruje się na tajnikach oszczędzania, planowaniu budżetu i odpowiedzialnych wydatkach. Cyfrowe skarbonki umożliwiają ustawianie celów oszczędnościowych z konkretnymi kwotami, terminami realizacji, nazwami i grafikami. Grywalizacja obejmuje personalizację (wybór pseudonimu, tworzenie awatara, dostosowanie tła), konkursy szkolne (rankingi klasowe, konkursy oszczędnościowe w szkole, nagrody) i wizualne śledzenie postępów. Panel Rodzica w aplikacji „Nasz Bank" umożliwia generowanie i udostępnianie kodów BLIK, zatwierdzanie transakcji, zarządzanie limitami, pełny nadzór nad wydatkami i blokowanie dostępu. Aplikacja może działać nawet dla dzieci, których rodzice nie mają konta w banku spółdzielczym (funkcja SKO). Edukacja cyberbezpieczeństwa obejmuje dyskusje o podejrzanych transakcjach i ochronę przed oszustwami internetowymi.

Link: https://naszbankjunior.pl/

PeoPay KIDS jako pionier rynku aplikacji bankowych dla dzieci

PeoPay KIDS, uruchomiona 1 czerwca 2020 roku przez Bank Pekao S.A., była pierwszą mobilną aplikacją bankową dla dzieci w Polsce. Aplikacja kierowana jest do dzieci w wieku 6–13 lat i osiągnęła imponującą skalę: ponad 210 000 otwartych pakietów, ponad 190 000 pobrań aplikacji i 1500 logowań na godzinę (dane 2025). Funkcjonalność obejmuje pełne zarządzanie kontem osobistym (Konto Przekorzystne) i oszczędnościowym (Mój Skarb), kartę debetową Mastercard z personalizowanymi grafikami (6 opcji), płatności BLIK (kody zakupowe, wypłaty z bankomatów, przelewy na telefon), doładowania telefonów i zakup kodów do gier. Elementy edukacyjne są szczególnie rozbudowane. Gra edukacyjna składa się z 10 sezonów, z których każdy zawiera 5 tematycznych etapów obejmujących podstawy pieniądza, budżetowanie, przedsiębiorczość i oszczędzanie. Gra zawiera quizy, pytania i zadania praktyczne, a została opracowana z ekspertami edukacyjnymi i przetestowana z dziećmi i rodzicami. Nauka oszczędzania realizowana jest poprzez wirtualne skarbonki w koncie oszczędnościowym z możliwością ustawiania celów oszczędnościowych i śledzenia postępów. Grywalizacja opiera się na trzech wirtualnych trenerach: Żubr (najbardziej popularny), Lis i Złotówka, którzy prowadzą dzieci przez edukację finansową. System obejmuje osiągnięcia za ukończenie sezonów gry, personalizację aplikacji (motywy tła, wybór trenera, ikony – 13 wariantów) oraz śledzenie postępów.

Link: https://media.pekao.com.pl/pr/835058/czwarte-urodziny-peopay-kids-jak-aplikacja-bankowa-wspomaga-dzieci-w-edukacji-finansowej

PKO Junior – laureat Mobile Trends Awards z rozbudowanym systemem wyzwań

PKO Junior, oferowana przez PKO Bank Polski, kierowana jest do dzieci do 12 lat posiadających PKO Konto Dziecka. Aplikacja zdobyła nagrodę Mobile Trends Awards w kategorii „Bankowość Mobilna dla Dzieci" oraz Nagrodę Główną. Funkcjonalność obejmuje sprawdzanie salda, historię transakcji, płatności zbliżeniowe BLIK NFC (Android z NFC, od 6 lat), inicjowanie przelewów (za zgodą rodzica), doładowania telefonów i możliwość proszenia rodziców o doładowanie karty. Dostępna jest również wersja webowa (junior.pkobp.pl). Elementy edukacyjne obejmują Mówiącego Robota–Asystenta, który prowadzi dzieci przez aplikację, wyjaśnia pojęcia bankowe i oferuje pomocne wskazówki. Wirtualne skarbonki pozwalają dzieciom tworzyć, nazywać i finansować wiele celów oszczędnościowych, a kalkulator oszczędności pokazuje potencjalne oszczędności w zależności od kwot, regularności i oprocentowania. Grywalizacja realizowana jest poprzez system odznak i osiągnięć (za tworzenie skarbonek, dokonywanie wpłat, wykonywanie wyzwań) oraz system wyzwań – rodzice ustawiają zadania (sprzątanie pokoju, wyprowadzanie psa) za pośrednictwem iPKO, a dzieci zdobywają nagrody za ich wykonanie, co tworzy strategiczną progresję jak w grze. Panel Rodzica dostępny przez IKO lub iPKO umożliwia aktywację/dezaktywację aplikacji, pełny nadzór finansowy, zatwierdzanie przelewów, powiadomienia push o oczekujących akceptacjach, zarządzanie kartą (limity, blokowanie) i zmianę

PIN–u dziecka. Unikalna funkcja „Podsumowanie roku" prezentuje roczny postęp finansowy dziecka.

Link: https://www.pkobp.pl/aktualnosci/bankowosc-elektroniczna/mamy-najlepsze-aplikacje-mobilne-w-kraju?srsltid=AfmBOoqWJBSpp3w2QJ-mhM7ilfVsJLqT-b14HoXQwkPWPd62PNs2WDyqk

Moje ING dla dzieci – integracja z platformą Roblox i Miastem ING

Moje ING dla dzieci, oferowana przez ING Bank Śląski, kierowana jest do dzieci w wieku 6–12 lat (osobna wersja dla 13–17 lat) i wykorzystuje to samo konto Mobi. Aplikacja zdobyła nagrodę dla najlepszej aplikacji mobilnej – Mobile Trends Awards 2024. Funkcjonalność obejmuje sprawdzanie salda (widoczne przed logowaniem), wysyłanie próśb o przelewy do rodziców, cele oszczędnościowe, przelewy BLIK na telefon, płatności mobilne (HCE tylko Android) i kartę debetową/prepaid z personalizowanymi grafikami. Innowacyjnym elementem edukacyjnym jest „Miasto ING" – gra edukacyjna na platformie Roblox stworzona specjalnie dla dzieci 7–17 lat. W grze dzieci uczą się dobrych nawyków finansowych, oszczędzania i mądrego wydawania pieniędzy poprzez aktywności takie jak sprzątanie śmieci, wyprowadzanie psów, mycie okien, mycie aut i serwowanie jedzenia w restauracjach. Punkty zdobywane za wykonane zadania można wymieniać na nagrody. Gra zawiera również moduł cyberbezpieczeństwa uczący tworzenia silnych haseł, rozpoznawania niebezpiecznych stron i ochrony przed phishingiem.

Link: https://www.ing.pl/lp/nastolatki/miasto-ing-4

mBank Junior – edukacja poprzez „Wirtualnego Sama"

mBank Junior (eKonto Junior) oferowana przez mBank S.A. kierowana jest do dzieci w wieku 0–13 lat, przy czym konto stanowi subkonto konta rodzica. Dziecko jest użytkownikiem konta, którego właścicielem prawnie jest rodzic. Elementy edukacyjne realizowane są poprzez platformę „Wirtualny Sam" na mBank.pl/junior, gdzie postać Sama uczy dzieci płacenia kartą, wypłacania pieniędzy z bankomatu, funkcji terminala płatniczego i zasad bezpieczeństwa produktów bankowych. Dostępna jest interaktywna gra przygotowująca do używania karty w rzeczywistości. mBank wysyła również fizyczny „Starter Pack" z materiałami edukacyjnymi przy otwieraniu konta.

Link: https://www.mbank.pl/lp2/2025/c1/indywidualny/konta/junior/przelotka/?option=port_google&kampania=konto_mbank_junior_p_c&gclsrc=aw.ds&gad_source=1&gad_campaignid=12071105671&gclid=Cj0KCQiAnJHMBhDAARIsABr7b87RHGtanofKGOLTFZkear-2AYUjEQVsv8Xh3EdKZRtHNgUuJiK5nAaAh-WEALw_wcB

2.2.3. Grywalizacja i elementy rywalizacji jako katalizatory zaangażowania w edukację finansową

Grywalizacja rozumiana jest jako wykorzystanie elementów i mechanizmów znanych z gier (punktów, odznak, poziomów, rankingów, wyzwań) w sytuacjach niezwiązanych z rozrywką, takich jak edukacja, marketing, biznes czy opieka zdrowotna, w celu zwiększenia zaangażowania, motywacji i zmiany zachowań (Makowiec i Witoszek-Kubicka (red), 2019). Celem wdrożenia gamifikacji jest zwiększenie motywacji osob do wykonywania danych czynności, podniesienie ich zaangażowania lub zmiana zachowań. Polega na przekształcaniu nudnych lub monotonnych czynności w angażujące doświadczenia, co sprzyja nauce przez zabawę i budowaniu nawyków Badania naukowe potwierdzają skuteczność grywalizacji w edukacji finansowej. Cannistrà i in. al. (2024) przeprowadzili pierwsze randomizowane badanie kontrolowane gry edukacyjnej o tematyce finansowej w kontekście wielokrajowym (2220 studentów z czterech krajów europejskich), wykazując, że gra online znacząco poprawiła kompetencje finansowe uczestników – porównywalnie do podejść tradycyjnych, ale z wyższym zaangażowaniem.

Score Hunter jako platforma edukacji o zdolności kredytowej

To platforma grywalizacyjna online stworzona przez Biuro Informacji Kredytowej (BIK) we współpracy z firmą Gamfi, uruchomiona w listopadzie 2017 roku. Dostępna jest również wersja szkolna Score Hunter Junior. Platforma kierowana jest do dorosłych posiadających lub planujących kredyty, studentów uczelni wyższych, a w wersji Junior do uczniów szkół ponadpodstawowych (od 16 lat za zgodą rodzica). Mechanika oparta jest na systemie punktowym za wykonywanie zadań, quizów i oglądanie filmów edukacyjnych, wyzwaniach dla

bardziej konkurencyjnych użytkowników, rankingu w czasie rzeczywistym oraz nagrodach wymienialnych za punkty. Edukacja obejmuje zdolność kredytową i sposób jej obliczania, budowanie wiarygodności finansowej, historię kredytową, poręczenie kredytu, ochronę przed kradzieżą tożsamości, bezpieczeństwo danych osobowych i zastrzeganie dokumentów. Współpraca z influencerami (Jan Favre/Stay Fly, Marek Hoffmann/AdBuster, Adam Drzewicki/Matura to bzdura, Natalia Tur/Nishka) zwiększa atrakcyjność materiałów wideo. Platforma jest bezpłatna, dostępna online na różnych urządzeniach i dystrybuowana poprzez partnerstwa ze szkołami i uczelniami (ponad 300 instytucji).

Link: https://nzb.pl/score-hunter/

„Cyber Geniusz"

To ogólnopolski, interaktywny konkurs edukacyjny o charakterze grywalizacyjnym, realizowany w ramach kampanii „Bezpieczeństwo w Cyberprzestrzeni" przez Fundacja Warszawski Instytut Bankowości we współpracy z partnerami instytucjonalnymi i branżowymi. Inicjatywa skierowana jest do uczniów szkół ponadpodstawowych oraz studentów uczelni wyższych i stanowi odpowiedź na potrzebę angażującej, dostosowanej do młodszych odbiorców edukacji w zakresie cyberbezpieczeństwa. Konkurs skierowany jest dla uczniów „Cyber Geniusz Uczeń" i studentów „Cyber Geniusz Student". Mechanizm konkursu opiera się na realizacji zadań edukacyjnych, quizów i testów wiedzy dostępnych na dedykowanej platformie online. Uczestnicy zdobywają punkty za poprawne odpowiedzi, a ich wyniki są porównywane w ramach rankingów, co wprowadza element rywalizacji i zwiększa motywację do pogłębiania wiedzy. Konkurs realizowany jest cyklicznie, a jego formuła umożliwia udział zarówno indywidualny, jak i zespołowy, w zależności od edycji.

Link: https://cyber.wib.edu.pl/cyber-geniusz/

Haki na cyberataki jako cyfrowy escape room o tematyce finansowo–cyberbezpieczeństwa

To interaktywna gra typu escape room stworzona przez Stowarzyszenie Ochrony Konsumentów Aquila, sfinansowana przez Fundację Santander Bank Polska w ramach programu grantowego „Haki na cyberataki". Gra uruchomiona została w grudniu 2022 roku. Gra kierowana jest do uczniów klas VII–VIII szkół podstawowych oraz uczniów szkół ponadpodstawowych i przeznaczona jest do użytku na lekcjach przedsiębiorczości, informatyki, godzinach wychowawczych lub przedmiotach zawodowych. Format escape room oznacza, że gracze nawigują przez wirtualne pokoje rozwiązując zagadki finansowe/cyberbezpieczeństwa, z progresywną strukturą wyzwań i elementami interaktywnymi wpływającymi na postęp. Edukacja finansowa obejmuje bezpieczną bankowość online, mikropłatności i ukryte koszty, podstawy kryptowalut, subskrypcje i opłaty cykliczne, podstawy kredytów i pożyczek, niebezpieczeństwa „chwilówek", różnice między bankami, SKOK–ami i parabankami, nieuczciwe praktyki rynkowe, system ochrony konsumenta (Rzecznik Finansowy, Rzecznik Konsumentów). Cyberbezpieczeństwo obejmuje rozpoznawanie phishingu, bezpieczne zachowanie online i ochronę danych. Gra jest całkowicie bezpłatna, dostępna na platformie itch.io (wersja desktopowa) i w Google Play Store (aplikacja mobilna). Materiały dodatkowe (broszury, przewodniki dla nauczycieli) dostępne są na prawo–konsumenckie.pl i dystrybuowane przez kuratoria oświaty.

Link: https://innowacje.newseria.pl/biuro-prasowe/edukacja/haki-na-cyberataki-,b651569786

Gra planszowa „Za tydzień impreza!" jako offline'owa edukacja finansowa w bankach spółdzielczych

„Za tydzień impreza!" to fizyczna gra planszowa stworzona w ramach programu TalentowiSKO organizowanego przez Bank Polskiej Spółdzielczości (BPS) i Banki Spółdzielcze z Grupy BPS. Ilustracje wykonała nagradzana polska ilustratorka Ola Woldańska–Płocińska.Gra dostępna jest w dwóch wersjach: szkolnej „3w1" (dla klas, umożliwiającej jednoczesną grę 4 dwuosobowych drużyn, z dużą planszą dla całej klasy) oraz domowej (dla 4–8 graczy). Kierowana jest do dzieci od 9 lat i uczestników programu TalentowiSKO (300 szkół zarejestrowanych w XIII edycji). Tematyka polega na tym, że gracze stają się organizatorami koncertu, planując wydarzenie od koncepcji do realizacji. Elementy rozgrywki obejmują zarządzanie budżetem (gracze otrzymują „talenty" jako walutę), planowanie strategiczne (wybór elementów sceny, atrakcji, strategii promocji), decyzje finansowe (zaciąganie kredytów lub otwieranie lokat), pracę zespołową (gracze pracują w parach) i elementy losowe (karty wprowadzające sytuacje jak w życiu). Komponenty gry (wersja szkolna) obejmują wiele pionków, „talen-

ty", ponad 500 kart (tajne informacje, zakupy, losy, praca, sponsoring banku spółdzielczego) i planszę w dużym formacie. Edukacja finansowa obejmuje tworzenie i zarządzanie budżetem, różnicę między wydawaniem a oszczędzaniem, podstawy kredytów, koncepcje lokat/oszczędności, śledzenie przychodów i wydatków oraz planowanie finansowe wydarzeń. Wartości bankowości spółdzielczej (odpowiedzialność, współdziałanie, troska o lokalną społeczność) są integralną częścią gry. Gra celowo jest offline'owa jako „odpowiedź na dominację ekranów" – 86% uczniów szkół podstawowych codziennie używa smartfonów (badania Narodowego Programu Zdrowia 2023).

Link: https://www.bankbps.pl/biuroprasowe/komunikaty-prasowe/edukacyjna-gra-planszowa-od-bankow-spoldzielczych-z-grupy-bps

Misja Edukacja BNP Paribas jako wieloformatowy program edukacyjny

Misja Edukacja z Strefą Dziecka, uruchomiona przez BNP Paribas Bank Polska w 2020 roku przy wsparciu Fundacji BNP Paribas, obejmuje podprogramy: Misja Samodzielność, Misja Kieszonkowe i Misja Oszczędzanie. Program kierowany jest do dzieci w wieku 6–13 lat (posiadaczy kont 7–13 lat), a także uczniów klas I–VIII oraz rodziców i nauczycieli. Format łączy gry interaktywne online, quizy (wyzwania rodzinne), grę planszową (offline), animacje wideo i platformę edukacyjną z misjami. Gra online „Misja Samodzielność" oferuje trzy poziomy misji: „Pieniądze od podszewki", „Bezpieczeństwo" i „Zarządzam budżetem", prowadzone przez postacie Benii, Benka i Kaczki Podpowiadaczki. Quiz „Podejmij Wyzwanie" to format rodzinny z porównaniem wyników z rodziną i przyjaciółmi. „Słowniczek Bankosłówek" to interaktywny słownik terminów finansowych dla dzieci. Edukacja obejmuje funkcjonowanie banku, bezpieczeństwo PIN–u i karty, zarządzanie budżetem, rozróżnianie potrzeb i zachcianek, nawyki oszczędnościowe, zarządzanie kieszonkowym i bezpieczną bankowość online. Dla szkół dostępne są scenariusze lekcji zgodne z podstawą programową dla klas I–VIII, dwie ścieżki edukacyjne (Misja Kieszonkowe i Misja Oszczędzanie), konkursy plastyczne z Grand Prix 5000 zł oraz certyfikaty Fundacji BNP Paribas. Program dociera do ponad 99 000 uczniów z około 3000 szkół i jest powiązany z produktami bankowymi: Konto Samodzielniaka, Karta Samodzielniaka i Mikrokarta z opaską płatniczą.

Link: https://lp.bnpparibas.pl/misjaedukacja/

ING gra edukacyjna jako metawersowa przestrzeń edukacji finansowej

ING Bank Śląski oferuje dwie główne inicjatywy grywalizacyjne: „Miasto ING" na platformie Roblox (uruchomione w 2022 roku, pierwsza polska bankowa obecność na Robloxie, 4 sezony wydane do 2024) oraz „Porozmawiajmy o pieniądzach" – offline'ową grę/wyzwanie 7–dniowe dla rodzin. „Miasto ING" to gra multiplayer na platformie Roblox kierowana do dzieci 7–17 lat. Gracze zarabiają punkty poprzez różne prace: zbieranie śmieci, wyprowadzanie psów, mycie okien, mycie aut, serwowanie posiłków. Punkty można wymieniać na wirtualne narzędzia (szybsze zarabianie), ubrania i akcesoria oraz dekoracje. W grze znajduje się wirtualny oddział banku, tryb multiplayer (dodany w lutym 2023) i wydarzenia specjalne (koncert Paliona – 55 000 wirtualnych uczestników, „Bitwa na rymy" z Edzio i Fusialką). Moduł cyberbezpieczeństwa „Akademia Cyberbezpieczeństwa" obejmuje: zhakowane wydarzenie koncertowe uczące cyberświadomości, szkolenie z tworzenia bezpiecznych haseł, rozpoznawanie niebezpiecznych stron, ochronę danych osobowych i edukację antyphishingową. Nowsze sezony uczą również rozpoznawania deepfake'ów. „Porozmawiajmy o pieniądzach" to 7–dniowe progresywne wyzwanie dla rodzin z codziennymi tematami i zadaniami: koncepcja pieniądza, zarabianie, potrzeby vs. zachcianki, oszczędzanie, pożyczanie, planowanie budżetu. Materiały do wydruku dostępne są bezpłatnie na stronie ING.

Badania ING wśród dzieci 7–17 lat wykazały rosnącą niepewność dotyczącą bezpieczeństwa online, 10% dzieci nie wyklucza możliwości kradzieży prawdziwych pieniędzy online, 6% starszych nastolatków (13–17) potwierdziło incydenty kradzieży (wzrost z 2% w 2023), 20% obu grup wiekowych zostało nakłonionych do kliknięcia podejrzanych linków, a ponad 50% dzieci chce dowiedzieć się więcej o bezpiecznym korzystaniu z internetu.

Link: https://www.ing.pl/wiem/bankowosc-codzienna/edukacja-finansowa-dla-dzieci-gra

2.2.4. Ekosystemy wiedzy – rola fundacji, organizacji pozarządowych i sektora bankowego w ekosystemie edukacji finansowej

Analiza inicjatyw edukacji finansowej w Polsce ujawnia wielopoziomowy i sieciowy ekosystem współpracy pomiędzy instytucjami publicznymi, sek-

torem bankowym oraz organizacjami trzeciego sektora. W strukturze tej banki funkcjonują nie tylko jako sponsorzy i patroni przedsięwzięć edukacyjnych, lecz coraz częściej jako inicjatorzy, projektanci oraz operatorzy długofalowych, kompleksowych programów edukacyjnych o charakterze systemowym. Model ten sprzyja trwałości działań edukacyjnych oraz ich integracji z realnymi wyzwaniami rynku finansowego i środowiska cyfrowego.

Koordynacja instytucjonalna i strategiczna

a. Ministerstwo Finansów uczestniczy w kształtowaniu ram instytucjonalnych i strategicznych edukacji finansowej, pełniąc funkcję wspierającą na poziomie polityk publicznych oraz sprzyjając koordynacji działań realizowanych przez podmioty sektora publicznego i finansowego.

b. Rada Edukacji Finansowej jest organem działającym przy ministrze właściwym do spraw instytucji finansowych. W jej skład wchodzą przedstawiciele instytucji publicznych realizujących zadania na rzecz prawidłowego i efektywnego funkcjonowania rynku finansowego. Rada pełni funkcję opiniodawczo-doradczą, w tym monitoruje działania podejmowane w obszarze powszechnej edukacji finansowej oraz wspiera rozwój spójnych i skutecznych rozwiązań edukacyjnych, ukierunkowanych na wzmacnianie ochrony konsumentów i stabilności rynku finansowego.

c. Krajowe Centrum Edukacji Ekonomicznej stanowi instytucjonalne zaplecze współpracy międzysektorowej w obszarze edukacji ekonomicznej i finansowej, powołane w celu zapewnienia trwałości oraz koordynacji inicjatyw realizowanych w ramach Roku Edukacji Ekonomicznej 2024. Centrum pełni funkcję platformy integrującej działania instytucji publicznych, sektora finansowego, organizacji pozarządowych oraz środowisk eksperckich, wspierając wymianę wiedzy, dobrych praktyk oraz rozwój spójnych standardów edukacyjnych. Jego działalność sprzyja systemowemu podejściu do edukacji finansowej, wzmacniając ciągłość działań oraz ograniczając ich fragmentaryzację po zakończeniu inicjatyw o charakterze czasowym.

d. Narodowy Bank Polski pełni rolę patrona honorowego licznych inicjatyw edukacyjnych oraz finansuje programy z zakresu edukacji ekonomicznej i finansowej poprzez system grantowy. Działania te wzmacniają instytucjonalne zaplecze edukacji finansowej oraz przyczyniają się do upowszechniania wiedzy ekonomicznej wśród różnych grup odbiorców.

e. Rzecznik Finansowy prowadzi działalność edukacyjną w obszarze ochrony praw konsumentów na rynku finansowym, przygotowując materiały informacyjne, raporty oraz kampanie edukacyjne dotyczące m.in. kredytów, ubezpieczeń oraz sporów z instytucjami finansowymi. Działania te wzmacniają kompetencje konsumentów w zakresie świadomego i bezpiecznego korzystania z usług finansowych.

f. Fundacja Warszawski Instytut Bankowości pełniąca funkcję krajowego koordynatora, odgrywa centralną rolę w organizowaniu i integrowaniu działań z zakresu edukacji finansowej. Fundacja realizuje projekty o zasięgu ogólnopolskim i międzynarodowym, stanowiąc platformę współpracy sektora bankowego, administracji publicznej oraz środowisk edukacyjnych.

Koordynacja infrastrukturalna

Instytucje płatnicze oraz operatorzy systemów płatności, we współpracy z zespołami reagowania na incydenty bezpieczeństwa komputerowego (CERT), pełnią istotną funkcję informacyjną i prewencyjną, dostarczając wiedzy o aktualnych zagrożeniach, mechanizmach oszustw oraz zasadach bezpiecznego korzystania z usług płatniczych. Integracja działań edukacyjnych prowadzonych przez te podmioty z inicjatywami banków, organizacji pozarządowych i instytucji publicznych wzmacnia odporność użytkowników na zagrożenia w środowisku finansów cyfrowych oraz sprzyja budowaniu spójnego systemu edukacji opartego na aktualnych i praktycznych doświadczeniach operacyjnych.

Koordynacja instytucji tworzących system bankowy

Banki komercyjne

Analiza wskazuje na wysokie zaangażowanie banków komercyjnych w projektowanie i realizację kompleksowych programów edukacyjnych, często o cha-

rakterze innowacyjnym i wielokanałowym. Działania te są w dużej mierze prowadzone za pośrednictwem fundacji powoływanych przez banki (przykłady inicjatyw przedstawiono we wcześniejszej części raportu). Taki model organizacyjny sprzyja długofalowemu charakterowi projektów edukacyjnych, zwiększa ich wiarygodność oraz umożliwia oddzielenie funkcji edukacyjnych od bieżącej działalności komercyjnej instytucji finansowych.

Banki spółdzielcze

Sektor banków spółdzielczych realizuje specyficzną misję edukacyjną, silnie zakorzenioną w społecznościach lokalnych. Działania te obejmują m.in. program TalentowiSKO (XIII edycja, 300 zarejestrowanych szkół), grę planszową „Za tydzień impreza!" promującą wartości spółdzielcze, aplikację Nasz Bank Junior z integracją Szkolnych Kas Oszczędności, a także konkursy „Spółdzielnia dobrych serc" oraz „Inkubator szkolnych biznesów". Inicjatywy te łączą edukację finansową z budowaniem postaw obywatelskich i przedsiębiorczych na poziomie lokalnym.

Koordynacja środowiskowa

a. Biuro Informacji Kredytowej poprzez platformę Score Hunter, realizuje działania edukacyjne w zakresie zdolności kredytowej, ochrony tożsamości oraz bezpiecznego korzystania z danych finansowych, angażując ponad 300 instytucji edukacyjnych w skali kraju.

b. Polskie Towarzystwo Ekonomiczne od 1987 roku organizuje Olimpiadę Wiedzy Ekonomicznej, w której wzięło udział ponad 340 tys. uczestników. Laureaci konkursu reprezentują Polskę w Międzynarodowej Olimpiadzie Ekonomicznej, co podkreśla znaczenie tej inicjatywy w rozwoju kompetencji ekonomicznych młodzieży.

c. Stowarzyszenie Krzewienia Edukacji Finansowej (SKEF) od 2006 roku organizuje Mistrzostwa Polski Młodych Ekonomistów, które w 19 edycjach zgromadziły ponad 12 tys. uczestników, wspierając rozwój wiedzy ekonomicznej oraz umiejętności analitycznych wśród uczniów.

d. Fundacja Młodzieżowej Przedsiębiorczości od lat realizuje programy edukacyjne z zakresu przedsiębiorczości, ekonomii oraz kompetencji cyfrowych młodzieży.

e. Fundacja Empiria i Wiedza realizuje działania na rzecz rozwoju kapitału społecznego i edukacji, ze szczególnym uwzględnieniem równego dostępu do wiedzy i nowoczesnych kompetencji.

Zarysowany ekosystem pokazuje, że edukacja finansowa w Polsce ma charakter rozproszony, lecz jednocześnie komplementarny. Łączy działania strategiczne, środowiskowe i lokalne w spójną strukturę, która wzmacnia odporność użytkowników na zagrożenia występujące w środowisku finansów cyfrowych. Taki model współdziałania sprzyja redukcji luk edukacyjnych, ogranicza dublowanie inicjatyw oraz umożliwia skalowanie skutecznych rozwiązań edukacyjnych, w szczególności w obszarze bezpieczeństwa płatności cyfrowych.

2.3. Nowe horyzonty – przyszłość edukacji cyfrowej

2.3.1. Sztuczna inteligencja i personalizacja treści edukacyjnych

Sztuczna inteligencja (AI) odgrywa coraz istotniejszą rolę w kształtowaniu nowoczesnych form edukacji finansowej i cyfrowej, w tym edukacji dotyczącej bezpiecznego korzystania z usług płatniczych. Jej zastosowanie umożliwia odejście od jednolitych, masowych przekazów informacyjnych na rzecz spersonalizowanych i adaptacyjnych procesów uczenia się, dostosowanych do indywidualnych potrzeb użytkowników, ich poziomu wiedzy, wzorców zachowań oraz profilu ryzyka (Sekścińska, 2024). W tym ujęciu AI przestaje być wyłącznie narzędziem technologicznym, a staje się integralnym elementem środowiska edukacyjnego, współtworzącym proces budowania kompetencji finansowych w sposób ciągły, kontekstowy i osadzony w realnych praktykach użytkowników. Jednocześnie ta sama technologia jest coraz częściej wykorzystywana przez cyberprzestępców, co nadaje jej roli w edukacji charakter ambiwalentny – z jednej strony wzmacniający bezpieczeństwo, z drugiej zaś potencjalnie destabilizujący ekosystem informacyjny (Lakshmi, 2024). Skuteczne wdrożenie rozwiązań opartych na AI wymaga zatem nie tylko wykorzystania ich potencjału dydaktycznego, lecz również identyfikacji oraz ograniczania ryzyk systemowych i poznawczych, jakie mogą się z nimi wiązać.

Z perspektywy pozytywnej, sztuczna inteligencja znacząco zwiększa skuteczność działań edukacyjnych poprzez możliwość precyzyjnej personalizacji treści, formatu oraz momentu przekazu (PARP. Grupa PFR, System Rad ds. Kompetencji, 2023). Algorytmy uczenia maszynowego umożliwiają analizę danych dotyczących sposobu korzystania z bankowości elektronicznej, reakcji użytkowników na komunikaty bezpieczeństwa oraz częstotliwości popełnianych błędów operacyjnych. Na tej podstawie możliwe staje się projektowanie indywidualnych ścieżek edukacyjnych, obejmujących m.in. kontekstowe ostrzeżenia w aplikacjach bankowych, spersonalizowane materiały informacyjne, quizy dostosowane do poziomu wiedzy użytkownika, a także symulacje scenariuszy oszustw najbardziej prawdopodobnych z punktu widzenia jego profilu ryzyka. Takie podejście wpisuje się w koncepcję uczenia się przez doświadczenie i znacząco zwiększa efektywność edukacji, gdyż przekaz edukacyjny pojawia się w bezpośrednim związku z realnym działaniem użytkownika, a nie jako informacja oderwana od praktyki.

Sztuczna inteligencja wspiera edukację finansową również poprzez automatyzację i wysoką skalowalność procesów dydaktycznych. Chatboty, wirtualni asystenci oraz systemy rekomendacyjne mogą pełnić funkcję swoistych „cyfrowych tutorów", odpowiadając na pytania użytkowników, wyjaśniając mechanizmy bezpieczeństwa płatności, przypominając o zasadach higieny cyfrowej oraz sygnalizując potencjalne ryzyka w czasie rzeczywistym. W odróżnieniu od tradycyjnych form edukacji rozwiązania te cechują się ciągłą dostępnością, możliwością natychmiastowej aktualizacji oraz osadzeniem w bieżącym kontekście działania użytkownika. W literaturze przedmiotu podkreśla się, że tego typu mikrointerwencje sprzyjają utrwalaniu bezpiecznych nawyków i mogą realnie ograniczać podatność na ataki socjotechniczne. Jednocześnie rozwój AI generuje nowe, jakościowo odmienne wyzwania dla edukacji finansowej, wynikające z jej coraz szerszego wykorzystania po stronie sprawców cyberprzestępstw.

Te same mechanizmy personalizacji i automatyzacji, które mogą wspierać proces uczenia się, są bowiem wykorzystywane przez cyberprzestępców do tworzenia wysoce przekonujących kampanii phishingowych, smishingowych czy vishingowych. Generatywne modele AI umożliwiają tworzenie spersonalizowanych komunikatów podszywających się pod instytucje finansowe, a także realistycznych deepfake'ów głosu i obrazu, które znacząco utrudniają ich rozpoznanie przez użytkowników. W rezultacie tradycyjne metody edukacji, oparte na identyfikowaniu schematycznych sygnałów ostrzegawczych, mogą okazać się niewystarczające. Zjawisko to wymusza nie tylko aktualizację treści edukacyjnych, lecz także zmianę samych strategii dydaktycznych, przesuwając akcent z prostego rozpoznawania zagrożeń na rozwijanie kompetencji krytycznego myślenia i refleksyjnej oceny sytuacji. Dodatkowym wyzwaniem jest ryzyko powstania fałszywego poczucia bezpieczeństwa. Użytkownicy, ufający zaawansowanym systemom opartym na AI, mogą zakładać, że technologia w pełni zabezpiecza ich interesy i nie wymaga aktywnego zaangażowania z ich strony. Tymczasem znaczna część oszustw finansowych, zwłaszcza tych opartych na manipulacji psychologicznej, wynika z decyzji podejmowanych przez samych użytkowników, a nie z luk technologicznych. Brak zrozumienia zasad działania oraz ograniczeń systemów opartych na AI może prowadzić do obniżenia czujności i wzrostu podatności na nadużycia. Z perspektywy edukacyjnej oznacza to konieczność konsekwentnego akcentowania roli użytkownika jako aktywnego uczestnika procesu bezpieczeństwa, a nie jedynie biernego beneficjenta ochrony technologicznej.

W tym kontekście kluczowe znaczenie ma nie tylko wdrażanie rozwiązań edukacyjnych opartych na AI, lecz także kształcenie użytkowników w zakresie zrozumienia zasad funkcjonowania tych technologii. Edukacja powinna obejmować m.in. świadomość istnienia mechanizmów personalizacji, umiejętność rozpoznawania manipulacji generowanych przez AI (np. deepfake'ów), krytyczną ocenę źródeł informacji oraz refleksję nad zakresem odpowiedzialności w warunkach zautomatyzowanej ochrony. Zagadnienie to nabiera szczególnego znaczenia w kontekście obowiązujących i projektowanych regulacji prawnych (Koźmiński (red.), 2024), w których coraz silniej akcentowana jest zasada przejrzystości oraz prawo użytkownika do rozumienia podstaw podejmowanych wobec niego decyzji. W sytuacji, gdy AI pełni rolę pośrednika w edukacji, rekomendacji czy ostrzeganiu przed ryzykiem, niezbędne staje się przeciwdziałanie asymetrii informacyjnej i wzmacnianie podmiotowości użytkownika.

Sztuczna inteligencja stanowi jeden z kluczowych kierunków rozwoju edukacji cyfrowej i finansowej, oferując narzędzia o wysokim potencjale efektywności, skalowalności i kontekstowości. Jej wdrożenie powinno jednak iść w parze z rozwojem świadomości poznawczej użytkowników oraz budowaniem

kompetencji krytycznych. W tym sensie edukacja wspierana przez AI nie może być traktowana jako mechanizm zastępujący czujność użytkownika, lecz jako cyfrowa tarcza ochronna – skuteczna wyłącznie wówczas, gdy opiera się na aktywnym, świadomym i refleksyjnym uczestnictwie w procesie uczenia się i bezpieczeństwa.

2.3.2. Biometria jako narzędzie edukacyjne

Biometria coraz częściej postrzegana jest nie tylko jako element technologicznego zabezpieczenia dostępu do usług finansowych, lecz także jako praktyczne narzędzie edukacyjne, które w sposób intuicyjny kształtuje świadomość użytkowników w zakresie cyberbezpieczeństwa (Jain i in. 2025). W kontekście usług płatniczych biometria – obejmująca m.in. rozpoznawanie odcisku palca, geometrii twarzy, głosu czy cech behawioralnych – pełni podwójną rolę: z jednej strony wzmacnia poziom ochrony transakcji, z drugiej zaś uczy klientów nowego podejścia do bezpieczeństwa, opartego na unikalności cech osobistych oraz odpowiedzialnym zarządzaniu własną tożsamością cyfrową.

Z perspektywy edukacji cyberbezpieczeństwa i finansów połączenie tych dwóch obszarów ma szczególne znaczenie, ponieważ technologie uwierzytelniania biometrycznego wpływają bezpośrednio na zachowania użytkowników oraz sposób postrzegania ryzyka. Nowoczesne systemy biometryczne eliminują konieczność stosowania haseł czy kodów PIN, co ogranicza część tradycyjnych błędów użytkownika, a jednocześnie skłania do refleksji nad istotą identyfikacji cyfrowej i jej znaczeniem dla bezpieczeństwa usług płatniczych. Mechanizmy te realizują zasadę „bezpieczeństwa przez doświadczenie", w której sama interakcja z systemem staje się elementem procesu uczenia się i budowania bezpiecznych nawyków.

Analizy rynku biometrii w bankowości wskazują, że technologie biometryczne stanowią obecnie jeden z kluczowych filarów budowania zaufania cyfrowego oraz ograniczania skali nadużyć finansowych. Ma to również wyraźny wymiar edukacyjny – użytkownik w praktyce doświadcza różnicy pomiędzy statycznym hasłem a dynamicznie weryfikowaną tożsamością. Odejście od tradycyjnych metod uwierzytelniania nie jest zatem wyłącznie innowacją technologiczną, lecz strategiczną koniecznością, która wpływa zarówno na poziom bezpieczeństwa klientów, jak i na konkurencyjność instytucji finansowych (Olczak i in., 2022).

Biometria funkcjonuje dziś na różnych poziomach doświadczenia użytkownika – od logowania i autoryzacji transakcji w aplikacjach mobilnych, po zaawansowane metody pasywnej weryfikacji behawioralnej działające w tle. Rozwiązania te zmniejszają tzw. tarcie użytkownika (ang. friction), czyli liczbę dodatkowych kroków, utrudnień lub czynności, które użytkownik musi wykonać podczas logowania lub autoryzacji operacji, poprawiając tym samym komfort korzystania z usług płatniczych. Jednocześnie wzmacniają świadomość, że bezpieczeństwo nie sprowadza się wyłącznie do pojedynczego aktu logowania, lecz jest procesem ciągłym. W dłuższej perspektywie sprzyja to budowaniu zaufania, lojalności klientów oraz bardziej dojrzałego podejścia do ochrony finansów w środowisku cyfrowym.

Z edukacyjnego punktu widzenia kluczowe znaczenie ma jednak transparentna komunikacja ze strony banków i dostawców usług płatniczych. Użytkownicy powinni rozumieć, jak działa uwierzytelnianie biometryczne, jakie dane są wykorzystywane, jakie korzyści niesie ta technologia, ale także jakie są jej ograniczenia. Brak tej wiedzy może prowadzić do nadmiernego zaufania do technologii lub błędnych założeń co do zakresu odpowiedzialności instytucji finansowych. Włączanie elementów edukacyjnych w proces wdrażania biometrii – poprzez komunikaty kontekstowe w aplikacjach, materiały informacyjne, tutoriale czy krótkie filmy instruktażowe – znacząco podnosi poziom kompetencji cyfrowych i zdolność użytkowników do świadomego reagowania na zagrożenia.

Warto również podkreślić ograniczenia biometrii jako rozwiązania bezpieczeństwa. Choć technologia ta jest skuteczna, nie eliminuje wszystkich rodzajów ryzyka, zwłaszcza w obliczu rozwoju zaawansowanych technik ataku, takich jak próby obejścia systemów uwierzytelniania czy wykorzystanie deepfake'ów biometrycznych. Jak wskazuje Bagłajewski (2024), w przypadku biometrii – szczególnie behawioralnej – istotnym wyzwaniem pozostaje poziom świadomości użytkowników dotyczący zakresu przetwarzania danych oraz potencjalnych konsekwencji dla prywatności. Niedostateczna wiedza w tym obszarze może prowadzić do fałszywego poczucia bezpieczeństwa, które samo w sobie stanowi istotny czynnik ryzyka. Z tego względu biometria powinna być prezentowana jako element wielowarstwowego systemu ochrony, a nie jako rozwiązanie samodzielne.

Biometria jako narzędzie edukacyjne wpisuje się w koncepcję uczenia poprzez doświadczenie, integrując aspekty technologiczne i behawioralne w codziennym korzystaniu z usług płatniczych. Jej rola wykracza poza funkcję zabezpieczającą – stanowi ona także formę nieinwazyjnej edukacji, która uczy użytkowników, jak i dlaczego powinni chronić swoją tożsamość cyfrową oraz rozumieć mechanizmy bezpieczeństwa stosowane w nowoczesnych systemach płatniczych. W połączeniu z odpowiednią komunikacją i systematyczną edukacją biometria może stać się istotnym filarem budowania długofalowej odporności klientów na cyberzagrożenia, spójnie wpisując się w cele całego raportu.

PROGRAM ANALITYCZNO BADAWCZY

Rozdział 3. Rok Edukacji Ekonomicznej 2024 – refleksje i wnioski

Rok Edukacji Ekonomicznej 2024 był pierwszą w Polsce inicjatywą o tak szerokim, kompleksowym charakterze, łączącą działania instytucji publicznych, sektora finansowego, organizacji pozarządowych, środowisk akademickich oraz edukacyjnych. Skala przedsięwzięcia, liczba zaangażowanych podmiotów oraz różnorodność form edukacyjnych sprawiają, że REE 2024 może być traktowany nie tylko jako cykl wydarzeń, lecz jako laboratorium polityki edukacyjnej, dostarczające wniosków o charakterze systemowym – w szczególności w kontekście wyzwań związanych z cyfryzacją finansów i bezpieczeństwem płatności online.

Inicjatywa ta pokazała, że edukacja finansowa w Polsce wymaga podejścia systemowego, długofalowego i silnie osadzonego w realiach cyfrowego ekosystemu finansowego, w którym bezpieczeństwo płatności online staje się jednym z kluczowych obszarów kompetencyjnych użytkowników. Doświadczenia REE 2024 pozwalają jednoznacznie stwierdzić, że skuteczna edukacja finansowa nie może ograniczać się do przekazywania wiedzy ekonomicznej, lecz musi integrować aspekty technologiczne, behawioralne oraz związane z ochroną użytkownika w środowisku cyfrowym.

Dodatkowym potwierdzeniem skali i systemowego charakteru Roku Edukacji Ekonomicznej 2024 jest liczba oraz zasięg inicjatyw zgłoszonych i realizowanych w jego ramach na poziomie regionalnym i lokalnym (KEE, 2024). Zestawienie inicjatyw prowadzonych w poszczególnych województwach pokazuje, że działania edukacyjne objęły wszystkie regiony kraju i były podejmowane przez bardzo zróżnicowane podmioty – od instytucji publicznych i organizacji pozarządowych, przez szkoły i uczelnie, po banki, biblioteki, domy kultury oraz lokalne środowiska eksperckie. Kilkaset zarejestrowanych inicjatyw, obejmujących m.in. lekcje online, warsztaty, konferencje, gry edukacyjne i wydarzenia otwarte, wskazuje na silne zaangażowanie oddolne oraz zdolność adaptowania idei edukacji ekonomicznej do lokalnych potrzeb i uwarunkowań. Taki rozproszony, a jednocześnie spójny model działań sprzyjał dotarciu z przekazem edukacyjnym do szerokiego grona odbiorców oraz wzmocnił widoczność zagadnień związanych z finansami cyfrowymi i bezpieczeństwem płatności online w debacie publicznej.

Doświadczenia zgromadzone w ramach Roku Edukacji Ekonomicznej 2024 pozwoliły również lepiej zrozumieć, w jaki sposób użytkownicy postrzegają bezpieczeństwo w środowisku cyfrowym oraz jakie obszary wymagają szczególnego wzmocnienia edukacyjnego. Analiza tematyki podejmowanej w inicjatywach realizowanych w różnych regionach kraju pokazuje, że zagadnienia związane z cyberbezpieczeństwem, ochroną danych, bezpiecznym korzystaniem z bankowości elektronicznej oraz płatnościami online stanowiły istotny i powracający element działań edukacyjnych. REE 2024 nauczył, że dla wielu odbiorców kluczowym wyzwaniem nie jest brak dostępu do usług finansowych, lecz ograniczona zdolność rozpoznawania zagrożeń, krytycznej oceny komunikatów oraz reagowania w sytuacjach presji charakterystycznych dla oszustw cyfrowych. W konsekwencji doświadczenia Roku Edukacji Ekonomicznej potwierdziły, że bezpieczeństwo płatności online powinno być traktowane nie jako wąski temat techniczny, lecz jako centralny komponent współczesnej edukacji finansowej, wymagający stałego, praktycznego i kontekstowego podejścia.

3.1. Wnioski z działań edukacyjnych

Zakres i różnorodność działań zrealizowanych w ramach Roku Edukacji Ekonomicznej 2024 pozwalają na sformułowanie katalogu obserwacji i wniosków dotyczących stanu edukacji finansowej w Polsce. Obejmują one: poziom i charakter kompetencji finansowych użytkowników, skuteczność form i narzędzi edukacyjnych, znaczenie koordynacji i efektu skali działań oraz rosnącą rolę technologii i bezpieczeństwa cyfrowego w edukacji ekonomicznej.

1. Utrzymująca się rozbieżność między deklarowanymi kompetencjami a realnym przygotowaniem użytkowników

Obserwacje poczynione w trakcie realizacji Roku Edukacji Ekonomicznej 2024 wskazują na rozbieżności pomiędzy wysokim poziomem korzystania z nowoczesnych usług finansowych a rzeczywistym poziomem kompetencji ekonomicznych i cyfrowych użytkowników. Inicjatywy realizowane w ramach REE 2024, podobnie jak wyniki badań empirycznych, wskazują, że powszechność bankowości elektronicznej, aplikacji mobilnych i płatności bezgotówkowych nie idzie w parze z adekwatnym poziomem wiedzy pozwalającej na świadome i bezpieczne funkcjonowanie w cyfrowym ekosystemie finansowym. Szczególnie istotna jest obserwowana w licznych działaniach edukacyjnych tendencja do przeszacowywania własnych kompetencji przez użytkowników. Respondenci często deklarują wyso-

kie poczucie wiedzy i kontroli, mimo jednoczesnej trudności w identyfikowaniu bardziej złożonych schematów oszustw, krytycznej ocenie komunikatów pochodzących z pozornie wiarygodnych źródeł oraz reagowaniu w sytuacjach presji czasowej. Z perspektywy bezpieczeństwa płatności online oznacza to zwiększoną podatność na ataki socjotechniczne, w których kluczową rolę odgrywają emocje, pośpiech oraz autorytet instytucji finansowych. Doświadczenia REE 2024 pokazują zatem, że skuteczna edukacja finansowa powinna w większym stopniu koncentrować się na korygowaniu nadmiernej pewności siebie użytkowników oraz budowaniu realistycznej oceny ryzyka.

2. Wyższa efektywność edukacji osadzonej w praktyce i doświadczeniu użytkownika

Istotnym zjawiskiem ujawnionym w toku działań REE 2024 jest potwierdzenie wyraźnej przewagi działań edukacyjnych osadzonych w praktycznym doświadczeniu użytkownika nad tradycyjnymi, deklaratywnymi formami przekazu. W ramach REE 2024 szczególnie wysokim poziomem zaangażowania charakteryzowały się warsztaty, symulacje, gry edukacyjne oraz inicjatywy bazujące na realistycznych scenariuszach decyzyjnych, odzwierciedlających codzienne sytuacje finansowe uczestników. Tego typu podejście umożliwia nie tylko przyswojenie wiedzy teoretycznej, lecz przede wszystkim rozwój umiejętności rozpoznawania zagrożeń, analizowania kontekstu oraz podejmowania decyzji w warunkach niepewności i presji. W kontekście płatności online edukacja „w działaniu" pozwala lepiej zrozumieć mechanizmy wykorzystywane w phishingu, podszywaniu się pod instytucje finansowe czy manipulowaniu procesem autoryzacji transakcji. Doświadczenia REE 2024 jednoznacznie wskazują, że skuteczność edukacji w obszarze cyberbezpieczeństwa rośnie, gdy punkt wyjścia stanowi realna sytuacja użytkownika, a nie abstrakcyjne ostrzeżenia oderwane od praktyki.

3. Znaczenie koordynacji, skali i spójności przekazu edukacyjnego

Szeroki zakres inicjatyw, obejmujący działania na poziomie centralnym, regionalnym i lokalnym, umożliwił dotarcie z przekazem edukacyjnym do zróżnicowanych grup odbiorców oraz zwiększył widoczność zagadnień związanych z finansami cyfrowymi i bezpieczeństwem płatności online w debacie publicznej. Jednocześnie doświadczenia REE 2024 pokazują, że w obszarze cyberbezpieczeństwa szczególnie istotna jest spójność komunikatów oraz ich powtarzalność. Użytkownicy lepiej przyswajają zasady bezpieczeństwa, gdy są one formułowane w jednolity sposób, niezależnie od kanału przekazu czy podmiotu prowadzącego działania edukacyjne. W kontekście płatności online oznacza to potrzebę konsekwentnego stosowania tych samych definicji zagrożeń, zasad postępowania oraz ścieżek reakcji na incydenty, co zwiększa szanse na ich utrwalenie i praktyczne zastosowanie.

4. Cyberbezpieczeństwo jako centralny komponent współczesnej edukacji finansowej

Z perspektywy funkcjonowania cyfrowego ekosystemu finansowego widoczna jest rosnąca roli cyberbezpieczeństwa jako integralnego elementu edukacji finansowej. W licznych inicjatywach realizowanych w ramach REE 2024 zagadnienia dotyczące zarządzania finansami osobistymi były naturalnie łączone z tematami ochrony danych, tożsamości cyfrowej oraz bezpiecznego korzystania z usług płatniczych. Takie podejście odzwierciedla realia współczesnego ekosystemu finansowego, w którym decyzje ekonomiczne coraz częściej mają bezpośrednie konsekwencje w obszarze bezpieczeństwa cyfrowego. Granica pomiędzy „błędem finansowym" a „incydentem bezpieczeństwa" ulega zatarciu, co sprawia, że edukacja finansowa XXI wieku powinna być projektowana jako edukacja funkcjonowania w środowisku cyfrowym. REE 2024 potwierdził, że bezpieczeństwo płatności online nie jest zagadnieniem technicznym zarezerwowanym dla specjalistów, lecz podstawową kompetencją każdego użytkownika usług finansowych.

3.2. Dobre praktyki i rekomendacje

Doświadczenia Roku Edukacji Ekonomicznej 2024 pozwalają na sformułowanie zestawu dobrych praktyk i rekomendacji istotnych z perspektywy dalszego rozwoju edukacji w obszarze bezpieczeństwa płatności online.

Obszar I: Przejście od edukacji incydentalnej do modelu ciągłego

Rekomendacja: Edukacja w zakresie bezpieczeństwa płatności online powinna mieć charakter procesowy i długofalowy

Jednorazowe kampanie informacyjne, choć istotne z punktu widzenia zasięgu, nie są wystarczające w obliczu dynamicznie zmieniających się zagrożeń w środowisku cyfrowym. Schematy oszustw finansowych ewoluują szybciej niż tradycyjne programy edukacyjne, co powoduje szybkie dezaktualizowanie się przekazywanych treści. Skuteczność działań edukacyjnych wyraźnie wzrasta w sytuacji, gdy edukacja towarzyszy użytkownikowi na różnych etapach korzystania z usług finansowych – od momentu zakładania konta, przez codzienne operacje płatnicze, aż po reagowanie na potencjalne incydenty. Model ciągły umożliwia nie tylko systematyczne aktualizowanie wiedzy, lecz także stopniowe budowanie nawyków ostrożności oraz wzmacnianie czujności użytkowników w dłuższej perspektywie.

Obszar II: Integracja edukacji z momentem podejmowania decyzji

Rekomendacja: Treści edukacyjne powinny być osadzane bezpośrednio w kontekście transakcji i decyzji finansowych

Największą skutecznością charakteryzują się te formy edukacji, które są powiązane z realnymi sytuacjami decyzyjnymi użytkowników. Krótkie komunikaty, ostrzeżenia oraz mechanizmy tzw. „pauzy bezpieczeństwa", pojawiające się bezpośrednio w procesie realizacji transakcji, pozwalają na zwrócenie uwagi użytkownika w momencie podwyższonego ryzyka. Takie rozwiązania są bardziej efektywne niż zewnętrzne materiały informacyjne, ponieważ ograniczają działanie impulsu, presji czasu oraz automatyzmu zachowań, które są często wykorzystywane w oszustwach cyfrowych. Integracja edukacji z momentem podejmowania decyzji sprzyja lepszemu przenoszeniu wiedzy teoretycznej na praktyczne działania ochronne.

Obszar III: Segmentacja działań edukacyjnych

Rekomendacja: Działania edukacyjne powinny być projektowane z uwzględnieniem profilu demograficznego i kompetencyjnego odbiorców

Działania edukacyjne powinny być projektowane z uwzględnieniem profilu demograficznego i kompetencyjnego odbiorców. Użytkownicy różnią się zarówno poziomem kompetencji cyfrowych, jak i sposobem postrzegania zagrożeń oraz preferowanymi formami edukacji. Czynniki takie jak wiek, miejsce zamieszkania czy status zawodowy wpływają na częstotliwość korzystania z płatności online, poziom ekspozycji na zagrożenia oraz gotowość do podejmowania działań prewencyjnych. Projektowanie uniwersalnych kampanii edukacyjnych bez uwzględnienia tych różnic może ograniczać ich skuteczność. Segmentacja działań pozwala na lepsze dopasowanie treści, języka oraz kanałów komunikacji do realnych potrzeb poszczególnych grup użytkowników, co zwiększa szanse na trwałe przyswojenie wiedzy i zmianę zachowań.

Obszar IV: Wzmocnienie roli instytucji z doświadczeniem operacyjnym

Rekomendacja: Warto rozwijać edukację prowadzoną przez podmioty posiadające praktyczną wiedzę o incydentach cyberbezpieczeństwa

Edukacja oparta na rzeczywistych przypadkach i scenariuszach incydentów jest postrzegana przez użytkowników jako bardziej wiarygodna i użyteczna niż przekaz teoretyczny. Banki, instytucje płatnicze oraz podmioty reagowania na incydenty cyberbezpieczeństwa dysponują unikalną wiedzą na temat aktualnych schematów oszustw, metod działania sprawców oraz typowych błędów popełnianych przez użytkowników. Wykorzystanie tej wiedzy w działaniach edukacyjnych pozwala lepiej przygotować użytkowników na realne zagrożenia oraz zwiększa ich zdolność do rozpoznawania i właściwego reagowania na niebezpieczne sytuacje.

Obszar V: Uwzględnienie nowych zagrożeń technologicznych

Rekomendacja: Programy edukacyjne powinny systematycznie uwzględniać zagrożenia związane z AI, deepfake'ami i zaawansowaną socjotechniką

Istotnym kierunkiem dalszych działań edukacyjnych jest systematyczne uwzględnianie nowych i rozwijających się zagrożeń technologicznych, takich jak deepfake'i, wykorzystanie sztucznej inteligencji w oszustwach czy zaawansowane techniki manipulacji. Świadomość tych zagrożeń rośnie, jednak wiedza użytkowników na temat mechanizmów ich działania pozostaje ograniczona. W kontekście płatności online oznacza to konieczność aktualizacji programów edukacyjnych oraz dostosowania ich do szybko zmieniającego się krajobrazu cyberzagrożeń, tak aby użytkownicy byli przygotowani nie tylko na znane, lecz także na nowe formy ryzyka.

Obszar VI: Budowa trwałego ekosystemu edukacji po REE 2024

Rekomendacja: Konieczne jest utrzymanie efektów REE 2024 poprzez stałą koordynację działań po zakończeniu inicjatywy

Dalszy rozwój ekosystemowego modelu edukacji finansowej, opartego na współpracy instytucji publicznych, sektora finansowego, organizacji pozarządowych oraz środowisk akademickich jest kluczowy dla kontynuacji już zaczętej misji edukacyjnej. Tylko skoordynowane i komplementarne działania różnych podmiotów pozwalają na utrzymanie efektu skali, spójności przekazu oraz ciągłości inicjatyw edukacyjnych. W tym kontekście powołanie Krajowego Centrum Edukacji Ekonomicznej stanowi istotny krok w kierunku instytucjonalnego zakotwiczenia działań zapoczątkowanych w ramach REE 2024 oraz zapewnienia ich trwałości, w tym w obszarze bezpieczeństwa usług płatniczych i funkcjonowania użytkowników w cyfrowym ekosystemie finansowym.

Rok Edukacji Ekonomicznej 2024 potwierdził, że skuteczna edukacja finansowa – zwłaszcza w zakresie bezpieczeństwa płatności online – wymaga długofalowego, skoordynowanego podejścia, łączącego wiedzę ekonomiczną, kompetencje cyfrowe oraz świadomość zagrożeń. Wnioski płynące z REE 2024 stanowią solidną podstawę do budowy trwałego systemu edukacji, który wzmacnia nie tylko wiedzę użytkowników, lecz również ich odporność na ryzyka funkcjonowania w cyfrowym ekosystemie finansowym.

PROGRAM ANALITYCZN BADAWCZY

Wnioski i rekomendacje

Dynamiczny rozwój usług płatniczych oraz postępująca cyfryzacja finansów w istotny sposób zmieniają sposób funkcjonowania użytkowników w ekosystemie finansowym. Płatności elektroniczne, bankowość internetowa i mobilna, portfele cyfrowe oraz rozwiązania oparte na automatyzacji i sztucznej inteligencji stały się integralnym elementem codziennych praktyk finansowych zarówno klientów indywidualnych, jak i przedsiębiorstw. Jednocześnie rozwój ten wiąże się z narastającą skalą i złożonością zagrożeń cyberbezpieczeństwa, które coraz częściej koncentrują się nie na infrastrukturze technicznej, lecz na zachowaniach, decyzjach i podatnościach użytkowników końcowych.

Analiza przeprowadzona w ramach niniejszego raportu wskazuje, że współczesne zagrożenia w obszarze usług płatniczych mają charakter wielowymiarowy. Obejmują one zarówno klasyczne formy oszustw oparte na socjotechnice, jak i coraz bardziej zaawansowane techniki wykorzystujące złośliwe oprogramowanie, przejęcia tożsamości, manipulacje procesami autoryzacyjnymi oraz technologie sztucznej inteligencji, w tym deepfake'i. Skala tych zagrożeń, potwierdzona danymi rynkowymi, raportami instytucji krajowych i europejskich oraz wynikami badania własnego, pokazuje, że nawet najbardziej zaawansowane zabezpieczenia techniczne i regulacyjne nie są wystarczające, jeśli nie są wspierane przez odpowiedni poziom świadomości i kompetencji użytkowników.

W tym kontekście edukacja finansowa i cyfrowa jawi się nie jako element uzupełniający system bezpieczeństwa, lecz jako jego kluczowy komponent. Wyniki badania własnego, jak i inne branżowe opracowanie przytaczane w niniejszym raporcie wskazują na rozbieżność pomiędzy deklarowanym poczuciem wiedzy respondentów a skalą ich doświadczeń z próbami oszustw, co potwierdza istnienie luki kompetencyjnej oraz ryzyka iluzji bezpieczeństwa. Użytkownicy intensywnie korzystający z płatności elektronicznych często postrzegają siebie jako osoby dobrze przygotowane do funkcjonowania w środowisku cyfrowym, mimo że regularnie stykają się z zagrożeniami o rosnącym stopniu zaawansowania. Zjawisko to wzmacnia potrzebę projektowania edukacji nie tylko jako transferu informacji, lecz jako procesu kształtowania realistycznej oceny ryzyka oraz umiejętności reagowania w sytuacjach presji i niepewności.

Istotnym elementem raportu była analiza form edukacji finansowej i cyfrowej, zarówno tych powszechnie wykorzystywanych, jak i dopiero rozwijanych. Zestawienie aktualnie stosowanych narzędzi z deklarowanymi oczekiwaniami użytkowników pokazuje wyraźny kierunek zmian – od form statycznych i biernych w stronę krótkich, wizualnych, interaktywnych i osadzonych w realnym kontekście decyzyjnym. Jednocześnie badanie ujawnia, że formy o największym potencjale edukacyjnym, takie jak warsztaty praktyczne, symulacje czy gry edukacyjne, pozostają nadal niedostatecznie rozpowszechnione. Wskazuje to na potrzebę lepszego wykorzystania istniejących narzędzi oraz projektowania nowych rozwiązań odpowiadających zróżnicowanym profilom użytkowników.

W obszarze edukacji ekonomicznej, w tym i tej dotyczącej bezpieczeństwa w płatnościach online istotną rolę odegrał Rok Edukacji Ekonomicznej 2024, który stanowił unikalną w skali kraju inicjatywę integrującą działania instytucji publicznych, sektora finansowego, organizacji pozarządowych oraz środowisk akademickich. Doświadczenia REE 2024 potwierdziły, że skuteczna edukacja finansowa wymaga podejścia systemowego, skoordynowanego i długofalowego. Skala zrealizowanych inicjatyw oraz ich zasięg pokazały, że możliwe jest budowanie wspólnej narracji edukacyjnej, która dociera do różnych grup odbiorców i uwzględnia lokalne uwarunkowania. Jednocześnie REE 2024 uwidocznił, że bezpieczeństwo płatności online powinno być traktowane jako jeden z centralnych obszarów współczesnej edukacji ekonomicznej, a nie jako temat poboczny lub techniczny.

Analiza zagrożeń w cyfrowych usługach płatniczych oraz przegląd inicjatyw edukacyjnych pokazują, że bezpieczeństwo użytkowników zależy nie tylko od poziomu zabezpieczeń technologicznych, lecz także od świadomości i zachowań samych użytkowników. Współczesne oszustwa finansowe coraz częściej wykorzystują mechanizmy socjotechniczne oraz luki w wiedzy użytkowników, dlatego działania edukacyjne stanowią istotny element systemu bezpieczeństwa usług płatniczych. Doświadczenia Roku Edukacji Ekonomicznej 2024 oraz przykłady inicjatyw edukacyjnych przedstawione w niniejszym raporcie wskazują, że skuteczna edukacja w zakresie bezpieczeństwa finansowego powinna łączyć wiedzę ekonomiczną z kompetencjami cyfrowymi oraz praktycznymi umiejętnościami rozpoznawania zagrożeń. W tym kontekście możliwe jest wskazanie kilku kierunków dalszych działań (rekomendacji), które mogą wspierać rozwój edukacji w zakresie cyberbezpieczeństwa usług płatniczych.

Rekomendacja 1. Integracja edukacji finansowej z edukacją w zakresie cyberbezpieczeństwa

Programy edukacyjne dotyczące finansów osobistych powinny w większym stopniu uwzględniać zagadnienia bezpieczeństwa cyfrowego. W praktyce oznacza to łączenie wiedzy ekonomicznej z umiejętnościami rozpoznawania zagrożeń w środowisku cyfrowym, takich jak phishing, smishing czy próby wyłudzeń inwestycyjnych. Integracja tych obszarów jest szczególnie istotna w warunkach rosnącej cyfryzacji usług finansowych, w których użytkownicy coraz częściej samodzielnie zarządzają swoimi finansami za pośrednictwem aplikacji mobilnych i bankowości elektronicznej.

Rekomendacja 2. Rozwijanie praktycznych i interaktywnych form edukacji

Skuteczność działań edukacyjnych w zakresie cyberbezpieczeństwa może być zwiększana poprzez wykorzystanie nowoczesnych form przekazu, takich jak aplikacje mobilne, symulacje prób oszustw, gry edukacyjne czy interaktywne scenariusze sytuacyjne. Formy te pozwalają użytkownikom lepiej zrozumieć mechanizmy działania cyberprzestępców oraz rozwijać praktyczne umiejętności reagowania na potencjalne zagrożenia.

Rekomendacja 3. Wzmocnienie komunikacji instytucji finansowych z klientami

Banki oraz inni dostawcy usług płatniczych powinni rozwijać działania informacyjne dotyczące aktualnych zagrożeń cybernetycznych, wykorzystując do tego kanały komunikacji, z których klienci korzystają najczęściej – w szczególności aplikacje mobilne, bankowość elektroniczną oraz media społecznościowe. Krótkie komunikaty ostrzegawcze, materiały edukacyjne czy powiadomienia o nowych schematach oszustw mogą skutecznie zwiększać świadomość klientów oraz ograniczać ryzyko nadużyć.

Rekomendacja 4. Rozwijanie edukacji w zakresie cyberbezpieczeństwa w sektorze MŚP

Małe i średnie przedsiębiorstwa stanowią szczególnie wrażliwą grupę użytkowników usług finansowych, ponieważ często nie dysponują wyspecjalizowanymi zespołami bezpieczeństwa informatycznego. Dlatego działania edukacyjne skierowane do tej grupy powinny obejmować m.in. zagadnienia związane z ochroną danych finansowych, rozpoznawaniem prób wyłudzeń typu Business Email Compromise czy zasadami bezpiecznego zarządzania dostępem do systemów finansowych przedsiębiorstwa.

Rekomendacja 5. Wzmacnianie współpracy między instytucjami

Skuteczna edukacja w zakresie cyberbezpieczeństwa wymaga współpracy wielu podmiotów, w tym instytucji publicznych, sektora finansowego, organizacji edukacyjnych oraz uczelni. Wspólne inicjatywy informacyjne, kampanie społeczne czy projekty edukacyjne mogą zwiększyć zasięg działań oraz przyczynić się do budowania bardziej spójnego systemu edukacji finansowej i cyfrowej.

Rekomendacja 6. Wspieranie odpowiedzialnych postaw użytkowników usług finansowych

Edukacja w zakresie bezpieczeństwa usług płatniczych powinna koncentrować się nie tylko na przekazywaniu wiedzy, lecz także na kształtowaniu odpowiedzialnych zachowań użytkowników. Obejmuje to m.in. stosowanie silnych metod uwierzytelniania, ostrożność wobec nieznanych komunikatów czy regularne aktualizowanie oprogramowania wykorzystywanego do obsługi finansów.

Rekomendacja 7. Rozwój platform wymiany doświadczeń dotyczących cyberincydentów

Warto rozważyć rozwój platform umożliwiających wymianę doświadczeń dotyczących cyberincydentów w sektorze usług płatniczych, wykraczających poza formalne systemy raportowania incydentów prowadzone przez instytucje takie jak CERT Polska czy CSIRT KNF. Tego typu inicjatywy mogłyby umożliwiać dzielenie się wiedzą o nowych schematach oszustw, dobrych praktykach w zakresie reagowania na incydenty oraz doświadczeniach użytkowników i instytucji finansowych. Platformy takie mogłyby stanowić ważny element ekosystemu edukacyjnego, wspierając szybsze rozpoznawanie zagrożeń oraz budowanie odporności użytkowników usług płatniczych. Jednocześnie funkcjonowanie tego typu narzędzi wymagałoby odpowiedniego nadzoru instytucjonalnego oraz mechanizmów weryfikacji publikowanych informacji, tak aby ograniczyć ryzyko rozpowszechniania niezweryfikowanych treści lub

powielania dezinformacji dotyczącej zagrożeń cybernetycznych.

Przedstawione rekomendacje wskazują, że skuteczna edukacja w zakresie cyberbezpieczeństwa usług płatniczych wymaga jednoczesnego działania na poziomie użytkownika, instytucji finansowych oraz systemu edukacyjnego.

Wnioski płynące z raportu pozwalają jednocześnie sformułować kilka kluczowych zasad, na których powinna opierać się przyszłość edukacji w obszarze usług płatniczych: ciągłość działań edukacyjnych, ich integrację z momentem podejmowania decyzji finansowych, segmentację przekazu oraz uwzględnianie dynamicznie zmieniających się zagrożeń technologicznych. W przyszłości działania edukacyjne w obszarze cyberbezpieczeństwa usług płatniczych powinny być projektowane w sposób bardziej zintegrowany z rzeczywistym kontekstem korzystania z usług finansowych, tak aby edukacja nie była jedynie przekazem informacyjnym, lecz elementem doświadczenia użytkownika w środowisku cyfrowym. Rola banków i instytucji płatniczych wykracza w tym ujęciu poza dostarczanie bezpiecznej infrastruktury – pełnią rolę edukatorów i partnerów w budowaniu odporności na ryzyko cybernetyczne. Jednocześnie doświadczenia REE 2024 pokazują, że skuteczność działań edukacyjnych znacząco wzrasta, gdy są one osadzone w realnych scenariuszach, oparte na praktyce i prowadzone w sposób systematyczny. Skuteczna ochrona użytkowników usług płatniczych wymaga połączenia technologii, regulacji oraz edukacji. Spośród tych elementów edukacja pełni rolę szczególną – jest bowiem czynnikiem, który wzmacnia efektywność pozostałych mechanizmów bezpieczeństwa i umożliwia użytkownikom świadome, odpowiedzialne funkcjonowanie w coraz bardziej złożonym środowisku finansowym.

Wnioski zaprezentowane w niniejszym opracowaniu mogą stanowić punkt odniesienia dla dalszych działań badawczych, edukacyjnych i strategicznych, ukierunkowanych na budowę bezpiecznego i odpornego cyfrowo ekosystemu płatniczego w Polsce.

PROGRAM ANALITYCZN BADAWCZY

Bibliografia

1. Amagir, A., Groot, W., Maassen van den Brink, H., & Wilschut, A. (2018). A review of financial-literacy education programs for children and adolescents. Citizenship, Social and Economics Education, 17(1), 56–80. https://doi.org/10.1177/2047173417719555

2. Bagłajewski, Z. (2024). Biometria behawioralna – naruszenie prywatności czy przyszłość bezpieczeństwa finansowego? Rzecznik Finansowy, https://rf.gov.pl/wp-content/uploads/2024/12/RZECZNIK-FINANSOWY-artykul-Ziemowita-Baglajewskiego_4X4_10.12_PRAWNIK.pdf

3. Batty, M., Collins, J. M., O'Rourke, C., & Odders-White, E. (2020). Experiential financial education: A field study of My Classroom Economy in elementary schools. Economics of Education Review, 78, 102014. https://doi.org/10.1016/j.econedurev.2020.102014

4. Cannistrà, M., De Beckker, K., Agasisti, T., Amagir, A., Põder, K., Vartiak, L., & De Witte, K. (2024). The impact of an online game-based financial education course: Multi-country experimental evidence. Journal of Comparative Economics, 52(4), 825–847. https://doi.org/10.1016/j.jce.2024.08.001

5. CERT Polska, NASK. (2025). Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu. Dostęp https://cert.pl/uploads/docs/Raport_CP_2024.pdf

6. CERT Polska. (2024). Krajobraz bezpieczeństwa polskiego Internetu w 2023 roku: Raport roczny CERT Polska. NASK – Państwowy Instytut Badawczy. https://cert.pl/posts/2024/04/raport-roczny-2023/

7. CSIRT KNF. (2024). Raport roczny CSIRT KNF za 2023 rok. Urząd Komisji Nadzoru Finansowego. https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_roczny_CSIRT_KNF_88762.pdf

8. CSIRT NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2023 roku. NASK – Państwowy Instytut Badawczy. https://csirt.gov.pl/download/3/220/RaportostaniebezpieczenstwacyberprzestrzeniRPw2023.pdf

9. DBIR. (2025). Data Breach Investigations Report. Dostęp https://www.verizon.com/business/resources/reports/dbir/

10. Desai, A., Kosse, A., Sharples, J. (2024). Finding a needle in a haystack: A machine learning framework for anomaly detection in payment systems (BIS Working Papers No. 1188). Bank for International Settlements.

11. DFP. Digital Fingerprints. (2025). Najbezpieczniejsze rozwiązania do ochrony danych, dostępów i zasobów dla firm. Dostęp: https://fingerprints.digital/

12. Dyrektywa 2015/2366, 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 (Tekst mający znaczenie dla EOG)

13. Dz. U. 2011 Nr 199 poz. 1175. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2011, nr 199, poz. 1175. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20111991175/U/D20111175Lj.pdf

14. EBA. European Banking Authority. (2025). Report on payment fraud. EBA.REP.2025/40, December 2025. Dostęp https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf

15. ENISA. (2024). ENISA Threat Landscape 2024, Dostęp: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

16. ENISA. (2025). ENISA Threat Landscape 2025, Dostęp: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf

17. EPC. European Payment Council. (2024). Payment Threats and Fraud Trends Report. EPC162-24/Version 1.0. Dostęp: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf

18. European Parliament & Council of the European Union. (2022a). Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA). Official Journal of the European Union.

19. European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2555 (NIS 2 Directive). Official Journal of the European Union.

20. European Payments Council. (2024). Payment Threats and Fraud Trends. Dostęp: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf

21. European Payments Council. (2024). Payments threats and fraud trends report (Version 1.0, EPC162-24). EPC. https://www.europeanpaymentscouncil.eu/document-library/reports/yearly-update-payment-threats-and-fraud-trends-report-0

22. European Union Agency for Cybersecurity. (2025). ENISA threat landscape: Finance sector. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

23. Iwańczuk-Kaliska, A., Marszałek, P., Schmidt, K., Warchlewska, A., (2021). Ocena zmian na rynku płatności w Polsce, Raport Sygn. WIB PAB 10/2021. https://pabwib.pl/produkt/ocena-zmian-na-rynku-platnosci-w-polsce/

24. Jain, A. K., Ross, A., Nandakumar, K., i Swearingen, T. (2025). Introduction to biometrics (2nd ed.). Springer.

25. Jurek, M., Marszałek, P., Warchlewska, A. (2019). Mapa edukacji finansowej, VI ed., cz. 2, ZBP i PIU.

26. KEFiP. (2024). Poziom wiedzy finansowej Polaków 2024. Edycja VII. https://ree2024.pl/wp-content/uploads/2024/04/ree-2024-kefip-baranie-poziom-wiedzy-finansowej-polakow-2024.03.pdf

27. KNF, CSIRT. (2024). Raport roczny 2024. Dostęp: https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf

28. KNF, CSIRT. (2024b). Dobre praktyki w zakresie zapobiegania i reagowania na ataki typu ransomware. Dostęp: https://www.knf.gov.pl/knf/pl/komponenty/img/Dobre%20praktyki%20w%20zakresie%20zapobiegania%20i%20reagowania%20na%20ataki%20typu%20ransomware.pdf

29. KNF.(2023). Zakres usług płatniczych, https://www.knf.gov.pl/dla_rynku/procesy_licencyjne/platniczy/informacje_ogolne/zakres_uslug_platniczych

30. KNF. (2024). Rynek usług płatniczych. https://www.knf.gov.pl/dla_rynku/stanowiska/uslugi_platnicze

31. Kostro, M., Sterczała, P., Brakoniecki, M., Tabor, M., Rzęsa, D., Żywicki, M., Wolski, M., & Stradowski, K. (2020). Bezpieczeństwo usług opartych o otwarte interfejsy programistyczne (API) w kontekście implementacji Dyrektywy PSD2 [Raport analityczny]. Fundacja Warszawski Instytut Bankowości, Program Analityczno-Badawczy

32. Koźmiński, K. W. (red.). (2025). Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym. Sygn. PAB/WIB 8/2024. Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości. https://pabwib.pl/wp-content/uploads/2024/01/PAB_WIB_Wyzwania_prawne_AI_Kozminski.pdf

33. KPMG. (2024). Barometr cyberbezpieczeństwa. Na fali, czy w labiryncie regulacji? Dostęp: https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2024/02/pl-Raport-KPMG-w-Polsce-Barometr-cyberbezpiecze%C5%84stwa-2024.pdf

34. Król, P. (2024). Phishing jako zagrożenie dla bezpieczeństwa bankowości cyfrowej. Bezpieczny Bank, 94(1), 25–42. https://doi.org/10.26354/bb.2.1.94.2024

35. Lakshmi, Y. (2024). The Impact of Artificial Intelligence on Financial Literacy. ShodhKosh: Journal of Visual and Performing Arts, 5(5), 8–28

36. Lookout. (2021). What you need to know about the banking trojan Anubis. Dostęp: https://www.lookout.com/threat-intelligence/article/anubis-targets-hundreds-of-financial-apps

37. Makowiec, M., Witoszek-Kubicka, A. (red.). (2019). Grywalizacja w edukacji i biznesie. Uniwersytet Ekonomiczny w Krakowie.

38. Ministerstwo Cyfryzacji. (b.d.). Grupa robocza AI. Dostęp: https://ai.gov.pl/aktualnosci

39. NBP. (2020). PayTech – innowacyjne rozwiązania płatnicze na rynku polskim. https://nbp.pl/wp-content/uploads/2022/09/paytech.pdf

40. NBP. (2025). Informacja o kartach płatniczych IV kwartał 2024 r. https://nbp.pl/wp-content/uploads/2026/01/Informacja-o-kartach-platniczych_2025-Q3.pdf

41. Olczak, M., Brakoniecki, M., Wolski, M., Krzyżański, M., i Rzęsa, D. (2022). Biometria w bankowości elektronicznej – Rynek, technologia, klient. SYGN. WIB PAB 8/2022. Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości. https://pabwib.pl/wp-content/uploads/2023/08/PAB_WIB_Biometria-w-bankowosci-elektronicznej_Brakoniecki.pdf

42. PARP. Grupa PFR, System Rad ds. Kompetencji (2023). Rynek pracy, edukacja, kompetencje. Wykorzystanie sztucznej inteligencji w edukacji. Raport. https://www.parp.gov.pl/storage/publications/pdf/Wykorzystanie-sztucznej-inteligencji-w-edukacji.pdf

43. Fundacja Polska Bezgotówkowa. (2026). Raport: Przyszłość płatności jest dziś. Polska liderem Europy, https://api.polskabezgotowkowa.pl/uploads/platnosci_raport_final_79ea6d7120.pdf

44. REE. (2024). Rok Edukacji Ekonomicznej. Historyczne inspiracje dla przyszłości. https://ree2024.pl/woj/

45. Sekścińska, K. (2025). AI w finansach i bankowości oczami polskiego konsumenta. Raport PAB/WIB 7/2025. Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości. https://pabwib.pl/wp-content/uploads/2025/05/PAB_WIB_AI-w-Finansach_Sekscinska.pdf

46. UKNF. (2026). Priorytety nadzorcze UKNF na 2026 rok, file:///C:/Users/user/Downloads/Priorytety_UKNF_2026_96517.pdf

47. Waliszewski, K., Nowakowski, M., & Warchlewska, A. (2024). Nowoczesne metody wspomagania zarządzania finansami osobistymi na przykładzie usługi robo-advice, Sygn. PAB/WIB 10/2024. Program Analityczno-Badawczy przy Fundacji Warszawski Instytut Bankowości https://pabwib.pl/produkt/nowoczesne-metody-wspomagania-zarzadzania-finansami-osobistymi-na-przykladzie-uslugi-robo-advice/

48. WIB, Bezpieczeństwo w cyberprzestrzeni. (2024). Raport Cyberbezpieczny portfel. ZBP. Dostęp: https://www.wib.org.pl/wp-content/uploads/2024/10/raport_Cyberbezpieczny-portfel-2024.pdf

49. ZPF. (2025). Związek Przedsiębiorstw Finansowych w Polsce. Nadużycia w sektorze finansowych. Dostęp https://zpf.pl/naduzycia-w-sektorze-finansowym-2025-nowy-raport-zpf-i-ey/

PROGRAM ANALITYCZN BADAWCZY

Aneks – ankieta

Szanowni Państwo,

niniejsza ankieta jest częścią badania prowadzonego na potrzeby raportu pt.„Edukacja klientów banków w zakresie usług płatniczych z uwzględnieniem kwestii cyberbezpieczeństwa", realizowanego we współpracy z Warszawskim Instytutem Bankowości. Celem badania jest poznanie opinii i doświadczeń różnych grup odbiorców – studentów, osób pracujących, seniorów oraz przedsiębiorców – dotyczących edukacji w zakresie bezpiecznego korzystania z płatności elektronicznych. Zebrane informacje posłużą do opracowania wniosków i rekomendacji dla instytucji finansowych i edukacyjnych. Ankieta jest anonimowa, a jej wypełnienie zajmie ok. 3–5 minut.

1. **Jak często korzystasz z płatności elektronicznych (np. przelewy online, aplikacje mobilne, BLIK)?**
   a. codziennie
   b. kilka razy w tygodniu
   c. kilka razy w miesiącu
   d. rzadziej

2. **Czy kiedykolwiek spotkałeś/aś się z próbą oszustwa związaną z płatnościami elektronicznymi (np. fałszywy e-mail z banku, podejrzany link, nieautoryzowana transakcja)?**
   a. tak, wielokrotnie
   b. tak, raz lub dwa razy
   c. nie
   d. nie wiem / nie mam pewności

3. **Jak oceniasz ogólny poziom edukacji o cyberbezpieczeństwie w Polsce?**
   a. bardzo dobry
   b. raczej dobry
   c. przeciętny
   d. raczej słaby
   e. bardzo słaby

4. **Jak oceniasz swój poziom edukacji o cyberbezpieczeństwie?**
   a. bardzo dobry
   b. raczej dobry
   c. przeciętny
   d. raczej słaby
   e. bardzo słaby

5. **Które z poniższych zjawisk uważasz za największe zagrożenia dla bezpieczeństwa finansowego użytkowników Internetu?**
   (można wybrać kilka odpowiedzi)
   a. Phishing – próby wyłudzenia danych logowania lub danych karty poprzez fałszywe e-maile, SMS-y lub strony internetowe podszywające się pod banki i instytucje.
   b. Deepfake – fałszywe nagrania audio lub wideo, tworzone przy użyciu sztucznej inteligencji, służące do manipulacji lub oszustw (np. podszywanie się pod znaną osobę).
   c. Złośliwe oprogramowanie (malware) – programy infekujące urządzenia w celu kradzieży danych lub pieniędzy.
   d. Ataki na aplikacje mobilne / bankowość online – próby przejęcia kont użytkowników poprzez luki w zabezpieczeniach lub nieświadome instalowanie podejrzanych aplikacji.

e. Oszustwa inwestycyjne / kryptowalutowe – fałszywe oferty inwestycji lub zysków „bez ryzyka".
f. Socjotechnika (manipulacje psychologiczne) – próby nakłonienia ofiary do ujawnienia danych lub dokonania przelewu, np. przez telefon.
g. Nieświadomość użytkowników / brak edukacji – niewiedza o podstawowych zasadach bezpieczeństwa w sieci.
h. Inne (jakie?)

6. Czy czujesz się dobrze poinformowany/a o zagrożeniach związanych z płatnościami w Internecie (np. phishing, fałszywe SMS-y, oszustwa)?
a. tak
b. częściowo
c. nie

7. Z jakich form edukacji o bezpieczeństwie finansowym lub cyfrowym korzystałeś/aś do tej pory?
(można wybrać kilka)
a. artykuły i poradniki online
b. kampanie informacyjne (TV, YouTube, media społecznościowe)
c. szkolenia, webinary lub warsztaty
d. podcasty
e. quizy/testy wiedzy
f. materiały edukacyjne banku (np. newsletter, komunikat w aplikacji)
g. gry, symulacje, escape roomy
h. inne (jakie?) _____

8. Która z tych form była dla Ciebie najbardziej użyteczna?
[lista jak wyżej]

9. Jakie formy edukacji mogłyby w przyszłości najbardziej pomóc Ci w bezpiecznym korzystaniu z płatności cyfrowych?
a. krótkie filmy instruktażowe
b. aplikacje lub gry edukacyjne
c. spotkania i warsztaty praktyczne
d. kampanie w mediach społecznościowych
e. inne: _____

10. Jaką rolę – Twoim zdaniem – powinny odgrywać banki w edukowaniu klientów o cyberbezpieczeństwie?
a. a. prowadzić regularne kampanie edukacyjne
b. b. przesyłać ostrzeżenia i porady w aplikacji bankowej
c. c. organizować szkolenia lub webinary
d. d. współpracować ze szkołami / uczelniami
e. e. inne: _____

11. Jakie jedno działanie lub forma edukacji Twoim zdaniem najbardziej zwiększyłaby bezpieczeństwo finansowe w Internecie?
(odpowiedź otwarta)

Dane statystyczno-demograficzne

Wiek:

- ○ poniżej 18 lat
- ○ 18–25
- ○ 26-30
- ○ 31–44
- ○ 45–59
- ○ 60+

Płeć:

- ○ kobieta
- ○ mężczyzna
- ○ inna / wolę nie podawać

Status zawodowy:

- ○ uczeń / student
- ○ osoba pracująca
- ○ przedsiębiorca
- ○ emeryt / rencista
- ○ osoba nieaktywna zawodowo
- ○ inny (jaki?) _____

Miejsce zamieszkania:

- ○ wieś
- ○ małe miasto (do 50 tys. mieszkańców)
- ○ średnie miasto (50–200 tys.)
- ○ duże miasto (powyżej 200 tys.)

PROGRAM
ANALITYCZNO
BADAWCZY

Raport opracowany na zlecenie
Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości