BONNIER Business Polska

Puls Biznesu

Bankier.pl

RAPORT 2026

BAROMETR SCAMMINGU

Jak Polacy wpadają w pułapki oszustów

EWOLUCJA, SKALA I FORMY OSZUSTW



BADANIE POWSTAŁO W RAMACH PROJEKTU Scamming Out 2026

PARTNERZY RAPORTU

VISA

PKO Bank Polski

PARTNER BADANIA

MINDS & ROSES

Realizacja badania i współpraca merytoryczna
Agencja Minds & Roses Sp. z o.o.

Nadzór merytoryczny i koordynacja projektu
Eliza Górska
Monika Tańska
Anna Więckowska

Wydawca
Bonnier Business Polska
ul. Kijowska 1
03-738 Warszawa

Opracowanie graficzne raportu
Patrycja Kurek

Warunki licencji
Bonnier Business Polska jest wyłącznym właścicielem praw majątkowych do raportu „Barometr Scammingu – Jak Polacy wpadają w pułapki oszustów". Z chwilą otrzymania raportu zamawiający uzyskuje prawo do jego wykorzystania wyłącznie na wewnętrzne potrzeby zamawiającego, z wyłączeniem udostępniania raportu w całości lub w częściach bądź w jakimkolwiek fragmencie podmiotom trzecim. Cytowanie fragmentów raportu nie może zmieniać sensu ich treści i jest dopuszczalne wyłącznie w materiałach sporządzonych przez zamawiającego na własne potrzeby, pod warunkiem opatrzenia cytowanych fragmentów informacją o Bonnier Business Polska jako autorze raportu oraz tytule raportu.

Warszawa, listopad 2026

BONNIER Business Polska

Puls Biznesu

Bankier.pl

RAPORT 2026

BAROMETR SCAMMINGU

Jak Polacy wpadają w pułapki oszustów

EWOLUCJA, SKALA I FORMY OSZUSTW

Nie ukrywam, że byłem sceptyczny, czy pomysł przeprowadzenia badania o scamach finansowych jest dobry.

Eugeniusz Twaróg
zastępca redaktora naczelnego
Pulsu Biznesu



Aż 16% z nas, Polaków, dało się oszukać scammerom w ciągu ostatniego roku.

Tomasz Goss-Strzelecki
zastępca redaktora naczelnego
Bankier.pl



Młodzi bardziej podatni na scam? Zaskakujące wyniki badania

Nie ukrywam, że byłem sceptyczny, czy pomysł przeprowadzenia badania o scamach finansowych jest dobry. Czy jesteśmy w stanie zmierzyć, zdiagnozować i opisać tak złożone zjawisko jak nowoczesna przestępczość, wykorzystująca bardzo wiele narzędzi do oszukiwania ludzi?

Na rynku co jakiś czas pojawiają się podobne publikacje o umiarkowanej wartości merytorycznej, bo koncentrują się zazwyczaj na jakimś fragmencie bardzo złożonego problemu. Często wynika to z faktu, że badania realizowane są na zlecenie firm komercyjnych.

A jednak się udało. Jestem bardzo zadowolony, że zrealizowaliśmy badanie i przygotowaliśmy raport „Barometr Scamu". Stanowi on doskonałe uzupełnienie projektu Scamming Out!, ponieważ daje nam wgląd w stan wiedzy społeczeństwa o oszustwach finansowych, świadomość zagrożeń i odporność na nowoczesne formy przestępczości.

Ale nie tylko. Dzięki dwóm wskaźnikom – Barometrowi Dynamiki Scamu i Indeksowi Podatności na Scam – możemy mierzyć zmiany w społecznym postrzeganiu oszustw i podatności na nie. Pozwolą nam one sprawdzać, czy rzeczywiście stajemy się bezpieczniejsi. Pierwsza edycja badania dostarcza punktu odniesienia. Najciekawsze będą jednak kolejne pomiary, gdy zobaczymy, czy maleje podatność Polaków na manipulację, a wzrasta ich zdolność do ochrony przed oszustwami.

Na dziś sytuacja wygląda następująco: Barometr Dynamiki Scamu wskazuje, że obawy przed oszustwami są znacznie większe, niż wynikałoby to ze skali faktycznie doznawanych szkód. Nie oznacza to jednak, że zagrożenie jest niewielkie.

Nader interesujący jest wniosek z analizy Indeksu Podatności na Scam. Otóż w grupie wiekowej do 29 lat wynosi on 42,9 pkt, wobec 36,4 pkt dla ogółu badanych. Młodzi są bardziej podatni na manipulację, przede wszystkim ze względu na skłonność do podejmowania impulsywnych decyzji.

Raport przygotowany w ramach projektu Scamming Out! ma szanse stać się kluczowym na rynku narzędziem do pomiaru odporności społecznej na oszustwa finansowe dzięki rozbudowanemu panelowi badawczemu analizującemu doświadczenie Polaków w kontakcie ze scamerami, postrzegania ryzyka stwarzanego przez oszustów.

Równocześnie pomiar podatności na scam pozwoli wskazać systemowe słabości, w które mogą uderzyć oszuści.
Serdecznie zachęcam do lektury.

Zarabianie to za mało, trzeba jeszcze nie dać się okraść

Technologia nieustannie zmienia sposób obchodzenia się z pieniędzmi. Zapewniła nam ogromną wygodę – płatności na jeden klik, przelewy na numer telefonu w kilka sekund czy zarządzanie portfelem inwestycyjnym z poziomu smartfona. Ale otworzyła też nowy front, na którym codziennie toczy się walka o nasze oszczędności. Cyberbezpieczeństwo to dzisiaj podstawa finansów osobistych.

Właśnie dlatego w Bankier.pl traktujemy ten temat priorytetowo i po raz trzeci wraz z „Pulsem Biznesu" prowadzimy akcję Scamming out!, skupioną na walce z oszustwami finansowymi i budowaniu cyberodporności. Nie możemy odpowiedzialnie pisać o pomnażaniu kapitału, kontach oszczędnościowych czy najlepszych lokatach, ignorując fakt, że często jedno nieostrożne kliknięcie dzieli Polaków od utraty dorobku życia.

Wyniki badania „Barometru scammingu", które zaprezentowane zostaną podczas konferencji Scamming out! Summit, wyraźnie pokazują, że problem uderza w społeczeństwo z coraz większą siłą. Aż 16% z nas, Polaków, dało się oszukać scammerom w ciągu ostatniego roku. Szczególnie alarmujący jest fakt, że w sidła cyberzłodziei tak łatwo wpadają dziś młodzi dorośli, rzekomo doskonale poruszający się w cyfrowym świecie.

Rzetelną informację i edukację postrzegamy jako skuteczną formę ochrony. Nie przestajemy wierzyć, że stałe nagłaśnianie metod działania oszustów oraz pokazywanie, jak w praktyce chronić swoje dane i pieniądze, to najlepsza tarcza, w jaką jako media finansowe możemy wyposażyć Polaków.

Współpraca kluczem do bezpiecznych płatności

Mateusz Oleksy
dyrektor generalny Visa
w Polsce

VISA

> Skuteczna ochrona wymaga nie tylko technologii, ale też współpracy.



Wraz z rozwojem technologii coraz bardziej wyrafinowane stają się też metody stosowane przez oszustów. Działają szybko, wykorzystują sztuczną inteligencję, podszywanie się pod znane marki czy osoby, a przede wszystkim manipulację. Znacznie częściej nie próbują przełamać zabezpieczeń, ale przekonać człowieka, żeby sam wykonał określone działanie. Dlatego ochrona musi działać wcześniej i w tle, pomagając wychwytywać niepokojące sygnały, zanim oszustwo przerodzi się w realną stratę.

Dla Visa bezpieczeństwo jest fundamentem całego ekosystemu płatniczego. Łączymy analizę danych, AI, doświadczenie z wielu rynków i odporną infrastrukturę, aby możliwie szybko identyfikować ryzyko i ograniczać je, zanim dotknie użytkownika.

Współczesne oszustwa coraz rzadziej mieszczą się jednak w granicach jednej firmy czy sektora – mogą zaczynać się na platformie cyfrowej, a kończyć transakcją w instytucji finansowej. Dlatego skuteczna ochrona wymaga nie tylko technologii, ale też współpracy. Banki, firmy technologiczne czy sprzedawcy widzą różne fragmenty tego samego zagrożenia. Im sprawniej więc potrafimy te sygnały połączyć, tym większa szansa, że zatrzymamy oszustwo na wcześniejszym etapie. Visa wspiera ten ekosystem poprzez infrastrukturę, skalę i doświadczenie, tak aby bezpieczeństwo było stałym elementem transakcji i działało stale, na wielu poziomach i możliwie niezauważalnie dla użytkownika.

Chronimy finansowy krwioobieg polskiej gospodarki

Radosław Janusz
dyrektor Biura Architektury i Rozwoju
Systemów Cyberbezpieczeństwa
w PKO Banku Polskim

Bank Polski

> Cyberodporność stała się kluczowym warunkiem ciągłości biznesu, a nie jedynie technicznym parametrem IT.



Dziś prowadzenie biznesu nie może obyć się bez cyberbezpieczeństwa. Skuteczny cyberatak może sparaliżować, a nawet zatrzymać działalność firmy. Dlatego cyberodporność jest warunkiem ciągłości działania, a nie tylko kwestią technologii. Jako największy bank w Polsce jesteśmy świadomi, że dynamiczna cyfryzacja przynosi organizacjom ogromne możliwości, ale jednocześnie zwiększa możliwości potencjalnych cyberataków.

Dlatego w bankowości odpowiedzialność za cyberodporność jest szczególna. Chronimy nie tylko bank i jego klientów, ale również zaufanie do instytucji, która odgrywa istotną rolę w polskiej gospodarce - PKO Bank Polski to około jednej trzeciej jej „finansowego krwioobiegu".

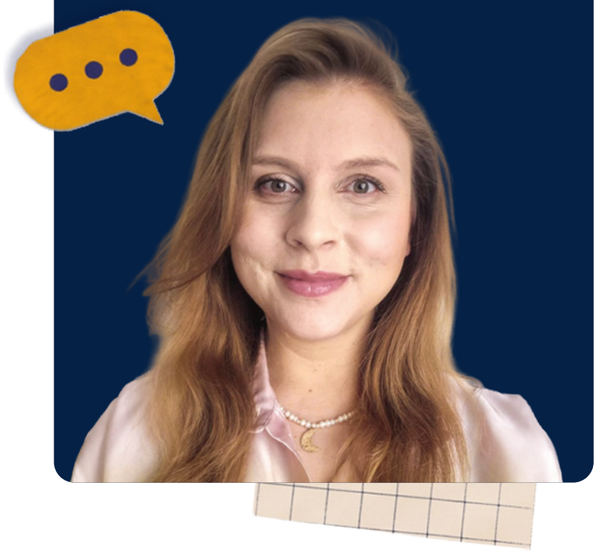
Skala zagrożeń wymaga zdecydowanych działań. Choć jak pokazuje raport Barometr Scammingu oszustwa stały się codziennym doświadczeniem wielu osób, banki pozostają naturalnym partnerem w budowaniu cyberodporności. Łączą bowiem zaufanie klientów z zaawansowanymi kompetencjami i doświadczeniem w przeciwdziałaniu nadużyciom. Dlatego stale doskonalimy technologię, procesy, a także edukujemy klientów dostarczając konkretne informacje i przykłady, jak działają oszuści i jak się chronić przed ich manipulacjami.

Współczesna bankowość to rozbudowany system zabezpieczeń, często niewidocznych dla klientów. Jednocześnie rosnąca skala i złożoność zagrożeń oraz nieustanny wyścig z cyberprzestępcami wymagają poszukiwania nowych rozwiązań. Mimo, że banki inwestują ogromne środki i zasoby w ochronę klientów, to jednak oszustwa zaczynają się dziś najczęściej na długo przed kontaktem z systemem bankowym – np. od mediów społecznościowych i wykorzystaniu tam przez oszustów socjotechniki oraz działania na emocje i wywieraniu presji na odbiorców. Dlatego skuteczna walka z cyberprzestępczością wymaga również większego zaangażowania i współodpowiedzialności wszystkich uczestników cyfrowego ekosystemu.

Naszym priorytetem jest konsekwentne budowanie dojrzałego, odpornego środowiska bezpieczeństwa, w którym ochrona klientów i ich danych stanowi fundament wszystkich działań banku.

Scamy w Polsce: stop przeciw oszustwom

Sztuczna inteligencja ułatwia doskonałe podszywanie się i kreowanie fałszywych komunikatów, ale też umożliwia prowadzenie oszustw w ogromnej liczbie.



Anna Siwińska
Partner Minds & Roses

MINDS &ROSES

Tematyka scamów jak w soczewce skupia w sobie ważne trendy dotyczące naszej rzeczywistości. Po pierwsze, żyjemy w świecie chaosu. Ważnym elementem ryzyka jest liczba i różnorodność scamów, które mogą nas dosięgnąć. 44% Polaków ma wrażenie, że zagrożenie scamami w Polsce w ciągu minionych 12 miesięcy było większe, niż wcześniej. Nie da się być stale czujnym i uważnym. Wraz ze wzrastającą ekspozycją na oszustwo, rośnie prawdopodobieństwo, że może być ono skuteczne. Po drugie, nie bez winy jest tutaj rozwój technologii, szczególnie AI. Sztuczna inteligencja ułatwia doskonałe podszywanie się i kreowanie fałszywych komunikatów, ale też umożliwia prowadzenie oszustw w ogromnej liczbie.

W oparciu o wyniki przeprowadzonego badania identyfikujemy również inne wyzwania. 46% Polaków nie wie gdzie zgłosić przypadek scamu, co trzeci (34%) nie wierzy w skuteczność takiego zgłoszenia, a co piąty (20%) odczuwa wstyd i obawia się oceny innych.

2/3 Polaków obawia się, że to właśnie ze względu na AI zagrożenie scamem będzie rosło.

W świetle powyższych wyzwań, wydaje się, że kluczowe jest podjęcie międzybranżowych działań, łączących systemy telekomunikacyjne, finansowe, czy państwowe, które udaremniałyby próby oszustw, śledziły je i w razie potrzeby, dostarczały dowodów na zaistnienie przestępstwa. Potrzebna jest również komunikacja niewiktymizująca ofiar oraz ciągła edukacja, która pozwoli wykształcić właściwe odruchy w sytuacjach zagrożenia scamem.

Warto wykorzystać potencjał wizerunkowy banków - to banki wskazywane są jako instytucje, którym Polacy ufają, i które posiadają kompetencje technologiczne, by stać się liderem bezpiecznych działań w obszarze scammingu.



46%
Polaków nie wie gdzie zgłosić przypadek scamu

SPIS TREŚCI

1. O badaniu 12
2. Wnioski i kluczowe wyniki 14
3. Barometr Dynamiki Scamu (BDS) 20
4. Stan obecny zjawiska scamów 26
5. Predykcje wobec scamów 38
6. Indeks Podatności na Scam (IPS) 44
7. Ochrona przed scamami 50
8. Zgłaszanie przestępstw 64
9. Dane demograficzne próby 70



Scam to powszechne doświadczenie, ale nie umiemy na niego właściwie reagować.

W ciągu ostatnich 12 miesięcy...

83% Polaków

Polaków otrzymywało wiadomości, telefony lub e-maile, które wyglądały na próbę oszustwa / scam.
N=1000

30%

Polaków w trakcie kontaktu z podejrzaną wiadomością, telefonem lub prośbą w Internecie rozpoczęło działanie zgodnie z instrukcją oszusta.
N=1000

16%

Polaków dało się oszukać poprzez scam.
N=1000

7%

Polaków zgłosiło przypadek scamu jakiejkolwiek instytucji (46% z oszukanych).
N=1000

Zetknięcie ze zjawiskiem scamu jest w zasadzie powszechne – **ponad 8 na 10 Polaków deklaruje, że w ciągu ostatniego roku było atakowanych podejrzanymi wiadomościami, telefonami czy e-mailami**. To, co może martwić, to **duża grupa osób, które w pierwszym odruchu zaczynają współpracować z przestępcą** – to 30% Polaków. Idąc dalej, 16% Polaków dało się nabrać na scam. Co ciekawe, wśród ofiar przeważają młodzi – 28% vs raptem 11% osób w wieku 46-65 lat; o powodach tej różnicy przeczytają Państwo w niniejszym raporcie. Widoczny jest również niewielki poziom zgłaszania przestępstw scammingowych – o oszustwie informuje organy niespełna połowa ofiar.

W poniższym opracowaniu omówimy percepcję liczby scamów i wartość poniesionych w ich konsekwencji strat, predykcje wobec tendencji zwiększania ich liczby (Percepcja ryzyka) oraz dotkniemy kwestii wpływu sztucznej inteligencji na liczbę scamów. Następnie przejdziemy do weryfikacji predyspozycji psychicznej, wiedzy i umiejętności Polaków do odpierania prób scamu, omówimy poziom stosowania zachowań ochronnych i wiedzę na temat zgłaszania przestępstw, do których faktycznie doszło. Całość materiału pozwala wychwycić jaki jest stan faktyczny, na ile jesteśmy świadomi i odporni, by zmienić go w przyszłości.

Przywołane liczby nie napawają optymizmem, ale jednocześnie nawołują do działania. Skala przestępstw jest duża, a jako społeczeństwo nadal nie jesteśmy na nie odporni.

E1. Jak często w ciągu ostatnich 12 miesięcy otrzymywałeś(aś) wiadomości, telefony lub e-maile, które wyglądały na próbę oszustwa / scam? N=1000 N1. Czy w ciągu ostatnich 12 miesięcy zdarzyło Ci się, że w trakcie kontaktu z podejrzaną wiadomością, telefonem lub prośbą w internecie rozpoczęłaś(aś) działanie zgodnie z instrukcją oszusta (np. kliknąłeś(aś) link, zacząłeś(aś) wpisywać dane, oddzwoniłeś(aś) na nieznany numer, odpowiedziałeś(aś) na wiadomość, zacząłeś(aś) przelew lub podawać dane) – ale w porę zorientowałeś(aś) się i wycofałeś(aś) się? N=813 V1. Czy w ciągu ostatnich 12 miesięcy zdarzyło Ci się, że ktoś świadomie Cię oszukał – zapłaciłe(a)ś pieniądze, podałe(a)ś dane lub przekazałe(a)ś coś wartościowego komuś, kto celowo wprowadził Cię w błąd co do tego, co w zamian otrzymasz? N=1000 I4. Wcześniej wspominałeś(aś), że w ciągu ostatnich 12 miesięcy zostałe(a)ś oszukany(a). Czy zgłosiłeś(aś) ten przypadek jakiejkolwiek instytucji (bank, policja, CERT Polska, inna)? N=160

1. O badaniu



Przebieg badania

„Barometr Scammingu” to cykliczne badanie konsumenckie monitorujące skalę, formy i ewolucję oszustw (scamów), z którymi spotykają się konsumenci.

Celem badania jest diagnoza problemu scammingu w Polsce, poziomu wiedzy Polaków, identyfikacja najczęstszych typów oszustw oraz najbardziej narażonych grup.



Metodologia:
CAWI
Ankieta internetowa
(Computer Asissted Web Interview)
długość wywiadu - 15 minut



Próba:
N=1000, reprezentatywna próba internautów w wieku 16-65 lat



Termin realizacji:
15-31.08.2026



2. Wnioski i kluczowe wyniki

Zaskakujące fakty i obserwacje z badania

Ponad

50%

młodych nie potrafi zweryfikować pracownika banku czy prawdziwości oferty.

Wydaje się, że mamy do czynienia z paradoksem podatności i pewności siebie młodego pokolenia – osoby do 29 r.ż. deklarują lepszą wiedzę, lecz jednocześnie najczęściej padają ofiarami oszustw z powodu braku odporności na różne socjotechniki oraz braku realnych umiejętności prewencyjnych.

67%

Polaków zgadza się, że rozwój AI wpływa na zwiększenie liczby i skuteczności scamów.

Sztuczna inteligencja sprawia, że liczba oszustw będzie rosnąć (73% Polaków zgadza się z tą tezą), ryzyko podszycia się pod inną osobę rośnie (77%), a jednocześnie coraz trudnej rozpoznać próbę oszustwa (74%).

64%

Polaków postrzega scam jako zjawisko powszechne.

Częściej scam zauważają starsi, niż osoby do 29 r. ż. Ale nie mówimy tylko o wrażeniach. Niemal co 4. Polak zna kogoś, kto w ciągu ostatnich 12 miesięcy został ofiarą skutecznego scamu.

37%

Polaków odczuwa, że scamy są coraz trudniejsze do wychwycenia.

44% Polaków zauważyło zwiększone zagrożenie scamami w kraju, choć wg nich, sytuacja ich bliskich jest stabilna. Coraz trudnej jednak właściwie rozpoznać oszustwa.

34%

Polaków wierzy, że to banki mogą skutecznie chronić przed scamami.

W zestawieniu banki osiągają lepsze wyniki, niż policja, CERT Polska czy operatorzy telekomunikacyjni. Banki posiadają kompetencje cyberbezpieczeństwa, a jednocześnie mają codzienny kontakt z milionami Polaków, co czyli pretekst do edukacji i wzmacniania odporności.

38,3

wyniósł Barometr Dynamiki Scamu.

Za jego wyższy poziom odpowiada przede wszystkim większa ekspozycja na scamy przy jednoczesnym poczuciu rosnącego zagrożenia, czyli skuteczności działań oszustów.

36,4

wyniósł Indeks Podatności na scam.

Poziom indeksu winduje brak działań ochronnych. O ile widoczność zjawiska scamu osiąga umiarkowane wartości, to stopień podejmowanych przez Polaków działań prewencji przed scamami jest niewystarczający.

Tylko

46%

ofiar zgłasza przypadki scamu

Główną barierą do większej zgłaszalności jest niemoc: brak wiary w to, że podjęte zostaną skuteczne działania, brak wiedzy gdzie zgłosić przestępstwo, jak i braki w dowodach. Do zgłaszania scamów zniechęcają również obawy o konsekwencje prawne lub społeczną ocenę.

Kluczowe wnioski i insighty

Działaj systemowo i współpracuj

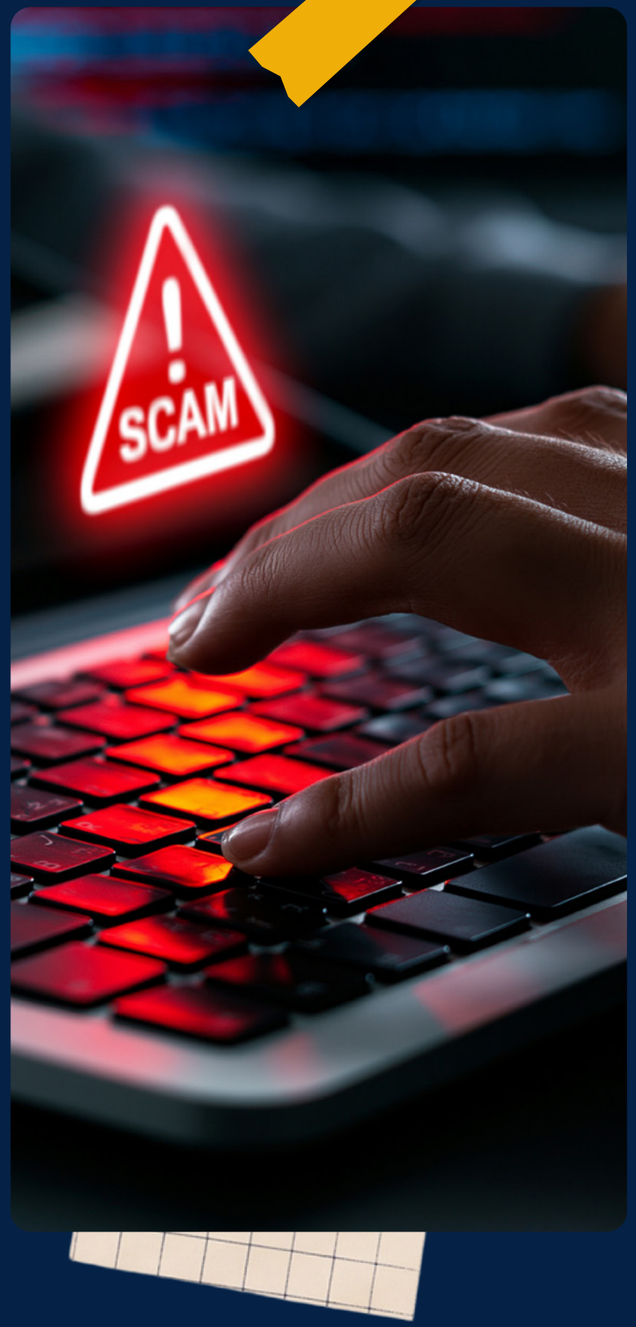
Większość scamów to ciąg zdarzeń. Dobra wymiana informacji i współpraca różnych podmiotów państwowych i prywatnych może budować cyberodporność.

Zwróć szczególną uwagę na młodych

Młodzież i młodzi dorośli działają bardziej impulsywnie i mniej krytycznie podchodzą do spotykanych ludzi i informacji. Twórz akcje, materiały, komunikaty specjalnie do nich.

Nadal istnieje potrzeba edukacji i ćwiczeń w obszarze scamów

Pomimo powszechności zjawiska, nadal wielu Polaków nie umie radzić sobie w sytuacjach oszustwa. Sprawy nie ułatwiają stale zmieniające się typy przestępstw – informuj klientów o nich na bieżąco.





Wymuszaj prawidłowe zachowania

Wiedza to nie wszystko. Użytkownicy nie zawsze stosują dostępne im możliwości prewencji. Dlatego projektuj procesy, procedury czy aplikacje tak, by wymuszały prawidłowe działania, tak samo, jak wymuszane są silniejsze hasła dostępu. Utrudniaj podejmowanie pochopnych decyzji i szybkich ruchów. Kontaktuj się z klientem, jeżeli zauważysz nietypowe zachowanie. Działaj proaktywnie i prewencyjnie.

Banki to świetni partnerzy do budowania cyberodporności

Banki mają zarówno potrzebne kompetencje, duże zaufanie, jak i codzienny pretekst do kontaktu z klientami. Buduj współprace z innymi organami, by dzięki przewagom banku lepiej edukować i chronić klientów.

3. Barometr Dynamiki Scamu (BDS)

Jak silna jest presja związana ze **scamem w Polsce**



By zilustrować zmiany w presji tworzonej przez scam, stworzyliśmy **Barometr Dynamiki Scamu (BDS)**

Barometr Dynamiki Scamu (BDS) pokazuje, jak silna jest presja związana ze scamem w Polsce. Opisuje natężenie samego zjawiska scamu.

Im wyższy BDS, tym silniejsza presja scamu. BDS składa się z trzech elementów: ekspozycji (BDS-E), oddziaływania scamu (BDS-S) oraz postrzeganej zmiany zagrożenia (BDS-O). Każdy z tych elementów ma taką samą wagę w końcowym wyniku. Barometr może przyjmować wartości od 0 do 100.

Barometr Dynamiki Scamu **Ekspozycja** (BDS-**E**)

Jak często oszuści próbują się z nami skontaktować?

Ekspozycja mówi o częstotliwości kontaktu z próbami scamu. Badanie obejmuje m.in. podejrzane SMS-y, e-maile i telefony.

Ważne jest nie tylko to, czy taki kontakt się pojawił, ale również jak często występował oraz czy takich prób jest obecnie więcej czy mniej niż wcześniej.

Wyższy BDS-E oznacza większą ekspozycję na próby oszustwa.

Barometr Dynamiki Scamu **Oddziaływanie scamu** (BDS-**S**)

Ile szkody scam rzeczywiście powoduje?

BDS-S uwzględnia m.in. to, ilu respondentów rzeczywiście zostało oszukanych, jak duże ponieśli straty, czy sytuacje oszustwa się powtarzały oraz czy ofiary zaczęły wykonywać instrukcje oszusta, zanim zorientowały się, że mają do czynienia ze scamem.

Wyższy BDS-S oznacza wyższy poziom wiktymizacji (skuteczność scamu).

Barometr Dynamiki Scamu **Postrzegana zmiana zagrożenia** (BDS-**O**)

Czy zagrożenie scamem rośnie?

BDS-O dotyczy postrzeganej zmiany zagrożenia. Respondenci oceniają, czy w porównaniu z wcześniejszym okresem zagrożenie scamem jest większe czy mniejsze – zarówno w Polsce, jak i w ich własnym otoczeniu. Oceniają również, czy próby oszustwa stały się łatwiejsze czy trudniejsze do rozpoznania.

Wysoki wynik BDS-O oznacza silniejsze poczucie, że zagrożenie rośnie i staje się trudniejsze do rozpoznania.

Dynamika presji związanej ze scamem w Polsce jest umiarkowana.

Napędza ją przede wszystkim percepcja rosnącego zagrożenia.

Barometr Dynamiki Scamu (BDS)

wyniósł

38,3



Ekspozycja (BDS-**E**)

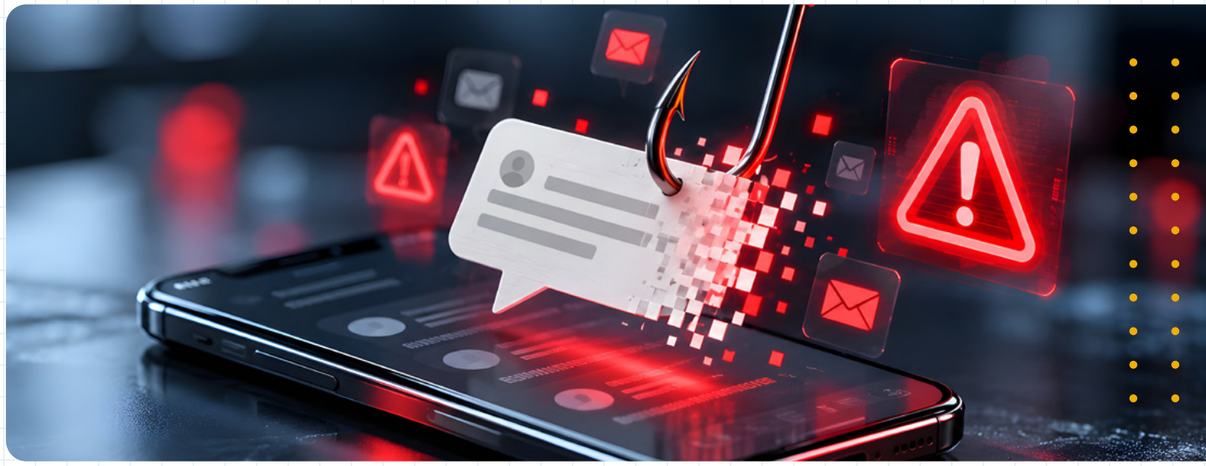
42,4

Oddziaływanie scamu (BDS-**S**)

15,2

Postrzegana zmiana zagrożenia (BDS-**O**)

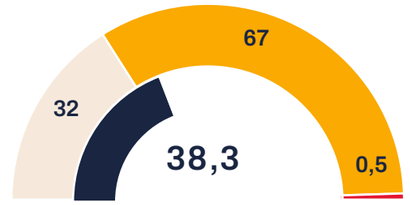
57,4





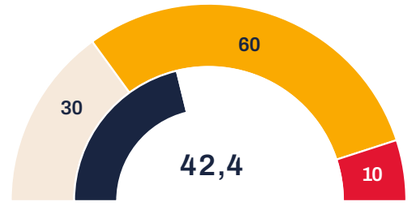
Barometr Dynamiki Scamu (BDS)

38,3



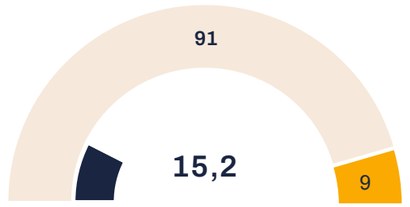
Ekspozycja (BDS-**E**)

42,4



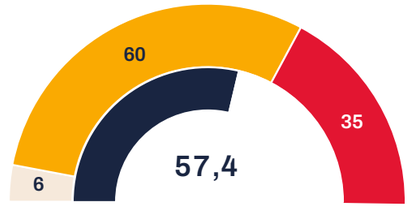
Oddziaływanie scamu (BDS-**S**)

15,2



Postrzegana zmiana zagrożenia (BDS-**O**)

57,4



Analizując składowe BDS, widzimy, że największy spokój czuć w obszarze szkód faktycznie wyrządzanych przez scam – BDS w obszarze Oddziaływania scamu przyjmuje wartość 15,2. Równolegle dostrzegamy, że scamów wokół Polaków jest coraz więcej – ekspozycja na nie rośnie (wartość BDS w obszarze Ekspozycji przyjmuje wartości umiarkowane, 42,4), przy jednoczesnym wzroście zagrożenia oszustwem (BDS Postrzeganej zmiany zagrożenia to 57,4 – to wynik zbliżający się do wysokiej wartości indeksu).

W kolejnych dwóch rozdziałach omówimy stan obecny zjawiska scamów oraz nastroje Polaków co do przyszłości tego zjawiska.

Wynik dla rynku | Niska wartość indeksu | Umiarkowana wartość indeksu | Wysoka wartość indeksu

4. Stan obecny zjawiska scamów

Percepcja liczby scamów i wartość poniesionych w ich konsekwencji strat



W oczach Polaków skala scamów jest na tyle duża, że **postrzegamy je jako element naszej codzienności.**

Niemal

2/3 Polaków

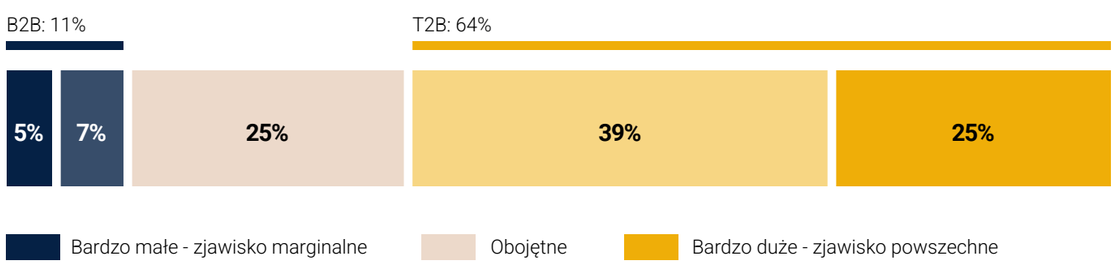
postrzega scam jako zjawisko powszechne.

Dane wskazują, że...

wyzwaniem może okazać się skuteczne dotarcie do młodych dorosłych z informacjami o scamie.

Odczucie większego natężenia zjawiska scamów mają starsi – zauważa je 55% osób do 29 r.ż. i aż 69% osób po 46 r.ż.; podobną zależność widać wśród osób wyżej wykształconych. Taka percepcja może wynikać nie tyle z większej świadomości problemu, co także z częstszego kontaktu z mediami i uważnego ich śledzenia.

Postrzeganie skali zjawiska scamu poprzez informacje w Internecie i innych mediach



R2. Na podstawie tego, co słyszysz lub czytasz w Internecie i innych mediach, jak oceniasz skalę problemu oszustw internetowych i telefonicznych w Polsce - jak powszechne jest to zjawisko? N=1000

Zjawisko scamu nie tylko wydaje się powszechne, ale i szeroko odczuwalne.



Niemal

co 4. Polak

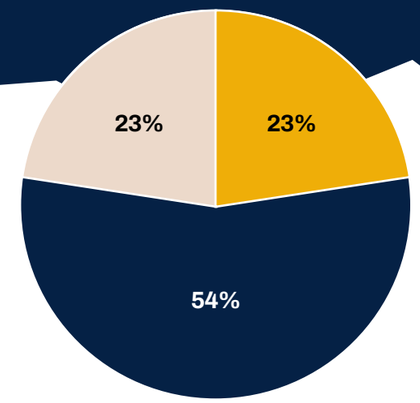
zna kogoś, kto został ofiarą scamu w ciągu ostatnich 12 miesięcy.



Poczucie wszechobecności scamu nie bierze się jedynie z kontaktu z notkami prasowymi. 23% Polaków potwierdza, że ktoś z ich najbliższego otoczenia został skutecznie oszukany poprzez celowe wprowadzenie w błąd.

Osobista znajomość z kimś, kto został ofiarą scamu w ciągu ostatnich 12 miesięcy





Wyniki te nie różnią się pomiędzy poszczególnymi grupami, co wskazuje na szeroką i powszechną skalę zjawiska.

V6. Czy znasz kogoś z Twojego najbliższego otoczenia, kto w ciągu ostatnich 12 miesięcy został oszukany - zapłacił pieniądze lub podał dane komuś, kto celowo go wprowadził w błąd? N=1000



Trzeba stale być czujnym - scamy otrzymujemy z dużą częstotliwością i różnymi kanałami. Oszuści stosują bardzo zróżnicowaną paletę scamów.

26% Polaków

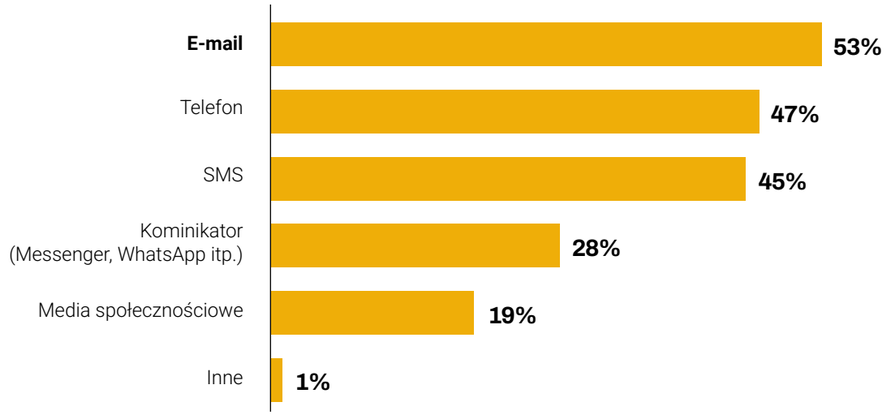
otrzymywało w ciągu ostatnich 12 miesięcy scamy częściej, niż kilka razy w miesiącu.

Zarówno sposoby podjęcia prób oszustwa, jak i typy prób oszustwa są bardzo zróżnicowane. Przestępcy kontaktują się różnorodnymi sposobami, a poszczególne kanały kontaktu (w tym komunikatory) są podobnie popularne we wszystkich grupach wiekowych.

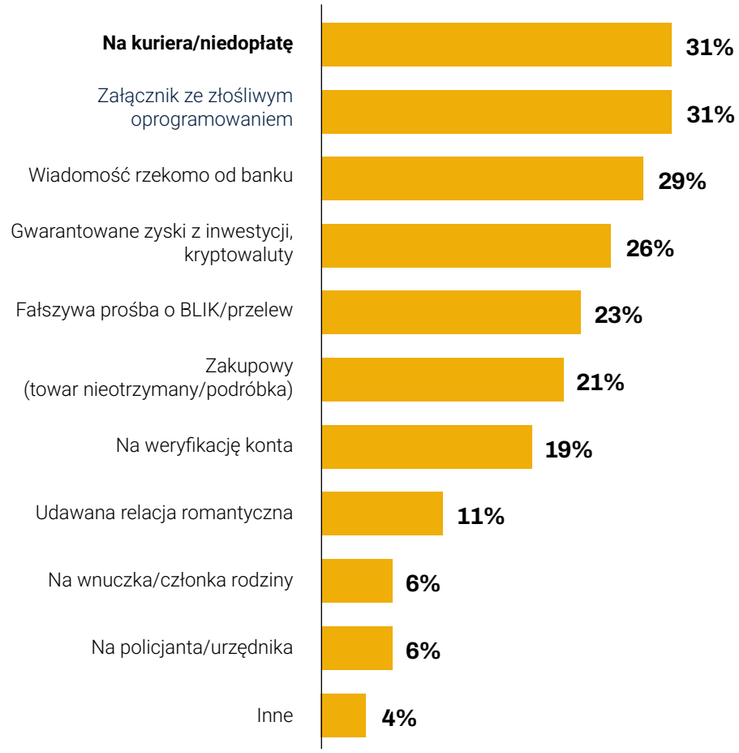
Rodzaje oszustw są zróżnicowane, od tych „fabularnych": „na kuriera" czy „na wnuczka", poprzez fałszywe informacje finansowe, aż po oszustwa technicznologiczne np. wysyłanie wirusów.

Mnogość dróg dotarcia do potencjalnych ofiar i pomysłów na oszustwo stanowi ogromne wyzwanie edukacyjne i prewencyjne. Nie należy marginalizować żadnego kanału kontaktu, ani żadnego rodzaju scamów.

Sposób podjęcia prób oszustwa



Rodzaj scamu



E1. Jak często w ciągu ostatnich 12 miesięcy otrzymywałeś(aś) wiadomości, telefony lub e-maile, które wyglądały na próbę oszustwa / scam? N=1000
E2. W jaki sposób dochodziło do tych prób oszustwa? N=813
E3. Z jakim rodzajem podejrzanej wiadomości/kontaktu się zetknąłeś/zetknęłaś? N=813

Choć Polscy mają świadomość występowania oszustw, nie każdy umie je nazwać i rozróżnić ich typy.

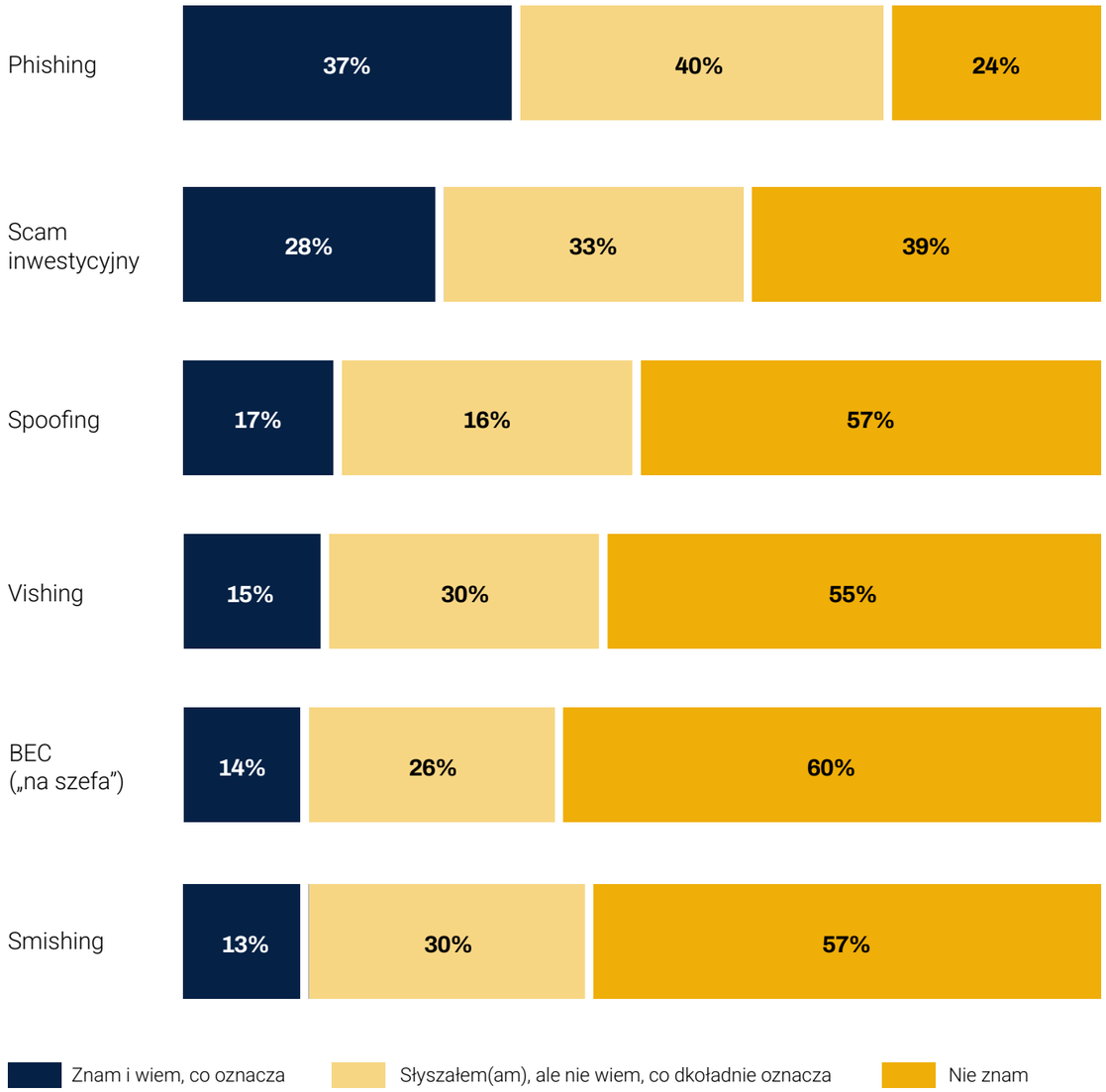
41% Polaków

rozumie znaczenie słowa „scam”.



Znajomość pojęć związanych ze scamem

Częściej do znajomości nazw poszczególnych oszustw przyznają się osoby młodsze, do 29 r.ż. np. 61% z nich słyszało o słowie „scam” (vs 41% ogółu Polaków). Wyjątkiem jest tu Phishing, którego znajomość jest największa w grupie 30-45 lat, co może świadczyć o pewnej skuteczności tradycyjnych form edukacji (szkolenia, testy w pracy, wiadomości w internecie i prasie).



W3. Czy znasz poniższe określenia: N=1000; Osoby do 29 r.ż. N=204

Scamy są skuteczną metodą oszustwa
- przekonanie ofiary do podążenia za instrukcjami oszusta jest częstsze, niż można by się spodziewać.

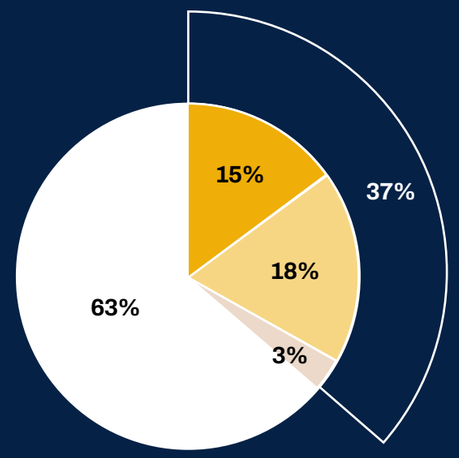
37%



osób, z którymi skontaktował się oszust rozpoczęło działania wg jego instrukcji.

Podjęcie działań zgodnie z intencją oszusta w ciągu ostatnich 12 miesięcy

Do podjęcia działań zgodnie z intencją sprawcy przyznają się dużo częściej młodzi w wieku do 29 r.ż. – takie zachowanie potwierdza aż 60% z nich (w porównaniu do 37% osób w wieku 30-45 lat i 25% w wieku 46-65 lat.



Nie | Tak, jedna taka sytuacja | Tak, kilka (2-3) | Tak, wiele (4 i więcej)

N1. Czy w ciągu ostatnich 12 miesięcy zdarzyło Ci się, że w trakcie kontaktu z podejrzaną wiadomością, telefonem lub prośbą w internecie rozpoczęłeś(aś) działanie zgodnie z instrukcją oszusta? N=813

Martwi szczególnie duży odsetek oszukanych, nawet kilkukrotnie, **wśród młodych dorosłych.**



16% osób

przyznaje, że stało się ofiarą scamu w ciągu ostatnich 12 miesięcy. 42% z nich zostało ofiarą oszustwa więcej niż raz.

Młodzi nie tylko częściej zauważają, że zaczęli postępować zgodnie z intencją oszusta, ale też realnie częściej padają jego ofiarami. Oznacza to, że kluczowe jest budowanie ich czujności i odporności na oszustwa.

W przypadku finalizacji oszustwa również przodują młodzi – aż 28% zostało ofiarą oszustwa (vs. 15% 30-45 latków i 11% 46-65-latków). To też oni padają ofiarami scamu kilkukrotnie.

Padnięcie ofiarą scamu w ciągu ostatnich 12 miesięcy



Jak często respondenci padli ofiarą scamu w ciągu ostatnich 12 miesięcy?



V1. Czy w ciągu ostatnich 12 miesięcy zdarzyło Ci się, że ktoś świadomie Cię oszukał – zapłaciłe(a)ś pieniądze, podałe(a)ś dane lub przekazałe(a)ś coś wartościowego komuś, kto celowo wprowadził Cię w błąd co do tego, co w zamian otrzymasz? N=1000
V2. Czy była to jedna sytuacja, czy kilka odrębnych przypadków? N=160

Oszustwa finansowe zdarzają się częściej, niż wyłudzenia danych. **Najczęściej kwota przestępstwa to kilka tysięcy złotych.**

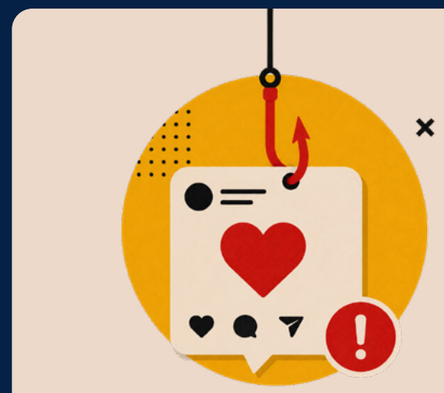
Kwoty oszustw wskazują, że część ze scamów jest przestępstwem z punktu widzenia prawa, więc śledztwo w ich sprawie mogłoby być podjęte.



Charakter łupu różni się nieco między pokoleniami

Oszustwa związane z wyłudzeniem pieniędzy dotykają nieco częściej starszych, natomiast scamy dot. niesfinalizowanych sprzedaży dotyczą raczej osób młodych.

Przestępstwa dot. wyłudzenia danych dotykają wszystkie grupy po równo.



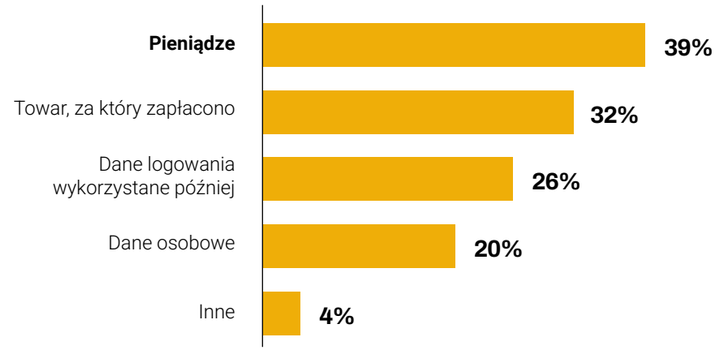
Większość scamów to nie groszowa sprawa

1000-5000 zł to najczęściej wskazywana wartość straty.

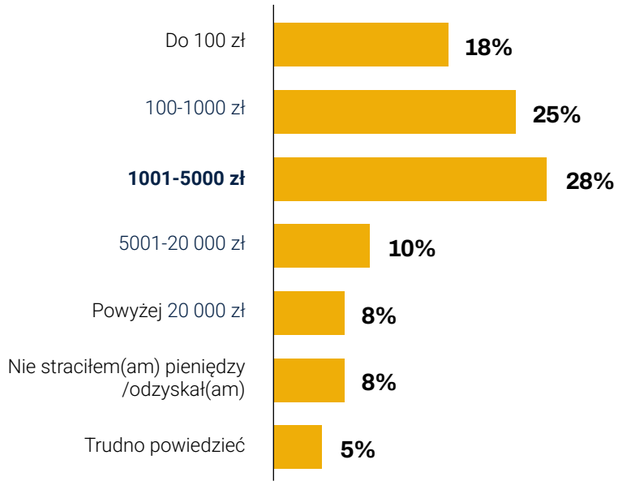
Co ciekawe 18% oszukanych wskazywało kwoty wyższe niż 5000 zł. Nawet młodzi są oszukiwani na wyższe kwoty.



Charakter straconych dóbr



Wartość straty



V3. Co dokładnie straciłe(a)ś? N=160
V4. Jaka była w przybliżeniu łączna wartość straty finansowej - czyli ile pieniędzy ostatecznie nie odzyskałe(a)ś? N=160

5. Predykcje wobec scamów

Szacunki wobec przyszłej skali scamów oraz wpływ AI na zjawisko oszustw zdalnych

W ciągu ostatnich 12 miesięcy obawialiśmy się scamów bardziej, niż w ciągu nadchodzących 12 miesięcy, ale ta tendencja wyhamowuje.

44% Polaków

ma wrażenie, że zagrożenie scamami w Polsce w ciągu minionych 12 miesięcy było większe, niż przed poprzednimi 12 miesiącami.

Odczucie wobec zagrożenia scamem wśród bliskich w ciągu...

Spokojniej Polacy myślą o ew. zagrożeniu dla ich bliskich – 32% miało poczucie, że zagrożenie oszustwem wobec ich bliskich wzrosło.

W nadchodzących 12 miesiącach nieco optymistyczniej patrzymy w przyszłość – nadal 32% Polaków spodziewa się zwiększenia zagrożenia scamem ich bliskich, ale 41% uznaje, że zagrożenie to pozostaje na niezmienionym poziomie, a aż 28% liczy, że zagrożenie to zmaleje.

Powoli oswajamy się z obecnością scamów. Stałe działania technologiczne i edukacyjne po stronie dostawców usług mogą skutecznie mitygować stres związany z ekspozycją nas czy naszych bliskich na oszustwa.



R4a. Czy w ciągu ostatnich 12 miesięcy, w porównaniu z wcześniejszymi 12 miesiącami, zagrożenie oszustwami internetowymi i telefonicznymi w Polsce było Twoim zdaniem mniejsze: N=1000
R4b. Czy w ciągu ostatnich 12 miesięcy, w porównaniu z wcześniejszymi 12 miesiącami, zagrożenie oszustwami internetowymi i telefonicznymi wśród Ciebie, Twojej rodziny i znajomych było: N=1000
R1b. Na ile prawdopodobne jest, że ktoś z Twojego najbliższego otoczenia w ciągu najbliższych 12 miesięcy będzie mieć kontakt z próbą oszustwa internetowego lub telefonicznego? N=1000

W minionym roku 79% Polaków nie odczuło zwiększenia liczby scamów. **Większym problemem wydaje się trudność w rozpoznaniu oszustw.**

37% Polaków

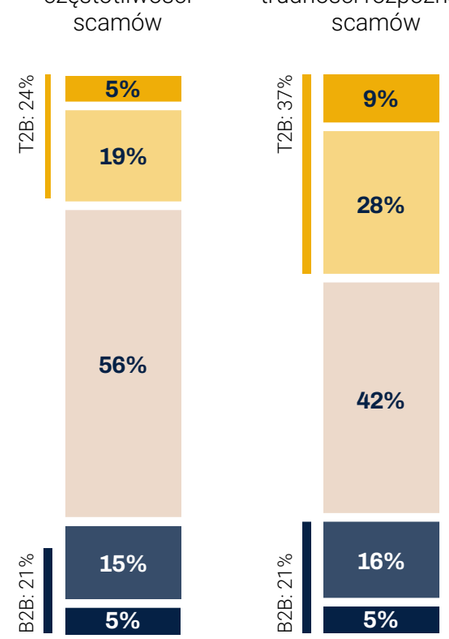
odczuwa, że scamy stają się coraz trudniejsze do wychwycenia.



Zmiany zaobserwowane w ostatnich 12 miesiącach w zakresie...

Co interesujące wyższy poziom obaw wobec trudności rozpoznania scamu wyrażają osoby częściej stosujące zabezpieczenia (40% dla osób silnie zabezpieczających się przed oszustwami vs. 31% dla osób przeciętnie chroniących siebie przed scamem).

Wiedza na temat zabezpieczeń, jak i świadomość zagrożeń odkrywają przed Polakami rozumienie złożoności mechanizmów oszustwa. Jednocześnie, im więcej się wie, tym większej liczby czy typów scamów można się obawiać.



E4. Czy w ostatnich 12 miesiącach prób scamu było mniej, mniej więcej tyle samo, czy więcej niż w poprzednich 12 miesiącach? N=813
R5. Czy w ciągu ostatnich 12 miesięcy, w porównaniu z wcześniejszymi 12 miesiącami, próby oszustwa internetowego i telefonicznego stały się Twoim zdaniem: N=1000

Rozwój sztucznej inteligencji istotnie zwiększa poczucie zagrożenia scamem i potrzebę systemowego wsparcia klientów.

67% Polaków

przyznaje, że rozwój sztucznej inteligencji sprawia, iż mocniej obawia się oszustw.

Rozwój technologii AI sprawia, że scamy można robić dużo szybciej, taniej i na wielką skalę. Przestępcy się profesjonalizują, stawiając profesjonalne firmy do obsługi scamów, a łączenie skutecznych socjotechnik z lepiej spreparowanymi fałszywymi materiałami oraz rosnącą skalą prób scamów zwiększają skuteczność oszustów. Zmiany te zauważają Polacy.

Po pierwsze, spodziewany jest wzrost liczby przestępstw scammingowych z użyciem AI – 74% Polaków uważa to za prawdopodobne. Skalowanie działalności opartej na oszustwach, również poprzez komunikaty z innych państw, jest dziś tanie i szybkie.

Przy wzmożonej liczbie prób scamu, rośnie ryzyko, że scam przyniesie realną szkodę.

Po drugie, AI komplikuje kwestię rozpoznania próby oszustwa (rośnie dezinformacja, spreparowane materiały są dużo lepszej jakości), jak i zwiększa ryzyko podszywania się pod inne osoby (z tymi tezami zgadza się odpowiednio 74% i 77% Polaków). W tym obszarze konieczne są działania instytucjonalne – skoordynowane działania Cyber Threat Intelligence (CTI), wzmacnianie systemów wykrywających AI.





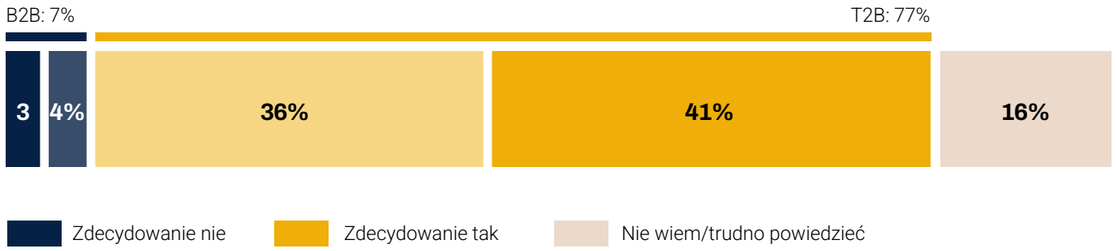
Sztuczna inteligencja sprawia, że **trudniej rozpoznać próbę oszustwa**



W przyszłości **liczba prób oszustw będzie rosła** z powodu rozwoju sztucznej inteligencji



Sztuczna inteligencja **zwiększa ryzyko podszywania się pod inne osoby** (np. głos lub wizerunek)



A1. Na ile zgadzasz się z następującymi stwierdzeniami dotyczącymi wykorzystania sztucznej inteligencji (AI)? N=1000

6. Indeks Podatności na Scam (IPS)

Na ile jesteśmy
podatni na scam



Indeks Podatności na Scam (IPS)
podsumowuje zachowania Polaków, cech i stosunku do zagrożeń mogących zwiększać prawdopodobieństwo zostania ofiarą scamu.

Najważniejszym indeksem opisującym zachowania ludzi jest Indeks Podatności na Scam (IPS). Ma pokazywać, na ile zestaw naszych cech, sposobu postrzegania zagrożenia i codziennych zachowań może sprzyjać skutecznemu oszustwu.

Im wyższy IPS, tym większa podatność na scam. IPS przyjmuje wartości od 0 do 100 i składa się z trzech elementów, a każdy ma taką samą wagę w wyniku końcowym. Pierwszy dot. naszych predyspozycji i zachowań (IPS-P), drugi – jak postrzegamy zagrożenie (IPS-R), a trzeci – jak się przed nim chronimy (IPS-O).

Indeks Podatności na Scam **Predyspozycje psychologiczne** (IPS-**P**)

Czy łatwo dajemy się zmanipulować?

Badanie sprawdza m.in., czy respondenci mają skłonność do impulsywnego wydawania pieniędzy, ufa nieznajomym, ulega osobom brzmiącym profesjonalnie albo podejmuje decyzje pod presją czasu. To zachowania, które mogą być wykorzystywane przez oszustów.

Wyższy wynik IPS-P oznacza bardziej ryzykowny profil predyspozycji.

Indeks Podatności na Scam **Percepcja ryzyka** (IPS-**R**)

Czy widzimy zagrożenie?

Respondenci oceniają m.in., czy sami mogą zetknąć się z oszustwem, czy scam jest zagrożeniem dla ich bliskich oraz jak duża jest – ich zdaniem – skala tego problemu.

Wyższy wynik IPS-R oznacza większą świadomość zagrożenia, a więc jest korzystny z punktu widzenia bezpieczeństwa. Dlatego w konstrukcji końcowego IPS ten komponent jest odwracany.

Indeks Podatności na Scam **Zachowania ochronne** (IPS-**O**)

Czy rzeczywiście stosujemy zasady bezpieczeństwa?

Badanie sprawdza m.in., czy używamy różnych haseł, korzystamy z uwierzytelniania dwuskładnikowego, sprawdzamy adresy stron internetowych i nadawców wiadomości oraz czy nie klikamy pochopnie w podejrzane linki.

Im wyższy IPS-O, tym lepsze deklarowane praktyki ochronne. Ponieważ lepsza ochrona oznacza mniejszą podatność, także ten wynik jest odwracany przy obliczaniu końcowego IPS.

Poziom indeksu podatności na scam nie zachwyca szczególnie ze względu na niski stopień podejmowania działań ochronnych.

Indeks Podatności na Scam (IPS)

wyniósł

36,4



Predyspozycje psychologiczne (IPS-**P**)

34,7

Percepcja ryzyka (IPS-**R**)

53,9

Zachowania ochronne (IPS-**O**)

71,5

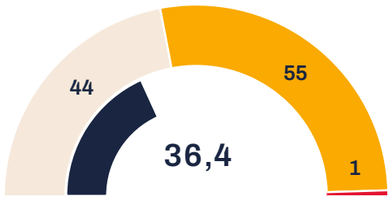
Wśród młodych dorosłych, do 29 r.ż., IPS wyniósł aż 42,9, czyli o 6,5 pkt. więcej, niż dla ogółu populacji i o 9,8 pkt. więcej, niż dla grupy 46-65 lat.

Różnice w wynikach dla najmłodszej grupy dorosłych wynikają przede wszystkim z wyższego wyniku IPS – P – predyspozycji psychologicznych. Dla ogółu Polaków przyjął on wartości niskie (34,7), a dla osób do 29 r.ż. Wartość umiarkowaną – 43,7.

Szczególną uwagę warto poświęcić wysokiej wartości IPS w obszarze działań ochronnych (71,5). Wynik ten cieszy, bo świadczy o dużej świadomości jak chronić się przed scamem.

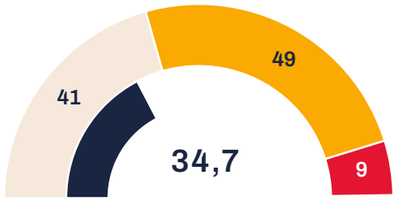
Indeks Podatności na Scam (IPS)

36,4



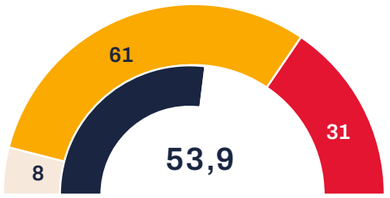
Predyspozycje psychologiczne (IPS-**P**)

34,7



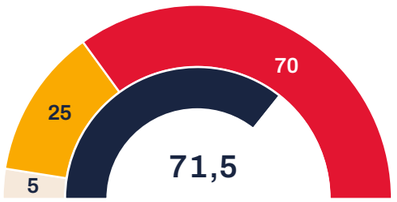
Percepcja ryzyka (IPS-**S**)

53,9



Zachowania ochronne (IPS-**O**)

71,5



Wynik dla rynku | Niska wartość indeksu | Umiarkowana wartość indeksu | Wysoka wartość indeksu

W kolejnych rozdziałach opisujemy jakie działania ochronne już podejmują Polacy, a które nadal zaniedbują; jakie sytuacje nadal są furtką dla oszustów. Analizujemy jak wygląda znajomość instytucji, do których można zgłaszać oszustwa; co zachęca, a co odwodzi od zgłaszania scamów.

O ile percepcja ryzyka scamu wydaje się duża – większość Polaków ma świadomość istnienia tego zjawiska – o tyle Indeks Podatności na Scam osiąga niską wartość dla ogółu Polaków.

Jednak odporność na oszustwa nie jest taka sama w całym społeczeństwie.



7. Ochrona przed scamami

Predyspozycje psychologiczne, wiedza i umiejętności dot. reagowania na scamy, działania ochronne

Większość Polaków wie trochę o scamach, ale nie czuje się pewnie w tym temacie.

Niecała 1/3

Polaków ocenia dobrze swoją wiedzę i umiejętności odnośnie unikania scamów.

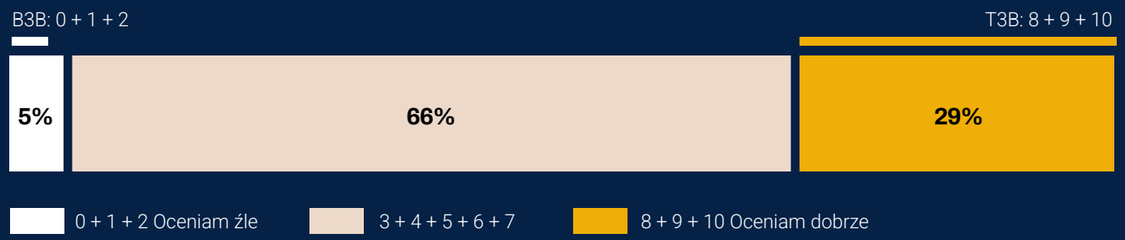
Delikatnie lepiej znajomość tematu oszustw internetowych i telefonicznych oraz własnych kompetencji w tym obszarze ocenia najmłodsza grupa – młodych dorosłych do 29 r.ż. Biorąc pod uwagę ich równoczesną ufność i otwartość do szybkiego działania, również pod wpływem osób trzecich – przecenianie swoich możliwości może być niebezpieczną furtką do stania się ofiarą oszustwa.

Warto zastanowić się nad miejscami, programami, w ramach których będzie można zweryfikować swoją wiedzę i ćwiczyć na bieżąco kompetencje przeciwdziałania scamom. Praktyczny trening i zderzenie się z własnymi błędami mogą być skuteczną drogą do stopniowego nabierania czujności.

Ocena **własnej wiedzy** na temat oszustw internetowych i telefonicznych



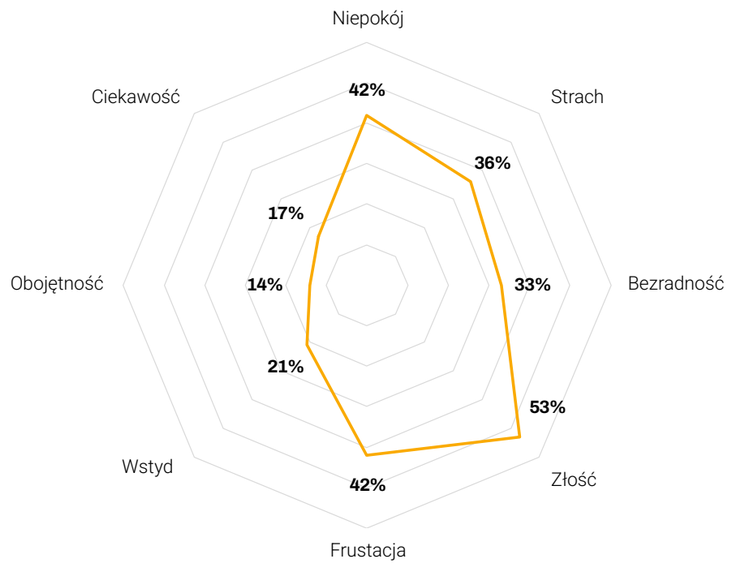
Ocena **własnych umiejętności** w zakresie identyfikacji i unikania prób oszustw internetowych i telefonicznych



W1. Jak oceniasz swoją wiedzę na temat oszustw internetowych i telefonicznych: N=1000
W2. Jak oceniasz swoje umiejętności w zakresie identyfikacji i unikania prób oszustw internetowych i telefonicznych: N=1000

Na myśl o scamie czujemy przede wszystkim aktywne emocje: złość, frustrację. Mogą one napędzać do działania.

Emocje wśród klientów banków podejmujących działania odpowiedzialne społecznie



53% Polaków

na myśl o byciu oszukanym czuje przede wszystkim złość.

Złość i frustracja są najczęściej wskazywanymi emocjami, gdy Polacy wyobrażają sobie sytuację, w której zostali ofiarą scamu. Takie emocje mogą prowadzić do działań – tylko czy faktycznie je podejmujemy w odpowiedniej skali? Z drugiej strony, smucić może duża popularność emocji pasywnych: niepokój (42%), strach (36%) czy bezradność (33%).

W działaniach społecznych, edukacyjnych warto dawać narzędzia do działania, by wspierać aktywne emocje: uczyć, jak zgłaszać scam, jak mu przeciwdziałać, zachęcać do dzielenia się swoim doświadczeniem z oszustwem wśród bliskich czy w lokalnych społecznościach. Należy być uważnym wobec (nawet nieświadomej) wiktymizacji ofiar i wzbudzania w nich poczucia wstydu, prowadzącego do zatajania przypadków scamu.

R3. Jakie uczucia towarzyszą Ci, gdy myślisz, że możesz stać się ofiarą oszustwa internetowego lub telefonicznego? N=1000 Pokazano odpowiedzi TOP2, czyli sumę odpowiedzi [5] Bardzo silnie odczuwam to uczucie+[4] Raczej silnie odczuwam to uczucie: N=1000

Młodzi Polacy znacznie częściej, **niż ogół populacji wydają pieniądze impulsywnie**, co silniej naraża ich na zostanie ofiarą scamu.

65% osobom do 29 r.ż.

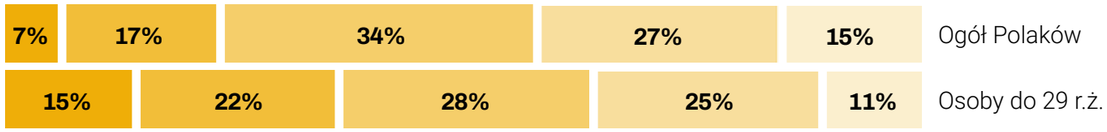
zdarza się pomyśleć przynajmniej czasami, że oszuści raczej ich nie oszukają.

Tymczasem, młodzi dorośli to najbardziej podatna na oszustwa grupa: aż 40% z nich co najmniej czasami ulega naciskom ze strony osób, które brzmią pewnie siebie i profesjonalnie, 59% min. czasami ufa ludziom, których wcześniej nie znało, 42% działa szybko na hasła typu „oferta tylko dziś".

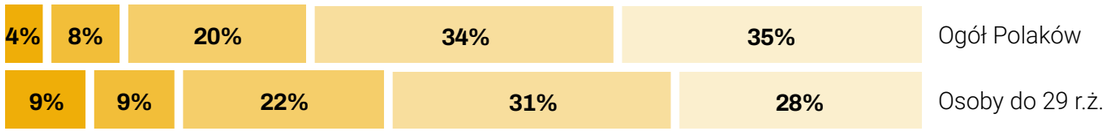
Oznacza to, że szczególnie młodzi narażeni są na scamy typu APP – „authorized payment scams", w których ktoś naciska na szybkie dokonanie transakcji.



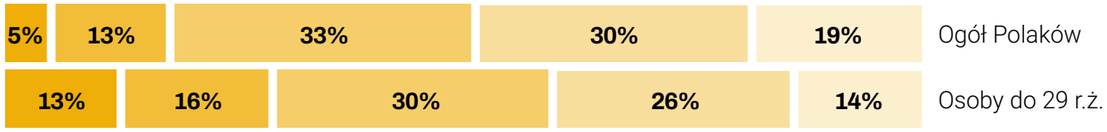
Jak często zdarza Ci się pomyśleć, że Ciebie oszuści raczej nie oszukają.



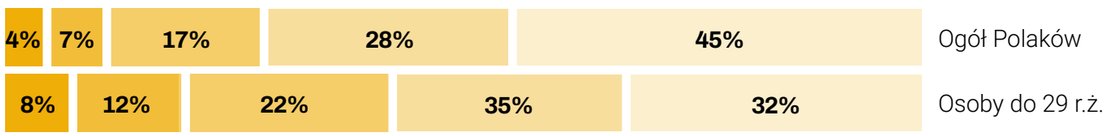
Mam tendencję do ulegania próbom lub naciskom ze strony osób, które brzmią pewnie siebie i profesjonalnie (np. podają się za pracowników banku, urzędu, firmy).



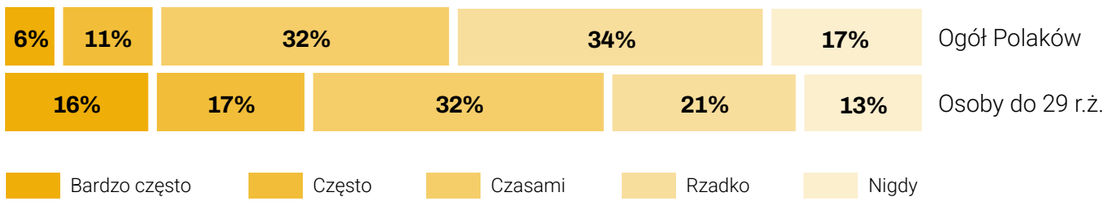
Zdarza mi się ufać osobom, które wcześniej nie znałem(am), jeśli wydają się życzliwe i pomocne.



Kiedy ktoś mi mówi, że muszę zareagować natychmiast - np. „oferta tylko dziś", „jak nie potwierdzisz teraz, stracisz pieniądze" - działam szybciej niż zwykle, bez pełnego zastanowienia.

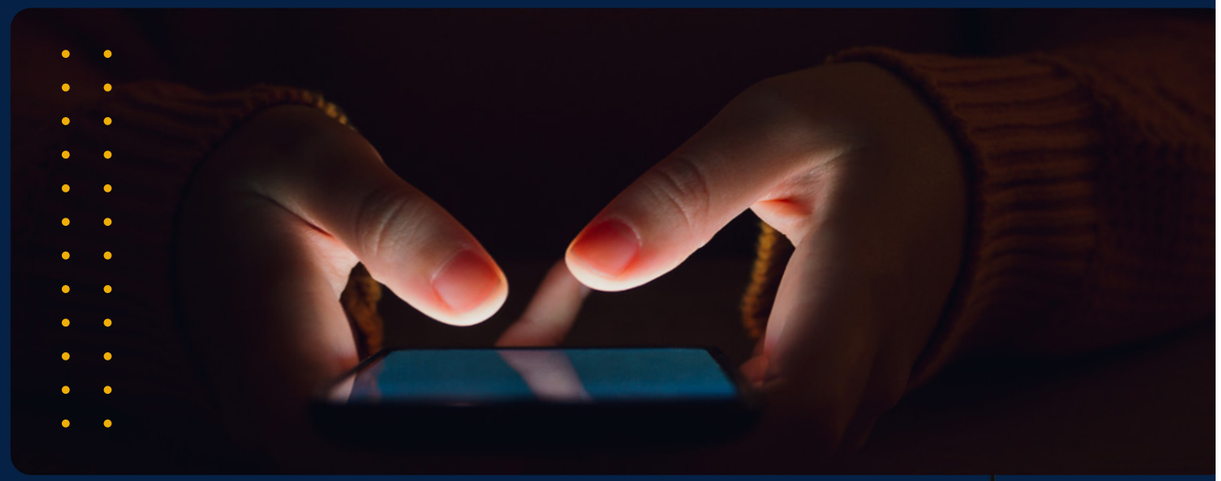


Zdarza mi się wydawać pieniądze impulsywnie, bez wcześniejszego zastanowienia się - pod wpływem chwili.



P1. Za chwilę zobaczysz różne stwierdzenia. Korzystając ze skali od 1 do 5, zaznacz jak często zdarza Ci się postępować lub zachowywać w opisany sposób. Ogół Polaków N=1000; Osoby wieku do 29 r.ż. N=204

Młodzi Polacy istotnie gorzej oceniają swoje umiejętności rozpoznania oszustwa, niż starsze od nich pokolenia.



Ponad

50% młodych

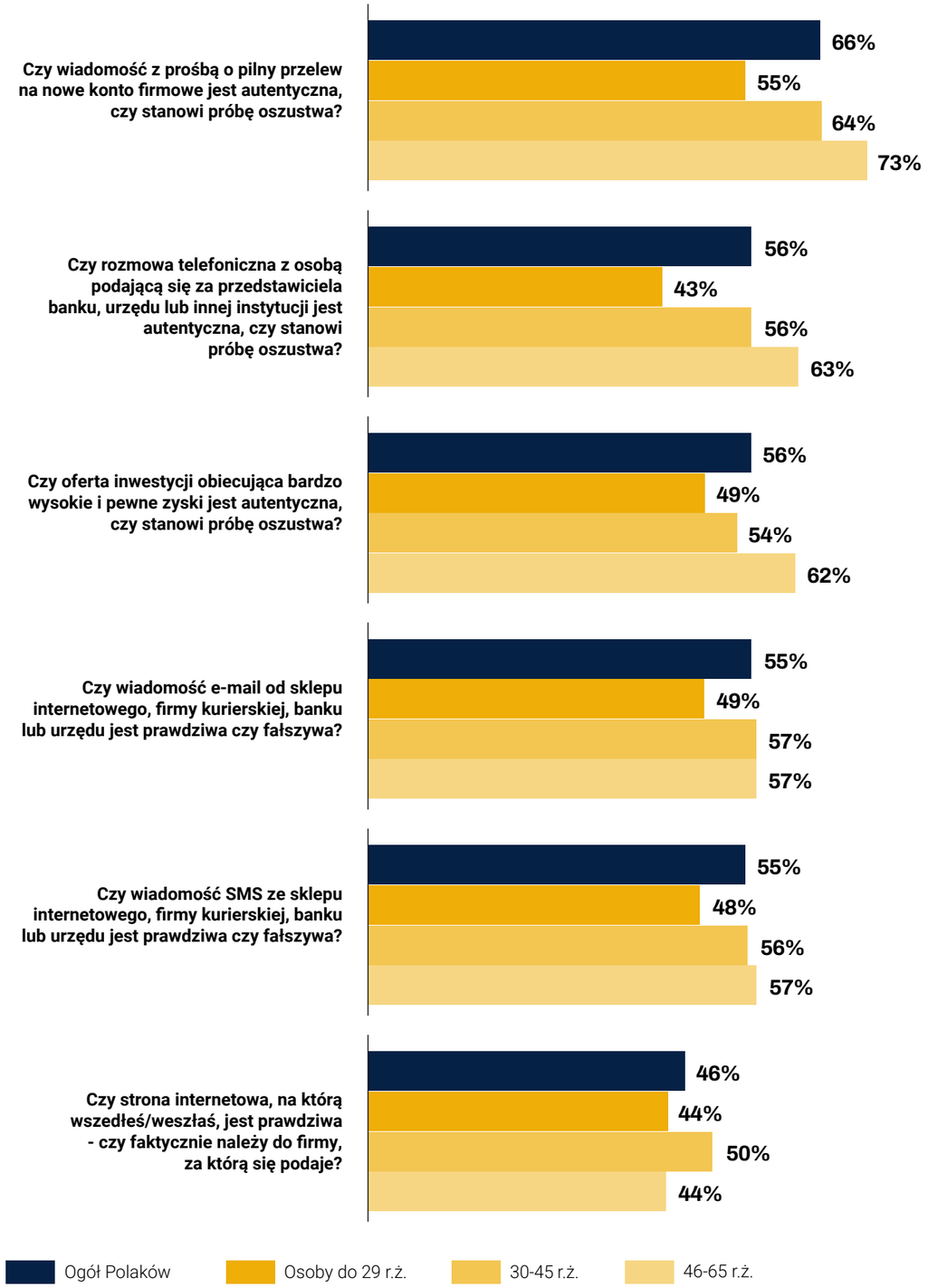


nie potrafi zweryfikować pracownika banku czy prawdziwości oferty inwestycyjnej.

Okazuje się, że osoby do 29 r.ż. są nie tylko emocjonalnie i społecznie podatne na socjotechniki przestępców. Brakuje im również wiedzy i umiejętności do krytycznej oceny prawdziwości wiadomości, telefonów, ofert. Oczywiście, wśród starszych pokoleń również sytuacja mogłaby być lepsza, szczególnie w obszarze weryfikacji prawdziwości stron internetowych.

Weryfikacja stron internetowych, SMSów i emaili to kluczowe obszary do edukacji, szczególnie wśród młodych.

Umiejętność samodzielnej weryfikacji poniższych zdarzeń



W4. Czy potrafił(a)byś samodzielnie sprawdzić poniższe informacje: N=1000; Pokazano odpowiedzi Top 2 Box, czyli sumę odpowiedzi [5] Zdecydowanie tak + [4] Raczej tak.



Niestety, ofiary scamu w ponad połowie przypadków nie zmieniają znacząco swojego postępowania.

51% Polaków

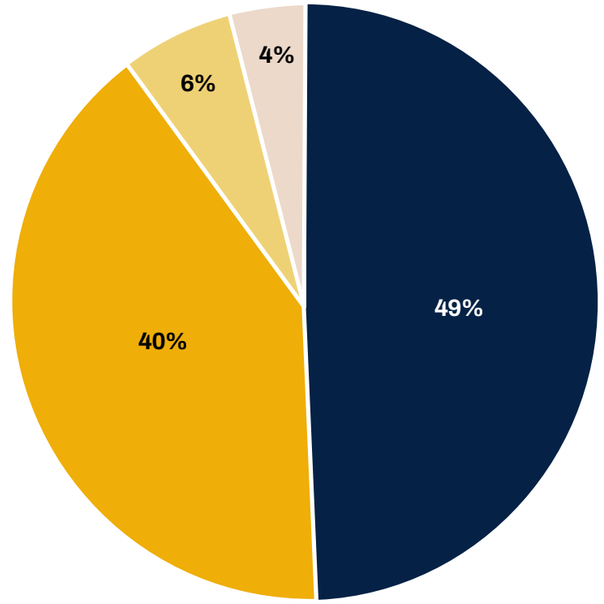
nie zmieniło całkowicie swojego zachowania po padnięciu ofiarą scamu.

Jednocześnie, 40% przyznaje, że wprowadziło jedynie drobne zmiany swojego zachowania, a 6% nie zmieniło nic.

Choć mamy świadomość, że technologia idzie do przodu, a sztuczna inteligencja ułatwia oszustom pracę, to nadal działania ofiar są częstokroć kluczem do sukcesu przestępców. Oszustwa takie jak „obieranie świniaka" czy, wspomniany już, APP opierają się na sprawdzonych socjotechnikach.

Regularne ćwiczenie umiejętności krytycznego podchodzenia do kontaktów i informacji oraz stałe przypominanie o pozostawaniu w czujności wydają się kluczowymi elementami walki ze scamem.

Zmiana zachowania po tym, jak zostało się poszkodowanym w wyniku oszustwa, scamu



V5. Czy Twoje zachowanie / podejście po tym jak padłeś(aś) ofiarą oszustwa uległo zmianie? N=160

Wiele działań zabezpieczających dostęp do kluczowych kont jest podejmowanych. **Zwiększenia popularności wymaga zastrzeżenie PESELu.**

56% Polaków

ma zastrzeżony numer PESEL.

Dbałość o skomplikowane hasła, zmianę haseł są od lat tematem komunikacji zarówno pracodawców, szkoły, jak i instytucji takich jak banki. Stałe informacje na ten temat, wymuszenie odświeżania haseł, wymyślania haseł trudnych, upomnienia, by nie podawać haseł osobom postronnym stale zagościły w UX większości stron finansowych czy e-commerce.

Efekt jest widoczny: 90% Polaków ma zróżnicowane hasła, 76% stosuje dwuskładnikowe uwierzytelnianie przy logowaniu do banku czy na pocztę e-mail, a 91% weryfikuje stronę bądź aplikację przed zalogowaniem się.

Powyższe dane oznaczają, że regulacje mają sens. Narzucenie obowiązku informacyjno-edukacyjnego na strony i aplikacje, by wymuszały na użytkownikach działania pożądane, stałe wzbudzanie czynności powodują powstanie dobrych nawyków.



Podejście do haseł np. w bankowości, skrzynkach e-mail, SM



Włączone dodatkowe potwierdzenie logowania (uwierzytelnienie dwuskładnikowe) do banku lub poczty e-mail



Przed zalogowaniem lub podaniem swoich danych sprawdzenie, czy znajduję się na właściwej stronie internetowej lub w oficjalnej aplikacji



Zastrzeżony numer PESEL



B1. Jakie masz podejście do haseł, np. w bankowości, skrzynkach e-mail, w mediach społecznościowych? Wskaż jedną odpowiedź, która najlepiej do Ciebie pasuje. N=1000
B2. Czy jeśli jest dostępne, masz włączone dodatkowe potwierdzenie logowania (uwierzytelnienie dwuskładnikowe) do banku lub poczty e-mail - np. dodatkowy kod SMS oprócz hasła, kod z aplikacji w telefonie, lub odcisk palca / rozpoznanie twarzy? N=1000
B3. Czy przed zalogowaniem lub podaniem swoich danych sprawdzasz, czy znajdujesz się na właściwej stronie internetowej lub w oficjalnej aplikacji? N=1000
B4. Czy masz zastrzeżony numer PESEL? N=1000



Działania prewencyjne
podejmowane są w sytuacjach,
o których wielokrotnie mówiono publicznie.



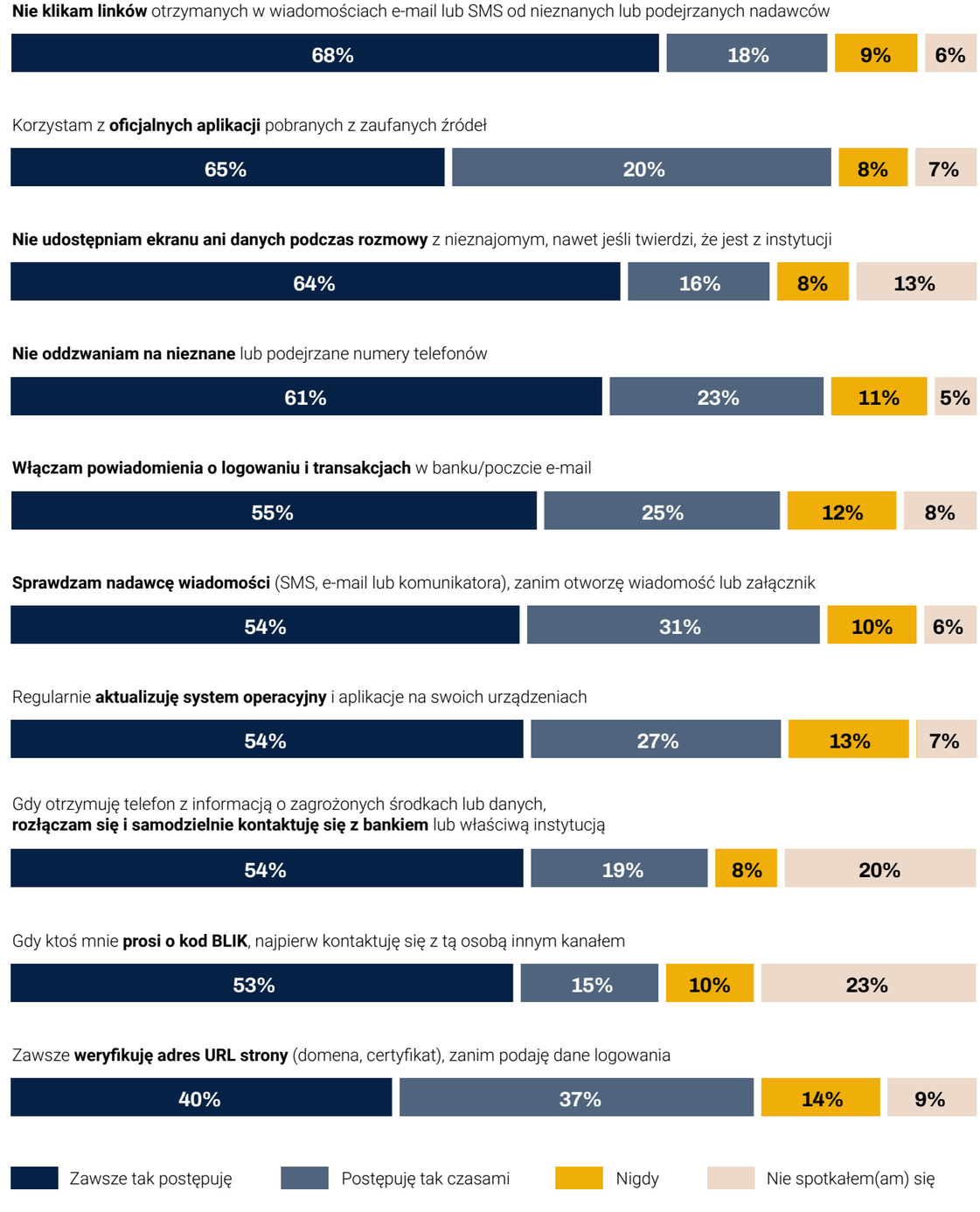
4 na 5 Polaków

ma włączone powiadomienia o transakcjach i logowaniu w banku/na poczcie e-mail.

Polacy w większości stosują działania prewencyjne w obszarach, o których słychać w mediach, informują banki, sklepy online. Widać, że popularność tematu wpływa na zachowanie konsumentów.

Popularność powiadomień o ruchach na koncie może świadczyć o głodzie narzędzi kontroli, jaki mają użytkownicy. Polacy chcą trzymać rękę na pulsie i mieć dostęp do informacji, co dzieje się z ich danymi i pieniędzmi.

Stosowane działania prewencyjne



B5. Które z poniższych działań stosujesz? N=1000

8. Zgłaszanie przestępstw

Stopień zgłaszalności scamów, wiedza o zgłaszaniu przestępstw

Jedynie 46% oszukanych zgłasza scam.
Powodem zaniechania jest bezsilność, brak wiary w powodzenie śledztwa i brak wiedzy, jak do niego doprowadzić.

34% ofiar,
które nie zgłosiły scamu

nie zrobiła tego, bo nie wierzy w skuteczność zgłoszenia, 29% wie, że szkodliwość czynu była za mała, a 28% przyznaje, że brakuje im dowodów.

W głosach oszukanych słychać niemoc: brak wiary w to, że organy ścigania podejmą realne działania, brak dowodów i wiedzy gdzie zgłosić się po pomoc to bariery przed ściganiem przestępców.

Scamy, w swoim charakterze, mają również uwikłanie ofiary w ciąg zdarzeń prowadzący do oszustwa. W tym kontekście dowiedzenie braku swojej winy może być stresujące zarówno ze względu na ew. konsekwencje prawne, jak i wstyd przed oceną.



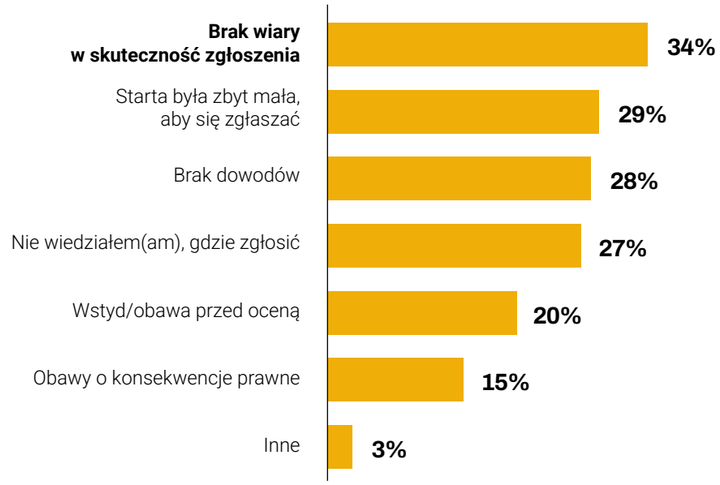
Dyskusja publiczna i edukacja powinny podejmować temat zgłaszania przestępstw. Nagłaśniać, że zgłoszenia scamów mogą pomóc zapobiec kolejnym oszustwom, wzmacniać, upodmiotawiać ofiary.



Zgłoszenie scamu jakiejkolwiek instytucji
(bank, policja, CERT Polska, inna)



Powody braku zgłoszenia scamu



I4. Czy zgłosiłeś(aś) ten przypadek jakiejkolwiek instytucji (bank, policja, CERT Polska, inna)? N=160
I5. Co było głównym powodem, dla którego nie zgłosiłe(a)ś tego przypadku? *N=86 UWAGA, mała próba!

Polacy nie mają świadomości do kogo zgłosić się po pomoc oraz wiedzy, czy działania podejmowane przez poszczególne instytucje są właściwie skoordynowane.

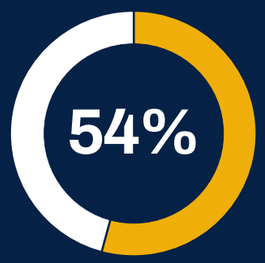
46% Polaków

nie ma wie gdzie zgłosić przypadek scamu.

Znajomość instytucji, do których można zgłosić scam wydaje się niewystarczająca. 62% Polaków nie wie, czym jest CERT Polska lub CSIRT NASK. Scamy zgłaszamy raczej do tych instytucji, których infrastruktura uczestniczyła w oszustwie lub na policję.

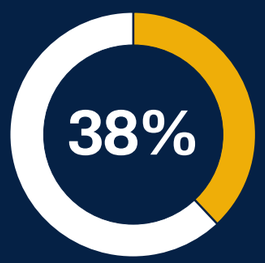
Brakuje świadomości działań skoordynowanych pomiędzy technologicznymi organami państwowymi, organami ścigania, a podmiotami prywatnymi, których systemy pośredniczą w dziejących się scamach.

Świadomość możliwości zgłoszenia przypadku scamu



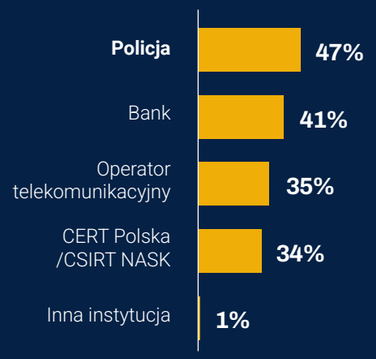
osób wie, gdzie zgłosić przypadek scamu

Znajomość CERT Polska lub CSIRT NASK



osób zna CERT Polska lub CSIRT NASK

Instytucja, do której zgłoszono scam



I1. Czy wiesz, gdzie w Polsce można zgłosić próbę lub przypadek oszustwa internetowego / telefonicznego? N=1000
I3. Czy słyszałeś(aś) o CERT Polska lub CSIRT NASK - instytucjach zajmujących się zgłaszaniem cyberprzestępstw? N=1000
I4. Czy zgłosiłeś(aś) ten przypadek jakiejkolwiek instytucji (bank, policja, CERT Polska, inna)? N=160
I6. Do jakiej instytucji zgłosiłeś ten incydent / przypadek oszustwa? *N=74 UWAGA, mała próba!

Banki są postrzegane jako instytucje, które najlepiej mogą chronić przed scamami. Lepiej niż np. policja.

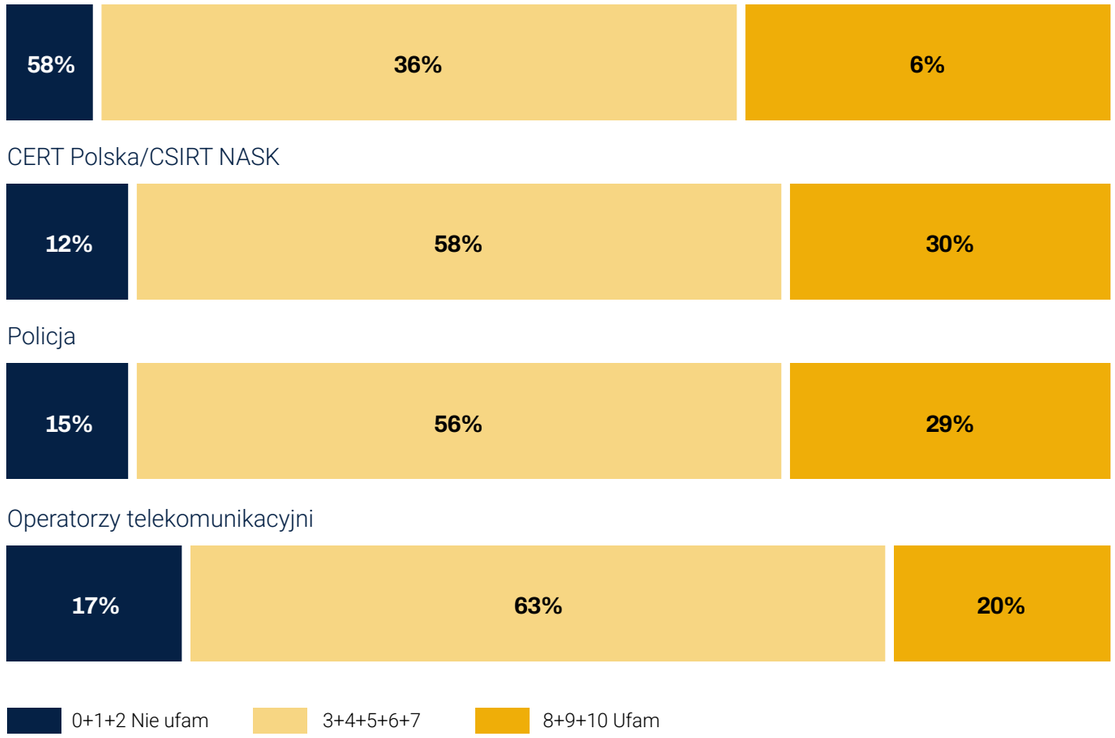
34%

Polaków wierzy, że banki mogą skutecznie chronić przed scamami.

Banki mają wszelkie kompetencje, by być postrzegane, jako merytoryczni partnerzy w walce ze scamem: mają rozbudowaną wiedzę technologiczną, w tym w obszarach cyberbezpieczeństwa. Komunikacja banków, w tym częste pushe w aplikacjach i wiadomości w bankowościach online, jak i UX kanałów zdalnych mają szansę wzmacniać cyberodporność klientów. Co więcej, banki to instytucje, z którymi mamy do czynienia na co dzień: częste touchpointy – w naturalny sposób towarzyszą w ciągu dnia, również w momentach newralgicznych – dzielenia się danymi lub podczas przepływów pieniężnych.

Warto wykorzystywać już zbudowaną przez banki pozycję ekspertów i posiadane zaufanie, w celu dalszego budowania odporności społeczeństwa na scamy.

Zaufanie, że dana instytucja jest w stanie skutecznie chronić przed oszustwami



I7. Określ w jakim stopniu ufasz, że poniższe instytucje są w stanie skutecznie chronić Cię przed oszustwami? N=1000

9. Dane demograficzne próby

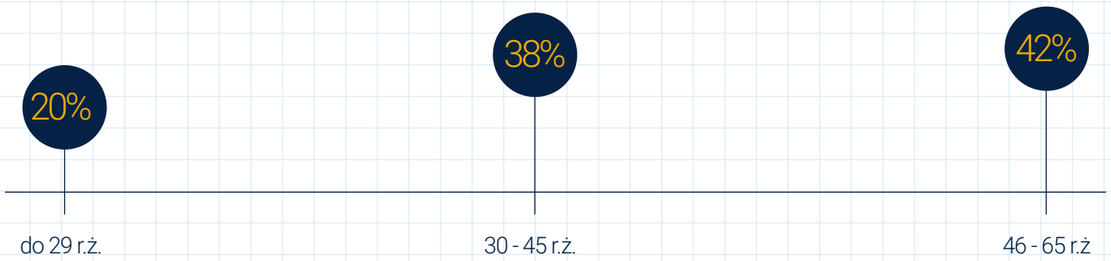


Płeć

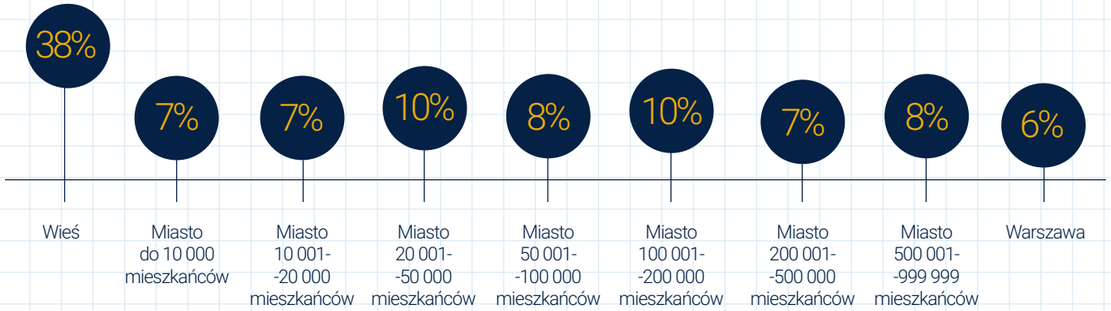
51% Kobieta

49% Mężczyzna

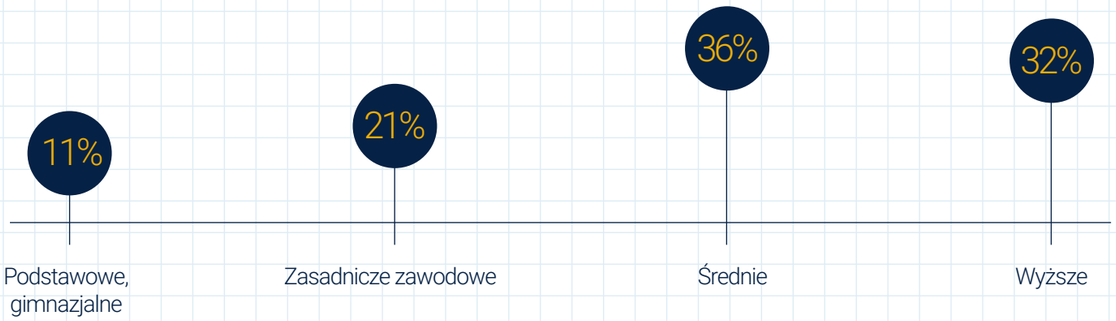
Wiek



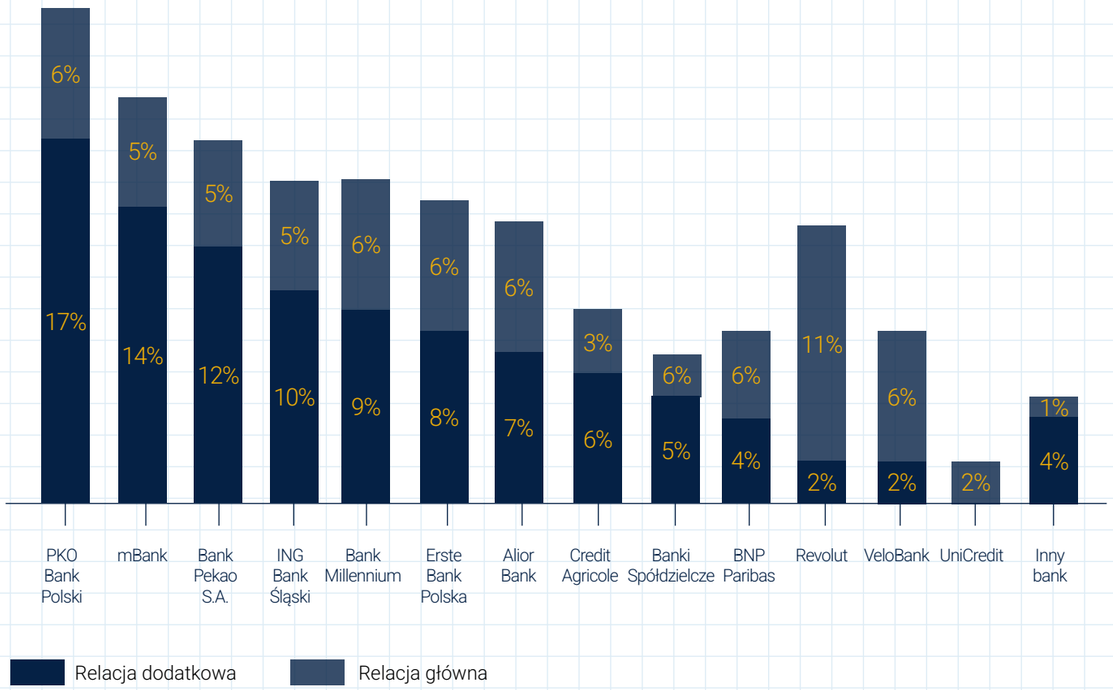
Wielkość miejsca zamieszkania



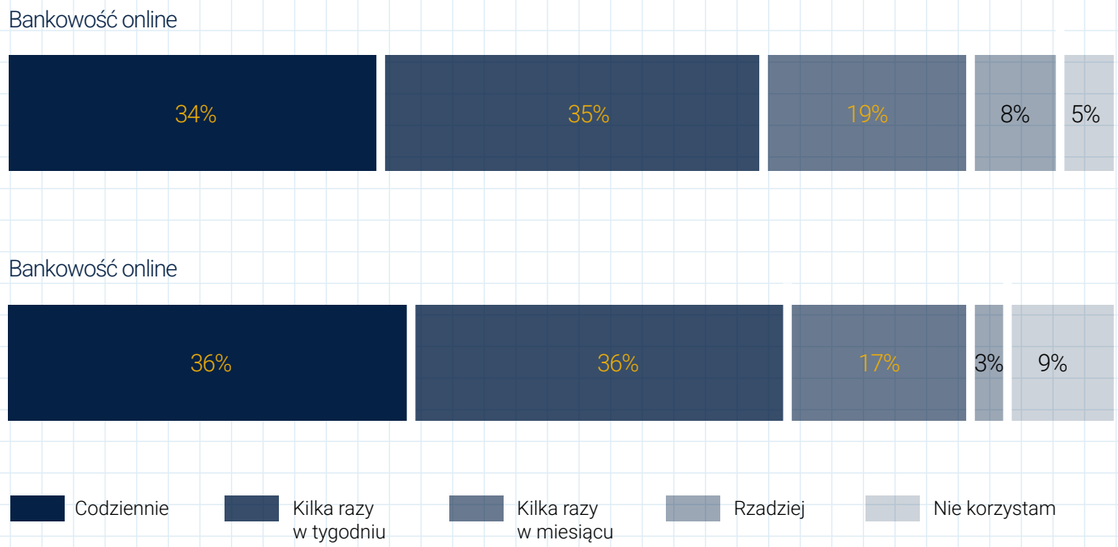
Wykształcenie



Marka banku



Korzystanie z kanałów zdalnych banku



Bankier • voice

Bankier.pl Tłumaczymy świat finansów.





Posłuchaj. Zobacz. Zrozum.

SPRAWDŹ







Puls Biznesu

PB APLIKACJA

Bądź pierwszy, gdy rynek się zmienia

POZNAJ FUNKCJE STWORZONE DLA TWOICH POTRZEB



POBIERZ • ZALOGUJ SIĘ
BĄDŹ NA BIEŻĄCO

Scamming Out! 2026

powered by Puls Biznesu Bankier.pl

BUDUJ Z NAMI CYBERODPORNOŚĆ

Bądź bezpieczny