



GRUPA BIK

Raport Antyfraudowy BIK 2026

Zagrożenia i Ochrona.



Spis treści

Wstęp	3
Zagrożenia na rynku finansowym	4
Narasta problem oszustw finansowych	4
Słownik popularnych cyberzagrożeń	5
Komentarz eksperta	7
Miroslaw Wróblewski	7
Klienci indywidualni	8
Wycieki danych	8
Działania po wycieku danych	9
Wyłudzenia pieniędzy	10
Polacy wobec realnych cyberzagrożeń	11
Najskuteczniejsze metody wyłudzeń 2026 r.	12
Najczęściej wykorzystywane kanały wyłudzeń	13
Komentarz eksperta	14
Andrzej Karpiński	14
Klienci indywidualni	15
Reakcje na wyłudzenia i sposoby ochrony	15
Komentarz eksperta	17
Joanna Charlińska	17
Klienci indywidualni	18
Cyberzagrożenia budzące największe obawy Polaków	18
Profilaktyka i ochrona przed wyłudzeniami	19
Profilaktyka i ochrona przed wyłudzeniami – analiza 2026 vs. 2025	20
Sposoby ochrony urzędów	21
Cyberataki	22
Komentarz eksperta	23
Robert Grabowski	23
Małe i średnie firmy	24
Rośnie skala zdarzeń fraudowych i cyberataków na firmy	24
Rodzaje oszustw i ataków	25
Wzrost liczby prób wyłudzeń i oszustw	26
Skala realnych strat	27

Komentarz eksperta	28
Olga Wiszowata	28
Małe i średnie firmy	29
Największe obawy przedsiębiorców	29
Ochrona firm przed fraudami	30
Bariery, obszary wsparcia firm i ich oczekiwania	31
Komentarz eksperta	32
Karol Głogowski	32
Korporacje	33
Skala zdarzeń fraudowych	33
Korporacje walczą z oszustami	35
Komentarz eksperta	36
Paweł Piekutowski	36
Korporacje	37
Skala realnych strat w wyniku wyłudzeń	37
Skuteczność w walce z fraudami	38
Komentarz eksperta	40
Andrzej Zduńczyk	40
Korporacje	41
Sprawcy oszustw i wyłudzeń w instytucjach finansowych i dużych korporacjach	41
Metody walki z fraudami	42
Komentarz eksperta	43
Piotr Wojewnik	43
Najważniejsze wnioski	44
Informacje o badaniach	45
O grupie BIK	46
Kontakt	46



Agnieszka Szopa-Maziukiewicz

Wiceprezes Zarządu BIK

Prezes Zarządu Digital Fingerprints

Szanowni Państwo,

w piątej edycji Raportu Antyfraudowego kontynuujemy analizę postaw, doświadczeń i poziomu bezpieczeństwa w trzech kluczowych segmentach: wśród klientów indywidualnych, przedsiębiorców oraz przedstawicieli banków i dużych organizacji. Dzięki temu możemy obserwować, jak zmieniają się zagrożenia, świadomość użytkowników i skuteczność działań podejmowanych na rzecz ochrony przed nadużyciami finansowymi.

Cyberprzestępcy nie zwalniają tempa – a dodatkowo zmieniają metody działania

Z naszych badań wynika, że niemal co drugi Polak (45%) zetknął się w ostatnim czasie z przynajmniej jedną próbą wyłudzenia. Jednocześnie aż 80% badanych uznaje wyciek danych za realny powód do niepokoju. To dowód, że świadomość zagrożeń rośnie. W sektorze MŚP wymagane jest podnoszenie świadomości o zagrożeniach i podstawowych zabezpieczeniach procesów biznesowych. Z kolei banki oraz duże organizacje konsekwentnie rozwijają rozwiązania antyfraudowe, skutecznie podnosząc poziom ochrony klientów i transakcji. Mimo że wciąż największe zagrożenie stanowią phishing, vishing, smishing czy quishing, to sztuczna inteligencja powoduje, że kolejne scenariusze oszustw mogą być dziś tworzone znacznie łatwiej i szybciej.

Co pokazuje tegoroczny raport?

Nowoczesne technologie coraz lepiej wspierają ochronę przed cyberzagrożeniami, jednak o skuteczności zabezpieczeń nadal często decyduje człowiek – kluczowe znaczenie ma umiejętność rozpoznawania prób manipulacji oraz poziom czujności. Obserwujemy niepokojące zjawisko nadmiernej pewności siebie i odkładanie decyzji o stosowaniu dodatkowych zabezpieczeń. Nadal wielu poszkodowanych nie zgłasza incydentów odpowiednim służbom, a część osób i firm odkłada decyzję o wdrożeniu dodatkowych zabezpieczeń, uznając je za zbędne lub zbyt kosztowne.

Przyszłość i wnioski, które warto wyciągnąć?

Niezwykle ważne pozostają inwestycje w technologie, lecz także konsekwentne budowanie wiedzy i świadomości użytkowników. Szczególną rolę odgrywają tu banki i instytucje finansowe, które są dla konsumentów najważniejszym źródłem informacji o cyberbezpieczeństwie. Ponad połowa (55%) konsumentów deklaruje w naszym badaniu, że właśnie z tego źródła czerpie wiedzę, jak chronić swoją tożsamość, dane i pieniądze przed cyberprzestępcami.

Raport Antyfraudowy BIK powstaje właśnie po to, by wspierać ten proces: dostarczać rzetelnej wiedzy, wskazywać kierunki zmian oraz pomagać lepiej rozumieć współczesne zagrożenia. Wierzę, że zawarte w nim tezy i wnioski staną się praktycznym wsparciem dla wszystkich uczestników rynku finansowego i przyczynią się do dalszego wzmacniania kultury bezpieczeństwa cyfrowego w Polsce.

Zagrożenia na rynku finansowym

Narasta problem oszustw finansowych

Głównym celem ataku wciąż pozostaje człowiek – phishing i manipulacja, coraz częściej wspierane przez AI, wciąż są niebezpiecznym orężem w starciu z klasycznymi zabezpieczeniami technicznymi. Szczególnie, że zarówno klienci indywidualni, jak i małe firmy, do dbałości o swoje bezpieczeństwo nadal podchodzą zbyt lekkomyślnie.

Oszustwa finansowe narastają nie tylko ilościowo, ale stają się coraz bardziej złożone i generują z roku na rok wyższe koszty zabezpieczeń. Przynoszą także coraz większe straty. Z danych za I kw. 2026 r. publikowanych przez Narodowy Bank Polski wynika, że liczba transakcji oszukańczych dokonanych przy użyciu bezgotówkowych instrumentów płatniczych (karty płatnicze, polecenia przelewu, polecenia zapłaty) zwiększyła się o 3,4% w porównaniu z IV kw. 2025 r., a ich wartość aż o 46,8%. W przypadku firm dochodzą do tego trudne do wyceny straty wizerunkowe czy utrata zaufania klientów. O skali tych strat decydują przede wszystkim ataki ransomware, wycieki danych i przejęcia tożsamości.

Jednocześnie systematycznie zwiększa się odsetek oszustw bazujących na manipulacji, socjotechnikach, w których decydujące znaczenie ma zachowanie i podatność klienta, a nie wyłącznie środowisko techniczne w jakim przeprowadzana jest transakcja.

Dla instytucji finansowych, priorytetem staje się odporność operacyjna – szybkie wykrycie, izolacja i odtworzenie usług są dziś ważniejsze niż samo zapobieganie incydentom.

Skuteczna odpowiedź to współpraca sektorowa i wymiana informacji w ramach systemu opartego na analizie behawioralnej. Każde wykrycie anomalii, wskazujących na próbę oszustwa, to sygnał do szybkiej reakcji w całym sektorze, co znacząco podnosi poziom bezpieczeństwa wszystkich klientów.

Choć już 11 banków w Polsce korzysta z tego rozwiązania, to nadal niska jest świadomość konsumentów, czym jest weryfikacja behawioralna. Tylko 20% poprawnie rozumie to pojęcie – wynika z badania zrealizowanego dla BIK w marcu 2026 r., na próbie 1040 osób.



35%

Spośród wszystkich oszustw najczęściej utratą środków finansowych kończy się wyłudzenie przez fałszywe sklepy internetowe – w 35% przypadków doszło do wymiernej straty finansowej. Nawet w przypadku najmniej skutecznych metod (maile sprzedażowe i super okazje, vishing/spoofing oraz phishing) około 7-9% prób wyłudzenia kończyło się stratą finansową.

Tylko w 2025 roku do CSIRT KNF zgłoszono ponad 41 tys. fałszywych domen.

Zagrożenia na rynku finansowym

Narasta problem oszustw finansowych



Klienci indywidualni

45% osób miało osobistą styczność z co najmniej jednym typem wyłudzenia.

45% 2026

47% 2025

37% 2024

36% 2023



Małe i średnie przedsiębiorstwa

38% małych i średnich firm miało do czynienia ze zdarzeniem fraudowym.

38% 2026

32% 2025

15% 2024

18% 2023



Korporacje

70% firm doświadczyło w minionym roku prób wyłudzeń finansowania (kredyt, pożyczka, leasing, faktoring).

70% 2026

62% 2025

66% 2024

66% 2023

Słownik popularnych cyberzagrożeń

Metody i techniki socjotechniczne z roku na rok stają się coraz bardziej wyrafinowane. Automatyzacja i sztuczna inteligencja znacząco obniżyły kosztowy próg wejścia dla kolejnych cyberprzestępców.

Poniżej prezentujemy najczęściej wskazywane typy ataków, z którymi spotykają się klienci indywidualni:



Phishing

Polega na podszywaniu się pod zaufane instytucje (np. banki, firmy kurierskie, urzędy). 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”

Najbardziej nasilający się 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 włamania 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 informują o rzekomym zagrożeniu i nakłaniają do podania danych lub wykonania przelewu.

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



Quishing

Polega na wyłudzeniu danych za pomocą kodów QR. Przestępcy podmieniają lub rozsyłają spreparowane kody, które przekierowują użytkownika na fałszywe strony podszywające się pod legalne instytucje.

Cel: kradzież haseł, danych karty lub loginu, na przykład do banku.



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 wnuczkę” / „na policjanta”

Klasyczne oszustwa telefoniczne, w których przestępcy podszywają się pod członka rodziny (np. wnuczkę) 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.



Deepfake audio/video

Technologia wykorzystująca sztuczną inteligencję (AI) do generowania lub manipulowania obrazami, dźwiękami i nagraniami wideo. Pozwala na tworzenie fałszywych materiałów, w tym wstawianie twarzy jednej osoby w miejsce innej lub klonowanie czyjegoś głosu.

Cel: Wyłudzenia pieniędzy.

Komentarz eksperta

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych



Cyberataki dotyczą zarówno konsumentów, jak i przedsiębiorstwa, a granica między tymi zagrożeniami coraz bardziej się zaciera. Dlatego cyberbezpieczeństwo stało się wspólną odpowiedzialnością wszystkich uczestników cyfrowej gospodarki.

Dla firm, zwłaszcza z sektora MŚP, cyberatak oznacza nie tylko ryzyko utraty pieniędzy. Równie dotkliwe mogą być konsekwencje związane z kradzieżą danych klientów, utratą zaufania oraz szkodami wizerunkowymi.

Cyberprzestępcy coraz częściej wykorzystują skradzione dane do wymuszania okupu. Zapłacenie żądanej kwoty nie gwarantuje jednak bezpieczeństwa. Dane mogą zostać później sprzedane w darknecie lub udostępnione w sieci, a informacja o samym incydencie i tak może ujrzeć światło dzienne.

Dla Prezesa UODO przyczyną nakładania kar zwykle nie jest sam incydent bezpieczeństwa danych, ale postawa administratora, która doprowadziła do naruszenia przepisów o ochronie danych osobowych. Nie ma bowiem zabezpieczeń w pełni szczelnych i naruszenia będą się zdarzały.

Kluczowe znaczenie ma prawidłowo przeprowadzona analiza i właściwe zabezpieczenie instytucji. Organizacje powinny też regularnie analizować nowe zagrożenia i wdrażać adekwatne środki ochrony.

Do podstawowych narzędzi ograniczających ryzyko należą m.in. uwierzytelnianie wieloskładnikowe, szyfrowanie danych oraz odpowiednie procedury bezpieczeństwa. Po wykryciu ataku równie ważne są szybka reakcja, zgłoszenie incydentu i działania zapobiegające jego powtórzeniu.

Nawet najlepsze technologie nie zastąpią świadomych użytkowników. Regularne szkolenia oraz znajomość procedur pomagają pracownikom szybciej rozpoznawać zagrożenia i skuteczniej reagować na próby oszustwa.

Choć świadomość cyberzagrożeń wśród przedsiębiorców rośnie, wiele firm zwiększa inwestycje w bezpieczeństwo dopiero po doświadczeniu incydentu. Tymczasem odpowiednie zabezpieczenia warto traktować jako inwestycję, a nie koszt ponoszony dopiero po wystąpieniu problemu.

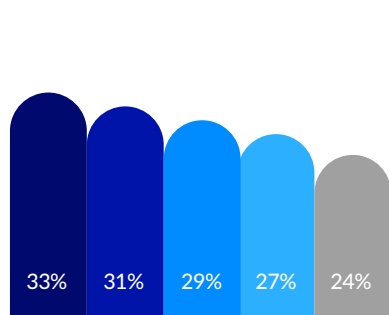
Klienci indywidualni

Wycieki danych

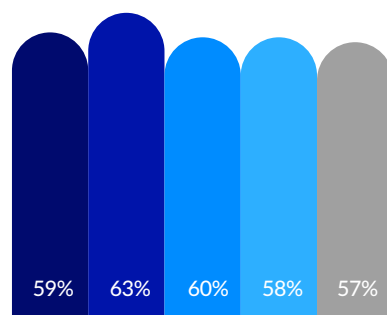
Już co trzeci Polak deklaruje styczność z wyciekiem danych osobowych. To systematyczny wzrost o 2 pkt proc. rok do roku. W 2026 roku aż 15% ankietowanych przyznało, że sprawa dotyczyła ich osobiście. Pogłósłnych medialnie wyciekach, takich jak ujawniony w sierpniu br. wyciek danych medycznych, można oczekiwać, że w kolejnych badaniach odsetek ten będzie jeszcze wyższy.

Mimo rosnącej skali incydentów oraz pierwszy od pięciu lat spadek ogólne poczucie zagrożenia wyciekiem danych osobowych, z 63% do 59%. Jednocześnie o 4 pkt proc. wzrósł odsetek osób deklarujących najwyższy poziom zagrożenia. Oznacza to, że spadek poczucia zagrożenia może mieć charakter pozorny. Nie wynika on bowiem z mniejszej liczby ataków, lecz może świadczyć o stopniowym oswojeniu się społeczeństwa z zagrożeniem oraz o rosnącej świadomości, jak reagować w przypadku naruszenia bezpieczeństwa danych.

Co trzeci Polak doświadczył wycieku danych osobowych



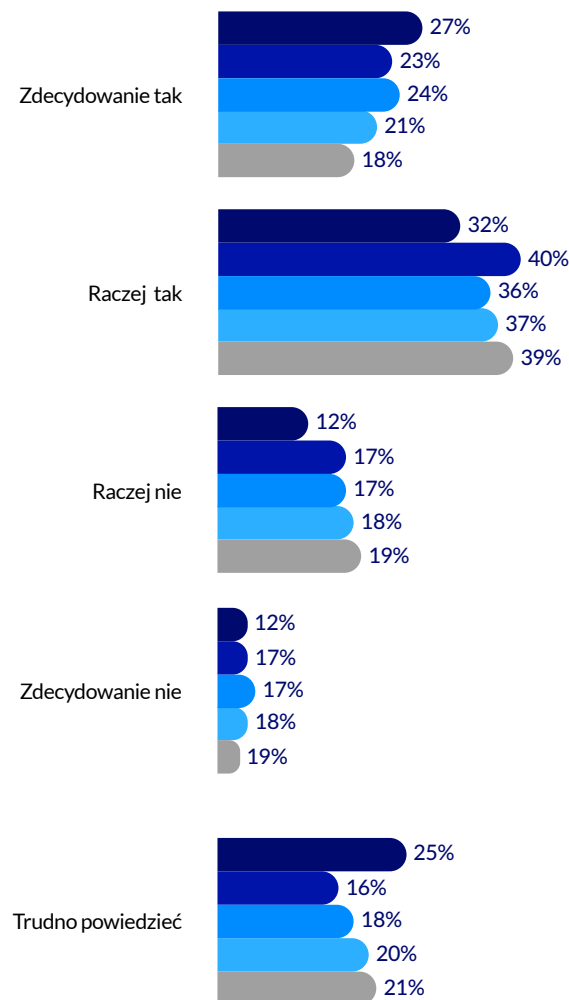
Spadek poczucia zagrożenia wyciekiem danych



● 2026 ● 2025 ● 2024 ● 2023 ● 2022

źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

Poziom poczucia zagrożenia wyciekiem danych



Klienci indywidualni

Działania po wycieku danych

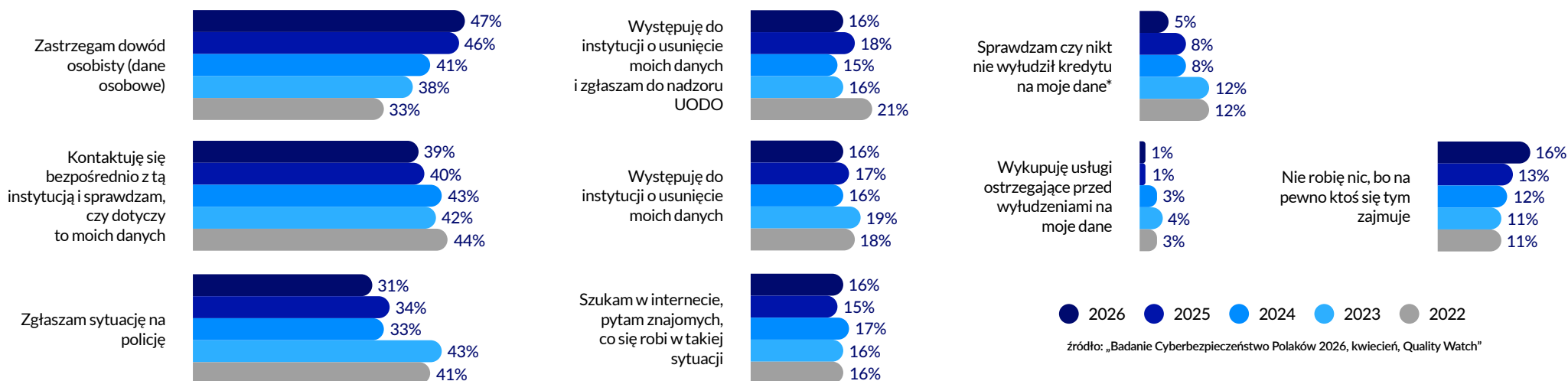
Coraz większa liczba Polaków deklaruje, że po informacji o wycieku danych w pierwszej kolejności zastrzegłaby dowód osobisty. Jednym z powodów jest rozwój usług w aplikacji mObywatel, które ułatwiają szybkie zabezpieczenie się przed wykorzystaniem skradzionych danych. Od 2022 roku grupa ta zwiększyła się z 33% do 47%. Rosnąca świadomość to także efekt zmian prawnych, a także cyfryzacji usług publicznych (ePUPAP, IKP, e-Urząd Skarbowy). Nie bez znaczenia pozostają także działania edukacyjne, prowadzone przez instytucje finansowe odpowiedzialne za cyberbezpieczeństwo finansowe, a także rządowe agendy odpowiedzialne za cyberbezpieczeństwo.

Drugim – oczywistym działaniem (39%) – jest bezpośredni kontakt z instytucją, z której dane wyciekły i sprawdzenie czy dotyczy to także „moich” danych. Choć tu, tendencja jest dokładnie odwrotna – z roku na rok zrobiłoby to coraz mniej osób.

I wreszcie – w trzeciej kolejności – deklarujemy zgłoszenie sprawy policji. Tu jednak zaskoczenie jest największe, ponieważ w ciągu minionych 4 lat (od 2023 roku) chęć oficjalnego zgłoszenia sprawy organom ścigania spadła aż o 12 pkt proc., a jednocześnie wzrosła grupa deklarująca: „Nie robię nic, bo na pewno ktoś się tym zajmuje” (z 11% do 16% do roku 2022).

W sytuacji wycieku danych osobowych Polacy najczęściej byłiby skłonni zastrzec dowód osobisty (47%) oraz skontaktować się z instytucją, z której dane wyciekły (39%). Jednocześnie 16% ankietowanych nie podjęłoby żadnych działań, ponieważ „na pewno ktoś się tym zajmuje”.

Reakcje podejmowane w wyniku wycieku danych



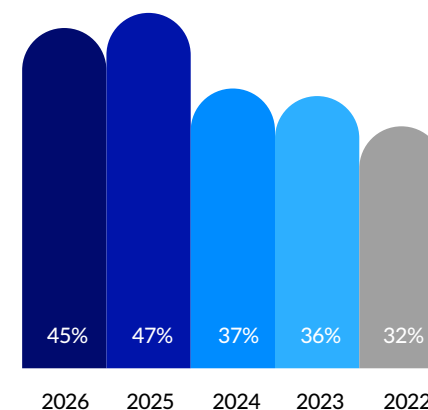
Klienci indywidualni

Wyłudzenia pieniędzy

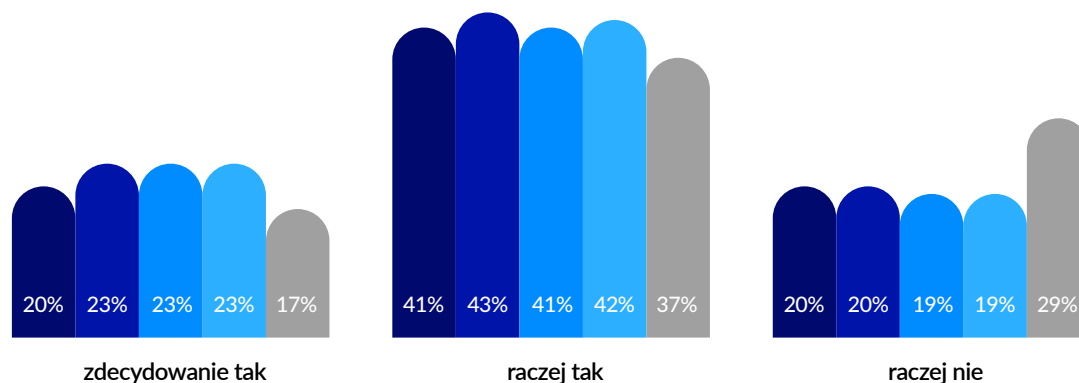
Osobistą styczność z co najmniej jednym typem wyłudzenia miało 45% ankietowanych. Wskaźnik ten nieznacznie spadł od roku ubiegłego, ale jest wyższy niż w latach 2022-2024. Większość Polaków (61%) obawia się wyłudzenia pieniędzy, a jednocześnie rośnie grupa osób, które nie widzą w wyłudzeniach istotnego zagrożenia. Łącznie co czwarty Polak (27%) podchodzi do tego problemu bez większych obaw.

To zjawisko rosnącej świadomości społecznej. Przynoszą efekty kampanie edukacyjne, instytucje finansowe wyposażają swoich klientów w dodatkową wiedzę i narzędzia, coraz lepiej zabezpieczają swoje serwisy, a także systematycznie przypominają o podstawowych zasadach bezpieczeństwa. Wszystko to przynosi poczucie przygotowania na odparcie ewentualnej próby ataku, co skutkuje mniejszym odsetkiem osób obawiających się wyłudzenia.

Skala doświadczeń z różnymi formami wyłudzeń

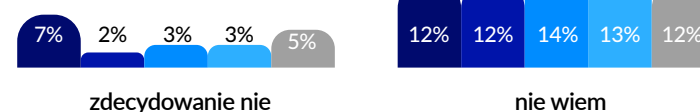


Skala poczucia zagrożenia wyłudzeniem pieniędzy



● 2026 ● 2025 ● 2024 ● 2023 ● 2022

źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”



Klienci indywidualni

Polacy wobec realnych cyberzagrożeń

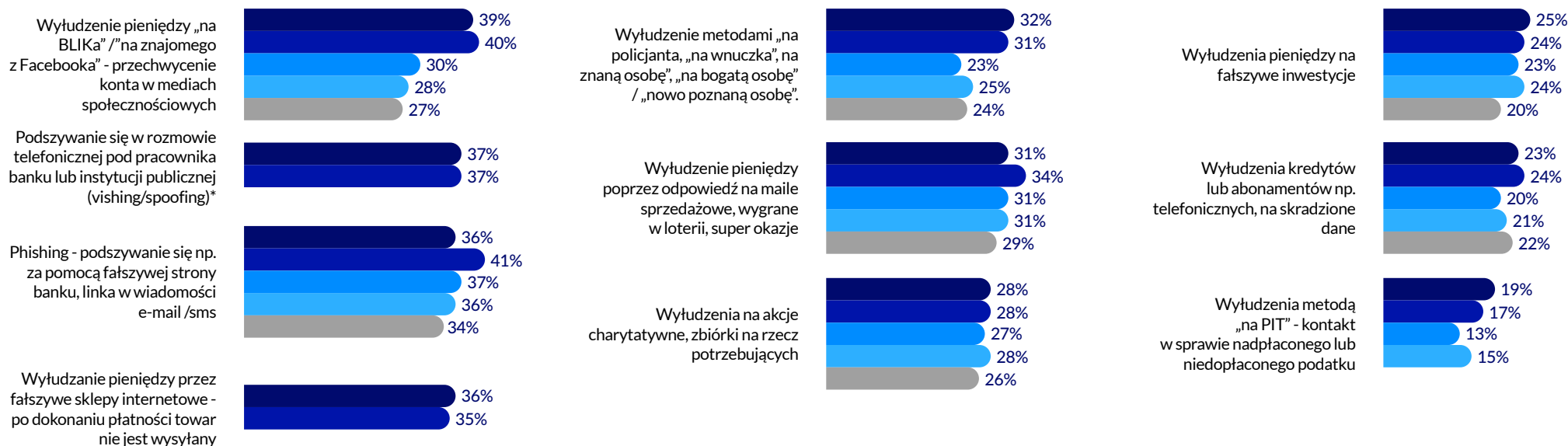
Zmienia się nie tylko nasze poczucie zagrożenia, ale także ocena dotycząca wagi zagrożeń płynących z poszczególnych metod oszustwa. O ile w ubiegłym roku najczęściej Polacy stykali się z phishingiem (41% w 2025 r.), to obecnie wskazują przede wszystkim na próby wyłudzenia pieniędzy „na BLIKa” lub „na znajomego z Facebooka” (39%). Wektor ataku przenosi się więc z bezpośredniego kontaktu telefonicznego na działania internetowe.

Odsetek osób dostrzegających nasilenie cyberzagrożeń jest niższy niż w poprzednich edycjach badania. Największy spadek dotyczy wyłudzeń wykorzystujących maile sprzedażowe i fałszywe promocje (o 5 pkt proc.). Rzadziej niż wcześniej respondenci wskazują także na phishing czy wykorzystywanie skradzionych danych do zaciągania zobowiązań.

39%

Polacy najczęściej mieli styczność z wyłudzeniami na znajomego z Facebooka oraz na BLIKa (39%, w tym 15% osobiście)

Doświadczenie Polaków z wyłudzeniami



● 2026 ● 2025 ● 2024 ● 2023 ● 2022

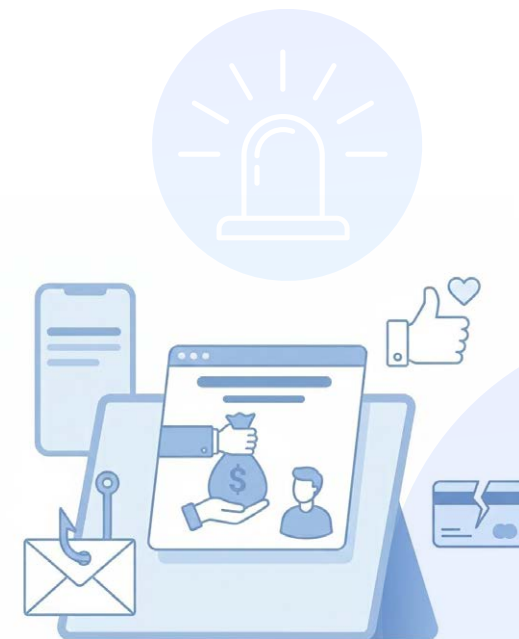
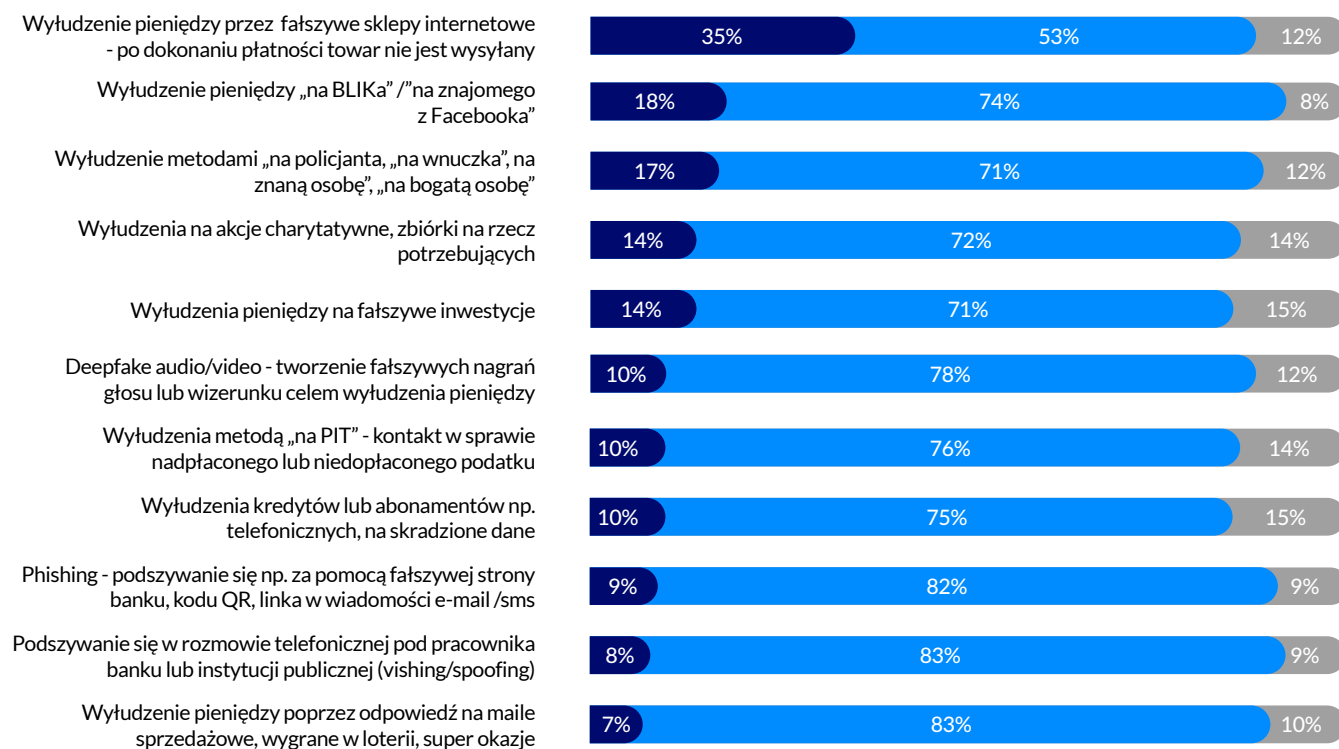
źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

Klienci indywidualni

Najskuteczniejsze metody wyłudzeń 2026 r.

Pod względem skuteczności wyłudzeń dominuje metoda na fałszywe sklepy internetowe, która w 35% przypadków prowadziła do utraty środków finansowych. Wśród najskuteczniejszych metod znalazły się także oszustwa „na BLIKA” oraz za pośrednictwem kont znajomych w mediach społecznościowych. Na trzecim miejscu - nadal skuteczne okazują się wyłudzenia „na wnuczka” czy „na policjanta”, zmodyfikowane do wersji na znaną lub bogatą osobę.

Najskuteczniejsze metody wyłudzeń 2026 r.



- ☒ Tak, doszło do straty finansowej
- ☐ Nie, nie doszło do straty finansowej
- ☐ Nie wiem, nie pamiętam

źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

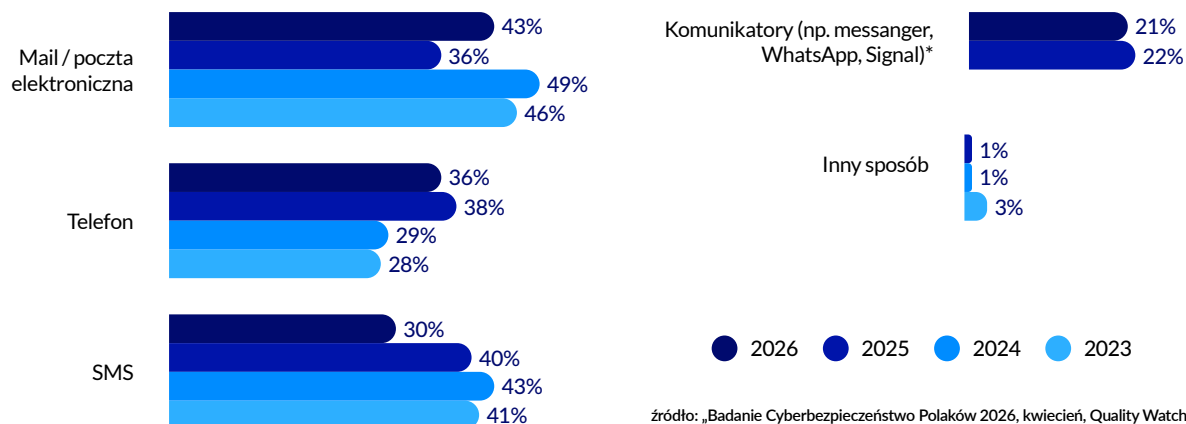
Klienci indywidualni

Najczęściej wykorzystywane kanały wyłudzeń

W stosunku do roku ubiegłego odsetek Polaków, którzy mieli bezpośredni lub pośredni kontakt z różnymi metodami wyłudzenia nie uległ większym zmianom. Wyjątek stanowi styczność z phishingiem (-5 pkt proc.) oraz z wyłudzeniami poprzez odpowiedzi na maile sprzedażowe/ wygrane w loterii (-3 pkt proc.). W obu przypadkach odsetek wrócił do poziomu porównywalnego z latami 2022-2024.

Ankietowani, którzy mieli styczność z próbą wyłudzenia metodą phishingu, wskazują najczęściej, że kontakt nastąpił za pośrednictwem poczty elektronicznej. W stosunku do poprzedniego badania, zmniejszyły się natomiast próby ataku za pośrednictwem telefonu i komunikatorów internetowych.

Kanały wykorzystywane w phishingu



14%

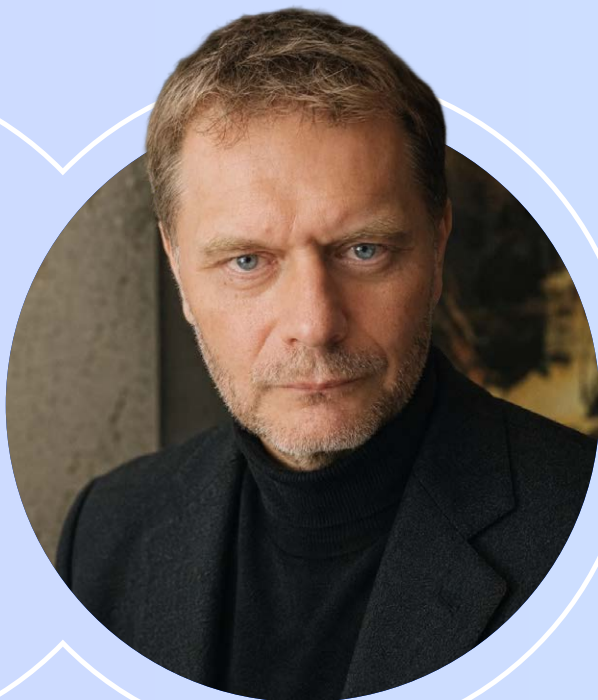
O 14 p.p. spadła skuteczność wyłudzeń na akcje charytatywne. To najwyższa zmiana względem roku 2025, pośród wszystkich metod wyłudzeń.

Należy zaznaczyć, że tegoroczne badanie potwierdza malejącą skuteczność wszystkich analizowanych metod wyłudzeń nie tylko r/r, ale także w całej historii badania. To dobra wiadomość, która potwierdza wyczulenie społeczeństwa podczas odbierania połączenia telefonicznego czy reakcji na sms.

Komentarz eksperta

Andrzej Karpiński

Dyrektor Departamentu Bezpieczeństwa BIK



Rosnąca skuteczność zabezpieczeń oraz większa świadomość użytkowników sprawiają, że cyberprzestępcy są zmuszeni stale modyfikować swoje metody działania i szukać nowych sposobów dotarcia do potencjalnych ofiar. Wynika to przede wszystkim z trzech czynników.

Po pierwsze, istotną rolę odegrały zmiany w prawie telekomunikacyjnym, które nałożyły na operatorów obowiązki związane m.in. z weryfikacją nadawców połączeń i ograniczaniem możliwości podszywania się pod zaufane instytucje. W efekcie liczba fałszywych połączeń oznaczonych nazwą banku czy urzędu wyraźnie spadła, a sam proceder stał się dla przestępców znacznie trudniejszy.

Po drugie, rośnie świadomość społeczna w zakresie cyberbezpieczeństwa. Coraz więcej osób z większą ostrożnością podchodzi do nieoczekiwanych telefonów, wiadomości SMS czy e-maili oraz częściej weryfikuje otrzymywane komunikaty.

Po trzecie, stale rozwijają się zabezpieczenia stosowane przez instytucje finansowe. Klienci są coraz częściej proszeni o potwierdzenie tożsamości w aplikacji mobilnej, co pozwala zweryfikować autentyczność kontaktu z bankiem i znacząco utrudnić oszustwo metodą „na pracownika banku”.

Choć obserwujemy wzrost liczby prób wyłudzeń prowadzonych za pośrednictwem poczty elektronicznej, badania wskazują, że w 2026 roku skuteczność oszustw osiągnęła najniższy poziom w historii pomiarów. To w dużej mierze efekt większej świadomości społeczeństwa w zakresie ochrony danych osobowych. Dobrym przykładem jest popularność usługi Zastrzeżenie PESEL, z której korzysta już około 10 milionów osób.

Warto jednak pamiętać, że cyberprzestępcy wykorzystują nie tylko numer PESEL, ale również dane bankowe, numery telefonów, adresy e-mail czy skany dokumentów. Dlatego warto korzystać z dodatkowych narzędzi ochrony, takich jak Alerty BIK, które powiadamiają o próbie wyłudzenia kredytu, podpisania umowy na nasze dane, a także monitorują dane pod kątem ich ujawnienia w darknecie.

Klienci indywidualni

Reakcje na wyłudzenia i sposoby ochrony

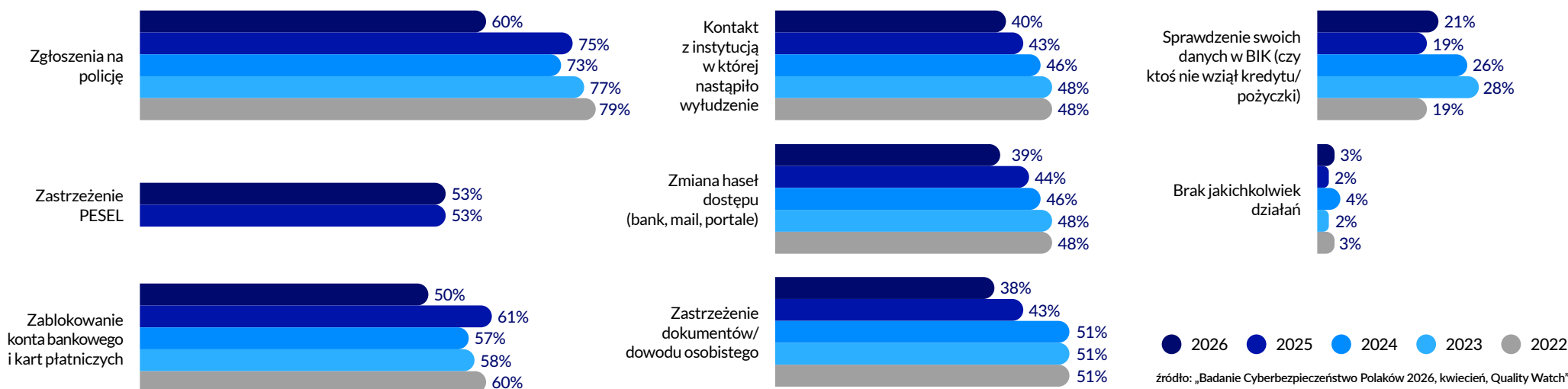
Najczęstszą reakcją na podejrzenie oszustwa lub wyłudzenie jest zastrzeżenie numeru PESEL (53%) oraz zablokowanie konta bankowego i kart płatniczych (50%). Działania te stają się coraz łatwiejsze, gdyż większość spraw można dzisiaj załatwić on-line, za pośrednictwem smartfona i aplikacji bankowej czy mObywatela. Obok zgłoszenia sprawy na policję to najczęściej wybierane sposoby zabezpieczenia się przed dalszymi stratami.

Tymczasem weryfikacja danych w BIK powinna być standardowym elementem postępowania po wykryciu wyłudzenia lub próby wyłudzenia. Sprawdzanie swoich danych w BIK deklaruje 21% osób (+2 pkt proc.r/r). Osoby te weryfikują w swoim Raporcie BIK, czy oszust nie wykorzystał ich danych do zaciągnięcia zobowiązań finansowych w różnych instytucjach (także tych, których nie jesteśmy stałym klientem).

53%

Polaków, słysząc o wyłudzeniu kredytu/pożyczki, dokonałoby zastrzeżenia numeru PESEL, a 50% zablokowałoby konta i karty płatnicze.

Działania po wykryciu wyłudzenia



źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

Klienci indywidualni

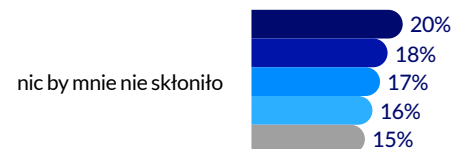
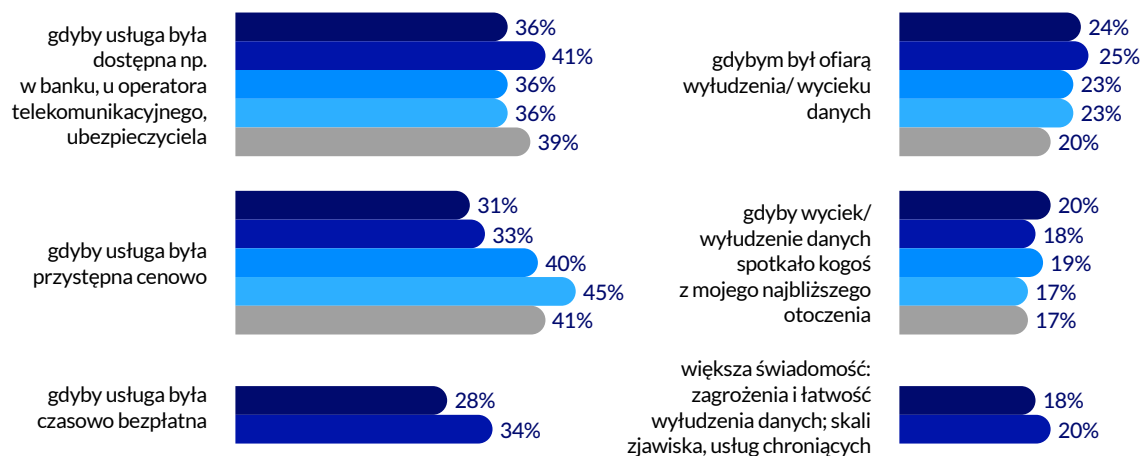
Reagowanie na wyłudzenia i ochrona przed nimi

Zapytani, co zachęciłoby ich do skorzystania z usługi ostrzegającej przed wyłudzeniem kredytów, pożyczek lub abonamentów, ankietowani najczęściej wymieniali łatwy dostęp, np. za pośrednictwem banku, operatora telekomunikacyjnego czy ubezpieczyciela, a także przystępną cenę usługi oraz możliwość bezpłatnego korzystania z niej przez pewien czas. Zatem sposób i jakość komunikacji, a także wygoda i użyteczność rozwiązań z zakresu cyberochrony ma kluczowe znaczenie w poprawie standardów bezpieczeństwa klientów.

Rok do roku wzrasta natomiast wskaźnik osób, deklarujących, że nic nie skłoni ich do korzystania z usług ostrzegających (od 15% w 2022 roku do 20% obecnie). To dość niepokojący trend, biorąc pod uwagę coraz bardziej wyrafinowane metody socjotechniczne, stosowane przez oszustów.



Czynniki zachęcające do skorzystania z usług ostrzegających - chroniących przed wyłudzeniem



● 2026 ● 2025 ● 2024 ● 2023 ● 2022

źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

Komentarz eksperta

Joanna Charlińska

Dyrektor Sprzedaży

w Departamencie Rynku Detalicznego BIK



Tegoroczne badania pokazują wyraźną rozbieżność między świadomością zagrożeń a działaniami podejmowanymi w celu ochrony przed nimi. Zaledwie 8% Polaków korzysta z narzędzi zabezpieczających przed wyłudzeniami, mimo że 61% obawia się takich przestępstw, a 79% uznaje wyciek danych za poważny problem.

Wciąż wiele osób zakłada, że wystarczy zachować ostrożność lub że problem ich nie dotyczy. To złudne poczucie bezpieczeństwa, zwłaszcza że oszuści nieustannie rozwijają swoje metody, wykorzystując zarówno tradycyjne schematy działania, jak i coraz bardziej zaawansowane techniki socjotechniczne oraz technologiczne.

Dlatego warto korzystać z dostępnych narzędzi wspierających ochronę danych. Przykładem jest weryfikacja behawioralna dostarczana przez BIK do 11 banków w Polsce. Rozwiązanie działa w tle, nie wymaga instalowania dodatkowej aplikacji i pozwala wykryć sytuacje, w których klient świadomie lub nieświadomie przekazuje kontrolę nad swoim urządzeniem osobie trzeciej lub gdy urządzenie zostaje przejęte bez jego wiedzy.

Nadal pokutuje przekonanie, że za nasze bezpieczeństwo odpowiadają wyłącznie banki czy instytucje państwowe. Tymczasem to użytkownik najczęściej staje się celem oszustów. Skuteczna ochrona wymaga więc współpracy i tzw. cyberhigieny, czyli własnych działań prewencyjnych. Dobrym przykładem są Alerty BIK, które informują o próbach wykorzystania naszych danych do zaciągnięcia kredytu, pożyczki, zakupów z odroczoną płatnością czy zawarcia umowy abonamentowej. Usługa ostrzega również o wykryciu naszych danych w darknetcie, pozwalając szybko zareagować na potencjalne zagrożenie.

Mimo to świadomość dostępnych rozwiązań pozostaje niewystarczająca. Co piąty Polak nie wie o istnieniu usług ostrzegających przed wyłudzeniami, a 32% uważa, że nie są im potrzebne. To pokazuje, że obok edukacji o zagrożeniach wciąż potrzebna jest edukacja dotycząca narzędzi, które pomagają skutecznie chronić dane i ograniczać ryzyko wyłudzeń.

Klienci indywidualni

Cyberzagrożenia budzące największe obawy Polaków

Ransomware i malware to typy ataków, które mogą prowadzić do utraty kontroli nad urządzeniem, kradzieży danych oraz strat finansowych.

- **Ransomware** to rodzaj złośliwego oprogramowania, które blokuje dostęp do komputera lub szyfruje dane zapisane na urządzeniu czy serwerze, a następnie wymusza zapłatę okupu za ich odblokowanie.
- **Malware** to z kolei szeroka grupa szkodliwego oprogramowania infekującego komputery, smartfony i tablety. Jego celem może być przejęcie kontroli nad urządzeniem, kradzież danych logowania czy uzyskanie dostępu do bankowości elektronicznej.

Zdaniem Polaków oba typy zagrożeń budzą szczególne obawy. Ponad połowa respondentów (52%) uważa, że w ostatnim roku wzrosło ryzyko ataków ransomware, natomiast 6 na 10 osób dostrzega wzrost zagrożenia związanego z infekowaniem urządzeń mobilnych w celu przejęcia dostępu do bankowości internetowej (58%) dostrzega. Co istotne, zagrożenia te często mają wymiar finansowy. Spośród osób, które zetknęły się z tego typu atakami, 9% przypadków ransomware oraz 11% infekcji urządzeń mobilnych zakończyło się stratą pieniędzy.



58%

Polaków uważa, że wzrosło ryzyko infekowania urządzeń mobilnych w celu przejęcia dostępu do bankowości

52%

Polaków dostrzega wzrost zagrożenia atakami ransomware

11%

ataków na urządzenia mobilne typu malware zakończyło się stratą finansową

9%

ataków typu ransomware doprowadziło do strat finansowych

Klienci indywidualni

Profilaktyka i ochrona przed wyłudzeniami

Dobrze radzimy sobie z rozpoznawaniem oczywistych zagrożeń, takich jak podejrzone wiadomości czy nieznane numery telefonów, jednak znacznie słabiej wypadamy w obszarze zaawansowanej cyberhigieny, czyli weryfikacji źródeł, adresów stron i sposobu instalowania oprogramowania, co pozostaje jednym z najczęściej wykorzystywanych przez cyberprzestępców wektorów ataku.

Pozytywnie należy ocenić fakt, że 68% Polaków deklaruje, że nigdy nie klika w linki przesyłane z nieznanych numerów lub reklam, a 67% nigdy nie otwiera załączników ani odsyłaczy od nieznanych nadawców. Ponadto ponad połowa badanych (55%) nie oddzwania na nieodebrane połączenia od nieznanych osób.

Poczucie bezpieczeństwa rośnie w przypadku komunikacji pochodzącej od pozornie zaufanych nadawców. Niemal co trzeci Polak (31%) przyznaje, że klika w linki otrzymywane w wiadomościach od znanych mu instytucji lub firm, takich jak bank czy dostawca energii. To szczególnie niebezpieczne, ponieważ właśnie pod zaufane marki najczęściej podszywają się oszuści prowadzący kampanie phishingowe.

Niepokojące są również luki w podstawowych nawykach związanych z weryfikacją źródła informacji. 22% badanych rzadko lub nigdy nie sprawdza adresu nadawcy wiadomości e-mail, natomiast 39% rzadko lub nigdy nie zwraca uwagi na adres strony internetowej, na którą wchodzi. Tymczasem fałszywe domeny i strony internetowe pozostają jednym z najskuteczniejszych narzędzi wykorzystywanych do wyłudzenia danych logowania oraz środków finansowych.

Największym sygnałem ostrzegawczym są jednak odpowiedzi dotyczące pobierania i instalowania oprogramowania. Aż 67% respondentów rzadko lub nigdy nie instaluje aplikacji bezpośrednio ze stron producentów lub dostawców, co może zwiększać podatność do pobrania złośliwego oprogramowania, przejęcia urządzenia lub uzyskania przez cyberprzestępców dostępu do bankowości elektronicznej.

67%

Polaków rzadko lub nigdy nie instaluje oprogramowania bezpośrednio ze stron producentów

39%

rzadko lub nigdy nie sprawdza adresu strony internetowej, na którą wchodzi

31%

klika w linki pochodzące od pozornie zaufanych nadawców

68%

nigdy nie klika w linki przesyłane z nieznanych numerów lub reklam

Klienci indywidualni

Profilaktyka i ochrona przed wyłudzeniami – analiza 2026 vs. 2025

Porównanie wyników z lat 2025 i 2026 pokazuje mieszany obraz. W części obszarów widać poprawę, że świadomość zagrożeń rośnie, ale nie zawsze przekłada się na konsekwencję w stosowaniu dobrych praktyk.

Na plus należy zaliczyć wzrost ostrożności wobec nieznanych załączników i odsyłaczy. Odsetek osób deklarujących, że nigdy nie otwierają załączników z nieznanych źródeł, wzrósł z 65% do 67%. Niewielką poprawę widać również w zakresie korzystania z publicznych sieci WiFi oraz instalowania oprogramowania bezpośrednio ze stron producentów, gdzie odsetek najbardziej pożądaných odpowiedzi wzrósł z 9% do 11%.

Pogorszyły się natomiast wyniki dotyczące kilku zachowań szczególnie istotnych z punktu widzenia ochrony przed phishingiem. Spadł odsetek osób, które nigdy nie klikają w linki przesyłane z nieznanych numerów lub reklam (68% vs. 71% rok wcześniej). Mniej osób zwraca uwagę na numer telefonu nadawcy SMS-a (43% vs. 50%) oraz na adres nadawcy wiadomości e-mail (39% vs. 44%). Negatywną zmianą jest także rzadsze sprawdzanie poprawności adresu strony internetowej przed wejściem na nią (22% vs. 25%).

-7 p.p.

spadek odsetka osób zwracających uwagę na numer telefonu nadawcy SMS-a

50% → 43%

-5 p.p.

spadek odsetka osób zwracających uwagę na adres nadawcy e-mail

44% → 39%

-3 p.p.

spadek odsetka osób, które nigdy nie klikają w linki od nieznanych nadawców

71% → 68%

+2 p.p.

wzrost odsetka osób, które nigdy nie otwierają załączników z nieznanych źródeł

65% → 67%

Klienci indywidualni

Sposoby ochrony urządzeń



Bezpieczeństwo smartfonów i komputerów postrzegane jest bardzo podobnie. W obu przypadkach za najważniejszą metodę ochrony uznawane jest unikanie otwierania wiadomości i załączników od nieznanych nadawców, a na drugim miejscu znajdują się silne hasła dostępu. Oznacza to, że respondenci coraz lepiej rozumieją znaczenie zagrożeń związanych z phishingiem i socjotechniką. Jednocześnie niżej oceniane są rozwiązania techniczne, takie jak uwierzytelnianie wieloskładnikowe, programy antywirusowe czy automatyczne aktualizacje, choć to właśnie one stanowią istotną warstwę ochrony przed współczesnymi cyberatakami.



Najważniejsze zabezpieczenia: Telefon

- Unikanie wiadomości i załączników od nieznanych nadawców (56%)
- Stosowanie bezpiecznych haseł (42%)
- Unikanie publicznych sieci WiFi (38%)

Trend r/r: w 2026 r. spadło znaczenie uwierzytelniania wieloskładnikowego (42% → 36%; -6 p.p.).



Najważniejsze zabezpieczenia: Komputer

- Unikanie wiadomości i załączników od nieznanych nadawców (55%)
- Stosowanie bezpiecznych haseł (44%)
- Korzystanie z oprogramowania antywirusowego (43%)

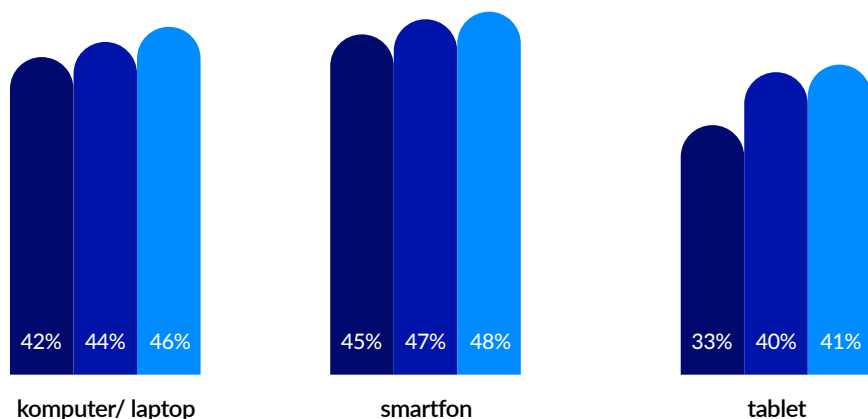
Trend r/r: w 2026 r. spadło znaczenie programów antywirusowych (50% → 43%; -7 p.p.) oraz uwierzytelniania wieloskładnikowego (40% → 35%; -5 p.p.).

Klienci indywidualni

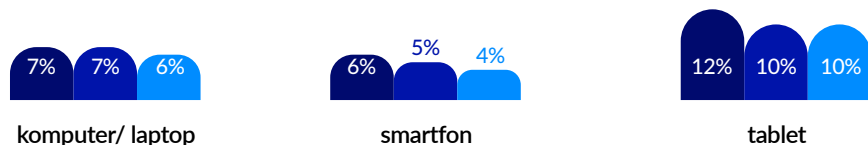
Cyberataki

Niestety, dane zebrane w 2024 i 2025 roku pokazują jednoznacznie, że użytkownicy wykazują mniejszą dbałość o aktualizowanie oprogramowania. Polacy najrzadziej aktualizują aplikacje w tabletach (33% automatycznie i 12% wcale), a najczęściej w smartfonach (45% automatycznie i 6% wcale).

Aktualizacja oprogramowania



Wcale nie aktualizuję

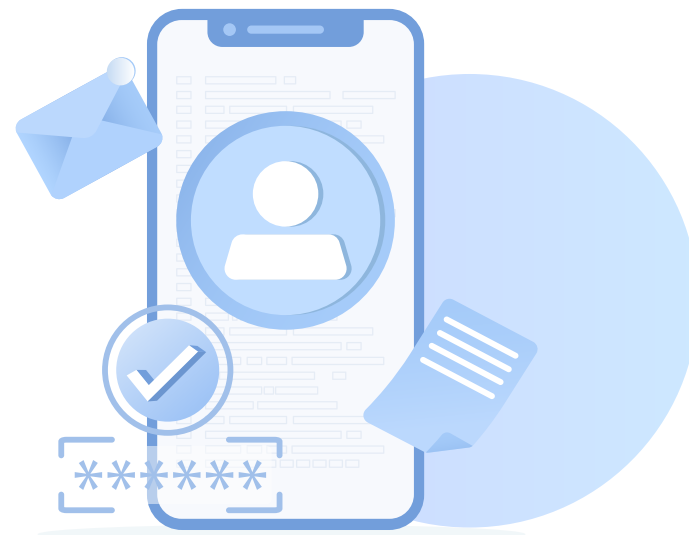


● 2026 ● 2025 ● 2024

źródło: „Badanie Cyberbezpieczeństwo Polaków 2026, kwiecień, Quality Watch”

16%

Polacy zabezpieczają własny telefon głównie kodem PIN (38%) lub odciskiem palca (34%), jednak 16% nie ma żadnej blokady ekranu w telefonie.



Komentarz eksperta

Robert Grabowski

Kierownik Wydziału CERT, Orange Polska



Od lat funkcjonuje przekonanie, że najłatwiejszym celem ataku jest człowiek, uznawany za najsłabsze ogniwo systemu bezpieczeństwa. To właśnie człowiek działa pod presją czasu, realizuje pilne płatności, mierzy się z codziennymi obowiązkami, emocjami i stresem. Dlatego jedną z kluczowych misji, które realizujemy w CERT Orange Polska, jest odwrócenie tej perspektywy.

Naszym celem jest wzmacnianie cyberodporności społeczeństwa i budowanie świadomości, dzięki którym człowiek staje się najmocniejszym, a nie najsłabszym elementem systemu bezpieczeństwa.

Wyposażeni w wiedzę i rzetelne informacje, dobre nawyki i świadomość zagrożeń, wspierani przez nowoczesne technologie, możemy skuteczniej chronić siebie i swoje otoczenie, szczególnie w momentach największej podatności na atak.

Budowa cyberodpornego społeczeństwa wymaga jednak znacznie więcej niż działań pojedynczej organizacji, grupy ekspertów czy nawet całego sektora. Cyberbezpieczeństwo powinno być elementem edukacji od najmłodszych lat. Również procesy biznesowe i komunikacja z użytkownikami powinny być projektowane z myślą nie tylko o wygodzie i prostocie, ale także o bezpieczeństwie.

Skutki zagrożeń fizycznych są zazwyczaj odczuwalne natychmiast, podczas gdy konsekwencje postępującej cyfryzacji nadal poznajemy, uczymy się rozumieć i właściwie oceniać. Dlatego zarówno sektor prywatny, jak i instytucje państwowe, powinny wspólnie wspierać społeczeństwo w budowaniu świadomości cyfrowych ryzyk, ich ograniczaniu oraz rozwijaniu kompetencji niezbędnych do bezpiecznego funkcjonowania w cyfrowym świecie.

Małe i średnie firmy

Rośnie skala zdarzeń fraudowych i cyberataków na firmy

Firmy z sektora małych i średnich przedsiębiorstw coraz częściej stają się celem oszustw oraz działań cyberprzestępczych. Najnowsze dane wskazują na wyraźny wzrost zarówno liczby incydentów fraudowych, jak i prób cyberataków.

W ciągu ostatnich 12 miesięcy wystąpienie zdarzeń fraudowych wskazało blisko 38 proc. przedsiębiorców, co oznacza wzrost o 5,8 pkt proc. w porównaniu z rokiem poprzednim. Jednocześnie zwiększyła się skala zagrożeń cybernetycznych. Odsetek firm deklarujących próby cyberataków wzrósł z 34,4 proc. do 39 proc., czyli o 4,6 pkt proc.

Zdarzenie fraudowe

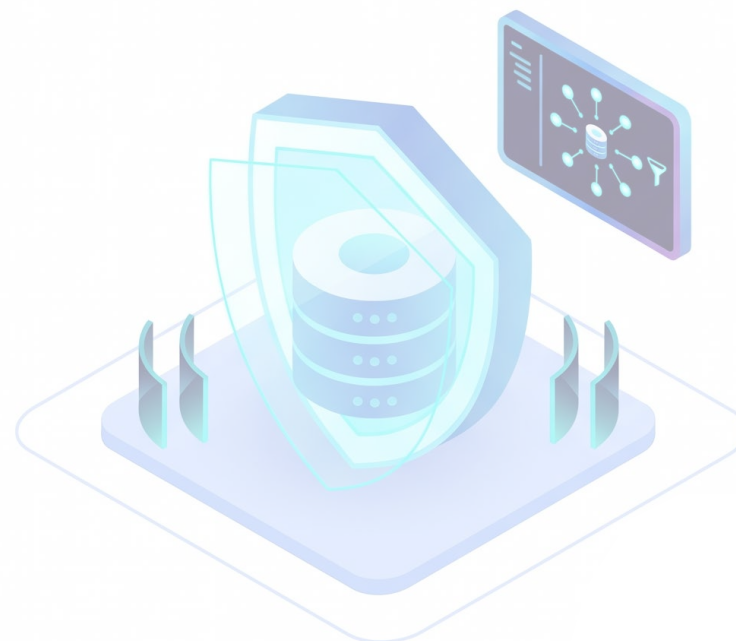
to działanie mające na celu wprowadzenie w błąd osoby lub organizacji w celu osiągnięcia korzyści finansowych lub innych nieuprawnionych korzyści. Najczęściej wykorzystuje techniki socjotechniczne i manipulację. Do przykładowych form fraudu należą kradzież tożsamości, phishing, podszywanie się pod zaufane instytucje czy wyłudzenia realizowane za pomocą fałszywych faktur.

Cyberatak

to celowe działanie zmierzające do uzyskania nieautoryzowanego dostępu do systemów informatycznych, sieci lub danych, a także do ich kradzieży, modyfikacji, zablokowania lub zniszczenia. Skutki cyberataków mogą obejmować wyciek poufnych informacji, straty finansowe, przejęcie tożsamości, zakłócenie ciągłości działania przedsiębiorstwa, a także przeciążenie infrastruktury cyfrowej, np. w wyniku ataków typu DDoS.

39%

Tylu przedsiębiorców wskazuje, że ich firmy stały się celem cyberataków



Małe i średnie firmy

Rodzaje oszustw i ataków

Najczęściej wskazywaną formą oszustwa są podejrzane wiadomości e-mail zawierające linki kierujące do płatności lub wirusy – co pokrywa się z danymi z segmentu klientów indywidualnych – na takie incydenty wskazuje 36,6% firm.

Wyraźnie wzrosła skala prób podszywania się pod różne podmioty - firmę, kontrahenta, bank. Odsetek takich wskazań zwiększył się z 21,1% do 34,6% - stanowi to największy wzrost spośród wszystkich analizowanych typów oszustw.

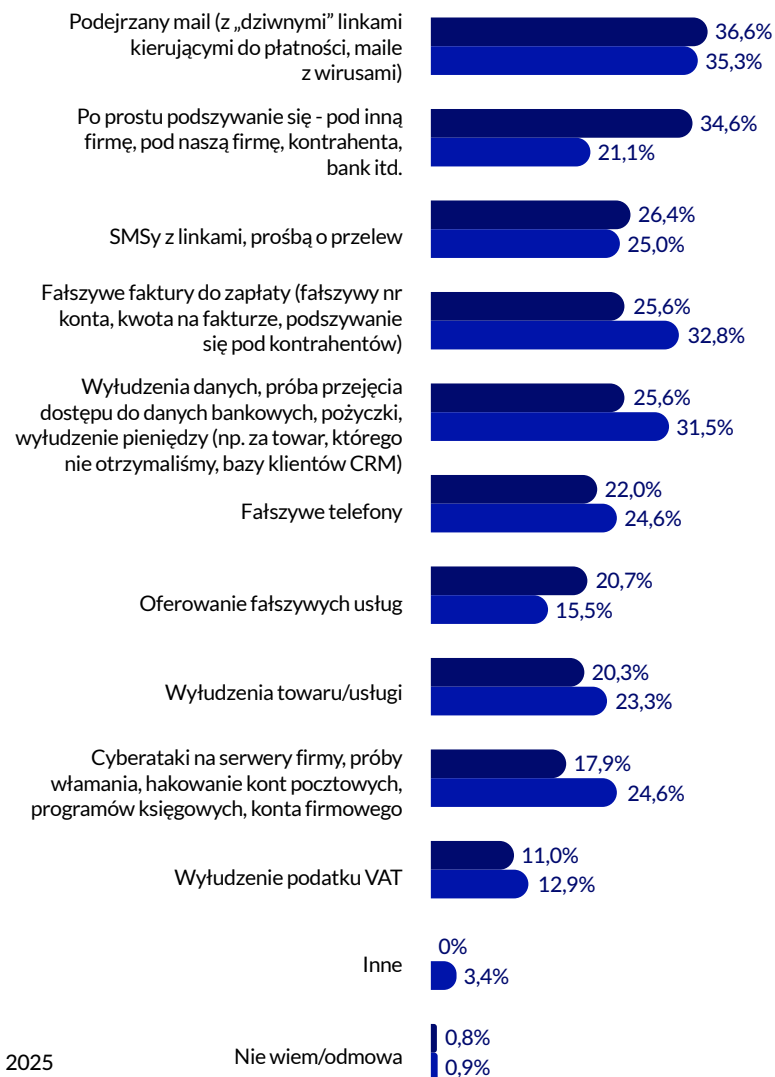
Jednocześnie znacząco spadły „Fałszywe faktury do zapłaty” i „Wyłudzenia danych, próba przejęcia dostępu do danych bankowych, pożyczki, wyłudzenie pieniędzy”.



13,5%

więcej prób phishingowych na firmy

Rodzaje oszustw wymierzonych w przedsiębiorstwa



● 2026 ● 2025

źródło: Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce, 2026, Keralla Research

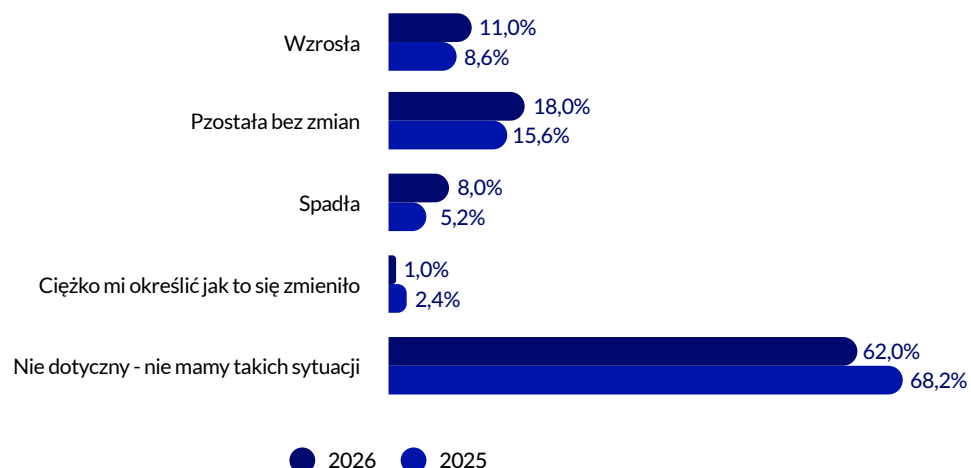
Małe i średnie firmy

Wzrost liczby prób wyłudzeń i oszustw

W 2026 r. pogłębia się zjawisko oszustw wymierzonych w przedsiębiorstwa. Odsetek firm wskazujących na nasilenie tego typu zagrożeń zwiększył się z 8,6 proc. do 11 proc.

Jednocześnie wzrósł udział przedsiębiorstw deklarujących, że liczba prób oszustw utrzymuje się na niezmiennym poziomie, z 15,6 proc. do 18 proc., co może świadczyć o utrwalaniu się problemu wyłudzeń i cyberzagrożeń, które stają się stałym elementem otoczenia biznesowego.

Dynamika skali wyłudzeń/oszustw w firmach



źródło: Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce, 2026, Keralla Research



Małe i średnie firmy

Skala realnych strat

Straty finansowe wynikające z oszustwa nie zawsze są wysokie, jednak dla małych i średnich firm bywają dotkliwe i mogą prowadzić do osłabienia zaufania oraz pogorszenia wizerunku firmy w relacjach z kontrahentami. Najczęściej wskazywana wartość strat mieści się obecnie w przedziale od 5 tys. do 10 tys. zł (27,7%).

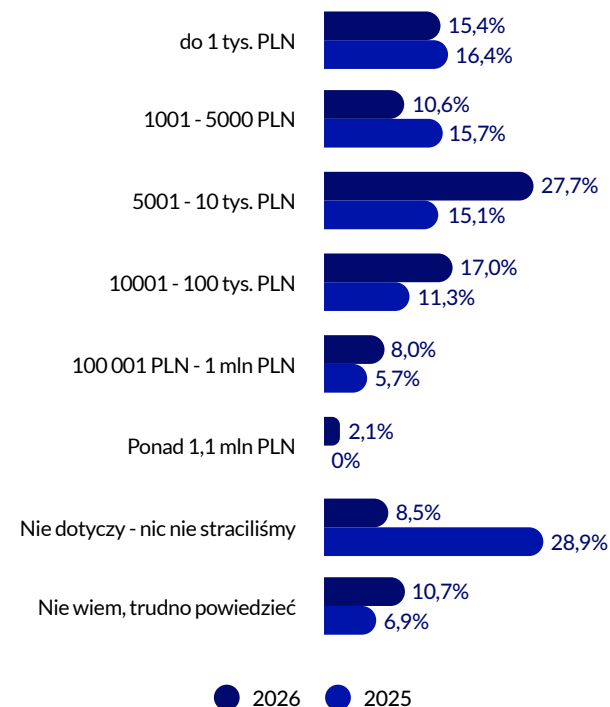
Wzrost odnotowano również w przypadku strat przekraczających 10 tys. zł, w tym powyżej 100 tys. zł.

Wyraźnie zmniejszył się natomiast odsetek firm deklarujących brak strat związanych z oszustwami – z 28,9% do 8,5%.

17%

przedsiębiorstw zgłaszających wartość poniesionych strat w przedziale od 10 tys. do 100 tys. zł.

Wartość strat w wyniku dokonanych oszustw



źródło: „Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce, 2026, Keralla Research”

Komentarz eksperta

Olga Wiszowata

Naczelnik Wydziału Regulacji Cyberbezpieczeństwa
i Chmury Obliczeniowej, Departament
Cyberbezpieczeństwa, Ministerstwo Cyfryzacji



Ataki hakerskie na MŚP, placówki medyczne i szeroko rozumiany sektor publiczny, skutkujące wyciekami danych, to nie tylko wyzwanie społeczne, ale przede wszystkim realne obciążenie dla polskiej gospodarki. Cyberbezpieczeństwo organizacji jest obecnie filarem stabilności rynkowej, a każde naruszenie w strukturze tego filaru niesie za sobą długofalowe konsekwencje, tak finansowe, jak i operacyjne.

Każdy cyberatak generuje koszty dla organizacji, zarówno te bezpośrednie za brak należytej ochrony danych osobowych, przestoje w działaniu podmiotu, odtworzenie po awarii oraz powrót do niezakłóconego działania, jak i te, które choć bezpośrednio finansowego charakteru nie mają, to dla każdego przedsiębiorcy i instytucji są równie ważne. Jest to przede wszystkim utrata zaufania odbiorców czy obniżenie wartości rynkowej firmy.

W porównaniu z krajami UE, Polska dysponuje zaawansowanymi rozwiązaniami w obszarze cyfryzacji usług państwowych. Mamy możliwość zastrzeżenia numeru PESEL w aplikacji mObywatel, co stanowi wzór prewencji w walce z fraudami. Uruchomiliśmy portal bezpiecznedane.gov.pl, gdzie każdy obywatel może sprawdzić, czy jego dane uległy wyciekowi, a także zapoznać się z rekomendacjami, co do dalszego postępowania, jeśli dane rzeczywiście zostały upublicznione. Działania podejmowane w obszarze edukacji i monitorowania zagrożeń stawiają Polskę w czołówce państw dbających o e-usługi i cyfrowe bezpieczeństwo obywateli. Mamy również skutecznie działającą ustawę o zwalczaniu nadużyć w komunikacji elektronicznej. W 2025 r. CSIRT NASK opublikował 790 wzorców złośliwych wiadomości, a w 2026 r. ten trend jest wzrostowy, co umożliwia efektywną walkę ze smishingiem. Wdrożyliśmy też rozwiązania Bezpiecznej Zatoki umożliwiającej przedsiębiorcom telekomunikacyjnym identyfikację, wymianę informacji oraz blokowanie fałszywych połączeń. W roku 2025 średnia liczba połączeń blokowanych lub z ukrytą prezentacją numeru przekraczała 5 mln tygodniowo. Dane tylko za pierwsze 4 miesiące 2026 r. zrównały się z tymi za cały rok 2025, co pokazuje skalę problemu, ale i intensywność podejmowanych działań.

Głównym wyzwaniem pozostaje jednak sektor MŚP oraz JST. O ile duże korporacje i administracja centralna, mają świadomość oraz możliwości wdrażania wymagań cyberbezpieczeństwa, o tyle MŚP i JST wciąż borykają się z brakiem środków oraz wykwalifikowanych kadr. Jest to obszar wymagający naszego szczególnego wsparcia na wielu płaszczyznach, np. przy wdrożeniu wymagań krajowego systemu cyberbezpieczeństwa, zacieśnianiu współpracy organów ścigania i instytucji rządowych, a także przy tworzeniu dedykowanych programów wsparcia i edukacji ukierunkowanych bezpośrednio na te podmioty.

Małe i średnie firmy

Największe obawy przedsiębiorców

Analizując swoje systemy bezpieczeństwa, przedsiębiorcy dostrzegają ryzyko występowania luk w różnych obszarach działalności firmy. Za największe zagrożenie uznają dziś cyberataki, czyli próby wykorzystania słabości infrastruktury IT i oprogramowania. To obawa szczególnie powszechna – wskazuje na nią co trzeci przedsiębiorca, czyniąc z cyberataków najczęściej wymieniane zagrożenie dla bezpieczeństwa firmy. Podobny odsetek ankietowanych (28%) za potencjalnie największe ryzyko uznaje kradzież danych klientów oraz wyprowadzenie informacji z firmy. Ten aspekt podnoszą przede wszystkim średnie firmy, zatrudniające od 50 do 249 pracowników. Dla co czwartego przedsiębiorstwa (26%) potencjalnym ryzykiem pozostaje również utrata towaru.

31%

przedsiębiorstw wskazuje cyberataki wykorzystujące luki w systemach IT jako największe zagrożenie dla swojej działalności. Obawy właścicieli obejmują też kradzież danych klientów oraz wyprowadzanie informacji z firmy.

Potencjalne największe ryzyka dla firmy (niezależnie od profilu działalności).



źródło: „Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce, 2026, Keralla Research”

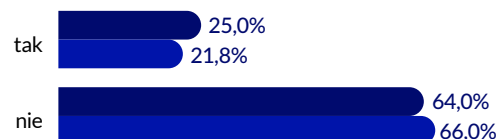
Małe i średnie firmy

Ochrona firm przed fraudami

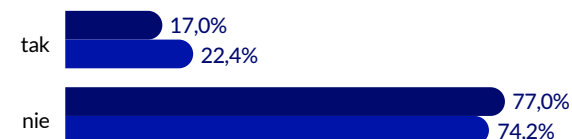
Mimo złych doświadczeń, a także realnych strat, tylko co czwarta firma z sektora mikro, małych i średnich przedsiębiorstw korzysta z usług antyfraudowych. Widoczny jest co prawda niewielki wzrost w stosunku do ubiegłego roku (+3,2 pkt proc.), ale jednocześnie spadł odsetek firm (-5,4 pkt proc.), które korzystały w tym zakresie z usług firm zewnętrznych.

Korzystanie z usług i narzędzi antyfraudowych

Czy aktualnie korzystają Państwo z usług/narzędzi antyfraudowych?



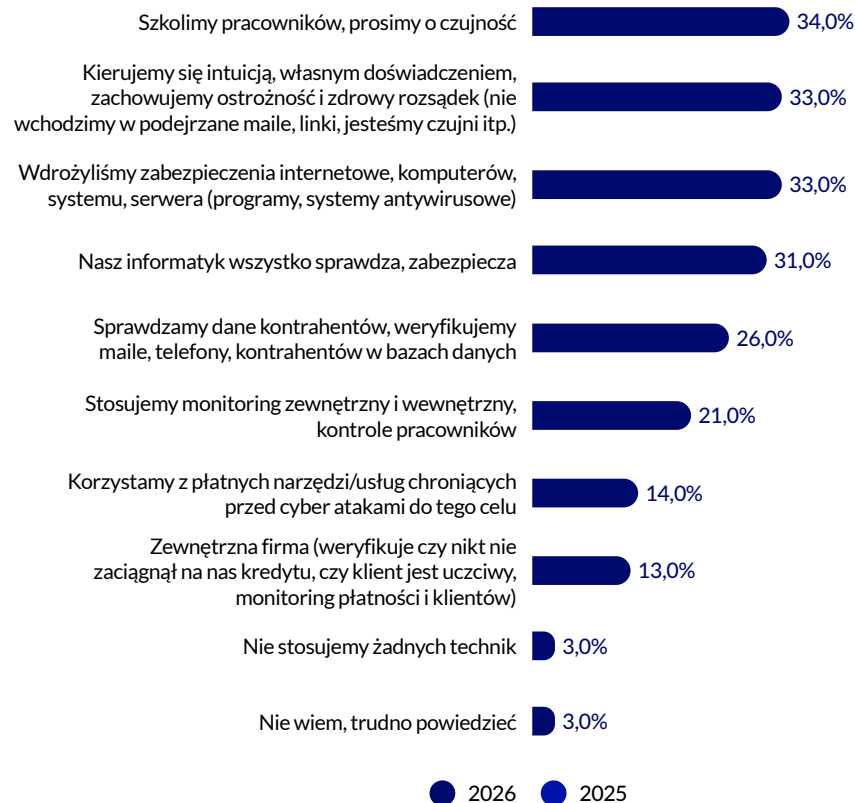
Czy zatrudniają Państwo firmę zewnętrzną odpowiedzialną za przeciwdziałanie wyłudzeniom?



● 2026 ● 2025

Najczęściej stosowanymi metodami przeciwdziałania fraudom są szkolenia pracowników (34%) oraz intuicja, doświadczenie i zdrowy rozsądek (33%). Taki sam odsetek firm stawia na dodatkowe zabezpieczenia internetowe, a także wsparcie specjalistów IT w firmie w zakresie bezpieczeństwa (31 proc.).

Sposoby ochrony przed wyłudzeniami stosowane w firmach



● 2026 ● 2025

źródło: „Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce, 2026, Keralla Research”

Małe i średnie firmy

Bariery, obszary wsparcia firm i ich oczekiwania

Firmy, które doświadczyły zdarzeń fraudowych, coraz częściej dostrzegają, że same szkolenia pracowników, działania prewencyjne działów IT oraz czujność personelu to nie jest wystarczająca ochrona. Przedsiębiorcy oczekują przede wszystkim konkretnych rozwiązań technologicznych i systemowych.

Co trzecia firma wskazuje na potrzebę stworzenia ogólnodostępnych baz oszustów, nierzetelnych kontrahentów i dłużników (32 proc.). Równie istotne są bardziej restrykcyjne przepisy rynkowe oraz skuteczniejsze egzekwowanie prawa wobec sprawców oszustw. Jednocześnie przedsiębiorcy podkreślają, że działania technologiczne powinny być uzupełniane ogólnodostępną edukacją, w tym szkoleniami pracowników oraz kampaniami informacyjnymi dotyczącymi zagrożeń fraudowych.

32%

Już 32 proc. firm, które doświadczyły fraudów, wskazuje wysokie koszty jako główne ograniczenie, wobec 19,5 proc. rok wcześniej. Wynikają one głównie z kosztów i braków kadrowych. Co czwarta firma podkreśla niedobór specjalistów IT, programistów i analityków antyfraudowych niezbędnych do skutecznego wdrażania takich rozwiązań.

32%

firm, które doświadczyły prób wyłudzeń uważa, że skutecznym sposobem ograniczenia tego typu zagrożeń byłoby stworzenie ogólnodostępnych baz oszustów, dłużników i tzw. czarnych list. Przedsiębiorcy oczekują również zaostrzenia przepisów oraz większej skuteczności organów ścigania w zwalczaniu sprawców takich przestępstw.

Rozwiązania, które pomogłyby zwiększyć ochronę przed nadużyciami



Komentarz eksperta

Karol Głogowski

Dyrektor IT Usług Antyfraudowych BIK



Małe i średnie firmy bardzo często nie dysponują wystarczającymi środkami, które pozwoliłyby na pełną ochronę antyfraudową. To przecież małe sklepy, zakłady fryzjerskie czy niewielkie firmy transportowe. Jednocześnie firmy o tej skali mogą nie dostrzegać problemu wyłudzeń, a co za tym idzie, wydaje im się, że nie potrzebują narzędzi i usług ochronnych. To się jednak zmienia.

Pozytywnym sygnałem jest to, że co trzeci mały przedsiębiorca deklaruje samodzielne radzenie sobie z cyberzagrożeniami. Firmy inwestują w edukację i szkolenia pracowników, a to właśnie wiedza zespołu pozostaje jednym z najskuteczniejszych elementów ochrony. Niepokoi jednak fakt, że równie wielu przedsiębiorców opiera swoje działania głównie na intuicji i „zdrowym rozsądku”. Są one ważne, ale nie powinny stanowić podstawy systemu bezpieczeństwa, zwłaszcza w obliczu coraz bardziej zaawansowanych metod oszustw. Warty podkreślenia jest fakt, że wciąż wiele firm nie stosuje żadnych zabezpieczeń ani narzędzi przeciwdziałających fraudom. Niewiele organizacji korzysta też ze wsparcia zewnętrznych ekspertów, choć taki niezależny audyt pozwala skutecznie ocenić poziom ochrony i zidentyfikować słabe punkty. Wreszcie, zaobserwować możemy także istotną barierę psychologiczną w postaci budżetu. Jeśli przez lata firma nie doświadczała ataku ani próby oszustwa, łatwo jej uznać, że obecne zabezpieczenia są wystarczające, a wydatki na cyberbezpieczeństwo niepotrzebne.

Wróćmy jednak do zmian, które zachodzą na rynku cyberprzestępczości, które mogą mieć znaczące konsekwencje dla sektora MŚP. W związku z tym, że duże firmy, instytucje finansowe czy korporacje coraz częściej stosują bardzo mocne i skuteczne zabezpieczenia, cyberzłodzieje coraz częściej kierują swoją uwagę na mniejsze firmy. Zadowolają się mniejszymi „zyskami”, ale za to osiąganymi częściej. Naturalną ofiarą są więc małe i średnie firmy, które – jak pokazują badania – podchodzą do systemów ochrony nieco mniej restrykcyjnie. I jeżeli dzisiaj MŚP radzą sobie z fraudami zadowolająco, to wcale nie oznacza, że tak będzie za rok czy za dwa lata.

Korporacje

Skala zdarzeń fraudowych

Instytucje finansowe, w tym duże korporacje, mimo ogromnych budżetów i zaangażowania w ochronę antyfraudową i cybernetyczną, nie są wolne od ataków, w tym także skutecznych.

W ocenie niemal połowy dużych firm (46%) liczba zdarzeń fraudowych w ciągu minionego roku pozostawała na podobnym poziomie, jednak co trzecia badana organizacja (37%) odnotowała wzrost prób ataków. Takie wyniki utrzymują się od kilku lat.

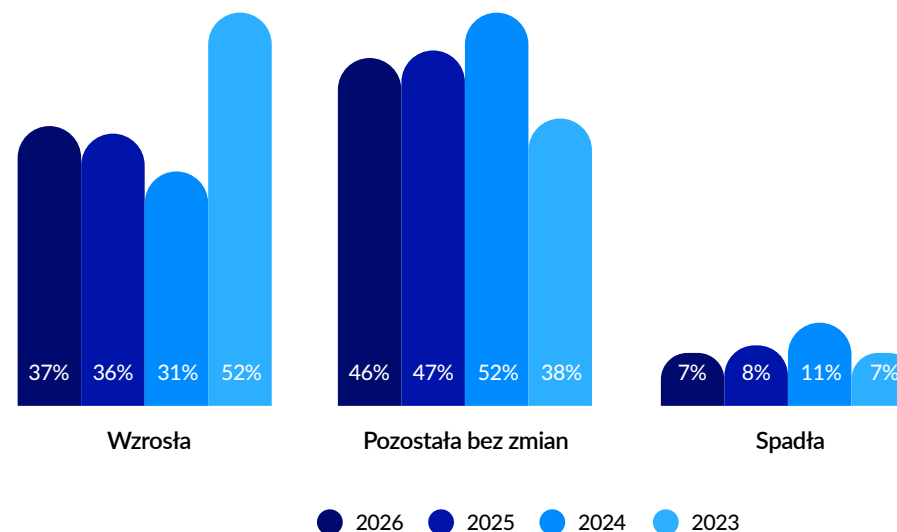
Co warto odnotowania, w ubiegłorocznych badaniach zaledwie 6% instytucji nie stwierdziło u siebie tego typu zagrożeń, co potwierdza powszechność problemu. Jednak w roku 2026 już co dziesiąta badana korporacja (10%) zadeklarowała, że nie miała takiej sytuacji.

46%

przedstawicieli korporacji uważa, że liczba zdarzeń fraudowych pozostaje bez zmian



Skala zdarzeń fraudowych w korporacjach i instytucjach finansowych



źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

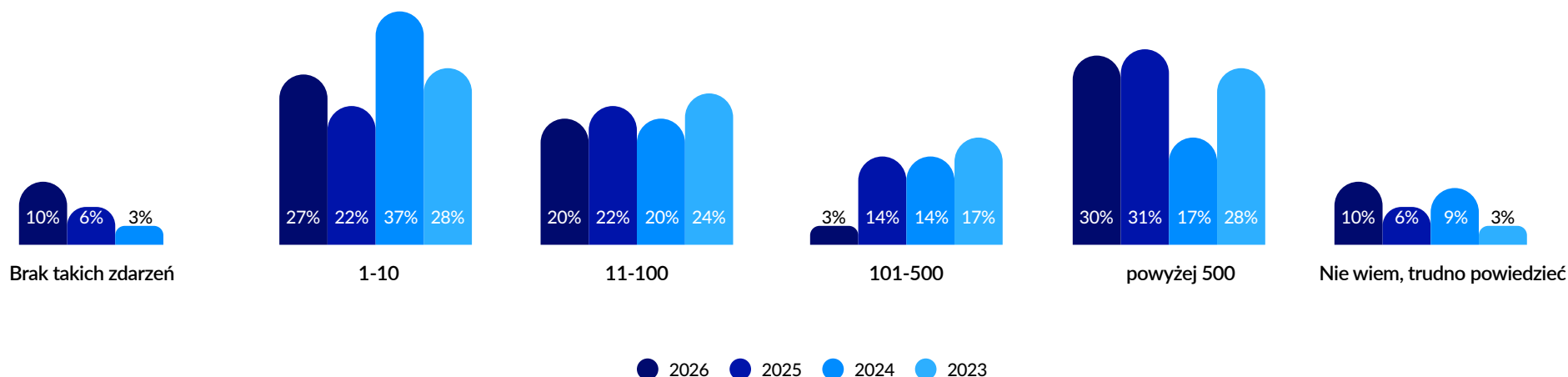
Korporacje

Skala zdarzeń fraudowych

Z zestawienia wynika, że w minionym roku do ataków na instytucje dochodziło masowo. Największą grupę ankietowanych (30%) stanowią organizacje, które odnotowały powyżej 500 zdarzeń fraudowych w ciągu 12 miesięcy, co oznacza, że do próby oszustwa dochodziło w co trzeciej korporacji prawie dwa razy dziennie.



Liczba zdarzeń fraudowych w ciągu roku



źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

Korporacje

Korporacje walczą z oszustami

Zdarzenia fraudowe, z którymi firmy spotykają się najczęściej, to wyłudzenia finansowania (70%), których liczba w stosunku do ubiegłego roku znacząco wzrosła (+8 pkt proc.). Bardzo często dochodzi także do transakcji oszukańczych wynikających z ataków na klientów z wykorzystaniem socjotechniki (52%). Tu jednak widać wyraźny spadek deklarowanych przypadków (-19 pkt proc.).

Znacząco spadł także odsetek nadużyć popełnionych przez klientów, innych niż wyłudzenie finansowania (-14 pkt proc.).

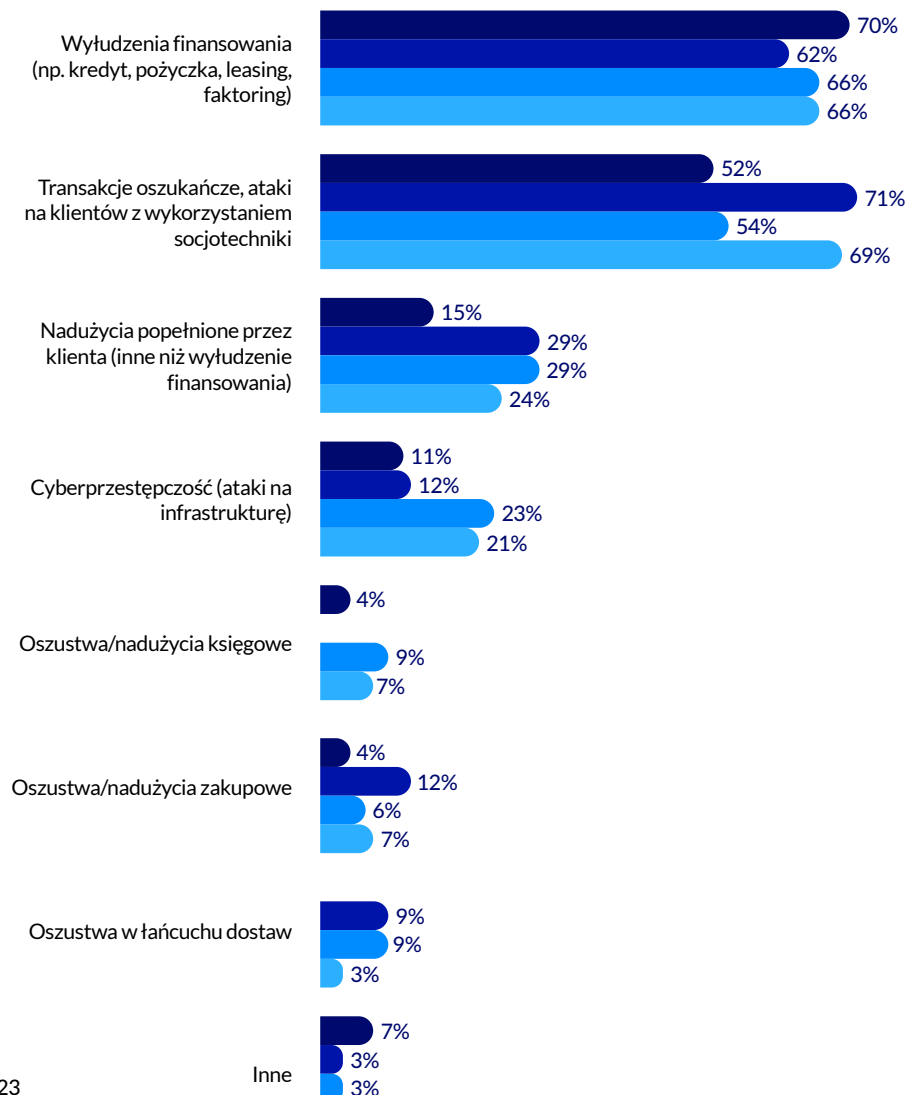
70%

zdarzeń fraudowych, z którymi firmy spotykają się najczęściej, to wyłudzenia finansowania – kredytów, pożyczek, leasingu, faktoringu. To wzrost o 8 pkt proc. względem 2025 roku.

● 2026 ● 2025 ● 2024 ● 2023

źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

Rodzaje zdarzeń fraudowych w instytucjach finansowych i korporacjach



Komentarz eksperta

Paweł Piekutowski

Zastępca Dyrektora Departamentu Cyberbezpieczeństwa,
Urząd Komisji Nadzoru Finansowego



Analizy prowadzone przez CSIRT KNF wskazują, że cyberprzestępczość finansowa staje się coraz bardziej zorganizowana i profesjonalna. Zmieniają się nie tylko wykorzystywane techniki, ale również sposób planowania i prowadzenia kampanii oszustw. Coraz częściej są one zautomatyzowane, realizowane równolegle w wielu kanałach komunikacji oraz oparte na precyzyjnie przygotowanych scenariuszach socjotechnicznych.

Jednym z najważniejszych trendów jest dynamiczny rozwój generatywnej sztucznej inteligencji. Modele językowe pozwalają cyberprzestępcom szybciej tworzyć wiarygodne treści, personalizować komunikację oraz przygotowywać coraz bardziej przekonujące scenariusze oszustw. Jednocześnie automatyzacja oraz łatwa dostępność narzędzi opartych na AI obniżają próg wejścia do cyberprzestępczości, umożliwiając prowadzenie skutecznych kampanii także osobom posiadającym znacznie mniejsze kompetencje techniczne.

Równolegle obserwujemy dalszą profesjonalizację zorganizowanych grup przestępczych. Coraz częściej działają one jak przedsiębiorstwa, wykorzystując model Cybercrime-as-a-Service, automatyzację oraz sztuczną inteligencję do prowadzenia kampanii na dużą skalę. Jednocześnie przestępcy coraz chętniej wykorzystują legalne platformy reklamowe i media społecznościowe, co znacząco utrudnia wykrywanie oraz blokowanie oszustw. Trend ten był wyraźnie widoczny również w analizach prowadzonych przez CSIRT KNF w 2025 roku.

W odpowiedzi na ewolucję zagrożeń coraz większego znaczenia nabiera współpraca całego sektora finansowego. Szybka wymiana informacji, wspólne działania z operatorami usług cyfrowych oraz bieżąca analiza nowych technik cyberprzestępców pozwalają skuteczniej ograniczać skalę oszustw. Równie ważna pozostaje edukacja klientów, ponieważ nawet najlepsze rozwiązania techniczne nie zastąpią świadomości zagrożeń.

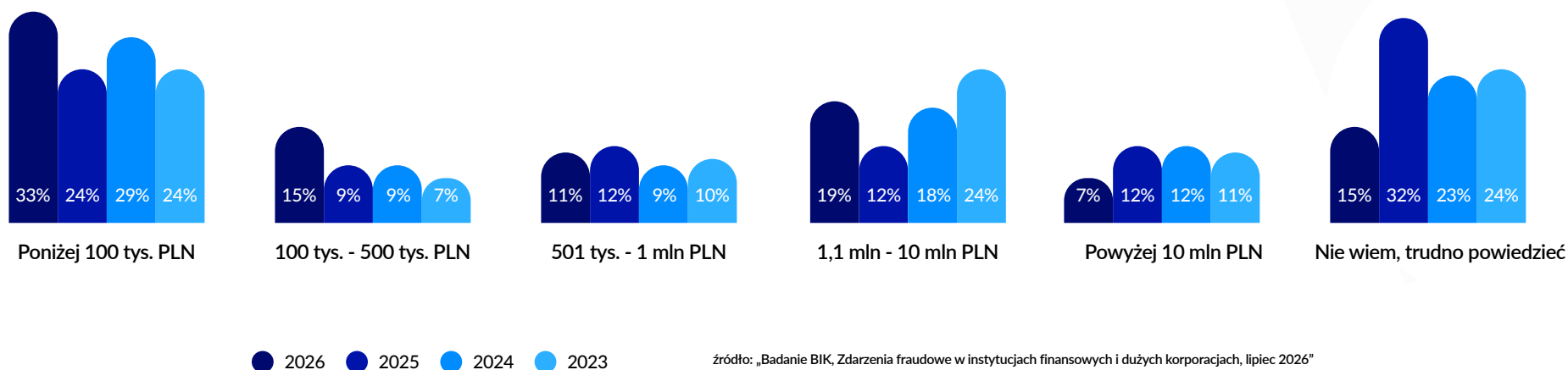
W najbliższych latach o skuteczności ochrony rynku finansowego będzie decydowała przede wszystkim zdolność do szybkiej adaptacji do nowych metod działania cyberprzestępców oraz efektywna współpraca pomiędzy instytucjami finansowymi, administracją publiczną i dostawcami usług cyfrowych.

Korporacje

Skala realnych strat w wyniku wyłudzeń

Straty poniesione z tytułu zdarzeń fraudowych, których nie udało się zatrzymać, w przypadku jednej trzeciej firm nie przekraczają 100 tys. zł (33%), jednak w przypadku 26% podmiotów przekraczają kwotę miliona złotych, w tym 7% stanowią firmy ze stratami przekraczającymi 10 mln zł. Powiewem optymizmu może być fakt, że w stosunku do 2025 roku skala strat uległa obniżeniu.

Wysokość strat poniesionych wskutek wyłudzeń



Korporacje

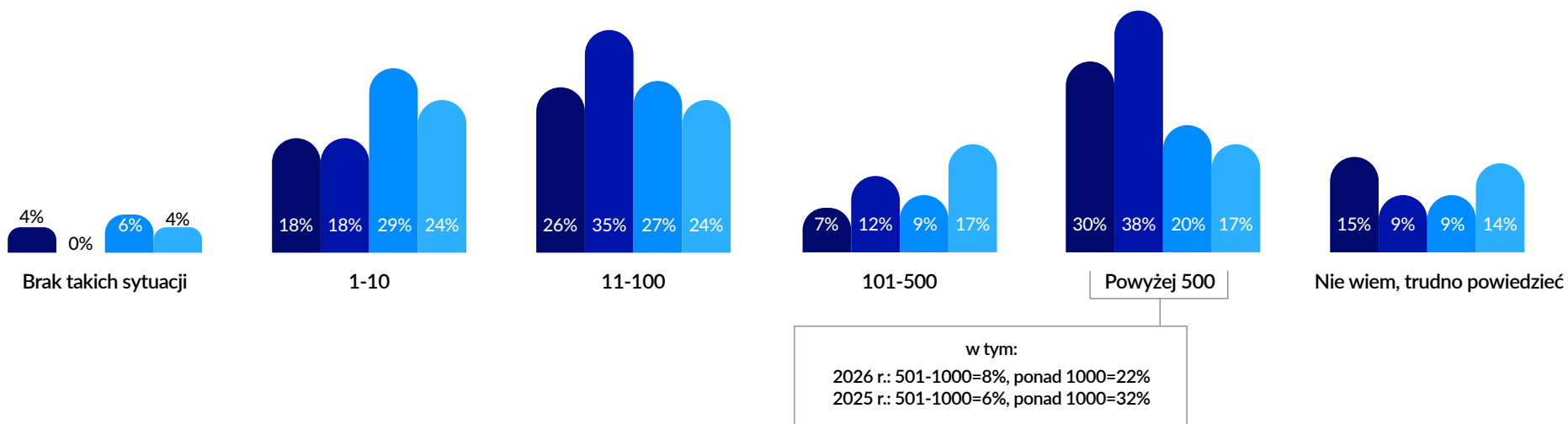
Skuteczność w walce z fraudami

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

Co trzecia firma, która odnotowywała zdarzenia fraudowe zadeklarowała, że w ostatnim roku zablokowała ponad 500 tego typu zdarzeń (30%).



Liczba zablokowanych prób wyłudzeń



● 2026 ● 2025 ● 2024 ● 2023

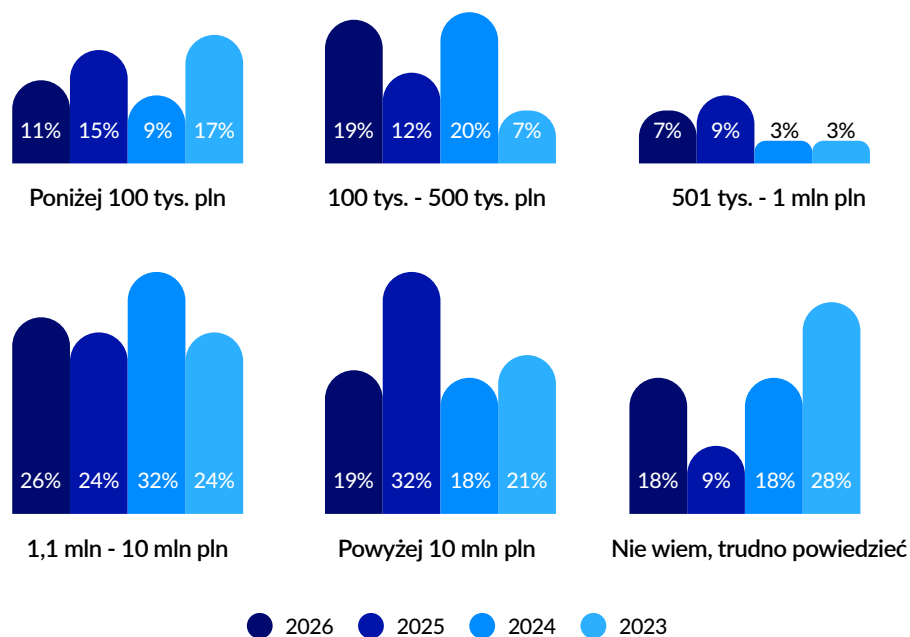
źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

Korporacje

Skuteczność w walce z fraudami

Skalę zjawiska potwierdzają również potencjalne straty, których udało się uniknąć dzięki wykryciu i zablokowaniu prób oszustw. W przypadku niemal co piątej firmy (19%) udaremnione wyłudzenia pozwoliły zapobiec stratom przekraczającym 10 mln zł. Jest to wynik istotnie niższy niż w 2025 roku, kiedy odsetek ten wynosił 32%. Łącznie 45% przedsiębiorstw wskazało, że dzięki skutecznemu przeciwdziałaniu oszustwom uniknęło strat przekraczających 1 mln zł.

Wartość strat powstrzymanych dzięki zablokowaniu wyłudzeń



źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

Komentarz eksperta

Andrzej Zduńczyk

Dyrektor Rynku Instytucji Finansowych BIK



Tegoroczne badanie przyniosło nam wiadomość, że wśród badanych korporacji, które w ostatnim roku doświadczyły zdarzeń fraudowych, niemal 26 proc. poniosło straty przekraczające milion złotych, a 7 proc. – wyższe niż 10 mln zł. Jednocześnie 45 proc. oceniło wartość strat unikniętych dzięki zablokowaniu fraudów na ponad milion złotych, a niemal co piąty podmiot – na ponad 10 mln zł.

Równie istotne jak straty realne są więc straty hipotetyczne, czyli środki, które zostałyby utracone, gdyby próba wyłudzenia nie została wykryta.

Co więcej, skutki oszustw wykraczają poza bezpośrednie straty finansowe i obejmują również koszty operacyjne oraz potencjalne szkody wizerunkowe.

W zakresie ochrony antyfraudowej każda instytucja ma własne procedury, systemy i zespoły bezpieczeństwa. Istotnym uzupełnieniem działań prowadzonych przez poszczególne instytucje są rozwiązania sektorowe, które pozwalają identyfikować schematy oszustw widoczne dopiero z perspektywy całego rynku.

Taką funkcję na etapie analizy wniosków pełni Platforma Antyfraudowa BIK. Od jej uruchomienia w 2017 r. do końca czerwca 2026 r. uczestniczące w niej instytucje uniknęły strat o wartości 1,8 mld zł. Każdy kolejny uczestnik zwiększa skuteczność wykrywania powtarzających się schematów oszustw. Wprawdzie alert wygenerowany przez system nie przesądza o fraudzie i nie zastępuje decyzji analityka, jednak pozwala skierować uwagę na zdarzenie, które wymaga dodatkowego sprawdzenia.

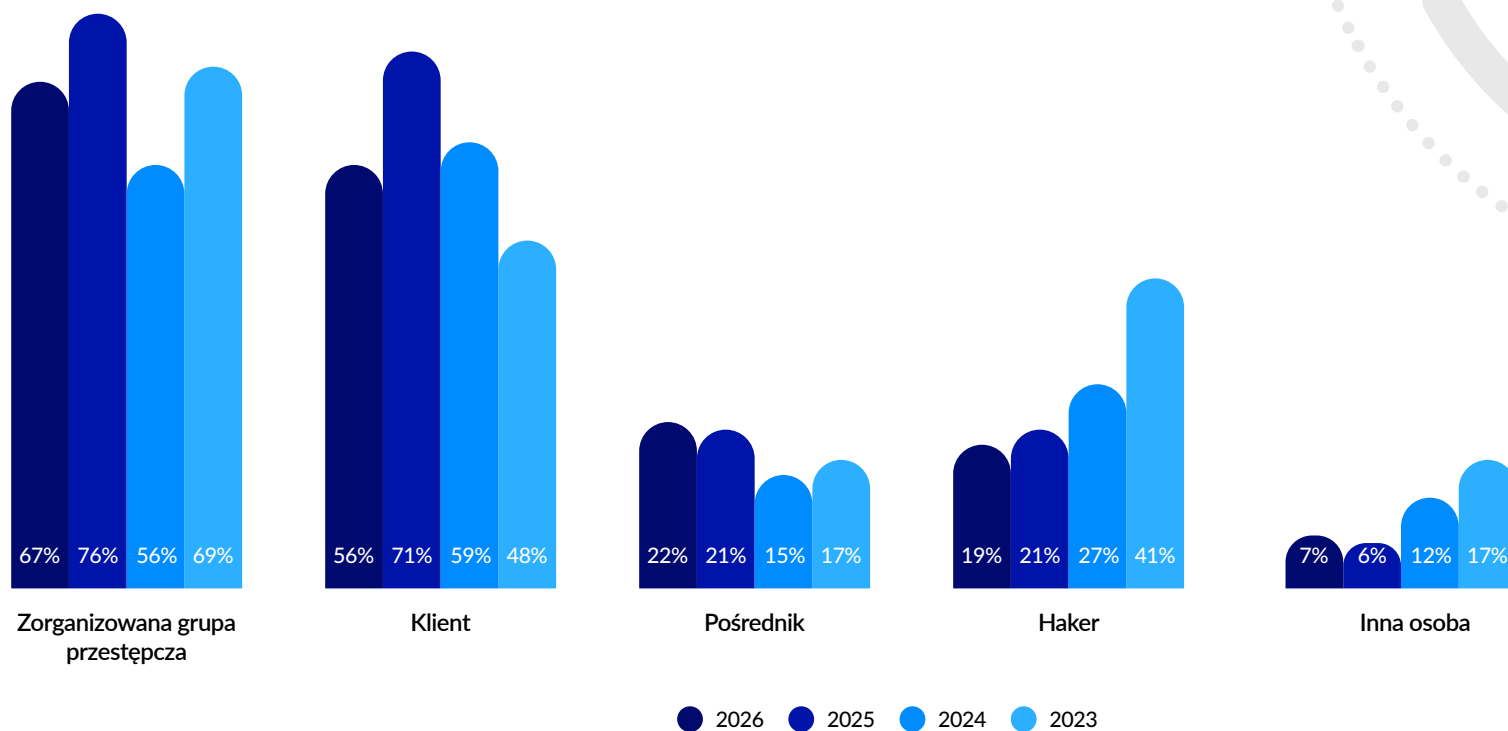
Choć najbardziej widoczne są straty finansowe, w dłuższej perspektywie równie dotkliwe mogą okazać się konsekwencje związane z utratą zaufania klientów. Jej konsekwencje są rozłożone w czasie i mogą dotyczyć znacznie większej grupy klientów niż samo zdarzenie.

Korporacje

Sprawcy oszustw i wyłudzeń w instytucjach finansowych i dużych korporacjach

Jako zewnętrznych sprawców ataków fraudowych w 2026 roku najczęściej wskazywano na zorganizowane grupy przestępcze (67%), a w drugiej kolejności na klientów (56%). W obu przypadkach spadł deklarowany udział tych grup w stosunku do 2025 roku. Wzrósł natomiast – choć nieznacznie – udział pośredników w przestępczym procederze.

Najczęściej wskazywani sprawcy oszustw



źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”



Korporacje

Metody walki z fraudami

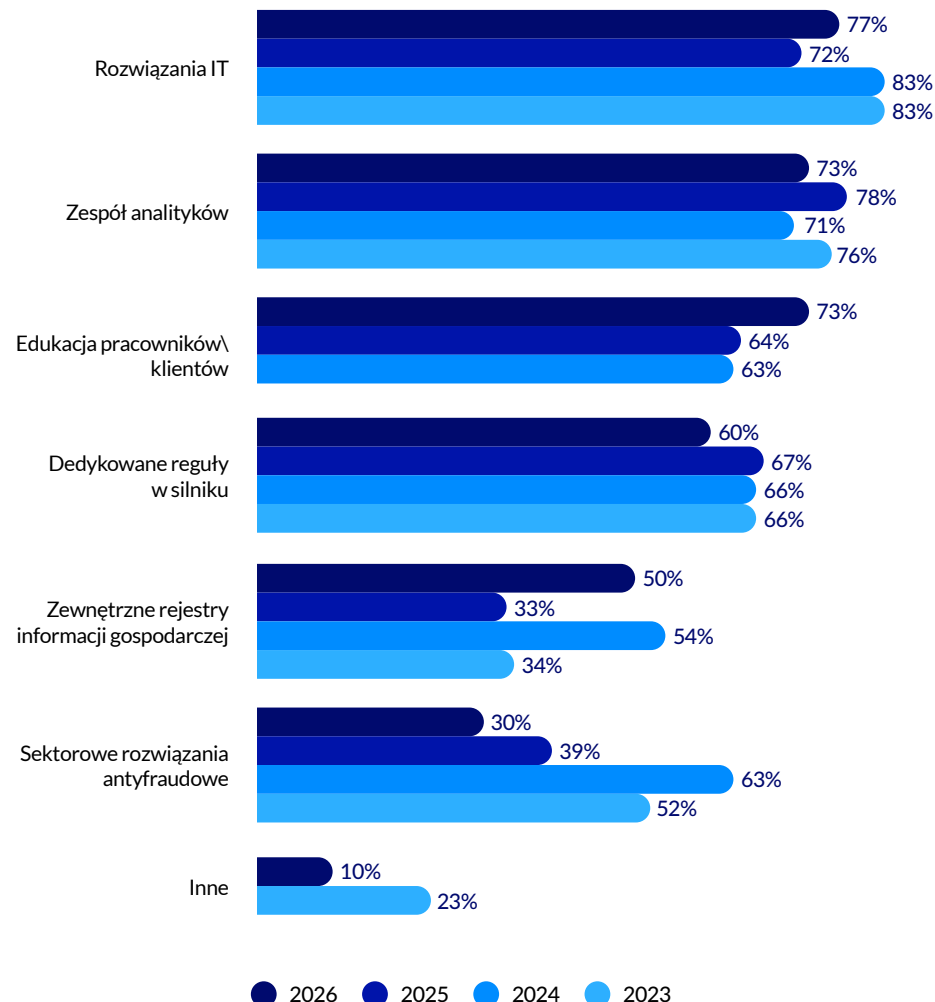
Za najskuteczniejsze działania zapobiegające tego typu zdarzeniom przedstawiciele firm uznają rozwój i wzmacnianie rozwiązań IT (77%). Zadeklarowało tak więcej badanych niż rok temu (+5 pkt proc.), choć wcześniej wskaźnik ten wynosił 83%.

Równie ważni – z punktu widzenia korporacji – są specjaliści i zespoły analityczne (73%), Coraz większą rolę odgrywa także edukacja pracowników i klientów (73%; +9 pkt proc.).

73%

korporacji stawia na edukację klientów i pracowników - odsetek wskazań wzrósł o 9% r/r. Zdaniem przedstawicieli instytucji i korporacji w walce z oszustwami w największym stopniu decydują nowoczesne rozwiązania IT.

Rozwiązania zapobiegające zdarzeniom fraudowym



źródło: „Badanie BIK, Zdarzenia fraudowe w instytucjach finansowych i dużych korporacjach, lipiec 2026”

Komentarz eksperta

Piotr Wojewnik

Dyrektor Data Science BIK,
Członek Zarządu Digital Fingerprints



Sektor finansowy obserwuje coraz silniejszą profesjonalizację ataków fraudowych. Zarówno narzędzia ataku, jak i wykorzystywane schematy psychologiczne, są coraz bardziej dopracowane i zindywidualizowane. Oszuści dopasowują się do informacji o atakowanej osobie na podstawie wyłudzonych informacji oraz informacji dostępnej publicznej.

Fraudsterzy, którzy działają w ten sposób, mają bardzo wysokie umiejętności IT i ogromne zasoby technologiczne. I dlatego właśnie banki wskazują, że głównymi sprawcami ataków fraudowych są zorganizowane grupy przestępcze.

Ale z drugiej strony, skoro te ataki są złożone i sprofesjonalizowane, to po stronie banków odpowiedź musi być adekwatna. I dlatego banki wskazują w badaniach, że przede wszystkim potrzebują doświadczonych analityków, którzy świetnie znają procesy bankowe, znakomicie poruszają się w gąszczu danych, korzystają z zaawansowanych narzędzi IT, i w efekcie mogą łączyć duże wolumeny danych z wiedzą i odpowiednim wnioskowaniem. Analitycy zaś potrzebują dobrej jakości danych, zatem proces zasilania ich danymi jest równie istotny, choć go nie widać, bo działa w drugim planie, w tle. Dlatego właśnie platformy sektorowe są podstawowym wsparciem dla rozwiązań, które banki konstruują indywidualnie po swojej stronie. Teoretycznie jest to uzupełnienie całego procesu antyfraudowego, w praktyce jednak te rozwiązania są swoistym krwiobiegiem systemu, który wszystko napędza i zasila konkretną informacją.

Do tego dochodzi – „zaszyta” w tych systemach – współpraca wewnątrzsektorowa. Powoduje ona, że każdy nowy scenariusz ataku przygotowany przez oszustów, po pierwszym użyciu staje się natychmiast znany wszystkim bankom wykorzystującym systemy antyfraudowe. Alert rozchodzi się błyskawicznie i nawet najbardziej wyrafinowana próba ataku bardzo szybko staje się nieskuteczna.

Najważniejsze wnioski

1

Coraz częściej doświadczamy wyłudzeń osobiście

Rośnie liczba osób, które bezpośrednio lub pośrednio zetknęły się z wyciekiem danych osobowych – doświadczył tego już co trzeci Polak. To systematyczny wieloletni wzrost o 2 pkt proc. rok do roku. W 2026 roku aż 15% ankietowanych przyznało, że sprawa dotyczyła ich osobiście.

2

Najwięcej strat finansowych przynoszą fałszywe sklepy internetowe

Polacy najczęściej mieli styczność z wyłudzeniami na „znajomego z Facebooka” i „na BLIKa” (39%, w tym 15% osobiście) oraz z vishingiem i spoofingiem (37%, w tym 18% osobiście). Jednak utratą środków finansowych najczęściej kończy się wyłudzenie przez fałszywe sklepy internetowe (w 35% przypadków doszło do straty finansowej).

3

Edukacja przynosi efekty: spada skuteczność oszustów

Po wyraźnym wzroście odnotowanym w 2025 roku, skuteczność wszystkich form wyłudzeń spadła, osiągając poziom niższy nie tylko w porównaniu z rokiem ubiegłym, ale najniższy w historii badania. Największa zmiana względem 2025 roku dotyczy spadku skuteczności wyłudzeń na akcje charytatywne (-14 pkt proc.).

4

Małe i średnie firmy są atakowane coraz częściej

Firmy z sektora MŚP odnotowują wzrost skali incydentów fraudowych. W ciągu ostatnich 12 miesięcy wystąpienie takich zdarzeń zadeklarowało niemal 38% przedsiębiorców – o 5,8 pkt proc. więcej niż rok wcześniej. Wzrosła również skala cyberzagrożeń. Odsetek firm deklarujących próby cyberataków zwiększył się z 34,4% do 39%.

5

Coraz więcej firm ponosi realne straty

Najczęściej wskazywana wartość poniesionych strat mieści się obecnie w przedziale od 5 tys. do 10 tys. zł (27,7%). Jednocześnie wyraźnie zmniejszył się odsetek firm deklarujących brak strat związanych z oszustwami – z 28,9% do 8,5%.

6

Cyberprzestępcy wciąż testują zabezpieczenia korporacji i instytucji finansowych

Udaremnione próby oszustw pozwoliły wielu firmom uniknąć istotnych strat finansowych. W przypadku 19% organizacji ich wartość przekroczyłaby 10 mln zł, a niemal połowa badanych (45%) ocenia ją na ponad 1 mln zł.

Informacje o badaniach

W Raporcie Antyfraudowym BIK 2026 zostały wykorzystane dane z bazy własnej Biura Informacji Kredytowej oraz informacje z badań opinii zrealizowanych na zlecenie BIK:

- **„Cyberbezpieczeństwo Polaków, 2026”** - badanie przeprowadzone w kwietniu 2026 r. przez Quality Watch na próbie 1040 osób.
- **„Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce 2026 r.”** – badanie przeprowadzone przez Instytut Keralla Research w maju 2026 na próbie 500 firm małych i średnich.
- **„Zdarzenia fraudowe w korporacjach, 2026 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. Badanie przeprowadzone przez BIK w okresie czerwiec-lipiec 2026 r., na próbie 30 korporacji i banków.
- **„Weryfikacja behawioralna – znajomość, korzystanie, opinie”** – badanie przeprowadzone w marcu 2026 r. przez Quality Watch na próbie 1040 osób.

Dziękujemy wszystkim Ekspertom za podzielenie się swoją wiedzą, doświadczeniem i perspektywą dotyczącą współczesnych cyberzagrożeń. Szczególne podziękowania kierujemy do przedstawicieli instytucji - tegorocznych gości specjalnych naszego Raportu, których wkład pozwolił wzbogacić raport o cenny kontekst oraz pogłębić analizę prezentowanych wyników.

Dziękujemy za udział:

pani Oldze Wiszowatej,

Naczelnik Wydziału Regulacji Cyberbezpieczeństwa
i Chmury Obliczeniowej Departament Cyberbezpieczeństwa,
Ministerstwo Cyfryzacji

panu Mirosławowi Wróblewskiemu,

Prezesowi Urzędu Ochrony Danych Osobowych,

pani Robertowi Grabowskiemu,

Kierownikowi Wydziału CERT Orange Polska

panu Pawłowi Piekutowskiemu,

Zastępcy Dyrektora Departamentu Cyberbezpieczeństwa,
Urzędu Komisji Nadzoru Finansowego

Niniejszy raport jest chroniony przepisami prawa autorskiego oraz innymi przepisami dotyczącymi ochrony własności intelektualnej. Jakiegokolwiek wykorzystywanie, w całości lub w części, poza własnym użytkiem osobistym i dalsze rozpowszechnianie, bez zgody Biura Informacji Kredytowej S.A. jest zabronione. Jeżeli jakkolwiek część raportu zostanie wykorzystana, musi zawierać wszelkie zawarte w oryginalnej wersji oznaczenia, wskazywać nazwę Biura Informacji Kredytowej S.A. i tytuł raportu. Logotypy BIK, BIG InfoMonitor oraz Digital Fingerprints są zastrzeżonymi znakami towarowymi.

O Grupie 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 wchodzi 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



BIG
InfoMonitor



DFP
Digital Fingerprints

.....
GRUPA BIK

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