BIK BIG InfoMonitor DFP Digital Fingerprints

GRUPA BIK

Raport Antyfraudowy BIK 2024

Zagrożenia i Ochrona.

Spis treści

Szanowni Państwo,

Raport Antyfraudowy 2024 przynosi informacje o kilku pozytywnych trendach, które potwierdzają wzrost świadomości zagrożeń zarówno wśród konsumentów, jak i przedsiębiorców.

Oto przykłady: już ponad jedna czwarta Polaków deklaruje, że w razie wyłudzenia danych sprawdzi w BIK, czy ktoś nie wykorzystał ich do wzięcia kredytu lub pożyczki. Świadomość w tym zakresie rośnie - jeszcze w 2022 r. ten odsetek sięgał 19%. Z kolei prawie już jedna piąta małych i średnich firm planuje wdrożyć narzędzia, które pomogą im chronić się przed próbami oszustw.

Te liczby pokazują, że edukacja społeczeństwa w zakresie bezpieczeństwa przynosi pozytywne efekty. Co nie zmienia faktu, że konieczne jest również ciągłe wdrażanie innowacyjnych rozwiązań podnoszących bezpieczeństwo konsumentów i przedsiębiorstw.

Nasz Raport pokazuje, że przestępcy cały czas udoskonalają metody i scenariusze ataków, zwłaszcza scenariusze, które bazują na socjotechnice i manipulacji.

Coraz bardziej wyrafinowane techniki wyłudzeń powodują, że ofiarą oszustów może paść każdy – wystarczy splot kilku czynników, jak chwila nieuwagi, presja czasu czy pośpiech.

Dlatego warto ciągle podnosić świadomość użytkowników o technikach stosowanych przez oszustów i sposobach ich przeciwdziałania. Klucz do skutecznej obrony to innowacyjne rozwiązania technologiczne, współpraca i wymiana wiedzy w sektorze oraz ciągła edukacja i szerzenie wiedzy na temat zagrożeń oraz sposobach obrony.

Wierzę, że kolejna edycja Raportu Antyfraudowego przyczyni się do realizacji misji edukacyjnej Grupy BIK, wesprze instytucje finansowe w określaniu priorytetowych kierunków działań i tematyki szeregu realizowanych kampanii społecznych.

Wspólnie możemy zadbać o większe bezpieczeństwo klientów indywidualnych i firm.

Zapraszam do lektury Raportu Antyfraudowego BIK 2024!

Agnieszka Szopa-Maziukiewicz

Dyrektor Zarządzająca Obszarem IT w Grupie BIK,
Prezes Zarządu Digital Fingerprints S.A.

Jak poważne są zagrożenia na rynku finansowym?

Skala zjawiska fraudów.

Klienci indywidualni

36% 2023
32% 2022

37%
zetknęło się z co najmniej jedną formą wyłudzenia. To najczęściej phishing.

10% 2023
9% 2022

10%
uważa, że wyciek danych nie stanowi powodu do niepokoju.

31% 2023
24% 2022

29%
tych, którzy mieli do czynienia z próbą wyłudzenia „na instytucję publiczną", było proszonych o podanie numeru PESEL.

Małe i średnie przedsiębiorstwa

18% 2023
24% 2022

15%
miało w 2024 r. do czynienia ze zdarzeniem fraudowym

16% 2023
31% 2022

21%
w gronie firm, które miały do czynienia z fraudami, doświadczyło próby oszustwa na fałszywe faktury bądź podszywania się pod kontrahentów.

82% 2023
80% 2022

77%
nie korzysta z narzędzi/usług antyfraudowych.

Korporacje

50% 2023
46% 2022

41%
banków uważa, że w 2024 r. liczba zdarzeń fraudowych wzrosła.

11% 2023
9% 2022

12%
korporacji twierdzi, że w ciągu roku w wyniku fraudów poniosły straty większe niż 10 mln zł.

69% 2023
65% 2022

56%
podmiotów wskazuje, że za fraudy najczęściej odpowiadają zorganizowane grupy przestępcze.

Definicja fraudu

Oto podstawowe metody fraudów.

Coraz więcej Polaków deklaruje, że miało do czynienia z przynajmniej jedną próbą oszustwa. Raport Antyfraudowy BIK pokazuje, że przestępcy wcale nie muszą sięgać po zaawansowane techniki, by okraść ofiarę. Często najskuteczniejsza okazuje się zwykła manipulacja.

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

Co to jest fraud?

W Raporcie definiujemy fraud jako działania znacznie szersze niż wyłącznie w cyberprzestrzeni. To wszelkie czynności, które wskazują na nieuczciwość, oszukiwanie i manipulowanie ofiarą, zmierzające do wyłudzenia korzyści majątkowej lub osobistej.

Fraudy mogą być realizowane przez podmioty zewnętrzne, ale również np. przez pracownika firmy, która pada ofiarą fraudu.

Fraudem jest również sytuacja, gdy oszust kradnie lub wykorzystuje dane osobowe ofiary w celu przejęcia konta. Zazwyczaj bowiem problem dotyczy rachunku bankowego lub innego miejsca, na którym zgromadzone są środki finansowe.

Przykładami fraudów mogą być też np. wyłudzenia kredytów lub pożyczek na fałszywe dane, podszycie się pod kontrahenta i zmiana numeru rachunku do płatności, kradzieże tożsamości, fałszowanie danych finansowych, oszustwa związane z obrotem fakturami, a także zwykłe kradzieże towaru z firmy.

Klienci instytucji finansowych są narażeni na 3 podstawowe rodzaje ataków:

Phishing - ma miejsce, gdy oszust nakłania ofiarę do kliknięcia w podstawiony, fałszywy link, np. do bankowości elektronicznej. Zwykle do przeprowadzenia oszustwa wykorzystywana jest poczta elektroniczna, media społecznościowe, komunikatory.

Vishing - dochodzi do niego, gdy złodziej podaje się zwykle za przedstawiciela ważnej instytucji, np. policjanta albo za pracownika banku.

Nakłania rozmówcę do konkretnych działań, np. ujawnienia wrażliwych danych bądź zainstalowania na urządzeniu zdalnego pulpitu, dzięki któremu zyskuje nieograniczony dostęp do urządzenia ofiary.

Spoofing – to podszycie się pod dane innej osoby bądź firmy z wykorzystaniem technologii. Atakujący wykorzystuje narzędzia, które pozwalają mu podszyć się pod numery telefonów, adresy mailowe czy adresy stron internetowych.

Komentarz eksperta

Karol Głogowski

Dyrektor IT Usług Antyfraudowych, BIK

Trzy czwarte Polaków wysoko ocenia własne bezpieczeństwo podczas transakcji online. Z kolei 43% ma zaufanie do zabezpieczeń stosowanych przez banki - to wyniki, które przyniosło badanie BIK na temat weryfikacji behawioralnej.

Badania wskazują na wciąż rosnące zaangażowanie instytucji finansowych w bezpieczeństwo swoich klientów oraz dowodzą, że inwestycje w systemy antyfraudowe coraz lepiej chronią środki klientów, a także reputację rynku finansowego.

Kolejna edycja naszego Raportu Antyfraudowego potwierdza, że oszuści doskonale zdają sobie z tego sprawę, upatrując szans na zyski wcale nie w typowych atakach hakerskich, a w socjotechnicznych sztuczkach, by klient sam wpuścił ich do swoich kanałów bankowości elektronicznej.

Można przypuszczać, że wraz z rozwojem narzędzi wykorzystujących sztuczną inteligencję to zjawisko będzie się nasilać - takiego zdania jest 46% ankietowanych przedstawicieli dużych instytucji finansowych i firm telekomunikacyjnych. W tym kontekście łatwo można sobie wyobrazić tworzenie coraz bardziej zaawansowanych reklam zachęcających do fałszywych inwestycji. A to tylko jedna z możliwości.

Dlatego rolą dużych podmiotów wciąż pozostaje edukacja klientów - nasze badania pokazują, że co dziesiąta osoba wciąż stosuje to samo hasło do wszystkich stron i aplikacji. A tylko 13% Polaków słyszało o rozwiązaniu weryfikacji behawioralnej.

Tymczasem to w tego rodzaju rozwiązaniach tkwi klucz do zwiększania bezpieczeństwa klientów oraz zminimalizowania następstw ewentualnych ataków socjotechnicznych. Warto ich w tym zakresie uświadamiać, a przy tym zachęcać do wzmożonej ostrożności i ograniczonego zaufania w cyberprzestrzeni.

Klienci indywidualni

TOP 5 skutecznych zdarzeń fraudowych.

Osoby, które padają ofiarą fraudów, najczęściej tracą pieniądze w wyniku oszustw „na BLIKa" oraz „na PIT". Prawie co czwarta (!) tego rodzaju próba wyłudzenia jest skuteczna.

Przestępcy niezmiennie najchętniej wykorzystują sztuczki socjotechniczne, by skłonić swoje ofiary do samodzielnego wykonania przelewu bądź udostępnienia danych, które umożliwią kradzież.

Respondenci, którzy zetknęli się z próbami wyłudzeń, wskazują, że największą skuteczność mają metody „na BLIKa" (23%), gdy np. przestępca przejmuje konto w mediach społecznościowych, a następnie wysyła do znajomych użytkownika prośby o udostępnienie kodu BLIK. Jeszcze w 2023 r. odsetek skutecznych prób wyłudzeń „na BLIKa" wynosił 20%.

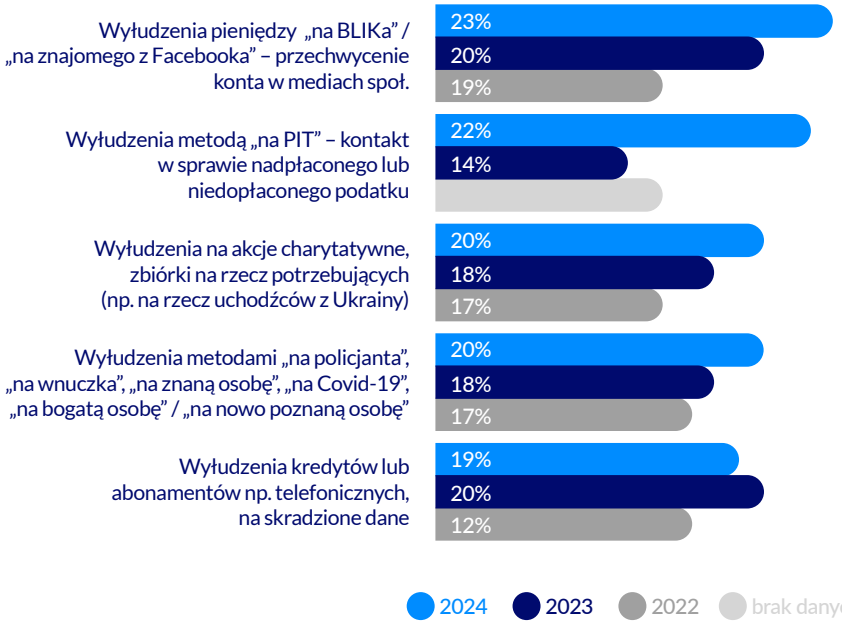
W 2024 r. wyraźnie wzrosła skuteczność oszustw „na PIT" (22%), w których złodzieje, podając się za pracowników urzędów skarbowych, kontaktują się z ofiarami w sprawie rzekomej niedopłaty podatku.

Na uwagę zasługuje fakt, że na pozostałych miejscach w TOP 5 skutecznych zdarzeń fraudowych umacniają się różnego rodzaju metody wykorzystujące socjotechnikę, np. „na wnuczka", „na policjanta", „na akcje charytatywne" itp.

Dzieje się tak pomimo kampanii społecznych, prowadzonych przez instytucje finansowe i publiczne.

8 pp. o tyle w porównaniu do 2023 r. wzrosła skuteczność wyłudzeń „na PIT". Styczność z tą metodą (osobistą lub w przypadku znajomego) miało 13% respondentów.

Proszę określić czy próba wyłudzenia była skuteczna



Klienci indywidualni

Skala zagrożenia fraudami.

Rośnie liczba Polaków, którzy mieli styczność z wyłudzeniami. Ich zdaniem najmocniej rośnie ryzyko ataków w formie phishingu oraz vishingu.

Już 37% Polaków deklaruje, że mieli styczność przynajmniej z jedną formą próby wyłudzenia. Ich odsetek **wzrósł o 1 pp. w porównaniu do 2023 r. i aż o 5 pp. wobec 2022 r.**

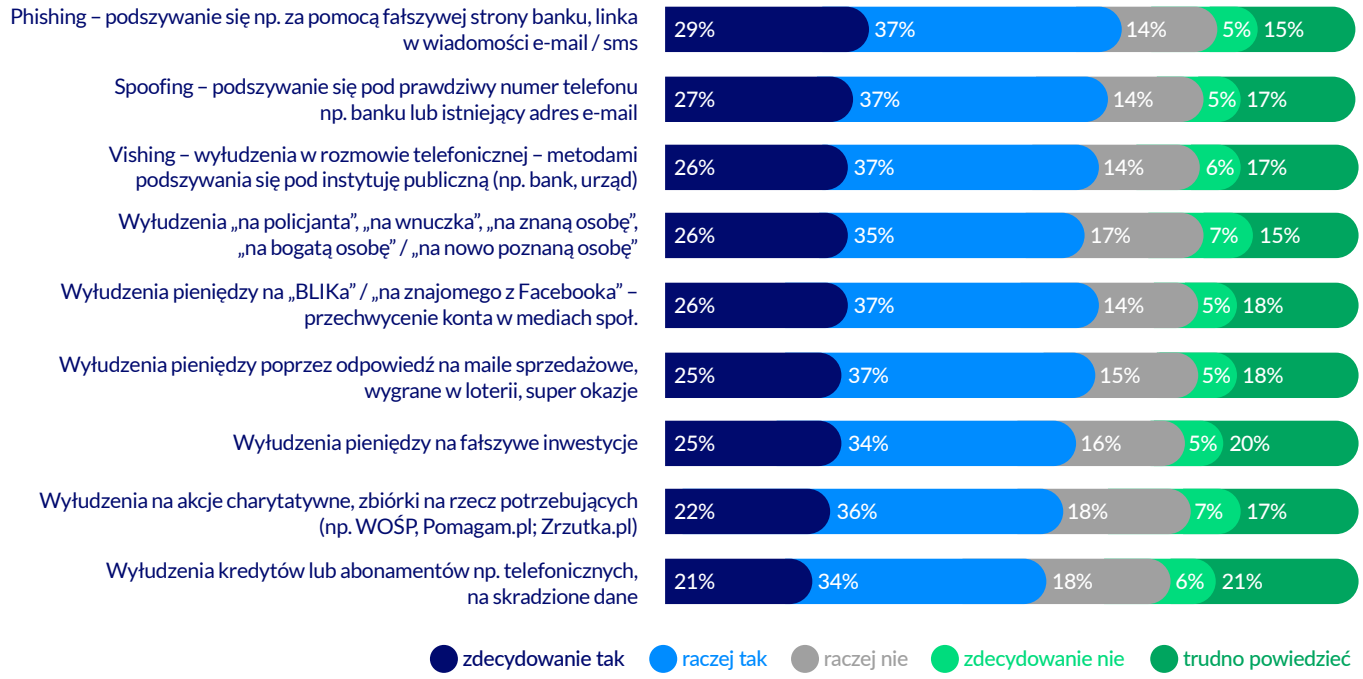
Wskazują duże znaczenie ataków socjotechnicznych jak phishing, spoofing czy vishing.

To również metody, których częstotliwość nasila się najbardziej - na phishing wskazało 66% ankietowanych, spoofing - 64%, a na vishing - 63%.

Jak złodzieje kontaktują się z ofiarami?

Najpopularniejszymi kanałami kontaktu ze strony przestępców w przypadku phishingu pozostają e-maile (49%, +3 pp. r/r), SMS-y (43%, +2 pp.), rozmowy telefoniczne (29%, +1 pp.).

Czy nasiliły się poniższe zagrożenia?



Klienci indywidualni

Jakie sztuczki stosują oszuści?

W 2024 r. wyraźnie wzrosła częstotliwość prób wyłudzeń loginów i haseł do bankowości internetowej.

Respondenci wskazują, że przestępcy, którzy nawiązują kontakt z ofiarą, najczęściej próbują skłonić ją, by:

- przekazała im numer PESEL w celu autoryzacji transakcji,
- potwierdziła im transakcję po przekierowaniu do rzekomego działu bezpieczeństwa (np. banku),
- przelała lub wypłaciła pieniądze.

Warto jednak zwrócić uwagę na to, że w 2024 r. znacząco wzrósł odsetek odpowiedzi wskazujących na próby pozyskania loginu i hasła do konta bankowego ofiary (22%, +7 pp. r/r). To potwierdzenie, że aktywność przestępców w wykorzystywaniu tej metody socjotechnicznej wyraźnie wzrosła.

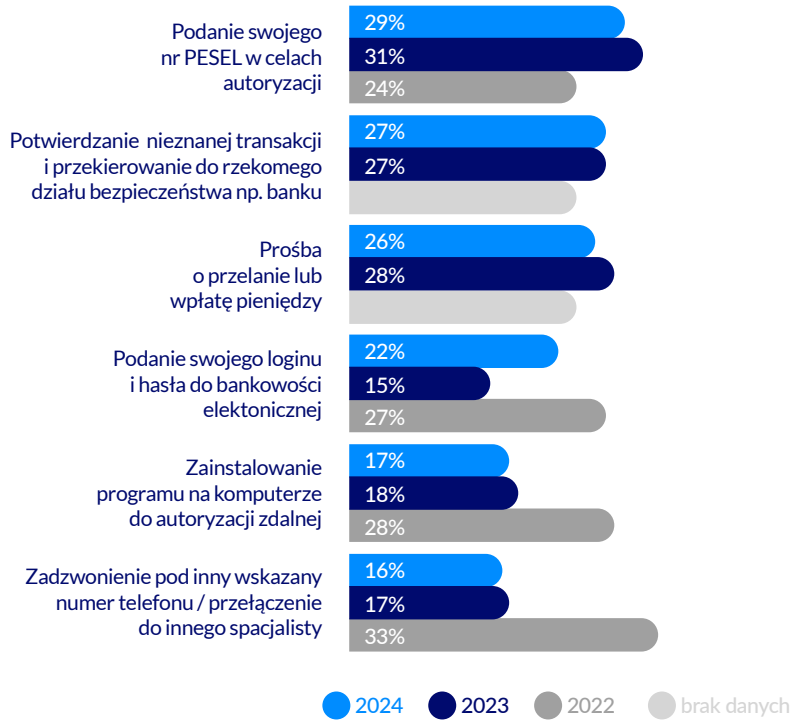
Andrzej Karpiński, Dyrektor Departamentu Bezpieczeństwa w BIK zwraca uwagę, że przestępcy coraz częściej wykorzystują reklamy wykupione w legalnych źródłach internetowych, by np. pod pretekstem okazji inwestycyjnych wyłudzać od użytkowników pieniądze lub dane. Więcej na ten temat można przeczytać w komentarzu na następnej stronie.

43% Polaków ma zaufanie do zabezpieczeń zapewnianych przez banki podczas logowania i realizacji transakcji online. Największe poczucie bezpieczeństwa wzbudza w nich możliwość dodatkowego potwierdzenia transakcji w aplikacji mobilnej.

26%

Polaków deklaruje, że w razie wyłudzenia sprawdzi w BIK, czy ktoś nie wykorzystał ich danych do wzięcia kredytu/pożyczki. Świadomość w tym zakresie rośnie – jeszcze w 2022 r. ten odsetek sięgał 19%.

Manipulacje stosowane przez oszustów. Jakich działań/ informacji wymagano?



Komentarz eksperta

Andrzej Karpiński

Dyrektor Departamentu Bezpieczeństwa Grupy BIK

Polska znajduje się w czołówce państw na świecie, w których użytkownicy internetu najczęściej korzystają z adblocków. To zjawisko wcale nie powinno dziwić. Te narzędzia już nie tylko wstrzymują nachalne reklamy, ale przez wielu są traktowane jako dodatkowy element poprawiający bezpieczeństwo. Zatrzymują bowiem napływ szkodliwych treści i linków, za pomocą których przestępcy namawiają np. na fałszywe inwestycje bądź wyłudzają dane.

Wykorzystywanie przez przestępców reklam wykupionych w legalnych źródłach internetowych jest obecnie bardzo poważnym problemem, z którym trudno walczyć. Zwykle zanim takie treści zostaną zgłoszone, zweryfikowane i usunięte, to oszuści już znajdą swoje ofiary.

Skala zjawiska jest tak duża, że czas wreszcie zapytać o odpowiedzialność wydawców za publikowane treści reklamowe. We własnym interesie powinni oni dbać o to, by do użytkowników nie trafiały reklamy, które służą wyłudzaniu pieniędzy lub danych. Być może wówczas spadnie odsetek tych, którzy decydują się na blokowanie wszystkich reklam.

Ostatnie miesiące przynoszą też optymistyczny trend polegający na wyraźnym spadku skuteczności mailowego spamu. Ten oczywiście wciąż przychodzi, ale zdecydowana większość konsumentów już wie, że nie należy np. otwierać linków przesyłanych przez nieznanych nadawców.

Podobnie klienci bankowi powinni nauczyć się tego, by nie ufać np. reklamom inwestycyjnym, wykorzystującym wizerunki znanych osób. Tym bardziej, że w najbliższym czasie przestępcy z pewnością będą udoskonalać narzędzia socjotechniczne, wykorzystując sztuczną inteligencję. To wyzwanie, na które cała branża finansowa powinna być dobrze przygotowana.

Komentarz eksperta

Piotr Konieczny

Ekspert ds. cyberbezpieczeństwa, Niebezpiecznik.pl

Badanie BIK pokazuje, że ponad połowa instytucji finansowych prognozuje, iż rozwój sztucznej inteligencji spowoduje wzrost zagrożenia fraudami. Te same firmy z pewnością będą rozwijać narzędzia AI, by wzmacniać ochronę przed zagrożeniami.

Zasadnicza różnica polega jednak na tym, że podmioty rynkowe będą działać w granicach regulacji prawnych dla AI, podczas gdy przestępców te zasady „nie obowiązują".

Wiele osób już teraz rysuje czarne scenariusze, według których grupy przestępcze będą sięgać po narzędzia AI, aby klonować głos i wizerunek, np. prezesa konkretnej spółki. Cel? Realizacja bardziej wiarygodnych ataków socjotechnicznych.

Na razie jednak nie obserwujemy takich ataków, choć narzędzia są już dostępne, a koszty ich użycia nie są wygórowane. Prawdopodobnie przyczyną jest czas. Stworzenie wiarygodnego „klona", zdolnego do interakcji w czasie rzeczywistym, wymaga przygotowań. A po cóż to robić, skoro i bez wykorzystania AI, za pomocą tradycyjnych, a o wiele szybszych w użyciu metod phishingowych wciąż z powodzeniem, codziennie okrada się z danych i pieniędzy setki firm?

Przedsiębiorstwa używają coraz nowocześniejszych zabezpieczeń zarówno oprogramowania, jak i sprzętu. Ale niezmiennie na końcu i tak jest człowiek, którego można „podejść". Ten problem dotyczy nie tylko pracowników firm, ale także wszystkich konsumentów, którzy padają ofiarą przestępców tworzących np. fałszywe strony banków, sklepów internetowych czy bramek płatniczych.

Kluczowe dla bezpieczeństwa jest to, by firmy - obok rozwijania narzędzi IT – wdrażały programy podnoszenia świadomości swoich pracowników w tym zakresie. Pomoże to przedsiębiorstwom, jak również przedsiębiorstwom i ich klientom, czyli w konsekwencji każdemu z nas.

Klienci indywidualni

Wiedza klientów o wyłudzeniach. Co robią w razie problemów?

Co piąty (!) Polak nie odczuwa obaw o to, że padnie ofiarą wyłudzenia.
Dla co dziesiątego wyciek danych nie stanowi powodu do niepokoju.

Badanie w 2024 r. potwierdziło dużą pewność siebie Polaków w kwestii tego, że problem wyłudzeń lub wycieku danych ich nie dotyczy. Chociaż coraz więcej osób ma styczność z fraudami i ocenia, że ich ryzyko rośnie (por. s. 8), to:

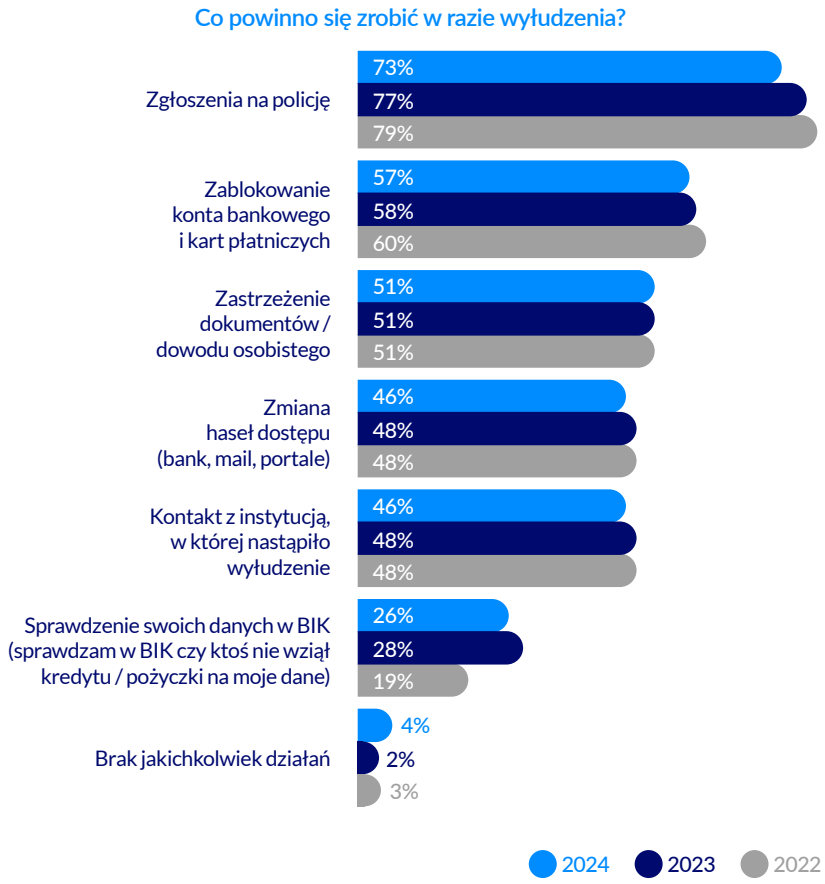
- 22% nie obawia się wyłudzenia.
- 10% uważa, że wyciek danych nie stanowi powodu do niepokoju.

W obu przypadkach wyniki są identyczne jak w 2023 r

W przypadku wyłudzenia środków Polacy wciąż najczęściej kierują kroki na policję (73%, -4 pp. r/r) i blokują dostęp do konta bankowego oraz kart płatniczych (57%, -1 pp. r/r).

Pewność siebie w zakresie ryzyka wyłudzeń pieniędzy i kradzieży danych potwierdzają informacje o powodach, dla których część osób nie korzysta z usług ostrzegających przed tego typu zdarzeniami.

- W gronie osób niekorzystających z takich usług 31% twierdzi, że nie ma takiej potrzeby.
- A 22% nie wiedziało, że takie usługi w ogóle istnieją.



Klienci indywidualni

Rośnie świadomość ryzyka cyberataków.

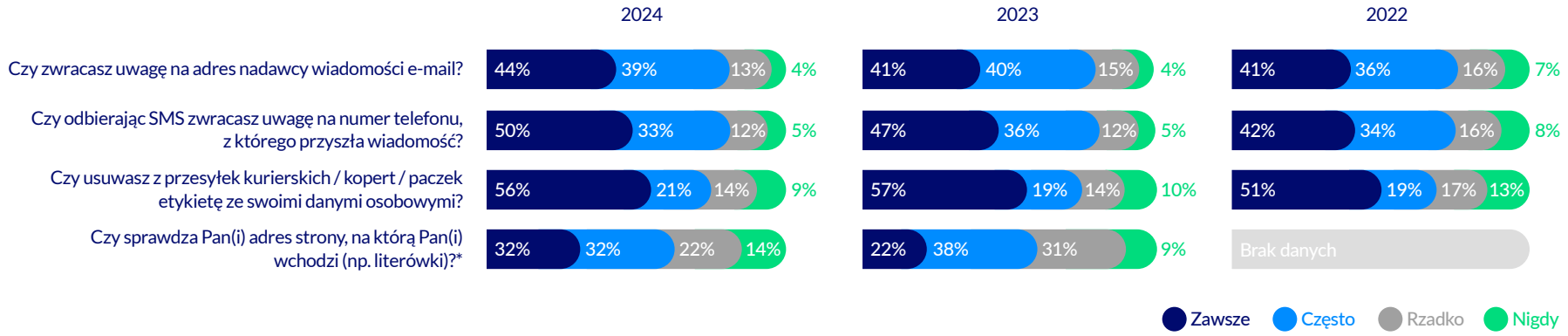
Polacy zachowują największą ostrożność w przypadku klikania w linki otrzymywane w SMS-ach.

Pozytywnym zjawiskiem jest to, że coraz więcej Polaków z większym dystansem podchodzi do wiadomości otrzymywanych różnymi kanałami od nieznanych nadawców.

- 74% nie klika w linki w wiadomościach SMS z nieznanego źródła (+1 pp. r/r).
- 69% nigdy nie otwiera załączników w e-mailach pochodzących z nieznanego adresu (+3 pp. r/r).
- 56% nigdy nie oddzwania na numery telefonów od nieznajomych (+1 pp. r/r).

Warto zwrócić uwagę na fakt, że Polacy mają coraz większą świadomość sztuczek stosowanych przez hakerów i np. częściej dokładnie sprawdzają adres strony internetowej, na którą wchodzą.

Zachowanie w konkretnych sytuacjach w cyberprzestrzeni



Klienci indywidualni

Bankowość w telefonie a bezpieczeństwo.

Już ponad połowa Polaków korzysta z bankowości elektronicznej za pomocą aplikacji w telefonach. Jak chronią swoje urządzenia?

Aż 53% Polaków, by skorzystać z bankowości elektronicznej, w pierwszej kolejności wybiera aplikację banku w smartfonie. Dopiero na drugim miejscu ze znacznie niższym wynikiem (28%) znajduje się dostęp przez stronę internetową w komputerze. Są i tacy klienci, którzy wpisują adres logowania do banku, korzystając z przeglądarki internetowej w telefonie (9%). Co dziesiąta osoba nie korzysta z bankowości elektronicznej.

Tak znacząca popularność aplikacji bankowych skłania do pytania o bezpieczeństwo samych smartfonów i zabezpieczanie ich przed atakami. Tylko 44% ankietowanych wskazuje, że instaluje programy antywirusowe w telefonach. Dla porównania, w przypadku komputerów ten odsetek wynosi 57%.

Za najskuteczniejszy sposób ochrony urządzeń mobilnych Polacy uznają zaś nieotwieranie wiadomości / załączników z nieznanych źródeł.

Zabezpieczenie telefonu przed kradzieżą danych

Ochrona smartfona przed włamaniem

Najpopularniejszymi sposobami zabezpieczenia dostępu do telefonu są: kod PIN (39%), odcisk palca (33%), hasło (21%). Ankietowani wskazali jeszcze wzór graficzny (19%) oraz rozpoznawanie twarzy (15%). Aż 18% ankietowanych nie stosuje żadnych blokad ekranów w telefonach.

Komentarz eksperta

Paweł Piekutowski

Kierownik Departamentu Cyberbezpieczeństwa, UKNF

30.140 - dokładnie tyle domen phishingowych zostało wykrytych przez CSIRT KNF w 2023 r. wobec 17.200 w 2022 r. i 11.468 w 2021 r. Wyraźnie widać więc, że trend jest rosnący i utrzyma taką tendencję również w 2024 r.

Cyberprzestępcy nieustannie udoskonalają swoje metody, aby maksymalizować zyski, minimalizować koszty i zwiększać skalę ataków. Zamiast zaawansowanych technicznie oszustw, stosują ataki oparte na manipulacji użytkownikiem, które przynoszą im większe korzyści przy mniejszych nakładach.

Na czele tych działań znajdują się oszustwa inwestycyjne, w których ofiary kuszone są wizją szybkich zysków bez ryzyka. Równie popularne stają się oszustwa telefoniczne, gdy przestępcy podszywają się pod konsultantów bankowych lub przedstawicieli instytucji publicznych. Kradzieży dokonuje się również, wykorzystując fałszywe strony internetowe, by wejść w posiadanie poświadczeń do bankowości internetowej lub numerów kart płatniczych. Dystrybucja linków do takich stron odbywa się za pomocą fałszywych wiadomości SMS, e-maili, a także coraz częściej przy wykorzystaniu reklam internetowych.

Cyberprzestępcy stale podnoszą swoje umiejętności. Dlatego kluczowe staje się odpowiednie edukowanie użytkowników, aby zwiększyć ich odporność i zmniejszyć skuteczność manipulacji.

Szczególnie niepokojącym trendem jest wzrost liczby ataków typu Ransomware. Przestępcy szyfrują pliki w organizacji, a następnie żądają okupu w zamian za przekazanie kluczy do ich odszyfrowania. Coraz częściej stosowany jest również szantaż, polegający na groźbie upublicznienia wrażliwych danych w internecie.

Kluczowym aspektem obrony przed zagrożeniami jest odpowiednie przygotowanie infrastruktury IT oraz ciągła optymalizacja i testowanie zabezpieczeń, aby lepiej dostosować je do zmieniających się metod działania cyberprzestępców.

Małe i średnie firmy

5 najskuteczniejszych fraudów, na które są narażeni przedsiębiorcy.

Otrzymywanie fałszywych faktur do zapłaty stało się prawdziwą plagą. Już co piąta firma była obiektem tego typu ataku.

15,4% przedsiębiorstw zetknęło się z próbą oszustwa w ciągu 12 miesięcy poprzedzających badanie. Wynik jest porównywalny z 2023 r., gdy o takim doświadczeniu wspomniało 18% ankietowanych.

W 2024 r. zmieniło się jednak nasilenie różnego rodzaju metod wykorzystywanych przez oszustów. O ile w 2023 r. firmy najczęściej wskazywały na problem podejrzanych maili z linkami kierującymi do płatności, to w 2024 r. zwracają uwagę głównie na fałszywe faktury do zapłaty: złodzieje podszywają się pod kontrahentów, a w fakturach podstawiają fałszywe numery kont.

Z problemem fałszywych faktur spotkało się 20,8% firm. Podobny odsetek twierdzi, że zdarzają się próby wyłudzenia danych potrzebnych do kradzieży środków z rachunków bądź zaciągnięcia zobowiązań finansowych - również w tym przypadku zjawisko wyraźnie nasiliło się w porównaniu do 2023 r.

10 nawet tyle prób wyłudzeń rocznie odnotowało 50% firm, które zorientowały się, że były obiektem ataków.

Małe i średnie firmy

Konsekwencje fraudów. Co może stracić firma?

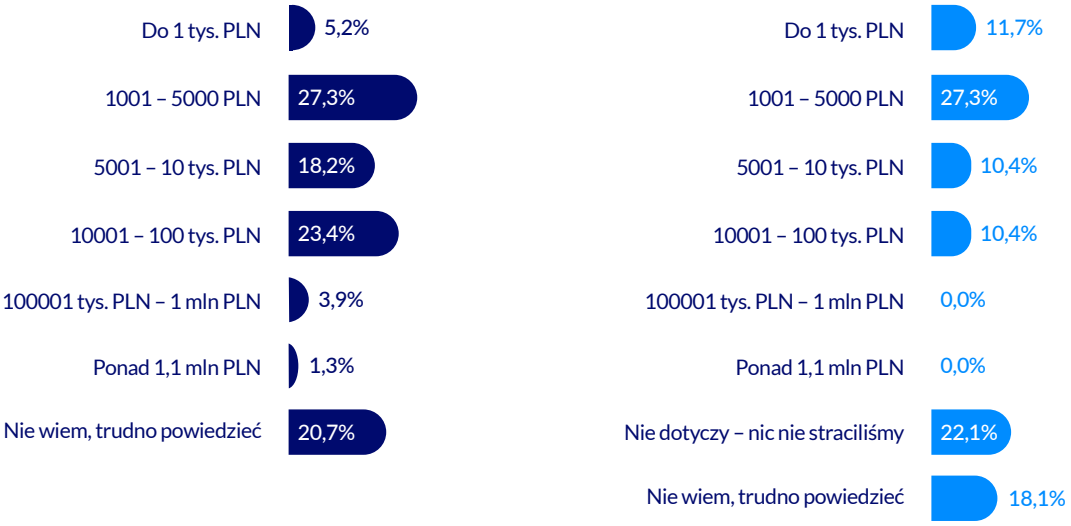
Co piąta firma, która była obiektem ataku, nie potrafi oszacować strat, które on spowodował. Ale co dziesiąta przyznaje, że nie zdołała zablokować oszustw na kwotę nawet 100 tys. zł.

Przedsiębiorcy częściej identyfikują próby oszustw i ich unikają niż padają ofiarą wyłudzeń – taki wniosek można wyciągnąć z porównania odpowiedzi dotyczących kwot ochronionych przed oszustwem z tymi, które firmy straciły.

W przypadku prób wyłudzeń kwot w przedziale od 5 do 10 tys. zł co piąte przedsiębiorstwo deklaruje, że udało się powstrzymać atak, a co dziesiąte - że poniosło straty tej wielkości. Jednocześnie widać, że firmy w wyniku oszustw łatwiej tracą małe kwoty (do 1 tys. zł) - straty tego rzędu deklaruje 11,7% podmiotów, podczas gdy tylko 5,2% twierdzi, że udało im się zablokować utratę takich środków.

Wyniki są porównywalne z odczytami z 2023 r.

Kwoty zablokowane vs. straty w wyniku oszustw



55,8%

przedsiębiorstw podaje, że w ciągu ostatniego roku udaremniło do 10 prób wyłudzeń. 15,6% twierdzi zaś, że zablokowało kilkadziesiąt ataków na firmę. Nawet o 100 blokadach oszustw wspomina 11,7% podmiotów.

Małe i średnie firmy

Działania antyfraudowe. Jakie metody stosują firmy?

Unikanie klikania w podejrzane linki - to niezmiennie podstawowa zasada ochrony w przedsiębiorstwach. Niemal trzy czwarte firm ma poczucie, że próby wyłudzeń ich nie dotyczą.

Na pytanie o techniki stosowane w celu wykrycia oszustw, przedsiębiorcy najczęściej odpowiadają, że zdają się na **zdrowy rozsądek** (37,4%). Ta metoda sprowadza się np. do tego, by nie otwierać podejrzanych maili.

Na ten sam sposób firmy wskazywały 2023 r., przy czym wówczas odsetek odpowiedzi sięgnął 16,4%. Jednak wtedy jedna trzecia podmiotów odpowiedziała, że nie stosuje żadnych technik obrony przed atakami. W 2024 r. tak odpowiedziała już tylko jedna dziesiąta firm.

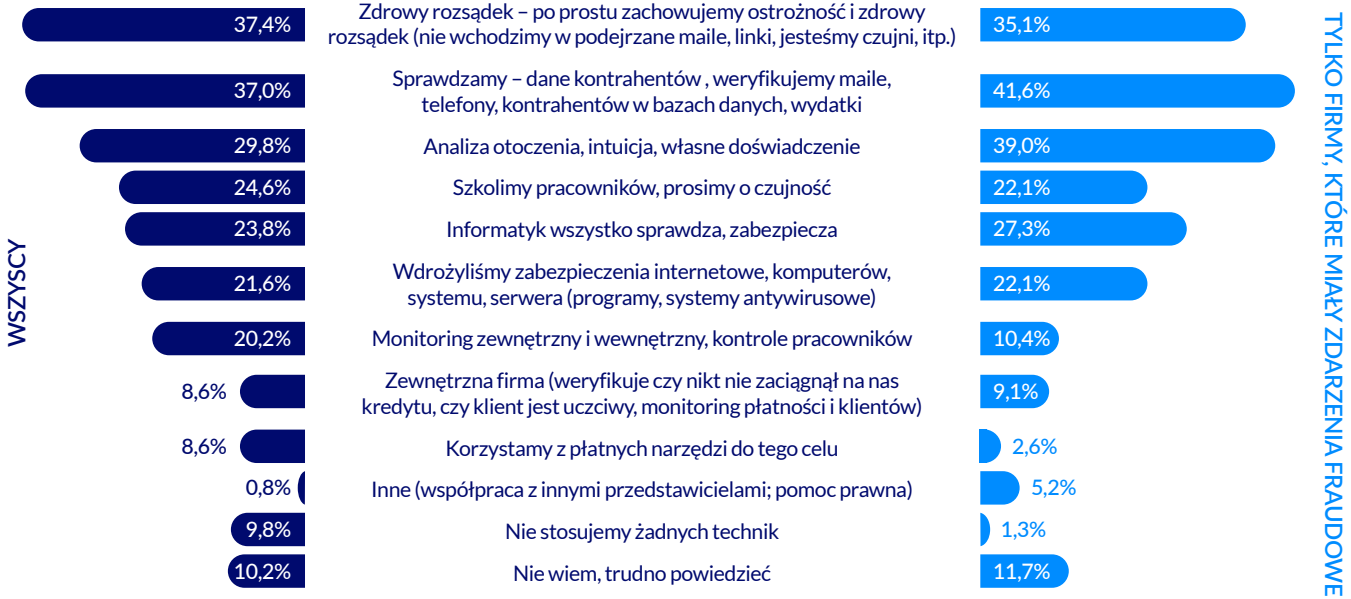
O tym, że zdrowy rozsądek to za mało, firmy przekonują się, gdy już doświadczą próby wyłudzenia. W takim gronie na pierwsze miejsce wśród stosowanych zabezpieczeń wysuwa się dokładne sprawdzanie danych kontrahentów (41,6%) i analiza otoczenia (39%).

74,8%

firm ma poczucie, że próby wyłudzeń ich nie dotyczą i nigdy nie miały z nimi do czynienia. W 2023 r. odsetek takich odpowiedzi wyniósł 80,2%.

Joanna Charlińska, Dyrektor ds. Sprzedaży Rynku Detalicznego BIK zauważa, że podejście przedsiębiorców do kwestii bezpieczeństwa zmienia się dopiero, gdy sami poniosą stratę w wyniku wyłudzenia. Więcej na ten temat można przeczytać w komentarzu na stronie 21.

Jakie techniki wykrywania wyłudzeń/oszustw stosujecie Państwo w firmie?



Małe i średnie firmy

Rośnie liczba firm, które chcą korzystać z narzędzi antyfraudowych.

Już 17,4% przedsiębiorstw deklaruje, że chce znaleźć odpowiednie narzędzia i usługi, które pomogą im chronić się przed próbami oszustw. Budżet na takie działania szybciej znajdują firmy, które wcześniej doświadczyły zdarzeń fraudowych.

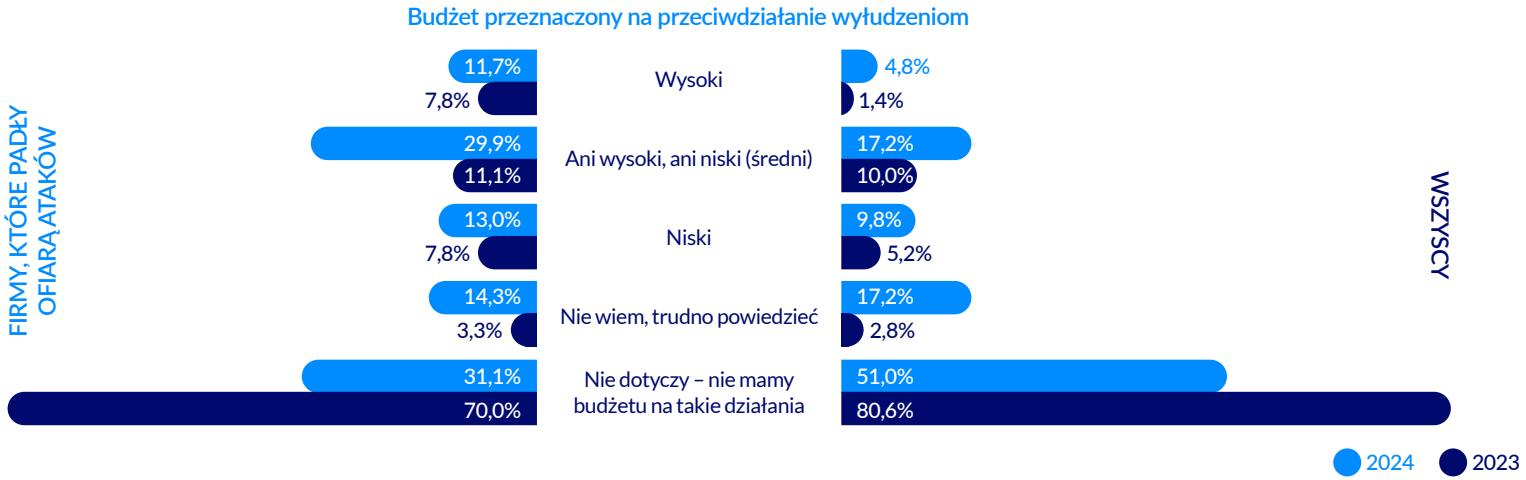
Jeszcze w 2023 r. plan znalezienia narzędzi bądź usług antyfraudowych miało zaledwie 1% firm. **Skok odsetka takich odpowiedzi do 17,4% może świadczyć o rosnącej świadomości zagrożeń.** Potwierdzają to również odpowiedzi na temat planów zatrudnienia specjalisty ds. przeciwdziałania wyłudzeniom (13%), a nawet stworzenia całego działu ekspertów w tym zakresie (10,8%).

Ewolucję podejścia firm do kwestii cyberbezpieczeństwa można też zauważyć w odpowiedziach na temat budżetu przeznaczanego na działania antyfraudowe. Wyższy niż w 2023 r. budżet przeznaczają na nie zarówno firmy, które już były obiektem ataków, jak i te, które dotychczas uniknęły prób wyłudzeń.

Jednocześnie w porównaniu do 2023 r. wyraźnie spadł odsetek przedsiębiorstw, które twierdzą, że nie mają środków na działania anyfraudowe.

22%

przedsiębiorców narzeka na skuteczność działania instytucji państwowych w przeciwdziałaniu oszustwom i nadużyciom.



Małe i średnie firmy

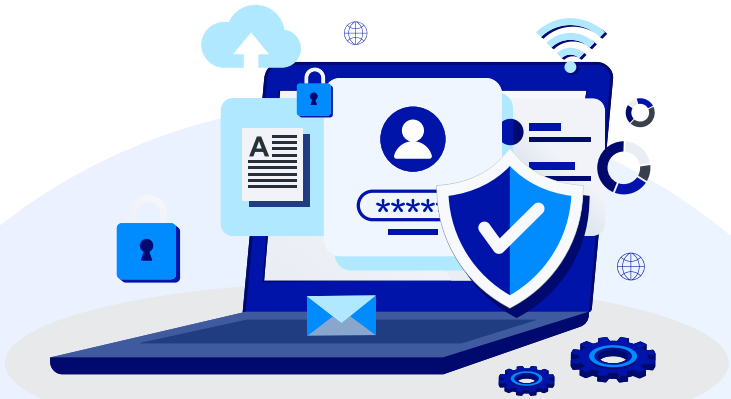
Bariery w stosowaniu rozwiązań antyfraudowych.

Firmy twierdzą najczęściej, że samodzielnie są w stanie sprostać wyzwaniom w zakresie bezpieczeństwa.

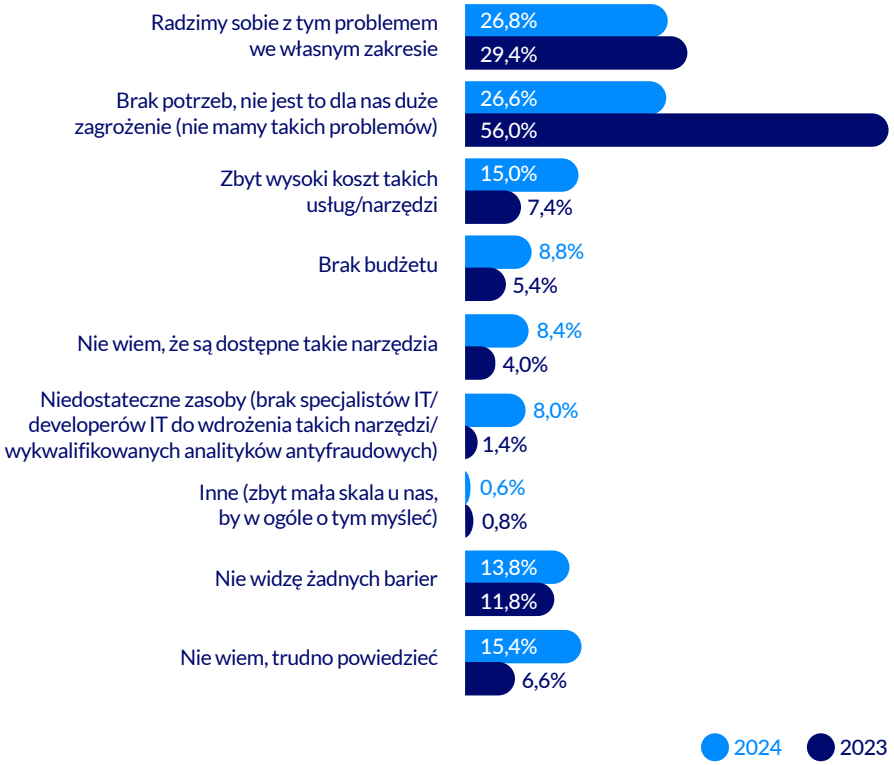
26,8% przedsiębiorców na pytanie o najważniejsze bariery w stosowaniu narzędzi antyfraudowych odpowiada, że z kwestią ochrony radzą sobie sami – wynik jest porównywalny do 2023 r.

Jednocześnie znacząco spadł odsetek przedsiębiorstw, które twierdzą, że w ogóle nie mają potrzeb w zakresie ochrony przed fraudami. Jeszcze w 2023 r. była ich ponad połowa, a obecnie - około jedna czwarta. To kolejna informacja potwierdzająca ewoluuję w biznesie w zakresie podejścia do kwestii bezpieczeństwa.

Wśród barier, które powstrzymują firmy od stosowania narzędzi antyfraudowych, znalazły się m.in. kwestie finansowe (brak budżetu, wysokie koszty), ale też brak wiedzy o istnieniu takich rozwiązań.



Główne bariery w stosowaniu usług/narzędzi antyfraudowych



Komentarz eksperta

Joanna Charlińska

Dyrektor ds. sprzedaży, Rynek Detaliczny, BIK

Prawie jedna piąta małych i średnich przedsiębiorstw planuje wzmocnić zabezpieczenia antyfraudowe bądź skorzystać z oferowanych w tym zakresie usług. W 2023 r. odsetek podobnych odpowiedzi sięgnął zaledwie 1%.

Ta wyraźna zmiana daje wreszcie nadzieję na to, że przedsiębiorcy dostrzegli potrzebę zaangażowania w obronę przed oszustami dodatkowych środków niż tylko… zdrowego rozsądku. Bo ten jest zwykle wystarczający do momentu, w którym firma nie padnie ofiarą fraudu.

Badania realizowane na zlecenie BIK od dawna wyraźnie pokazują, że podejście przedsiębiorców do kwestii bezpieczeństwa zmienia się dopiero, gdy sami poniosą stratę w wyniku wyłudzenia. Wówczas budzi się czujność, wzmożona weryfikacja kontrahentów sięgająca nawet takich szczegółów, jak sprawdzanie poprawności numerów kont podawanych na fakturach. Warto przy tym zaznaczyć, że z problemem fałszywych faktur spotkała się już co piąta firma.

Raport antyfraudowy BIK potwierdza, że **skala zagrożenia, przed którym stoją przedsiębiorcy jest bardzo duża**. Tym bardziej wciąż niezrozumiały pozostaje optymizm zarządzających firmami, wśród których trzy czwarte twierdzi, że próby wyłudzeń ich nie dotyczą.

Takie przekonanie jest złudne. Bowiem każda firma, jest potencjalnym celem ataku oszustów działających na szeroką skalę.

Tym bardziej istotne są kampanie uświadamiające skalę zagrożeń, w tym także działania komunikacyjne, wskazujące na możliwe rodzaje zabezpieczeń antyfraudowych. Wśród nich ważną rolę pełnią rozwiązania o charakterze prewencyjnym, w tym udostępniane przez BIK. Należy do nich niewątpliwie **Pakiet BIK Bezpieczna Firma**. To prosty i skuteczny sposób, by mieć pod kontrolą finanse swojej firmy, aktualne informacje o swoich kontrahentach- czy płacą na czas oraz korzystać z aktywnej ochrony przed wyłudzeniami.

W dobie cyberzagrożeń tego typu rozwiązanie pomoże ochronić firmę przed poważnymi konsekwencjami nie tylko finansowymi, ale w dużym stopniu również reputacyjnymi.

Komentarz eksperta

Jarosław Biegański

Dyrektor Zespołu Bezpieczeństwa Banków, Związek Banków Polskich

Wymiana informacji między instytucjami finansowymi jest kluczowa i jej znaczenie będzie rosło. To droga do tego, by jeszcze lepiej chronić klientów i same podmioty obecne na rynku. Współdzielenie informacji zwiększa bowiem szansę na zablokowanie próby oszustwa, którą wcześniej zidentyfikował i oznaczył bank we wspólnym systemie. Działa to na zasadzie wzajemnego ostrzegania.

Sytuację można więc porównać do budowania zbiorowej odporności systemu płatniczego. Służą temu narzędzia, które stosują banki do monitorowania transakcji bankowych. W przypadkach, gdy np. kwota przelewu lub pora przelewu są niestandardowe, praktykowana jest bezpośrednia komunikacja banku z klientem.

Wszystko po to, by wykluczyć wszelkie próby manipulacji klientem i ataki socjotechniczne, które przestępcy modyfikują, stosują skutecznie na szeroką skalę. Nadal bowiem łatwiej jest oszustom wywierać presję i nakłaniać pokrzywdzonych do wykonania konkretnej czynności niż złamać zaawansowane zabezpieczenia bankowe.

Nie bez przyczyny banki dążą do stosowania na coraz większą skalę technologii weryfikacji behawioralnej, w której zachodzi na bieżąco analiza zachowań klienta. Np. zmiana modelu wpisywania znaków na klawiaturze czy inna wychwycona anomalia, pozwala zweryfikować czy transakcji dokonuje klient czy ktoś, kto podszywa się pod klienta i drogą manipulacji chce zrealizować przelew.

Dla lepszego zrozumienia roli tego systemu bezpieczeństwa przez klientów banków, konieczna jest szeroka edukacja, wyjaśniająca że analiza behawioralna jest bezkontekstowa i służy lepszej ochronie przed nieuprawnionym przelewem z konta albo złożeniem wniosku kredytowego.

Lepszej ochronie klientów sprzyjają też wszelkie inne elementy procesów bankowych, które pozwalają upewnić się, że czynności dokonuje klient, a nie oszust na podstawie wyłudzonych danych. Przykładem takiej bezpiecznej procedury może być dodawanie kart płatniczych do wirtualnych portfeli, wyłącznie za pośrednictwem aplikacji bankowej i po silnym uwierzytelnieniu.

Korporacje

Instytucje na celowniku oszustów. Gdzie jest największe ryzyko?

Niemal jedna trzecia korporacji z rynku finansowego wskazuje, że zjawisko fraudów przybiera na sile. Niezmiennie wskazują one, że dużym problemem pozostają ataki socjotechniczne na klientów.

31% ankietowanych przedstawicieli korporacji uważa, że w 2024 r. liczba zdarzeń fraudowych wzrosła w porównaniu do 2023 r. Według 52% skala zjawiska nie zmieniła się. Na wzrost zagrożenia oszustwami wskazują przede wszystkim banki komercyjne (41%) oraz banki spółdzielcze (33%).

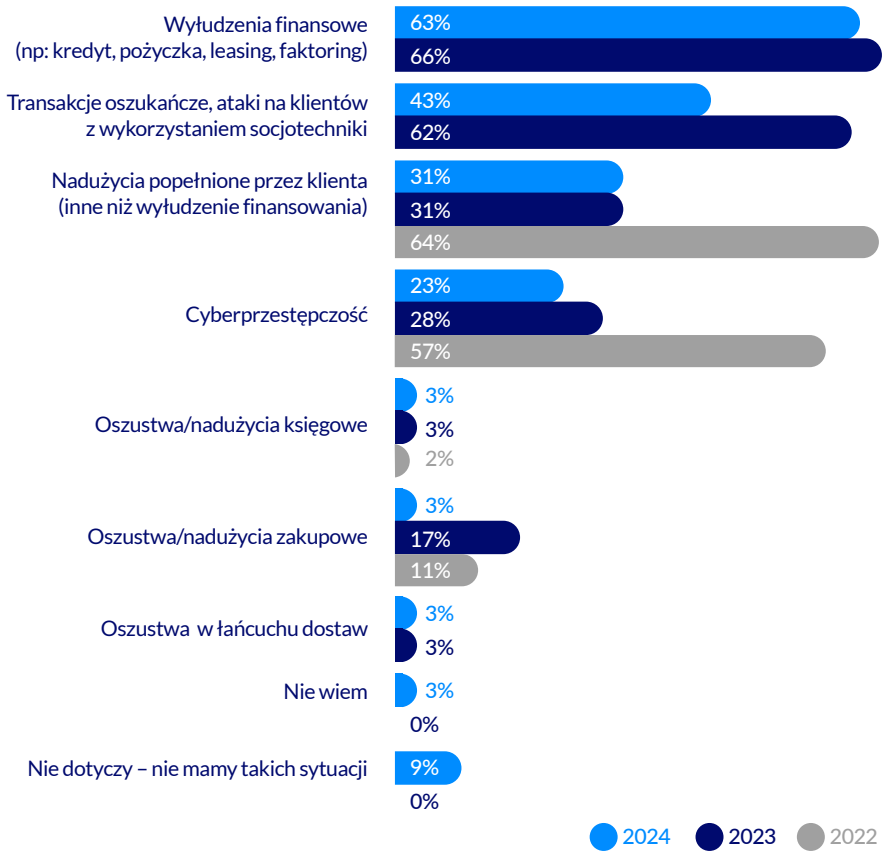
Te wyniki potwierdzają, że banki – **a przede wszystkim ich klienci** – pozostają kluczowym celem ataków, ze względu na skalę działalności i korzyści możliwe do uzyskania.

Respondenci wskazują, że kluczowymi obszarami, w których przestępcy są aktywni, pozostają różne formy finansowania oraz transakcje. Skupiają się więc na wyłudzeniach kredytów, pożyczek itp. oraz atakach socjotechnicznych na klientów w celu zrealizowania oszukańczych transakcji.

17%

korporacji odnotowało w 2024 r. więcej niż 500 zdarzeń fraudowych. W 2023 r. ten odsetek sięgnął 28%.

Jakich obszarów Państwa działalności dotyczyły zdarzenia fraudowe?



Korporacje

Schematy działań oszustów.

Ataki socjotechniczne na klientów, ale też fałszowanie dokumentów czy tworzenie firm na tzw. słupy – to metody fraudów, z którymi regularnie spotkają się duże podmioty rynku finansowego.

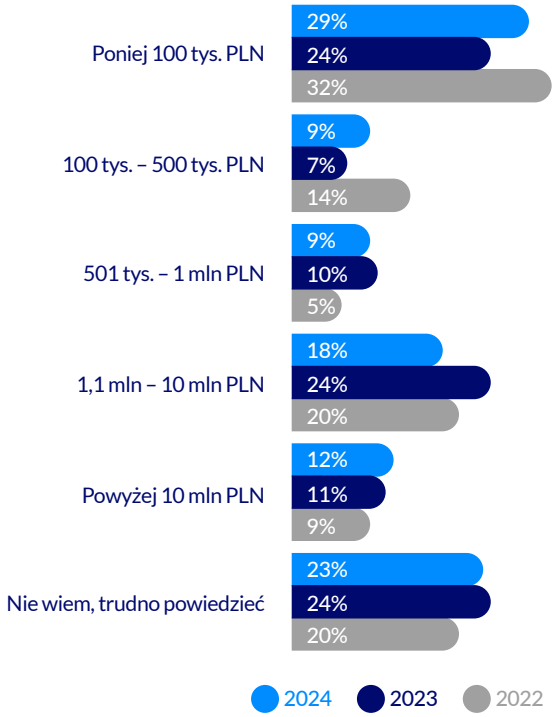
Respondenci z dużych firm podkreślają, że to osoby spoza ich organizacji odpowiadają za zdarzenia fraudowe. Zapytani o to, kto jest odpowiedzialny za oszustwa, zwykle wskazują: klientów (59%) oraz zorganizowane grupy przestępcze (56%). Mniejsze znaczenie przypisują typowym atakom hakerskim (27%).

Najczęściej pojawiające się schematy oszustw:

- oszustwa z wykorzystaniem socjotechniki, np. wyłudzanie kodów BLIK, oszustwa kartowe,
- poświadczenie nieprawdy, sfałszowane dokumenty w celu wyłudzenia finansowania,
- wnioski kredytowe na skradzione tożsamości,
- przedkładanie fikcyjnych faktur do finansowania,
- fraudy inwestycyjne.

Niemal jedna trzecia korporacji objętych badaniem stwierdziła, że w 2024 r. straty poniesione przez nie w wyniku fraudów przekroczyły **1 mln zł**

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



Korporacje

Walka z fraudami. Ile ataków udaje się powstrzymać?

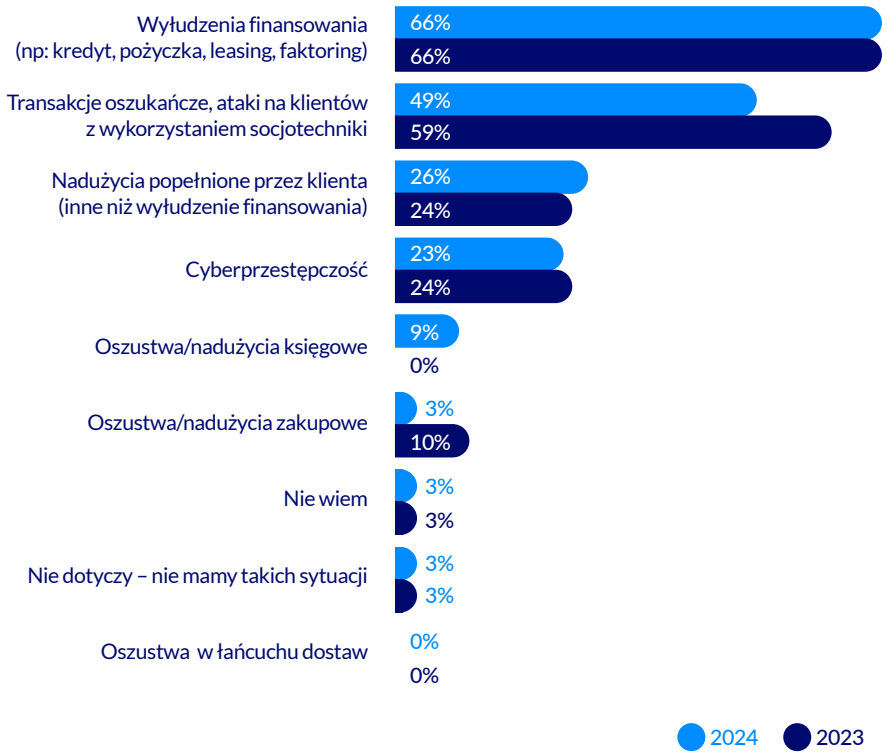
Duże firmy są coraz skuteczniejsze w identyfikowaniu i blokowaniu zdarzeń fraudowych.

Taki wniosek można wyciągnąć z odpowiedzi respondentów na pytanie o liczbę zatrzymanych prób oszustw. 20% podmiotów wskazuje, że w 2024 r. powstrzymała ponad 500 fraudów. Rok wcześniej tak deklarowało 17% ankietowanych korporacji.

Odpowiedzi potwierdzają również, że największej uwagi wymagają te obszary, w których oszuści wykazują się największą aktywnością. Jednostki odpowiedzialne za walkę z fraudami w instytucjach finansowych deklarują, że najwięcej ataków zostało powstrzymanych w zakresie wyłudzeń (66%) i transakcji realizowanych m.in. przez zmanipulowanych przez oszustów klientów (49%).

18% korporacji deklaruje, że w 2024 r. powstrzymały zdarzenia fraudowe na kwotę powyżej 10 mln zł. Jedna trzecia firm wskazała na kwoty w przedziale 1,1-10 mln zł.

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



Korporacje

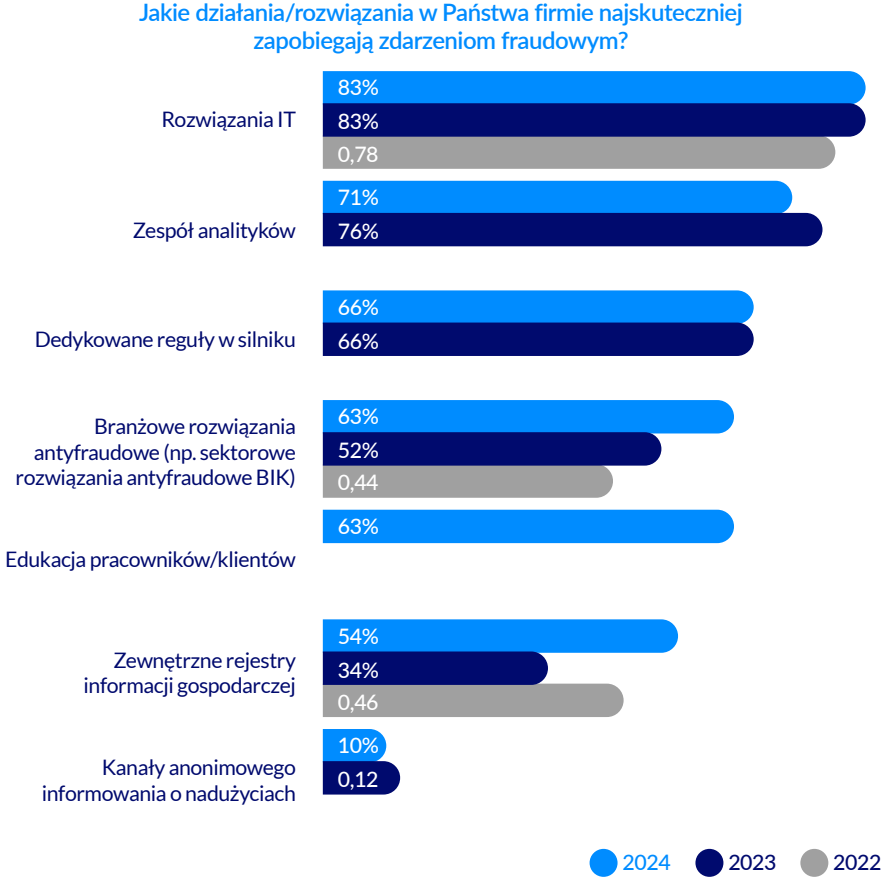
Metody zapobiegania fraudom.

Dziewięć na dziesięć firm posiada odrębne zespoły odpowiedzialne za przeciwdziałanie nadużyciom. Kluczowe są dla nich nowoczesne rozwiązania IT.

83% respondentów odpowiedziało, że najskuteczniejszym sposobem walki z fraudami są rozwiązania IT. Odsetek odpowiedzi jest porównywalny z 2023 r. Ponad 70% ankietowanych wskazało również, że duże znaczenie mają dla nich zespoły analityków.

Warto zwrócić uwagę na wzrost znaczenia sektorowych rozwiązań antyfraudowych – na ich skuteczność wskazuje 63% korporacji w porównaniu do 52% w 2023 r.

W obliczu wzmożonej aktywności przestępców w obszarze ataków socjotechnicznych duże firmy doceniają również działania związane z edukacją klientów i pracowników (63%).



Zespoły ds. walki z nadużyciami

89%

dużych podmiotów deklaruje, że posiadają odrębne zespoły odpowiedzialne za monitorowanie i zwalczanie oszustw. Jedna trzecia z nich twierdzi, że te jednostki zatrudniają po ponad 10 osób.

Korporacje rzadziej decydują się na angażowanie zewnętrznych firm do przeciwdziałania atakom. Robi to 23% ankietowanych instytucji.

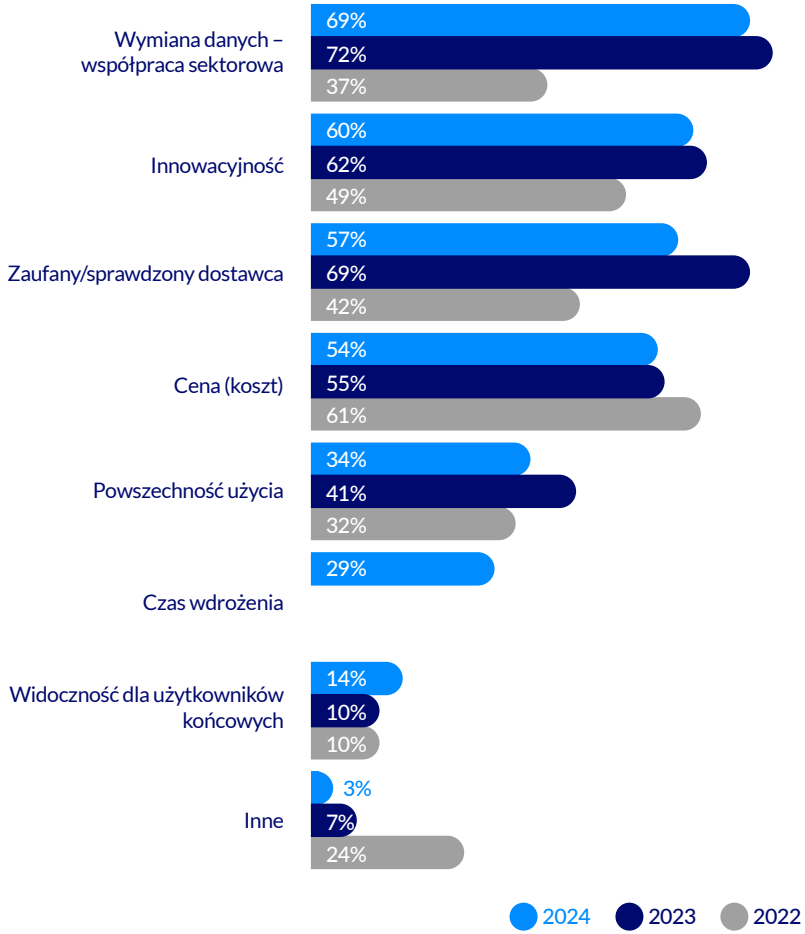
Korporacje

Rośnie popularność rozwiązań antyfraudowych.

Firmy planują uzupełnianie narzędzi antyfraudowych przede wszystkim w obszarze udzielania finansowania.

Współpraca sektorowa oparta na możliwości wymiany informacji – to podstawowe kryterium, które duże firmy biorą pod uwagę, rozważając wdrożenie rozwiązań antyfraudowych. Zwracają również uwagę na takie kluczowe czynniki jak m.in. innowacyjność oraz zaufanie do dostawcy.

Jakie główne kryteria stosują Państwo przy decyzji o wyborze rozwiązań antyfraudowych?



Korporacje

Rośnie popularność rozwiązań antyfraudowych.

Firmy planują uzupełnianie narzędzi antyfraudowych przede wszystkim w obszarze udzielania finansowania.

68% respondentów z korporacji stwierdziło, że w ich firmach wykorzystuje się dwa systemy antyfraudowe lub więcej. Pracują one przede wszystkim przy wykrywaniu nadużyć związanych z udzielaniem finansowania, transakcjami w bankowości elektronicznej, a także używaniem loginów i haseł w kanałach zdalnych.

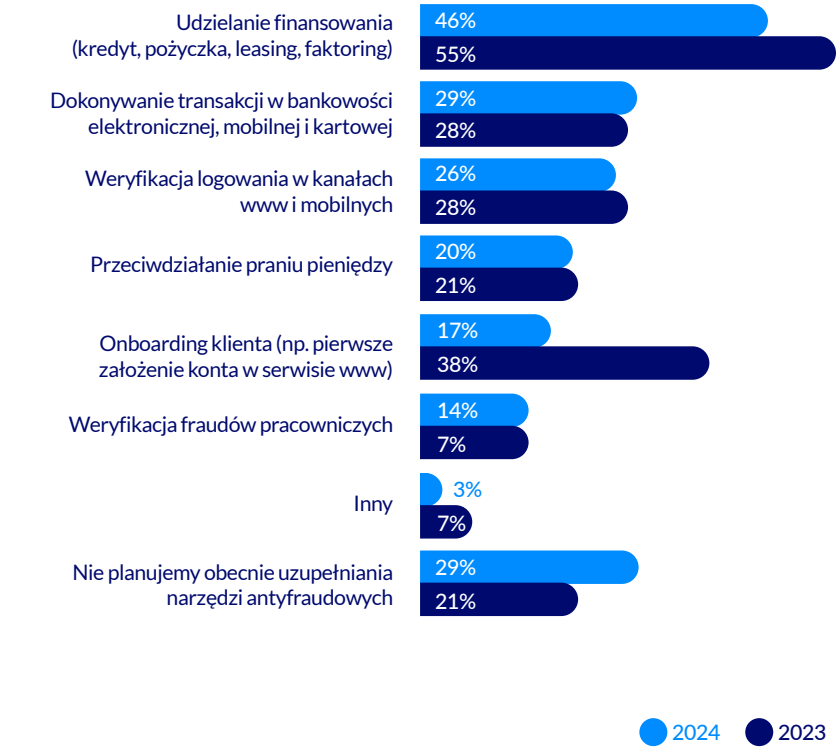
I właśnie te obszary będą dalej wzmacniane przez firmy. Podmioty zapytane o plany rozwoju narzędzi antyfraudowych zwykle wskazują na zapotrzebowanie właśnie w zakresie wyzwań związanych z wyłudzeniami kredytów, pożyczek i oszukańczymi transakcjami w bankowości elektronicznej.

94% dużych firm korzysta z narzędzi antyfraudowych.

Skala zagrożeń fraudami a AI

Według 46% ankietowanych przedstawicieli korporacji rozwój narzędzi wykorzystywanych do przestępstw opartych na sztucznej inteligencji (AI) spowoduje, że skala zagrożenia fraudami w firmach wzrośnie. Przeciwnego zdania jest 14% respondentów.

W jakich obszarach planują Państwo uzupełnienie narzędzi antyfraudowych?



Najważniejsze wnioski

1

Rośnie odsetek Polaków, którzy mieli styczność przynajmniej z jedną formą próby wyłudzenia.

Jest ich już 37%. Największym problemem pozostają ataki socjotechniczne, mające na celu zmanipulowanie ofiary, by ta samodzielnie przelała pieniądze na konto oszustów, bądź udostępniła im dane umożliwiające kradzież.

2

Kampanie edukacyjne wśród konsumentów przynoszą pożądane skutki, niemniej wciąż są bardzo potrzebne.

To m.in. dzięki nim już trzy czwarte Polaków nie klika w linki otrzymywane z nieznanego źródła, a 69% deklaruje, że nie otwiera załączników od nieznanych nadawców.

3

Przestępcy modyfikują metody ataków na małe i średnie firmy.

Przedsiębiorcy wskazują, że obecnie dużym problemem jest podszywanie się pod kontrahentów i np. przesyłanie fałszywych faktur – z tym problemem spotkała się już co piąta firma.

4

Wśród przedsiębiorców rośnie świadomość zagrożeń.

Ponad 17% z nich deklaruje, że chce znaleźć odpowiednie narzędzia i usługi, które pomogą im chronić się przed próbami fraudów. Firmy coraz częściej rozważają też zatrudnianie specjalistów ds. przeciwdziałania wyłudzeniom.

5

Istotną rolę w zmaganiach z cyberprzestępcami w kolejnych kwartałach odegra rozwój sztucznej inteligencji.

Przedstawiciele korporacji (46%) wskazują, że rozwój narzędzi opartych na AI spowoduje, iż skala zagrożeń fraudami wzrośnie.

6

Zdecydowana większość dużych firm korzysta z rozwiązań antyfraudowych.

Przy ich wyborze stawiają przede wszystkim na współpracę sektorową, opartą na możliwości wymiany informacji. Zwracają również uwagę na takie kluczowe czynniki jak m.in. innowacyjność oraz zaufanie do dostawcy.

Narzędzia BIK

Ochrona przed fraudami.

Oto rozwiązania technologiczne dla sektora finansowego.

Platforma Antyfraudowa (PAF) – to rozwiązanie, które wspiera banki, instytucje pożyczkowe, a także firmy leasingowe i faktoringowe w procesie oceny klientów wnioskujących o finansowanie.

PAF wykorzystuje szereg reguł antyfraudowych, które w czasie rzeczywistym ułatwiają identyfikację zagrożeń już na etapie składania wniosku przez klienta. Dotyczą one np. weryfikacji tożsamości, informacji teleadresowych czy danych o zatrudnieniu. W ten sposób instytucja finansowa zwiększa swoje szanse na zatrzymanie prób wyłudzeń, np. przy użyciu skradzionych danych.

O skuteczności PAF świadczą liczby: od 2017 r. PAF pozwoliła zaoszczędzić ponad 930 mln zł, zatrzymując wyłudzenia produktów kredytowych dla osób fizycznych. Z kolei od 2020 r. PAF zatrzymała nadużycia na kwotę ponad 146 mln zł, związane z produktami finansowymi dla firm. (Dane na koniec maja 2024 r.).

Platforma Cyber Fraud Detection (CFD) – to narzędzie w obszarze analiz IT, które chroni klientów w kanale online. CFD na podstawie szeregu danych identyfikuje m.in. sytuacje, w przypadku których zachodzi podejrzenie, że przestępca wszedł w posiadanie loginu oraz hasła klienta, by dokonać transakcji fraudowej. CFD zawiera w sobie narzędzia umożliwiające przeprowadzanie postępowania wyjaśniającego, powiązanego z urządzeniem i danymi transakcji.

Szybkość działania CFD umożliwia instytucji finansowej sprawną reakcję i zablokowanie podejrzanego przelewu lub wypłaty środków. CFD chroni w ten sposób zarówno klienta, jak również instytucję finansową.

Zaletą CFD jest elastyczność w zakresie budowy modeli ochrony, w oparciu o indywidualne potrzeby instytucji finansowej. Narzędzie to umożliwia również sektorową wymianę informacji między instytucjami finansowymi o podejrzanych urządzeniach, które mogą zostać wykorzystane do nielegalnych działań.

Platforma Weryfikacji Behawioralnej – ten system wykorzystuje mechanizmy uczenia maszynowego (Machine Learning), by analizować zachowania klientów korzystających z bankowości internetowej i mobilnej. „Uczy się" np. tempa wciskania klawiszy na klawiaturze, sposobu używania myszy i charakterystycznych zachowań klienta korzystającego z urządzenia mobilnego.

Dzięki temu narzędzie jest w stanie zidentyfikować sytuacje, w których dostęp do bankowości elektronicznej klienta uzyskuje osoba nieuprawniona. Po otrzymaniu takiej informacji instytucja finansowa może szybko zablokować dostęp do konta i uchronić środki klienta.

Działanie Platformy Weryfikacji Behawioralnej nabiera szczególnego znaczenia podczas prób wyłudzeń i oszustw, w których złodzieje nakłaniają klienta do instalacji w urządzeniu tzw. zdalnego pulpitu i przejmują nad nim kontrolę.

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 2024 r. przez Quality Watch.
- Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce 2024 r., zrealizowane przez Instytut Keralla Research.
- Zdarzenia fraudowe w korporacjach, 2024 r. - badanie ankietowe wśród przedstawicieli dużych firm z rynku finansowego, zrealizowane przez BIK.

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