BIK BIG InfoMonitor DFP Digital Fingerprints

GRUPA BIK

Raport Antyfraudowy BIK 2025

Zagrożenia i Ochrona.

Spis treści

Szanowni Państwo,

Analizy poprzedzające przygotowanie Raportu Antyfraudowego BIK 2025 wskazują, że ciągłe podnoszenie poziomu bezpieczeństwa, budowanie świadomości w zakresie cyberbezpieczeństwa oraz systematyczne informowanie użytkowników o zagrożeniach pozostają niezmiennie priorytetowymi działaniami dla instytucji finansowych. Realizujemy tę misję konsekwentnie m.in. poprzez następujące aktywności:

- W ramach Alertów BIK wdrożyliśmy w tym roku nową funkcjonalność – monitoring darknetu pod kątem ujawnienia danych osobowych,
- Cały czas rozwijamy sektorowe rozwiązania antyfraudowe, dostosowane do potrzeb rynku, z których korzysta coraz większa liczba instytucji finansowych.

Tego rodzaju działania są niezbędne, zwłaszcza w kontekście rosnącej skali zagrożeń – już 47% Polaków zetknęło się z próbą wyłudzenia danych (wzrost o 10 punktów procentowych rok do roku), a niemal co trzeci doświadczył próby zainfekowania komputera lub urządzenia mobilnego. Tymczasem to właśnie smartfony i tablety stały się dla większości użytkowników podstawowym narzędziem kontaktu z bankiem, co czyni je szczególnie narażonymi na cyberataki.

Jak co roku, wierzę, że kolejna edycja Raportu Antyfraudowego będzie istotnym wsparciem w realizacji edukacyjnej misji Grupy BIK. Liczę, że zainspiruje i pomoże instytucjom finansowym w wyznaczaniu strategicznych kierunków działań oraz w kształtowaniu tematyki licznych kampanii społecznych. Zachęcam Państwa do lektury Raportu Antyfraudowego BIK 2025.

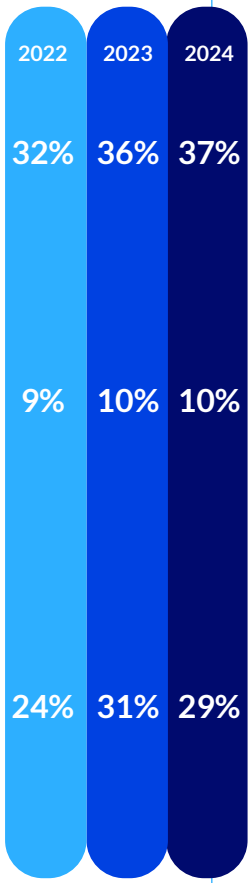
Wspólnie dbajmy o bezpieczeństwo i edukacją klientów instytucji finansowych.

Agnieszka Szopa-Maziukiewicz

Wiceprezes Zarządu BIK S.A.
Prezes Zarządu Digital Fingerprints S.A.

Jak poważne są zagrożenia na rynku finansowym?

Skala zjawiska fraudów



Klienci indywidualni

47%

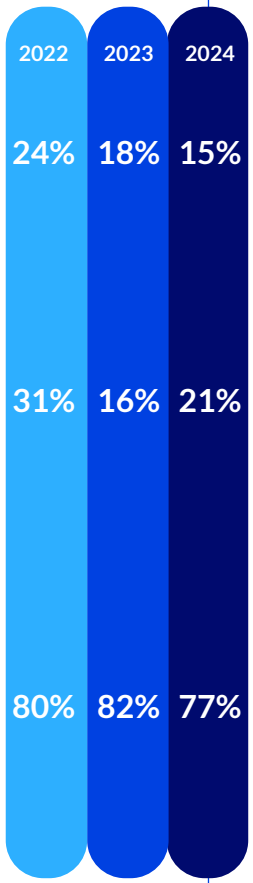
zetknęło się z co najmniej jedną formą wyłudzenia. To najczęściej phishing.

10%

uważa, że wyciek danych nie stanowi powodu do niepokoju.

35%

tych, którzy mieli do czynienia z próbą wyłudzenia „na instytucję publiczną", było proszonych o podanie numeru PESEL.



Małe i średnie przedsiębiorstwa

32%

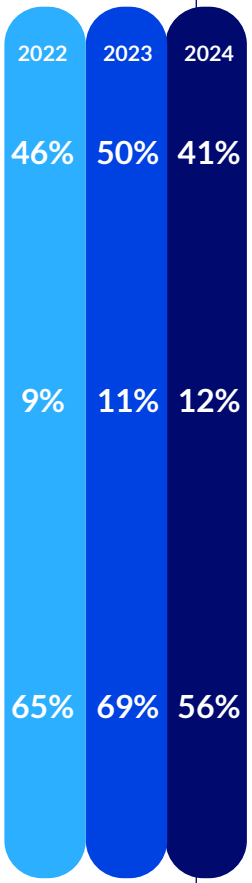
miało w 2024 r. do czynienia ze zdarzeniem fraudowym

35%

w gronie firm, które miały do czynienia z fraudami, doświadczyło próby oszustwa na fałszywe faktury bądź podszywania się pod kontrahentów.

66%

nie korzysta z narzędzi/usług antyfraudowych.



Korporacje

36%

banków uważa, że w 2024 r. liczba zdarzeń fraudowych wzrosła.

12%

korporacji twierdzi, że w ciągu roku w wyniku fraudów poniosły straty większe niż 10 mln zł.

76%

podmiotów wskazuje, że za fraudy najczęściej odpowiadają zorganizowane grupy przestępcze.

Definicja fraudu

By jeszcze lepiej chronić klientów instytucji finansowych, kluczowa jest ciągła edukacja, tłumaczenie pojęć związanych z fraudami i powtarzanie podstawowych zasad bezpieczeństwa.

Zgodnie z raportem Antyfraudowym BIK, liczba prób oszustw w Polsce stale rośnie. Co istotne, przestępcy nie muszą stosować skomplikowanych metod – wystarczy dobrze zaplanowana manipulacja.

Dlatego tak ważne jest, by klienci instytucji finansowych czuli się bezpieczni – dzięki edukacji, prostym zasadom i jasnym komunikatom.

Najczęstsze metody oszustw wobec klientów indywidualnych – definicje

Współczesne oszustwa finansowe przybierają różnorodne formy i coraz częściej opierają się na manipulacji emocjonalnej, socjotechnice oraz wykorzystaniu nowych technologii. Poniżej przedstawiamy pięć najczęściej zgłaszanych typów ataków, z którymi spotykają się klienci indywidualni:

Phishing - Phishing to metoda oszustwa polegająca na podszywaniu się pod zaufane instytucje (np. banki, firmy kurierskie, urzędy) w celu wyłudzenia danych logowania, informacji osobistych lub danych kart płatniczych. Atak odbywa się zazwyczaj za pośrednictwem fałszywych e-maili, SMS-ów lub stron internetowych.

Cel: Przejęcie danych umożliwiających dostęp do konta bankowego lub innych usług finansowych.

Wyłudzenia „na BLIK-a" / „na znajomego z Facebooka" - Ten typ oszustwa polega na przejęciu konta w mediach społecznościowych i podszywaniu się pod znajomego ofiary. Oszust prosi o pilną pomoc finansową – najczęściej w formie kodu BLIK – tłumacząc to nagłą sytuacją.

Cel: Szybkie uzyskanie środków finansowych bez konieczności włamywania się na konto bankowe.

Vishing / Spoofing - Vishing to oszustwo telefoniczne, w którym przestępca podszywa się pod pracownika banku, policjanta lub innego urzędnika. Spoofing polega na fałszowaniu numeru telefonu, by wyglądał na autentyczny. Oszuści często informują o rzekomym zagrożeniu i nakłaniają do podania danych lub wykonania przelewu.

Cel: Wyłudzenie danych logowania, kodów autoryzacyjnych lub bezpośrednie przejęcie środków.

Fałszywe sklepy internetowe - Oszuści tworzą profesjonalnie wyglądające strony internetowe, oferujące atrakcyjne produkty w niskich cenach. Po dokonaniu płatności klient nie otrzymuje zamówienia, a kontakt ze „sklepem" się urywa.

Cel: Wyłudzenie pieniędzy oraz – w niektórych przypadkach – danych osobowych i płatniczych.

Oszustwa „na wnuczka" / „na policjanta" - To klasyczne oszustwa telefoniczne, w których przestępcy podszywają się pod członka rodziny (np. wnuczka) lub funkcjonariusza policji. Wykorzystując stres i presję czasu, nakłaniają ofiarę – najczęściej osobę starszą – do przekazania gotówki lub kosztowności.

Cel: Bezpośrednie wyłudzenie pieniędzy w gotówce lub przelewem.

Klienci indywidualni

Skala zagrożenia fraudami

Wyraźny wzrost skali wyłudzeń wśród Polaków: Odsetek Polaków, którzy mieli styczność z co najmniej jedną formą wyłudzenia wzrósł o 10 pp. względem ubiegłego roku.

47% klientów instytucji finansowych deklaruje, że zetknęło się z problemem wyłudzeń. To o 10 pp. więcej niż w 2024 r. oraz o 11 pp. niż w 2023 r.

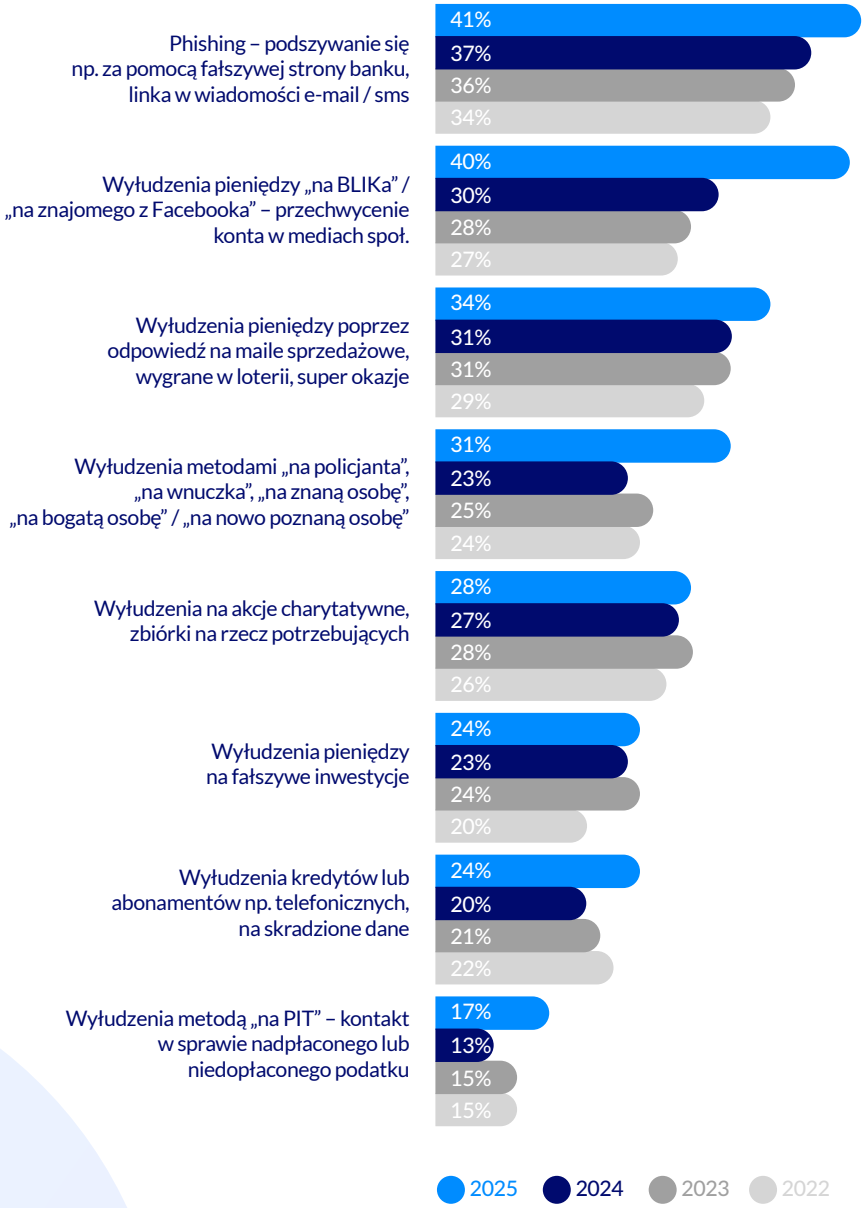
Najczęściej zgłaszane incydenty dotyczą phishingu – 41% respondentów potwierdza kontakt z tego typu oszustwem, co stanowi wzrost o 4 pp. rok do roku. Równie alarmujące są dane dotyczące wyłudzeń kodów BLIK oraz przejęć kont w mediach społecznościowych – oba typy zagrożeń wskazało 40% badanych, czyli **o 10 pp. więcej niż rok wcześniej.**

Szczególną uwagę zwraca rosnąca liczba prób wyłudzeń za pośrednictwem **urządzeń mobilnych**. 40% ankietowanych wskazuje na oszustwa SMS-owe, a 22% – na próby kontaktu przez komunikatory internetowe, takie jak Messenger czy WhatsApp.

35%

35% Polaków, którzy mieli styczność z osobą podszywającą się pod przedstawiciela instytucji publicznej, zostało poproszonych o podanie numeru PESEL. To jeden z najczęstszych sposobów pozyskiwania osobowych danych przez oszustów. Coraz częściej przestępcy próbują również nakłonić ofiary do wykonania przelewu – takiej próby doświadczyło 26% badanych – lub do potwierdzenia nieznanej transakcji (23%).

Skala styczności z próbami wyłudzeń



Klienci indywidualni

Najskuteczniejsze ataki 2025

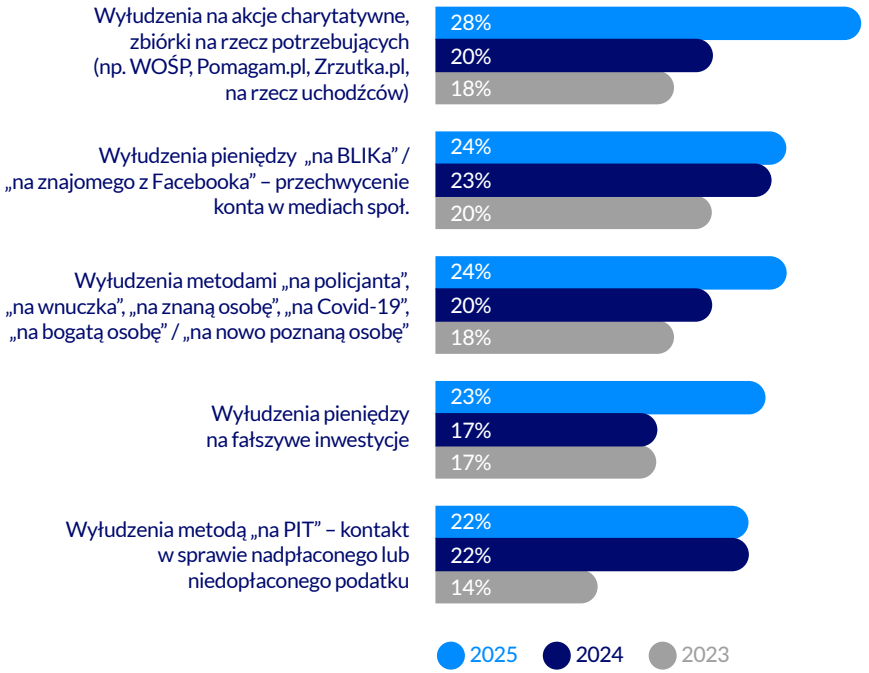
Dużym problemem na polskim rynku wciąż pozostają wyłudzenia na oszukańcze zbiórki charytatywne.

W 2025 roku wyłudzenia związane z fałszywymi zbiórkami charytatywnymi okazały się najbardziej skuteczną metodą oszustwa. 28% osób, które zetknęły się z tego typu próbą, poniosło straty finansowe. To wzrost o 8 pp. w porównaniu z rokiem poprzednim, co pokazuje, że przestępcy coraz lepiej wykorzystują emocje i zaufanie społeczne.

Na wysokim poziomie utrzymuje się również skuteczność innych form wyłudzeń. Przejęcia kont w mediach społecznościowych oraz oszustwa związane z kodami płatniczymi dotknęły 24% badanych. Co prawda jest to niewielki wzrost, o 1 pp., ale warto zwrócić uwagę na fakt, że te formy wyłudzenia zajmują niezmiennie wysokie miejsca. Z kolei metody socjotechniczne, polegające na podszywaniu się pod członka rodziny lub przedstawiciela instytucji publicznej również osiągnęły poziom 24%, co oznacza wzrost o 4 pp. r/r.

Warto zwrócić uwagę, że rośnie także skuteczność oszustw inwestycyjnych – 22% osób, które miały z nimi kontakt, poniosło straty finansowe (+6 pp. r/r). Natomiast wyłudzenia „na PIT" nie tracą na znaczeniu – nie przynoszą już przestępcom wymiernych korzyści.

Top 5 skutecznych wyłudzeń



43%

Wśród osób, które miały kontakt z fałszywymi sklepami internetowymi, **odsetek poniesionych strat finansowych wynosi 43%** i przewyższa poziom strat związanych z wyłudzeniami „na fałszywe inwestycje" (23%). Dane te wskazują na rosnącą skuteczność oszustw oraz, że przestępcy coraz lepiej wykorzystują zaufanie konsumentów do e-commerce. Straty finansowe są tu realne i częste.

Komentarz eksperta

Andrzej Karpiński

Dyrektor Departamentu Bezpieczeństwa, BIK S.A.

Wyniki badań zrealizownych na potrzeby Raportu Antyfraudowego BIK 2025 po raz kolejny dowodzą, że nadal należy pracować nad edukacją i zwiększaniem świadomości klientów w zakresie cyberbezpieczeństwa Wciąż co szósty użytkownik nie zabezpiecza dostępu do swojego smartfonu, nie używa ani haseł dostępu, ani zabezpieczeń biometrycznych, np. odcisku palca.

Zdecydowana większość przypadków wyłudzeń środków i danych klientów instytucji finansowych zaczyna się od kliknięcia w reklamy publikowane serwisach społecznościowych i wyszukiwarkach. Niestety, wydawcy czerpią korzyści z emisji niezweryfikowanych treści takich jak np. fałszywe inwestycje. Nieodzowne wydaje się, żeby wielkie firmy technologiczne miały obowiązek lepiej chronić użytkowników i nie publikowały takich reklam? Skala zjawiska jest już tak duża, że wymaga działań systemowych.

Na szczęście mamy też dobre rozwiązania jak np. możliwość blokowania numeru PESEL w aplikacji mObywatel. To metoda, która skutecznie chroni przed wyłudzeniami – pod warunkiem, że użytkownik nie da się zmanipulować i nie zdejmie blokady.

Brak wiedzy, a często wręcz naiwność Polaków, to wyzwanie nie tylko z biznesowego punktu widzenia. To poważny problem społeczny, który niesie ze sobą ludzkie dramaty. Trzeba pamiętać, że przestępcy są bezwzględni - gdy tylko pojawia się możliwość, kradną oszczędności życia, a także zaciągają nowe katastrofalne w skutkach zobowiązania.

Dlatego skuteczne docieranie z przekazem o możliwych zagrożeniach do przedstawicieli wszystkich grup wiekowych wciąż pozostaje jednym z najważniejszych zadań dla sektora finansowego.

Klienci indywidualni

Smartfony na celowniku cyberprzestępców – rośnie skala zagrożeń

Już 27% Polaków podkreśla, że miało styczność z próbami zainfekowania urządzeń mobilnych.

Urządzenia mobilne coraz częściej stają się celem działań przestępczych. Już 27% Polaków deklaruje, że miało styczność z próbą zainfekowania swojego smartfona, co potwierdza rosnącą aktywność cyberprzestępców w tym obszarze.

Aż **61%** respondentów uważa, że ryzyko związane z atakami na urządzenia mobilne – szczególnie w kontekście dostępu do bankowości elektronicznej, wyraźnie wzrosło, podczas gdy tylko **21%** nie zauważa zmiany. Taka rozbieżność opinii może świadczyć o różnym poziomie świadomości cyfrowego bezpieczeństwa wśród Polaków.

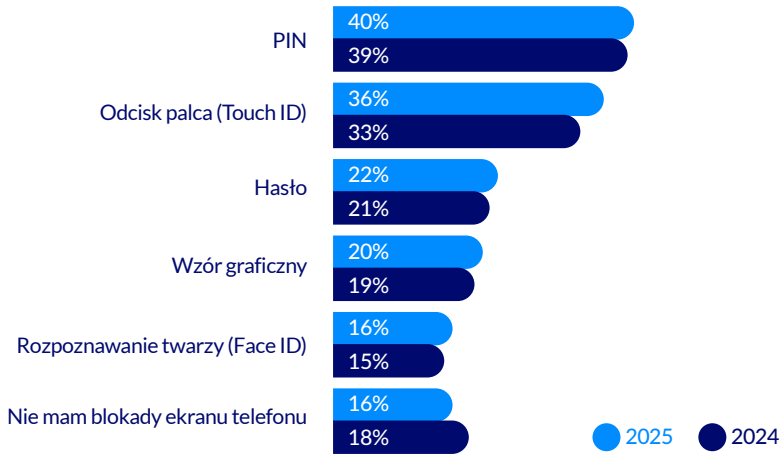
Szczególnie niepokojące są dane dotyczące skuteczności tych ataków. Co piąty poszkodowany poniósł straty finansowe, co pokazuje, że ataki nie tylko są częstsze, ale też coraz bardziej dotkliwe.

Jak Polacy zabezpieczają smartfony?

Brak podstawowej ochrony – alarmujące dane o zabezpieczeniach smartfonów

Aż 16% ankietowanych wskazuje, że w ogóle nie stosuje żadnej blokady ekranu telefonu! Chociaż ten odsetek spadł o 2 pp. r/r, to wynik nadal pozostaje niepokojący. Najczęściej stosowanymi zabezpieczeniami smartfonów są kod PIN (40%) oraz odcisk palca (36%), co może świadczyć o rosnącej popularności rozwiązań biometrycznych.

Główne metody blokowania ekranów telefonów



Bankowość mobilna zyskuje na znaczeniu

Brak podstawowej ochrony – alarmujące dane o zabezpieczeniach smartfonów

Bankowość mobilna staje się głównym kanałem obsługi klientów indywidualnych. Już 18 mln osób korzysta z niej wyłącznie przez urządzenia mobilne. Stanowi to 72% wszystkich aktywnych użytkowników aplikacji bankowych, których liczba sięgnęła 25 mln – to wzrost o 13,7% rok do roku.

Źródło: ZBP, raport NetB@nk, I kw. 2025.

59% respondentów deklaruje, że najczęściej korzysta z bankowości online za pośrednictwem aplikacji bankowej. To o 6 pp. więcej niż w 2024 r.

Komentarz eksperta

Karol Głogowski

Dyrektor IT Usług Antyfraudowych, BIK S.A.

Raport Antyfraudowy BIK 2025 wskazuje, że prawie 60% Polaków w codziennym bankowaniu korzysta głównie z aplikacji mobilnych – wyraźnie widać, że mobilne bankowanie staje się podstawą relacji z bankiem. Oszustwa związane z tym kanałem komunikacji zyskiwać będą zatem na popularności.

Oszuści nieustannie doskonalą swoje metody socjotechniczne, np. poprzez obietnice wysokich zysków z inwestycji, co powoduje wyraźnie zwiększone ryzyko dla klientów banków. Nierzadko klienci, poddani manipulacji, dokonują transakcji na rachunek oszusta samodzielnie. W takich przypadkach w grę wchodzą wyłudzenia dużych kwot, a takich przelewów zwykle nie realizuje się z aplikacji mobilnej, lecz za pośrednictwem serwisu internetowego banku.

Tego rodzaju zagrożenia we wszystkich kanałach bankowości – zarówno internetowej, jak i mobilnej – wymagają zwiększania dostępności narzędzi wspierających przeciwdziałanie nadużyciom. Klienci indywidualni oraz przedstawiciele firm podkreślają w badaniu, że kluczowym czynnikiem przy wyborze usługi jest jej dostępność i łatwość użycia, a nie cena.

Rozwój technik antyfraudowych zdecydowanie zmierza w kierunku zwiększania ochrony użytkowników, także poprzez proaktywne działania mające na celu ostrzeżenie klientów przed autoryzowaniem transakcji noszących znamiona oszustwa. Proaktywna ochrona klientów jest niezwykle istotna również z punktu widzenia samych instytucji finansowych – to one, zgodnie z obowiązującymi regulacjami, są zobowiązane do dołożenia wszelkich starań w celu poprawnej autoryzacji każdej transakcji.

Dlatego tak ważne są odpowiednio zastosowane narzędzia, które pomagają w identyfikacji podejrzanych zdarzeń i generują adekwatne ostrzeżenia związane ze zwiększonym ryzykiem danej operacji. To z kolei pozwala na zastosowanie, na przykład, dodatkowej weryfikacji w celu potwierdzenia intencji klienta, co może przyczynić się do ochrony środków zgromadzonych na jego koncie.

Klienci indywidualni

Polacy a wiedza o cyberbezpieczeństwie

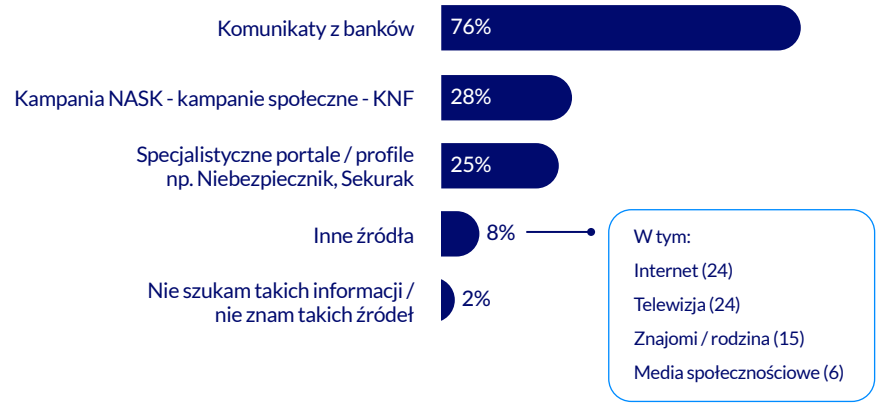
Banki odgrywają kluczową rolę w edukacji klientów na temat bezpieczeństwa w sieci i zagrożeń cyfrowych.

Kradzieże tożsamości, wyłudzenia, przejęcia kontroli nad rachunkami to zjawiska, których ryzyko instytucje finansowe pomagają zrozumieć i ograniczyć.

Aż 75% respondentów wskazuje banki jako główne źródło wiedzy z zakresu cyberbezpieczeństwa. Istotne są dla nich również kampanie społeczne (28%) oraz specjalistyczne portale (25%).

Wyniki te potwierdzają, jak istotna jest rola banków i administracji publicznej w budowaniu świadomości cyfrowej Polaków.

Źródła wiedzy o cyberbezpieczeństwie



7%

Tylko 7% Polaków chroni się przed wyłudzeniami kredytów i pożyczek, korzystając z dostępnych narzędzi. Co mogłoby to zmienić? Według 41% badanych – łatwy dostęp do takich usług w bankach, u operatorów komórkowych czy ubezpieczycieli. To jasny sygnał, że wygoda i integracja z codziennymi usługami mają kluczowe znaczenie.

Komentarz eksperta

Paweł Piekutowski

Kierownik Departamentu Cyberbezpieczeństwa, UKNF

Skala zagrożeń, na jakie narażeni są użytkownicy cyberprzestrzeni, stale się powiększa, co potwierdza dynamiczny wzrost liczby wykrywanych przez CSIRT KNF domen phishingowych. W 2022 roku zidentyfikowano 17 200 oszukańczych domen, w 2023 roku liczba ta wzrosła do 30 140, a w 2024 roku osiągnęła już 51 241.

Cyberprzestępcy z każdym rokiem wykorzystują coraz bardziej wyrafinowane metody i techniki socjotechniczne, co wpływa na skuteczniejsze oddziaływanie na zachowania użytkowników.

Wśród dominujących zagrożeń znajdują się oferty fałszywych inwestycji dystrybuowane za pośrednictwem nośników reklamowych w popularnych portalach społecznościowych, wyszukiwarkach czy serwisach internetowych. Mechanizm tych oszustw opiera się na manipulacji i fałszywych obietnicach wysokich zysków przy minimalnym ryzyku. Reklamy fałszywych inwestycji zamieszczane przez cyberprzestępców zachęcają użytkowników możliwością szybkiego wzbogacenia się.

Cyberprzestępcy nie ustępują także w tworzeniu kampanii phishingowych. Poza nowymi scenariuszami, udoskonalają również te, które skutecznie od lat wykorzystują w celu manipulacji ofiarą i kradzieży środków finansowych. Jak co roku, swoje złośliwe treści dystrybuują przy wykorzystaniu wiadomości SMS lub e-mail, gdzie podszywają się pod banki, firmy kurierskie, dostawców energii elektrycznej, znane sklepy bądź instytucje administracji publicznej. Celem cyberprzestępców jest skłonienie ofiary do kliknięcia w przesyłany link i wprowadzenia poświadczeń logowania do bankowości elektronicznej bądź informacji o karcie płatniczej.

Oszuści nieustannie udoskonalają swoje sposoby działania, dlatego konieczne jest stałe dostosowywanie i rozwijanie mechanizmów obronnych.

Komentarz eksperta

Paweł Piekutowski

Kierownik Departamentu Cyberbezpieczeństwa, UKNF

Cyberprzestępcy tworzą także kampanie złośliwego oprogramowania należącego do różnorodnych rodzin malware. Zwiększyło się również wykorzystywanie złośliwego oprogramowania typu stealer zaprojektowanego do kradzieży poufnych informacji takich jak dane logowania, hasła i dane finansowe.

Wśród zagrożeń wymierzonych użytkowników cyberprzestrzeni należy wskazać ataki z wykorzystaniem narzędzi opartych o sztuczną inteligencję (AI), które stają się coraz bardziej powszechne i zaawansowane. Przykładem takiej technologii jest deepfake, czyli narzędzie oparte na sztucznej inteligencji, które pozwala generować realistyczne, lecz nieprawdziwe obrazy, nagrania wideo czy dźwięki. Może ono służyć do podszywania się pod zaufane osoby, co stwarza ryzyko oszustw finansowych czy kradzieży tożsamości.

Cyberprzestępcy coraz częściej kierują swoje działania przeciwko dostawcom usług i oprogramowania w celu uzyskania dostępu do systemów oraz danych użytkowników końcowych. Tego typu ataki mogą skutkować szeroko zakrojonymi wyciekami informacji oraz poważnymi zakłóceniami w funkcjonowaniu instytucji finansowych.

Rosnąca liczba ataków ransomware prowadzących do utraty dostępu do kluczowych danych, wymuszania okupów, zakłóceń w działalności operacyjnej, stawia przed sektorem finansowym nowe wyzwania. Poza wdrażaniem zaawansowanych technologii zabezpieczeń ważnym jest także rozwijanie kultury bezpieczeństwa w organizacji poprzez regularne szkolenia i podnoszenie świadomości pracowników.

Świadomość obecnych trendów i zagrożeń stanowi podstawę dla skutecznej ochrony przed działaniami cyberprzestępców w 2025 roku.

Klienci indywidualni

Najważniejsze sposoby ochrony przed oszustami

Jak chronić się przed zagrożeniami? Instytucje finansowe powinny aktywnie promować zasady bezpieczeństwa:

Ograniczone zaufanie – przestępcy nie rezygnują z ataków socjotechnicznych. A to oznacza, że klienci wciąż muszą liczyć się z tym, że odbiorą telefon od rzekomego pracownika banku lub policjanta. **Warto przypominać, że przedstawiciele instytucji publicznych nigdy nie proszą o pieniądze, autoryzowanie transakcji czy podawanie wrażliwych danych.**

Ta sama zasada powinna dotyczyć osób podających się za znajomych lub członków rodziny, zwłaszcza gdy wykorzystują do tego celu media społecznościowe.

Zabezpieczanie komputera i urządzeń mobilnych – programy antywirusowe należy instalować nie tylko w komputerach stacjonarnych czy laptopach, ale również w smartfonach i tabletach. Tym bardziej, że **telefon to już podstawowe narzędzie kontaktu z bankiem**.

Aktualizacje - istotne jest również aktualizowanie aplikacji w urządzeniach mobilnych.

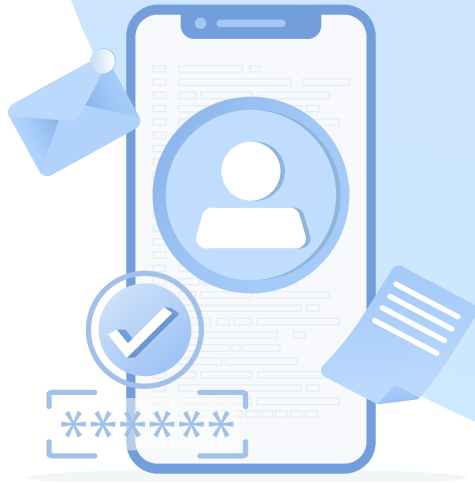
Podstawowe zasady bezpieczeństwa w sieci – warto ciągle przypominać, by nieklikać w linki i nie otwierać załączników od nieznanych nadawców, stosować różne hasła dostępu do różnych serwisów internetowych, stosować dwuskładnikowe metody uwierzytelniania.

Ostrzeżenia przed wyłudzeniami - te proste rozwiązania mogą uchronić klientów przed problemami wynikającymi z zaciągnięcia zobowiązań na ich dane.

47%

użytkowników deklaruje, że korzysta z funkcji automatycznych aktualizacji w smartfonach, podczas gdy 5% w ogóle nie aktualizuje oprogramowania.

Jednocześnie **59%** klientów uważa, że najskuteczniejszym sposobem ochrony telefonu jest unikanie otwierania wiadomości i załączników od nieznanych nadawców.



Klienci indywidualni

Najczęstsze reakcje na wyciek danych

> **13% klientów w razie wycieku danych nie robi nic, … bo już na pewno ktoś się tym zajmuje.**

Ograniczone zaufanie - przestępcy nie rezygnują z ataków socjotechnicznych. A to oznacza, że klienci wciąż muszą liczyć się z tym, że odbiorą telefon od rzekomego pracownika banku lub policjanta. **Warto przypominać, że przedstawiciele instytucji publicznych nigdy nie proszą o pieniądze, autoryzowanie transakcji czy podawanie wrażliwych danych.**

Ta sama zasada powinna dotyczyć osób podających się za znajomych lub członków rodziny, zwłaszcza gdy wykorzystują do tego celu media społecznościowe.

Zabezpieczanie komputera i urządzeń mobilnych - programy antywirusowe należy instalować nie tylko w komputerach stacjonarnych czy laptopach, ale również w smartfonach i tabletach. Tym bardziej, że **telefon to już podstawowe narzędzie kontaktu z bankiem**.

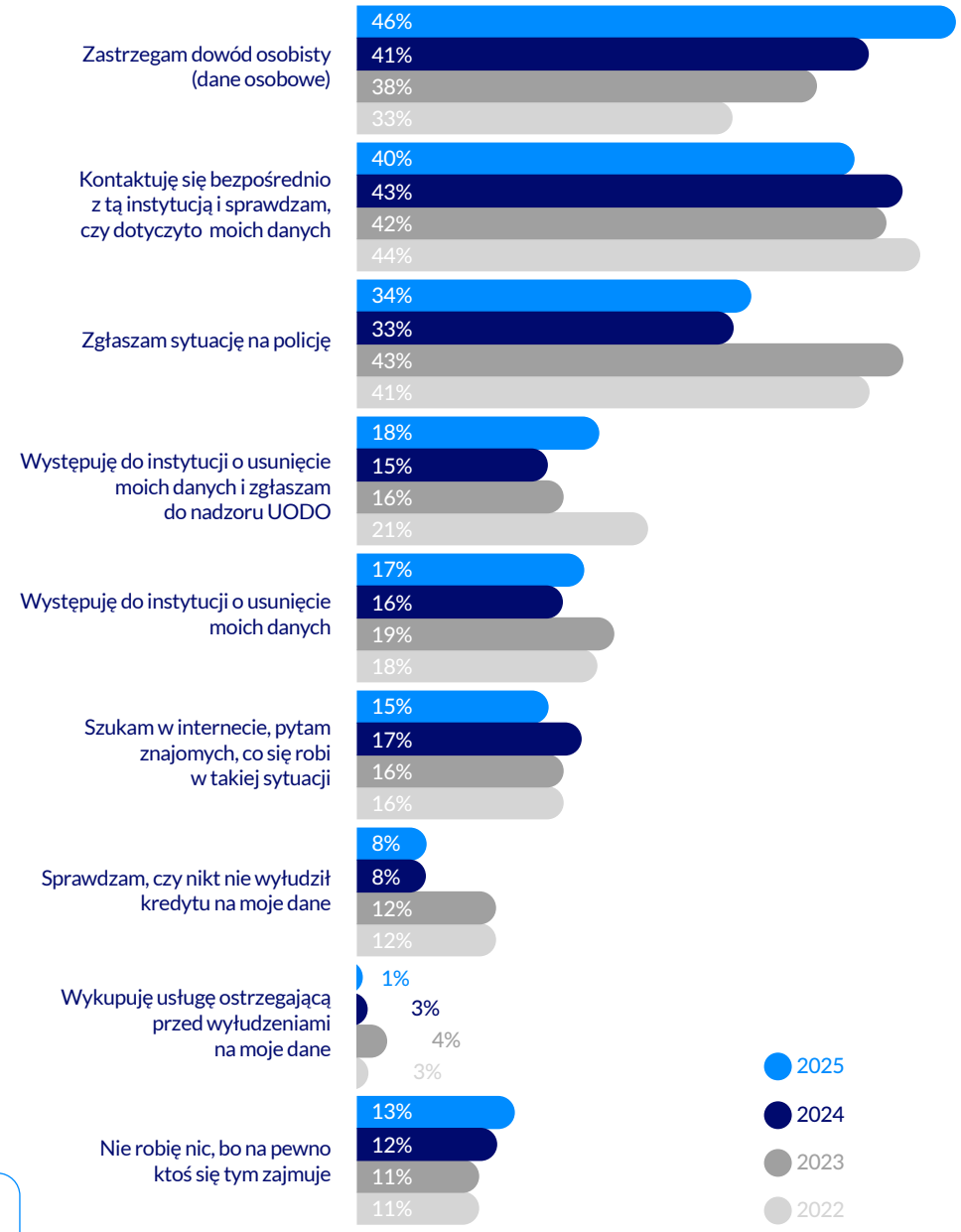
Aktualizacje - istotne jest również aktualizowanie aplikacji w urządzeniach mobilnych.

Podstawowe zasady bezpieczeństwa w sieci - warto ciągle przypominać, by nieklikać w linki i nie otwierać załączników od nieznanych nadawców, stosować różne hasła dostępu do różnych serwisów internetowych, stosować dwuskładnikowe metody uwierzytelniania.

Ostrzeżenia przed wyłudzeniami - te proste rozwiązania mogą uchronić klientów przed problemami wynikającymi z zaciągnięcia zobowiązań na ich dane.

63% Polaków uważa, że zagrożenie wyciekiem danych osobowych wzrosło, to o 3 pp. więcej niż w 2024 r.

Tak reagują Polacy na informacje o wycieku danych osobowych



Komentarz eksperta

Joanna Charlińska

Dyrektor ds. Sprzedaży,
Departament Rynku Detalicznego,
BIK S.A.

Aż o 10 p.p. wzrósł w ciągu roku odsetek Polaków, którzy mieli styczność z co najmniej jednym typem wyłudzenia. Z obserwacji BIK wynika, że w tym czasie w szczególności nasiliło się zjawisko tzw. voice phishing, a więc podszywania się przez oszustów pod przedstawicieli administracji publicznej bądź instytucji finansowych. Tego rodzaju ataki, opierające się na socjotechnice, często prowadzą do wyłudzenia środków finansowych bądź ważnych danych.

Raport Antyfraudowy BIK przynosi też pozytywną informację o tym, że banki odgrywają kluczową rolę w edukowaniu klientów w zakresie cyberbezpieczeństwa. Trzy czwarte respondentów potwierdza, że to właśnie z nich czerpią wiedzę o tym, jak uniknąć cyberataków np. kradzieży tożsamości.

Warto wspomnieć, że również BIK spełnia rolę edukacyjną, proponując klientom Ostrzeżenia BIK. To mailowe powiadomienia o niebezpiecznych zjawiskach w cyberprzestrzeni (np. masowych wyciekach danych, metodach kradzieży stosowanych przez przestępców, a także podejrzanych firmach obecnych na rynku finansowym). Dzięki Ostrzeżeniom z BIK klienci mogą zachować większą czujność. Wystarczy założyć konto w BIK i aktywować Alerty, w ramach których są wysyłane Ostrzeżenia BIK.

W Raporcie Antyfraudowym BIK 2025 zwraca również uwagę rosnący odsetek Polaków, którzy dostrzegają wzrost zagrożenia ransomware - 27% miało styczność z próbą zainfekowania komputera. Razem z innymi atakami (np. phishingowymi) to prosta droga, by dane trafiły do darknetu. To część internetu, ukryta dla zwykłych wyszukiwarek, często wykorzystywana do działań przestępczych, m.in. handlu wykradzionymi danymi. Oszuści mogą ich użyć m.in. do wyłudzenia kredytu, podszycia się pod kogoś w mediach społecznościowych lub pozyskania kolejnych informacji, które doprowadzą do konta bankowego.

Dlatego tak ważne jest, aby reagować natychmiast po wycieku danych. Od kwietnia 2025 r. BIK monitoruje również darknet. Klienci otrzymują informacje o wyciekach danych do darknetu i wspieramy ich poradami, co robić w tej sytuacji.

Najczęściej wymienianym czynnikiem, który mógłby zachęcić Polaków do korzystania z usług ostrzegających przed wyłudzeniami, jest łatwy dostęp do nich, np. za pośrednictwem banku, operatora telekomunikacyjnego czy ubezpieczyciela. Kilka banków już oferuje swoim klientom usługi BIK, dzięki czemu ich klienci czują się bezpieczniej. Zapraszamy wszystkie instytucje do współpracy w tym zakresie.

Małe i średnie firmy

Coraz więcej ataków na firmy

Aż o 16,4 pp. w ciągu roku wzrósł odsetek przedsiębiorców, którzy mieli do czynienia z próbami oszustw.

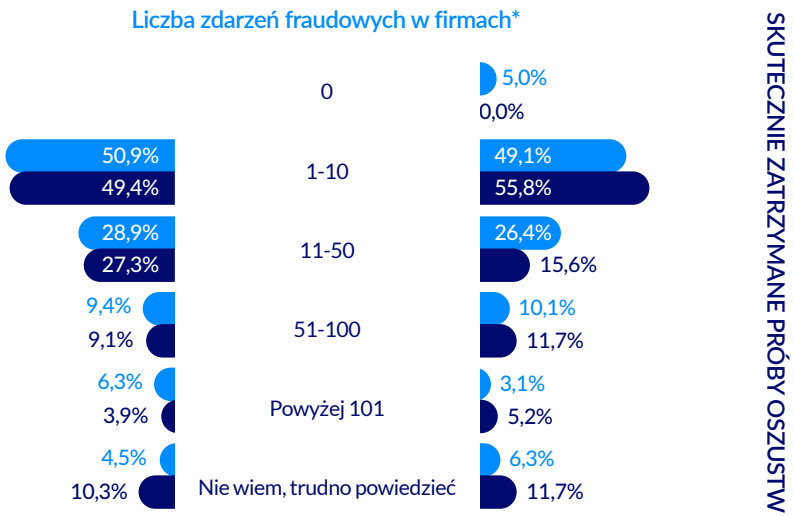
W 2025 r. styczność ze zdarzeniami fraudowymi miało 31,8% przedsiębiorców. Skali zjawiska nie determinują ani branża, ani wielkość firmy — zagrożone są wszystkie podmioty.

Właściciele firm coraz częściej wskazują również, że powszechność zjawisk fraudowych potęguje poczucie narastającego ryzyka oszustw - tak twierdzi 8,6% respondentów, podczas gdy w 2024 r. ich odsetek nie przekraczał 5%.

Skala wyłudzeń w firmach

Wśród przedsiębiorstw, które padły ofiarą prób wyłudzeń, aż 50,9% deklaruje, że incydenty te występowały nawet 10 razy w ciągu roku. Jednocześnie w przypadku 45% firm skala prób ataków była jeszcze większa - od kilkunastu do nawet stu rocznie.

Straty finansowe poniesione przez firmy, które znalazły się na celowniku oszustów, w prawie połowie przypadków (47,2%) nie przekroczyły 10 tys. zł, jednak 11,3% przedsiębiorstw poniosło straty sięgające do 100 tys. zł, a dla 5,7% - nawet 1 mln zł.



34,4% przedsiębiorców wskazuje, że ich firmy stały się celem cyberataków.

Małe i średnie firmy

Metody najczęściej stosowane przez oszustów

Fałszywe maile z linkami do systemów płatności oraz oszukańcze faktury – to plaga w firmach. A pomysłowość złodziei wciąż rośnie.

Najczęściej stosowaną metodą oszustwa wobec firm są wiadomości e-mail zawierające złośliwe linki – wskazuje na nie 35,3% przedsiębiorców, co oznacza wzrost o 11,6 pp. r/r.

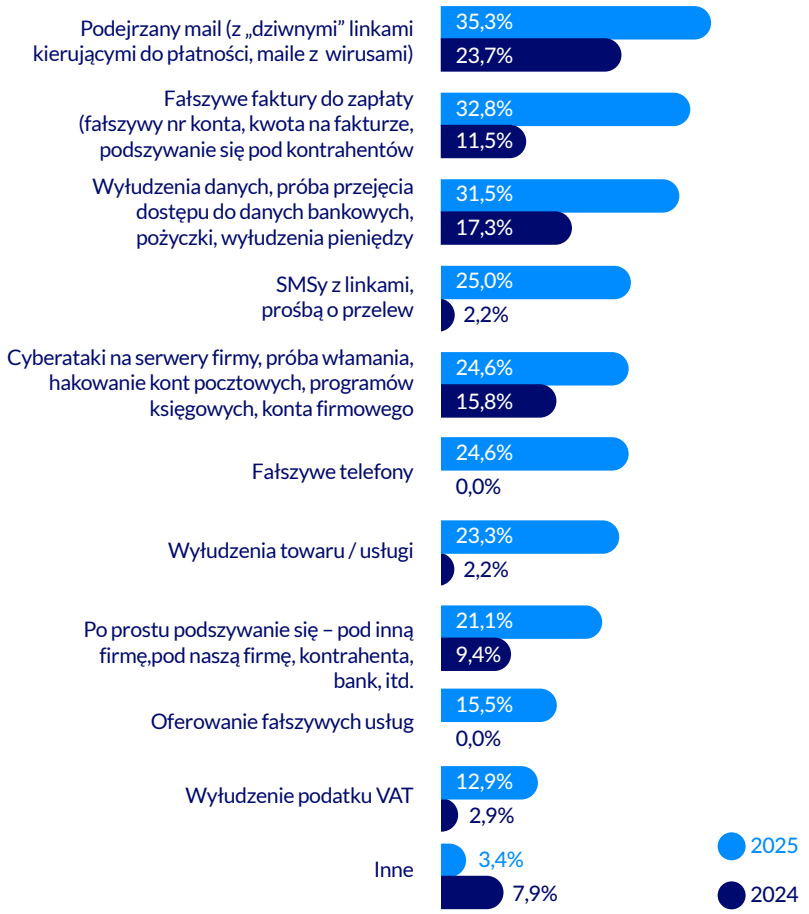
W jednej trzeciej przypadków respondenci wskazali też, że otrzymują fałszywe faktury do zapłaty – np. za usługi, których nie zamawiali bądź ze zmienionym numerem konta kontrahenta.

Lista pomysłów na kradzieże jest wśród oszustów bardzo długa - próbują oni przejmować dane dostępowe do rachunków bankowych i baz klientów, wysyłają SMS-y z prośbami o przelew albo wyłudzają towary lub usługi.

Co szczególnie istotne, w każdym przypadku skala zjawiska od 2024 r. wzrosła, co oznacza, że oszuści w żaden sposób nie dają za wygraną, a firmy muszą przygotować się do coraz lepszej obrony swoich zasobów.

Wzrost skali tych działań w 2025 roku potwierdza konieczność ciągłej edukacji w tym zakresie i wdrażania skuteczniejszych mechanizmów ochrony.

Sposoby oszukiwania firm



Oszustwa, których najbardziej obawiają się firmy

Firmy coraz bardziej boją się kradzieży danych klientów i wyprowadzania informacji z firmy — to dziś największe zagrożenie według 29% przedsiębiorców.

W czołówce zagrożeń są też cyberataki (24,6%), a także utrata towaru, polegająca np. na zakupie go na fałszywe dane i braku zapłaty (21%, -3 pp. r/r).

Co istotne, rośnie też niepokój związany z oszustwami wewnątrz organizacji — aż 19,2% właścicieli obawia się nadużyć ze strony pracowników. Wszystkie te ryzyka zyskały na znaczeniu względem 2024 roku.

Małe i średnie firmy

Ochrona firm przed fraudami

Zdrowy rozsądek, szkolenia pracowników, weryfikacja kontrahentów – te metody są dla przedsiębiorców kluczowe, by zabezpieczyć majątek i dane firmy.

Ponad jedna trzecia właścicieli firm wskazuje, że w celu wykrycia prób wyłudzeń i oszustw najczęściej zdają się na własne doświadczenie – unikają klikania w podejrzane linki czy otwierania maili od nieznanych nadawców.

Ale to nie wszystko – o podobną czujność proszą swoich pracowników, organizując szkolenia z zakresu bezpieczeństwa (34,4%). Coraz częściej stosowaną, choć jeszcze niepowszechną, praktyką jest weryfikowanie kontrahentów w zewnętrznych bazach danych (28,2%), gdzie sprawdzane są takie informacje o podmiotach, jak adresy e-mail czy telefony.

5,8% firm twierdzi, że nie stosuje żadnych technik, by ochronić się przed oszustami — ale wśród tych, które już padły ofiarą fraudu, nie ma ani jednej takiej firmy.

9,4% to odsetek firm, które deklarują wysoki budżet na działania antyfraudowe, choć w grupie tych, które miały już takie doświadczenia, wynosi on 18,2%.

Techniki wykrywania wyłudzeń i oszustw w firmach

Małe i średnie firmy

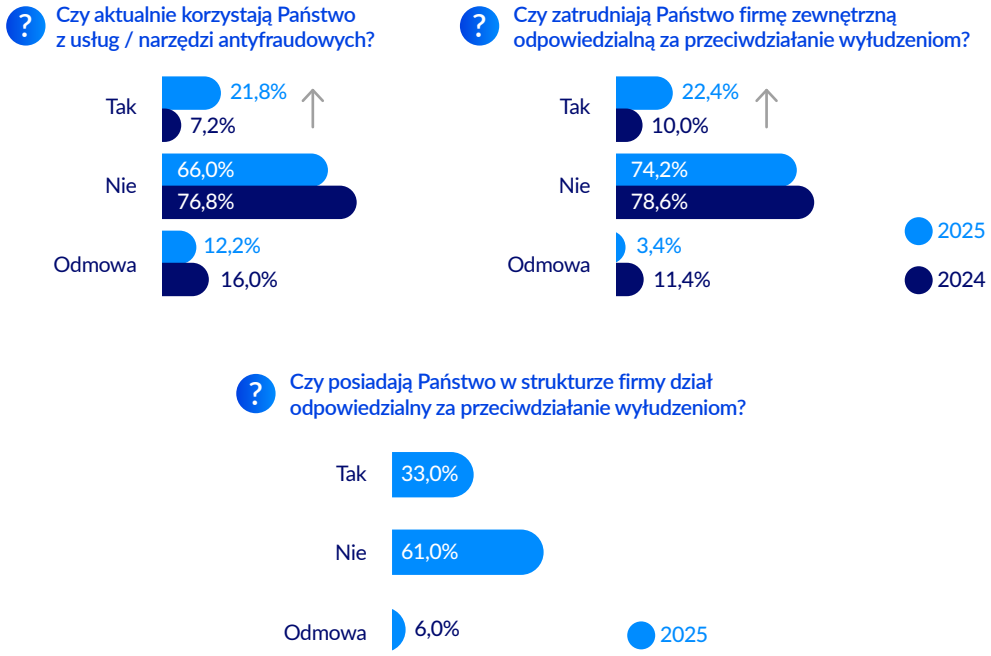
Rośnie liczba firm, które korzystają z rozwiązań antyfraudowych

Pozytywnym zjawiskiem jest również to, że jedna trzecia firm posiada w swoich strukturach komórki odpowiedzialne za przeciwdziałanie wyłudzeniom.

W odpowiedzi na rosnące ryzyko fraudów, coraz więcej firm decyduje się na wdrożenie narzędzi antyfraudowych. Ponad jedna piąta (21,8%) twierdzi, że z nich korzysta – to wyraźna zmiana wobec 2024 r., gdy podobną deklarację złożyło tylko 7,2% respondentów.

Jednocześnie co czwarte przedsiębiorstwo (25,1%) zapowiada, że będzie wdrażać rozwiązania antyfraudowe - również w tym przypadku można zauważyć wyraźny skok z 17,4% w 2024 r. To wyraźny sygnał, że firmy coraz poważniej traktują ryzyko oszustw.

Korzystanie z usług i narzędzi antyfraudowych



33% średnich firm (zatrudnienie od 50 do 249 pracowników) informuje, że posiadają w swoich strukturach działy odpowiedzialne za przeciwdziałanie wyłudzeniom.

Czego brakuje przedsiębiorcom?

Firmy chcą lepiej chronić się przed oszustami, ale potrzebują wsparcia.

27,6% przedsiębiorców wskazuje na potrzebę alertów i list spamowych numerów. 25% oczekuje więcej szkoleń dla pracowników, a 22,4% – skutecznych narzędzi do wykrywania prób oszustw.

Warto zwrócić uwagę, że aż 22% firm chciałoby, by większą odpowiedzialność w walce z fraudami przejęły instytucje finansowe — wśród tych, które już padły ofiarą oszustwa, ten odsetek rośnie do 27%.

Komentarz eksperta

Rafał Gołębiewski

Menedżer ds. sprzedaży międzynarodowej produktów antyfraudowych, BIK S.A.

Stopień ostrożności przedsiębiorców w zakresie potencjalnych oszustw jest zależny od tego, czy doświadczyli oni już zdarzenia fraudowego, czy jeszcze nie. Taki wniosek można wyciągnąć z porównania odpowiedzi na pytanie o to, jakie techniki wykrywania wyłudzeń są wykorzystywane w firmach.

Aż 5,8% w ogólnej liczbie respondentów z sektora małych i średnich podmiotów odpowiedziało, że nie stosują żadnych zabezpieczeń! Ale ten odsetek spada do zera w grupie, która ma za sobą zderzenie z oszustami. Ci, którzy nie doświadczyli do tej pory próby wyłudzenia, zwykle zdają się na intuicję i zdrowy rozsądek. Ale ci, którzy padli ofiarą złodziei, wiedzą już, że to za mało – w tej grupie wyraźnie rośnie znaczenie płatnych narzędzi antyfraudowych, zewnętrznych firm weryfikujących kontrahentów itp.

To zestawienie odpowiedzi powinno uświadomić każdemu, że ryzyko potencjalnych oszustw dotyczy każdego - zarówno klientów indywidualnych, jak i firm. Wszyscy są również potencjalnymi celami ataków z wykorzystaniem metod socjotechnicznych. Co więcej, firmy są narażone na stratę nie „tylko" środków finansowych, ale również kradzież informacji i danych osobowych klientów, które obecnie są jednym z najcenniejszych zasobów każdej organizacji – i to tego rodzaju zdarzenia uznają za największe zagrożenie w swojej działalności.

Jednocześnie w Raporcie Antyfraudowym BIK pozytywnie zaskakuje informacja o zauważalnym wzroście liczby przedsiębiorstw, które mają w planach wdrożenie usług i narzędzi antyfraudowych – deklaruje to co czwarty podmiot, chociaż jeszcze w 2024 r. ich odsetek sięgnął 17,4%.

Rolą instytucji finansowych jest dbanie o bezpieczeństwo oraz ciągłe przekonywanie klientów do wzmożonej ostrożności. Bez niej nawet najlepsze zabezpieczenia mogą okazać się niewystarczające.

Korporacje

Korporacje walczą z oszustami. Jak poważne jest zagrożenie?

| Ponad jedna trzecia przedstawicieli instytucji finansowych twierdzi, że ryzyko zdarzeń fraudowych rośnie.

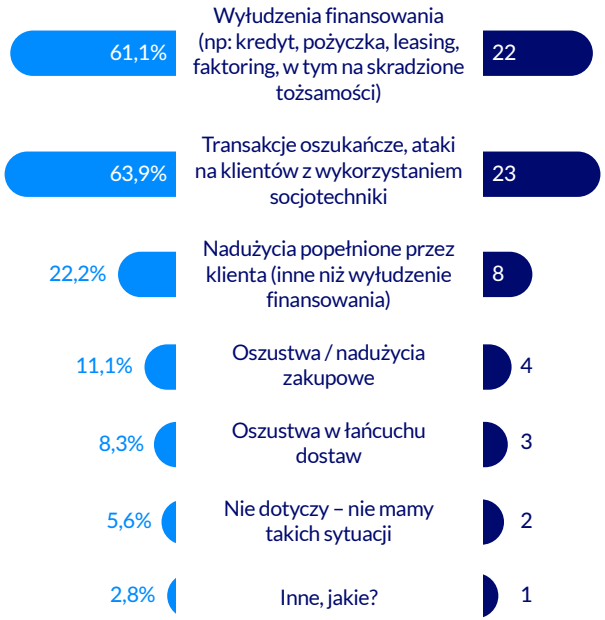
36% przedstawicieli korporacji dostrzega nasilające się przypadki oszustw – to wzrost o 5 p.p. w porównaniu z 2024 r. Z kolei 47% badanych uważa, że ryzyko jest podobne jak przed rokiem. Co istotne, żaden ankietowany nie odpowiedział, jego firma nie doświadcza tego typu zagrożeń, co potwierdza powszechność problemu.

Korporacje niezmiennie upatrują największych zagrożeń w atakach socjotechnicznych na swoich klientów (64%). Kolejnym problemem budzącym poważne obawy są wyłudzenia finansowania (kredyty, pożyczki, leasingi), na które wskazało 61% badanych.

81%

respondentów uważa, że rozwój sztucznej inteligencji spowoduje nasilenie zjawiska fraudów.

Jakich obszarów Państwa działalności dotyczyły zdarzenia fraudowe?



Korporacje

Skala strat w wyniku kradzieży

Co piąta instytucja finansowa traci w wyniku fraudów od 1,1 do 10 mln zł rocznie. Najczęściej wskazywanymi sprawcami są zorganizowane grupy przestępcze.

W co trzeciej instytucji liczba incydentów fraudowych przekracza tysiąc rocznie. Zwykle stoją za nimi: zorganizowane grupy przestępcze (76%) oraz sami klienci (71%). Indywidualni hakerzy czy pośrednicy pojawiają się w odpowiedziach rzadziej.

Struktura odpowiedzi jest zbliżona do obserwowanych trendów z poprzednich lat, w których również największą odpowiedzialność za oszustwa przypisywano grupom przestępczym, specjalizującym się w konkretnych rodzajach ataków.

Jakiego rzędu straty odnotowali Państwo z powodu fraudów w ciągu ostatniego roku?

71%

przedstawicieli instytucji finansowych wskazuje, że najczęściej spotykanym typem oszustw są transakcje oszukańcze, wykorzystujące socjotechniki wobec klientów. Mogą to być np. obietnice wysokich zysków z inwestycji, mające na celu skłonić klienta do przelania środków, a także wyłudzanie kodów autoryzujących do płatności.

Korporacje

Coraz większa skuteczność w walce z fraudami

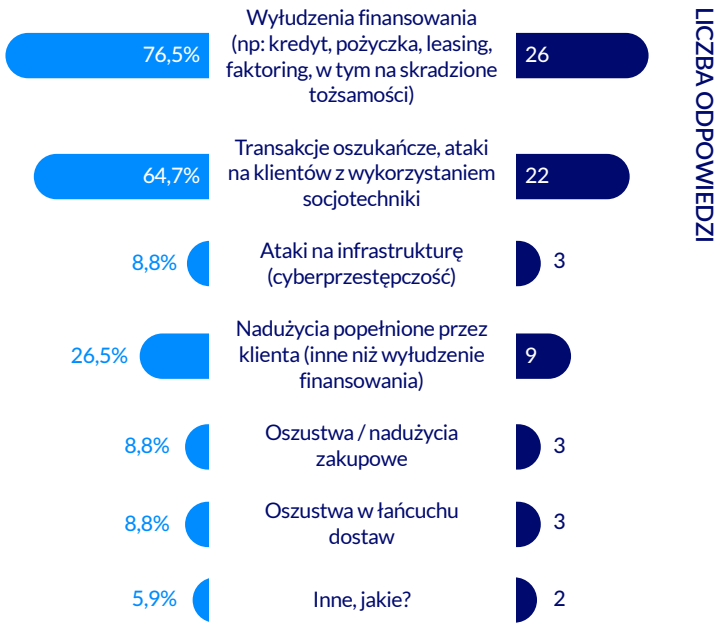
Instytucje finansowe udoskonalają narzędzia i procesy, by minimalizować ryzyko strat.

Niemal jedna trzecia dużych instytucji deklaruje skuteczne działania antyfraudowe, wskazując, że ich organizacje blokują nawet ponad tysiąc zdarzeń fraudowych rocznie. W 2024 r. odsetek podobnych odpowiedzi sięgnął 20%*

To dowód na rosnącą dojrzałość instytucji finansowych w walce z oszustwami. Najczęściej udaje im się zatrzymać wyłudzenia finansowania (76%), oraz ataki socjotechniczne na klientów (65%). Co czwarta organizacja skutecznie przeciwdziała także nadużyciom ze strony klientów.

32% respondentów deklaruje, że oszczędności wynikające z blokady zdarzeń fraudowych przekraczają w ich organizacjach 10 mln zł rocznie. To również lepszy wynik niż w 2024 r., gdy ten odsetek wyniósł 18%.

? W jakich obszarach udało się zablokować zdarzenia fraudowe w Państwa firmie?



* W 2024 r. nie było kategorii „powyżej 1 tys.", pytano zaś o „więcej niż 500".

Korporacje

Metody walki z fraudami

O skuteczności instytucji w walce z oszustami przesądzają nowoczesne rozwiązania IT.

Podobnie jak w poprzednich latach ankietowani podkreślają, że zdarzeniom fraudowym najlepiej zapobiegają rozwiązania IT (72%). Jednocześnie jednak wyraźnie wskazują na istotną rolę zespołów analityków w organizacjach (78%). Duże znaczenie mają dla nich również wszelkiego rodzaju rozwiązania sektorowe, tworzone na potrzeby walki z fraudsterami (39%).

Jakie działania w Państwa firmie najlepiej zapobiegają zdarzeniom fraudowym?

97%

respondentów z instytucji finansowych wskazuje, że ich firmy korzystają z narzędzi antyfraudowych. 88% dodaje również, że w strukturach ich organizacji funkcjonują jednostki odpowiedzialne za przeciwdziałanie cyberatakom.

Komentarz eksperta

Przemysław Augustjański

Dyrektor Departamentu Zgodności i Bezpieczeństwa Transakcji,
PKO Leasing

Dzięki nowelizacji Kodeksu cywilnego, od lipca 2025 roku możliwe stało się zawieranie umów leasingu w formie dokumentowej. To otwiera przed branżą leasingową szeroką drogę do pełnej cyfryzacji procesów. W tym kontekście kluczowego znaczenia nabiera kwestia bezpieczeństwa transakcji realizowanych w całkowicie zdalnych kanałach sprzedaży (proces end-to-end).

Tymczasem wciąż rośnie skala zdarzeń fraudowych w kanałach elektronicznych, a ich wspólnym mianownikiem są zabiegi socjotechniczne. Mechanizm działania cyberprzestępców opiera się na kilku powtarzalnych etapach, choć jest to ciąg precyzyjnie zaplanowanych zabiegów socjotechnicznych: od podszywania się, wzbudzenie obawy lub nadziei na „intratną inwestycję" wzbudzając zaufanie aż do momentu nakłonienia użytkownika do zainstalowania aplikacji umożliwiającej współdzielenie ekranu. Ten pozornie prosty ciąg zdarzeń prowadzi w efekcie do przejęcia danych uwierzytelniających, a w konsekwencji – do kradzieży środków finansowych.

Sektor finansowy, a przede wszystkim banki, nie pozostaje obojętny na te zagrożenia, zwłaszcza że ataki socjotechniczne wymierzone są w klienta końcowego – konsumenta, który pod wpływem manipulacji oszusta może nieświadomie udostępnić dane lub zainicjować niebezpieczne działania. Pomimo, że w systemie ochrony przed cyberoszustwami, same instytucje finansowe dysponują zaawansowanymi narzędziami antyfraudowymi, to sukcesywnie wdrażają coraz wyższy poziom ochrony.

Wśród nowatorskich mechanizmów antyfraudowych, sektor finansowy wdraża coraz bardziej zaawansowane narzędzia oparte, m.in. na analizie behawioralnej i identyfikacji urządzeń końcowych. Niemniej, skuteczność tych rozwiązań zależy nie tylko od technologii, ale także od świadomości użytkowników – a ta, jak pokazują statystyki, wciąż wymaga wzmacniania.

Korporacje

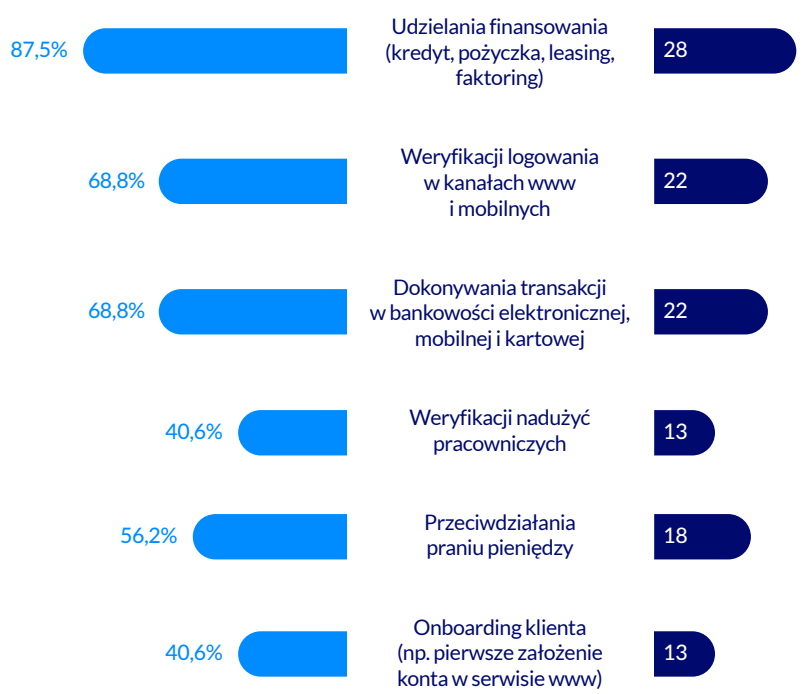
Instytucje finansowe stawiają na współpracę sektorową

Udzielanie finansowania i weryfikacja transakcji klientów - to podstawowe obszary, w których instytucje wykorzystują rozwiązania antyfraudowe.

Prawie dwie trzecie ankietowanych podkreśla znaczenie współpracy między instytucjami w zwalczaniu cyberprzestępczości – właśnie sektorowość rozwiązań wskazują jako podstawowy czynnik decydujący o wyborze narzędzi antyfraudowych.

Ważny jest też dla nich aspekt zastosowania rozwiązań w poszczególnych kanałach – 91% firm wskazuje, że korzysta z rozwiązań antyfraudowych na poziomie www., 47% – w kanale mobilnym, a 60% - w oddziałach.

W jakich obszarach w Państwa organizacjach są wykorzystywane narzędzia antyfraudowe?



Komentarz eksperta

Piotr Wojewnik

Dyrektor Data Science BIK S.A.,
Członek Zarządu Digital Fingerprints S.A.

Raport Antyfraudowy BIK 2025 przynosi informację o tym, że już 47% (+10 p.p. r/r) Polaków zetknęło się z co najmniej jedną formą wyłudzenia. Potwierdza to nasze obserwacje: ataków jest znacząco więcej, są one istotnie bardziej precyzyjne i silne.

Powodem tej sytuacji są zmiany w obszarze technologii IT i procesów bankowych, do których dostosowują się oszuści. Z jednej strony klienci zyskali wygodną bankowość cyfrową. Z drugiej - mnogość systemów i ich otwarty charakter zwiększyły liczbę punktów kontaktu systemów IT ze światem zewnętrznym, umożliwiając wzrost liczby ataków DDoS. Oszuści, dzięki posiadanej wiedzy, profesjonalizują też ataki socjotechniczne, często wykorzystując narzędzia AI.

Te trendy warunkują oczekiwania banków wobec dostawców nowych rozwiązań. Skoro oszuści mogą coraz sprytniej przejmować login i hasło klienta przez phishing, smishing, vishing lub doprowadzić do instalacji u klienta niebezpiecznego oprogramowania (remote desktop), to również banki w coraz większym stopniu potrzebują wprowadzania dodatkowych linii obrony - poza klasyczną ochroną systemów bankowych i „zdrowym rozsądkiem" klienta.

Banki potrzebują ochrony, która będzie monitorować działania konsumenta i interweniować w sytuacji zagrożenia. Jednak działanie takich systemów nie powinno zakłócać doświadczeń klienta (customer experience), a zatem powinno przebiegać w tle normalnej pracy z aplikacją, bez opóźnień w jej działaniu czy dodatkowo wymaganych akcji od użytkownika.

Jesteśmy przekonani, że w przyszłości kluczowa dla systemów antyfraudowych będzie inteligentna synteza możliwie różnorodnych i rozproszonych sygnałów. Chodzi tu zarówno o analizę bezpośrednich informacji o kliencie z baz wewnętrznych i zewnętrznych, o jego urządzeniu oraz zachowaniu – a następnie wzajemna weryfikacja pozyskanych informacji w celu wychwycenia nieścisłości i anomalii.

Rozwiązania BIK do analizy aplikacji (Platforma Antyfraudowa BIK), urządzenia (Platforma CyberFraud Detection) i interakcji (Platforma Weryfikacji Behawioralnej BIK) stanowią znakomitą bazę do zbudowania szczelnej zapory o dodatkowym walorze - współdziałania sektorowego.

Ścisła kooperacja pomiędzy użytkownikiem platformy a jej dostawcą oraz szybkie wdrożenie rekomendowanych usprawnień są kluczem do skutecznego zwalczania oszustw finansowych.

Najważniejsze wnioski

1

Coraz więcej Polaków spotyka się z różnymi formami wyłudzeń.

Bezpośrednio styczność z tym problemem miało już 47% respondentów, a więc aż o 10 p.p. więcej niż 2024 r. Przestępcy nie ustają w atakach socjotechnicznych, które mają na celu skłonienie ofiar do przelewu środków bądź udostępnienia danych do logowania.

2

Rośnie skala ataków na urządzenia mobilne.

Już 27% Polaków podkreśla, że mieli do czynienia z próbami zainfekowania smartfonów. Aż 61% obawia się, że zagrożenie w tym zakresie jest coraz większe.

3

Aplikacje bankowe są coraz popularniejsze.

59% Polaków deklaruje, że najchętniej korzysta z usług bankowych za pośrednictwem aplikacji mobilnej. Wielu ankietowanym brakuje jednak podstawowej wiedzy z zakresu ochrony smartfonów – 16% nie blokuje nawet ekranu.

4

Kampanie banków pełnią coraz istotniejszą rolę w edukacji społeczeństwa.

Dla trzech czwartych Polaków to właśnie komunikaty z instytucji finansowych są podstawowym źródłem wiedzy z zakresu cyberbezpieczeństwa. wyłudzeniom.

5

Przedsiębiorcy dostrzegają potrzebę inwestycji w narzędzia antyfraudowe.

również na chęć nawiązania współpracy z zewnętrznymi podmiotami zajmującymi się przeciwdziałaniem wyłudzeniom.

6

Coraz większa skuteczność dużych instytucji w walce z oszustami.

Jedna trzecia instytucji finansowych skutecznie blokuje po ponad tysiąc zdarzeń fraudowych rocznie. Wskazują, że najczęściej zatrzymują wyłudzenia finansowania, a także próby socjotechnicznych ataków na klientów.

Fraud w nowej rzeczywistości

jak instytucje finansowe mogą skutecznie chronić klientów

Oszustwa finansowe ewoluują – dziś to już nie tylko kradzież danych czy podszywanie się pod bank. W 2025 roku fraud oznacza także manipulację emocjami, wykorzystanie sztucznej inteligencji, deepfake'ów czy nawet gotowe usługi przestępcze dostępne online, tzw. fraud-as-a-service.

W odpowiedzi na te wyzwania, instytucje finansowe muszą działać kompleksowo. Skuteczna strategia ochrony klientów indywidualnych powinna opierać się na czterech filarach:

Nowoczesne technologie wykrywania zagrożeń

W tym sztuczna inteligencja, analiza zachowań użytkowników, biometria behawioralna czy monitoring transakcji w czasie rzeczywistym.

Współpraca międzysektorowa

Banki, regulatorzy, firmy technologiczne i organy ścigania muszą działać razem, by skutecznie przeciwdziałać coraz bardziej złożonym schematom fraudowym.

Edukacja i świadomość klientów

Regularne kampanie informacyjne, szkolenia online, powiadomienia o zagrożeniach – wszystko po to, by klient wiedział, jak rozpoznać próbę oszustwa.

Kontrola wewnętrzna i etyka organizacyjna

Zapobieganie nadużyciom ze strony pracowników, monitorowanie ryzyk operacyjnych i budowanie kultury odpowiedzialności.

Narzędzia BIK

Ochrona przed fraudami.

Oto rozwiązania technologiczne dla sektora finansowego.

Platforma Antyfraudowa (PAF) To kompleksowe rozwiązanie wspiera szerokie grono instytucji finansowych – od banków, przez firmy pożyczkowe, aż po podmioty działające w obszarze leasingu i faktoringu – w skutecznej ocenie ryzyka związanego z klientami ubiegającymi się o finansowanie.

System PAF (Platforma Antyfraudowa) działa w czasie rzeczywistym, wykorzystując zaawansowany zestaw reguł antyfraudowych, które umożliwiają szybkie wykrycie potencjalnych zagrożeń już na etapie składania wniosku. Mechanizmy te obejmują m.in. weryfikację danych klienta, analizę danych teleadresowych oraz sprawdzanie informacji o zatrudnieniu. Dzięki temu instytucje finansowe zyskują realną szansę na zatrzymanie prób wyłudzeń – szczególnie tych, które opierają się na wykorzystaniu skradzionych danych osobowych.

Skuteczność działania PAF potwierdzają konkretne liczby. Od momentu wdrożenia w 2017 roku, system umożliwił zatrzymanie prób wyłudzeń dla danych osób fizycznych i przedsiębiorców o łącznej wartości przekraczającej miliard złotych (dokładnie 1,181 mld). Co więcej, od 2020 roku PAF zidentyfikował i zablokował nadużycia związane z produktami finansowymi dla firm na kwotę ponad 186,6 milionów złotych. Dane te pochodzą z końca lipca 2025 roku i pokazują, jak istotną rolę odgrywa PAF w budowaniu bezpiecznego ekosystemu finansowego.

Platforma Cyber Fraud Detection (CFD) To zaawansowane narzędzie analityczne wykorzystywane w obszarze IT, które wspiera instytucje finansowe w ochronie klientów korzystających z kanałów online.

System ten analizuje szereg danych technicznych, by w czasie rzeczywistym identyfikować sytuacje, w których istnieje podejrzenie, że osoba trzecia – najczęściej przestępca – uzyskała dostęp do danych logowania klienta, takich jak login i hasło, w celu dokonania transakcji o charakterze fraudowym.

CFD nie tylko wykrywa zagrożenia, ale również umożliwia prowadzenie szczegółowego postępowania wyjaśniającego. W ramach tego procesu analizowane są informacje dotyczące urządzenia, z którego dokonano próby transakcji, oraz dane techniczne związane z samą operacją. Dzięki temu instytucja finansowa może szybko podjąć decyzję o zablokowaniu podejrzanego przelewu lub wypłaty środków, minimalizując ryzyko strat zarówno po stronie klienta, jak i samej instytucji.

Jedną z kluczowych zalet CFD jest jego elastyczność – narzędzie pozwala na budowanie modeli ochrony dostosowanych do indywidualnych potrzeb konkretnej instytucji finansowej. Co więcej, CFD wspiera sektorową współpracę poprzez możliwość wymiany informacji o podejrzanych urządzeniach oraz rachunkach bankowych między różnymi podmiotami rynku finansowego. Taka wymiana danych zwiększa skuteczność działań prewencyjnych i pozwala na szybsze reagowanie na nowe schematy oszustw.

CFD stanowi zatem nie tylko technologiczną barierę dla cyberprzestępców, ale również element strategii budowania zaufania i bezpieczeństwa w relacji z klientem.

Platforma Weryfikacji Behawioralnej to zaawansowane narzędzie oparte na mechanizmach uczenia maszynowego (Machine Learning), które wspiera instytucje finansowe w ochronie klientów korzystających z bankowości internetowej i mobilnej. System analizuje indywidualne wzorce zachowań użytkownika – takie jak tempo pisania na klawiaturze, sposób poruszania myszką czy charakterystyczne gesty wykonywane na ekranie urządzenia mobilnego.

Dzięki ciągłemu „uczeniu się" zachowań klienta, platforma jest w stanie wykryć sytuacje, w których dostęp do konta bankowego uzyskuje osoba nieuprawniona – nawet jeśli posiada poprawne dane logowania. W momencie wykrycia nieprawidłowości instytucja finansowa otrzymuje sygnał ostrzegawczy, który umożliwia natychmiastową reakcję, np. zablokowanie dostępu do konta lub zatrzymanie podejrzanej transakcji.

Szczególne znaczenie działania platformy ujawnia się w przypadku prób wyłudzeń, w których przestępcy nakłaniają klienta do zainstalowania oprogramowania typu „zdalny pulpit" (remote desktop). W takich scenariuszach oszust przejmuje kontrolę nad urządzeniem klienta, co może prowadzić do nieautoryzowanych operacji finansowych. Platforma Weryfikacji Behawioralnej pozwala na szybkie wykrycie takich incydentów, chroniąc zarówno środki klienta, jak i reputację instytucji finansowej.

To rozwiązanie stanowi istotny element nowoczesnej strategii antyfraudowej, łącząc technologię, bezpieczeństwo i personalizację w jednym, elastycznym systemie.

Informacje o badaniach

W niniejszym Raporcie Antyfraudowym zostały wykorzystane dane z bazy własnej Biura Informacji Kredytowej oraz informacje z badań opinii zrealizowanych na zlecenie BIK:

- Badanie CAWI na temat cyberbezpieczeństwa, zrealizowane w 2025 r. przez Quality Watch.
- Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce 2025 r., zrealizowane przez Instytut Keralla Research.
- Zdarzenia fraudowe w korporacjach, 2025 r. – badanie ankietowe wśród przedstawicieli dużych firm z następujących segmentów rynku: banki komercyjne, banki spółdzielcze, SKOK-i, firmy pożyczkowe, firmy leasingowe, firmy faktoringowe, firmy ubezpieczeniowe, firmy telekomunikacyjne.

Inne źródła:

- Raport NetB@nk, I kw. 2025., Związek Banków Polskich,

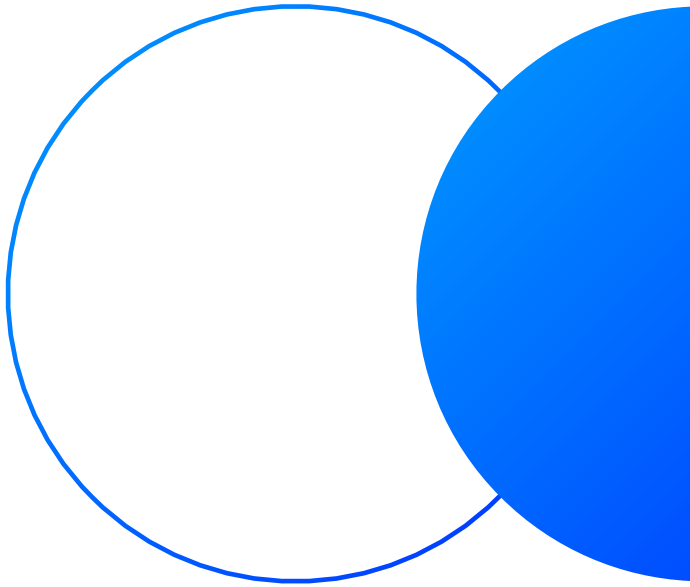
Informacje o BIK

Grupa BIK jest głównym źródłem informacji kredytowej i gospodarczej w Polsce, wspiera bezpieczeństwo instytucji finansowych i ich klientów. Dzięki Spółkom, wchodzącym w skład Grupy, łączy atrybuty instytucji zaufania publicznego i kompetencje nowoczesnych firm technologicznych.

Współpracują z nami wszystkie banki w Polsce, większość firm pożyczkowych oraz instytucji pozabankowych. Posiadamy najwyższe kompetencje w zakresie analizy danych i nowoczesnych technologii, służących zarówno klientom instytucjonalnym, jak i indywidualnym.

W skład Grupy BIK wchodzą Biuro Informacji Kredytowej S.A. i Biuro Informacji Gospodarczej InfoMonitor S.A. oraz Digital Fingerprints S.A.

www.bik.pl
www.big.pl
fingerprints.digital



Zapraszamy do kontaktu

Kontakt w sprawie usług antyfraudowych:

pomoc@bik.pl

Kontakt w sprawie Raportu Antyfraudowego:

Aleksandra Stankiewicz-Billewicz
Biuro prasowe BIK

+48 512 164 131
aleksandra.stankiewicz-billewicz@bik.pl

BIK BIG InfoMonitor DFP Digital Fingerprints

GRUPA BIK