WARSZAWSKI INSTYTUT BANKOWOŚCI

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

ZWIĄZEK BANKÓW POLSKICH

BADANIE

„Postawy Polaków wobec cyberbezpieczeństwa 2025”

EDYCJA VI

październik 2025

Badanie „Postawy Polaków wobec cyberbezpieczeństwa 2025”

- Badanie zrealizowano w ramach projektu Bezpieczeństwo w Cyberprzestrzeni przez firmę badawczą SW Research na zlecenie Warszawskiego Instytutu Bankowości.

Termin realizacji: 1-4 września 2025 roku

Technika badawcza: badanie zrealizowane metodą wspomaganego komputerowo wywiadu przy pomocy strony www (CAWI)

Próba: n=1008 osób. Reprezentatywna grupa internautów w wieku 18-65+ lat w podziale na płeć, wykształcenie i wielkość miejscowości.

W niniejszym opracowaniu dane procentowe zostały stosownie zaokrąglone dla przejrzystości przekazu oraz porównane z wynikami badania z poprzednich edycji.

Patron honorowy:

Ministerstwo Cyfryzacji

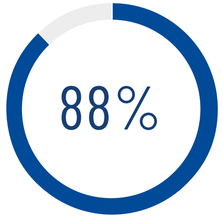
Partner merytoryczny:

NASK

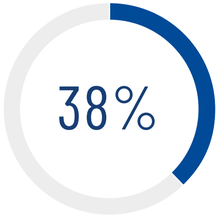
Partnerzy wspierający projekt Bezpieczeństwo w Cyberprzestrzeni:

allegro, blik, VISA, DAGMA BEZPIECZEŃSTWO IT, eset Digital Security Progress. Protected., ING, Santander, Santander Fundacja

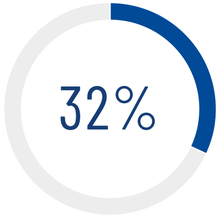
Kluczowe wnioski z badania i najważniejsze dane



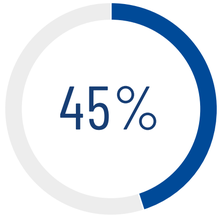
88 proc. Polaków za największe zagrożenie w cyfrowym świecie uznaje phishing



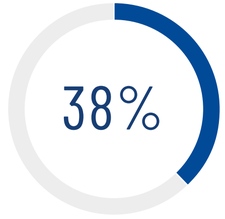
38 proc. respondentów uważa za niebezpieczny atak na cyfrową tożsamość (zaraz po phishingu)



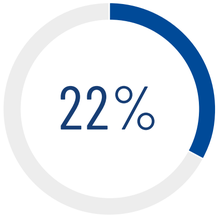
32 proc. badanych uznaje zjawisko dezinformacji i fake newsów jako trzecie najgroźniejsze zagrożenie



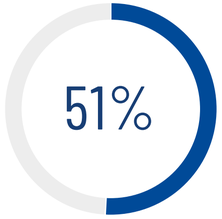
ale równocześnie 45 proc. sprawdza wiarygodność informacji tylko czasami i w zależności od źródła



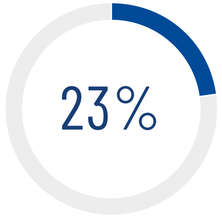
a 38% Polaków twierdzi, że nie traktuje social mediów jako głównego źródła wiedzy, co ma stanowić ochronę przed dezinformacją



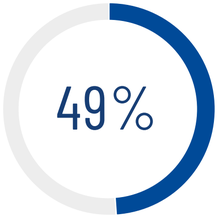
22 proc. badanych zhakowano konta w social mediach – to najwięcej spośród doświadczanych oszustw



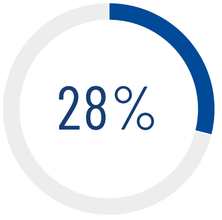
51 proc. Polaków twierdzi, że umie rozpoznać deepfake'i w sieci



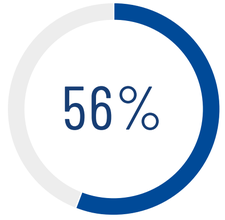
tylko 23 proc. uważa sztuczną inteligencję (poprzez którą tworzone są deepfake'i) za największe zagrożenie



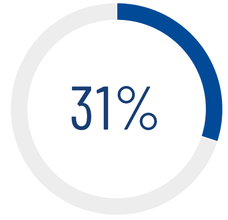
49 proc. Polaków ma stosunek ambiwalentny do AI (nie jest ani dobra, ani zła)



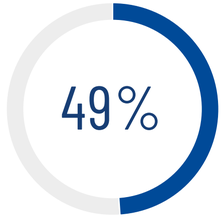
ale liczba zwolenników AI jest większa niż przeciwników: 28 proc. Polaków uznaje ją za wsparcie, a 17 proc. obawia się jej



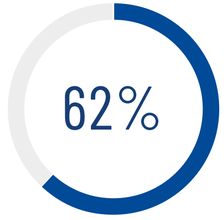
56 proc. badanych odblokowuje smartfony technologiami biometrycznymi, w tym rośnie popularność metody skanowania twarzy



tylko 31 proc. respondentów sprawdza tożsamość dzwoniącej osoby i podającej się za pracownika banku, wykonując telefon do placówki bankowej



co drugi Polak (49 proc.) posiada tylko orientacyjną wiedzę w zakresie cyberbezpieczeństwa



a jednocześnie deklarując dość wysokie poczucie bezpieczeństwa w cyfrowym świecie – 62 proc. czuje się w nim bezpiecznie

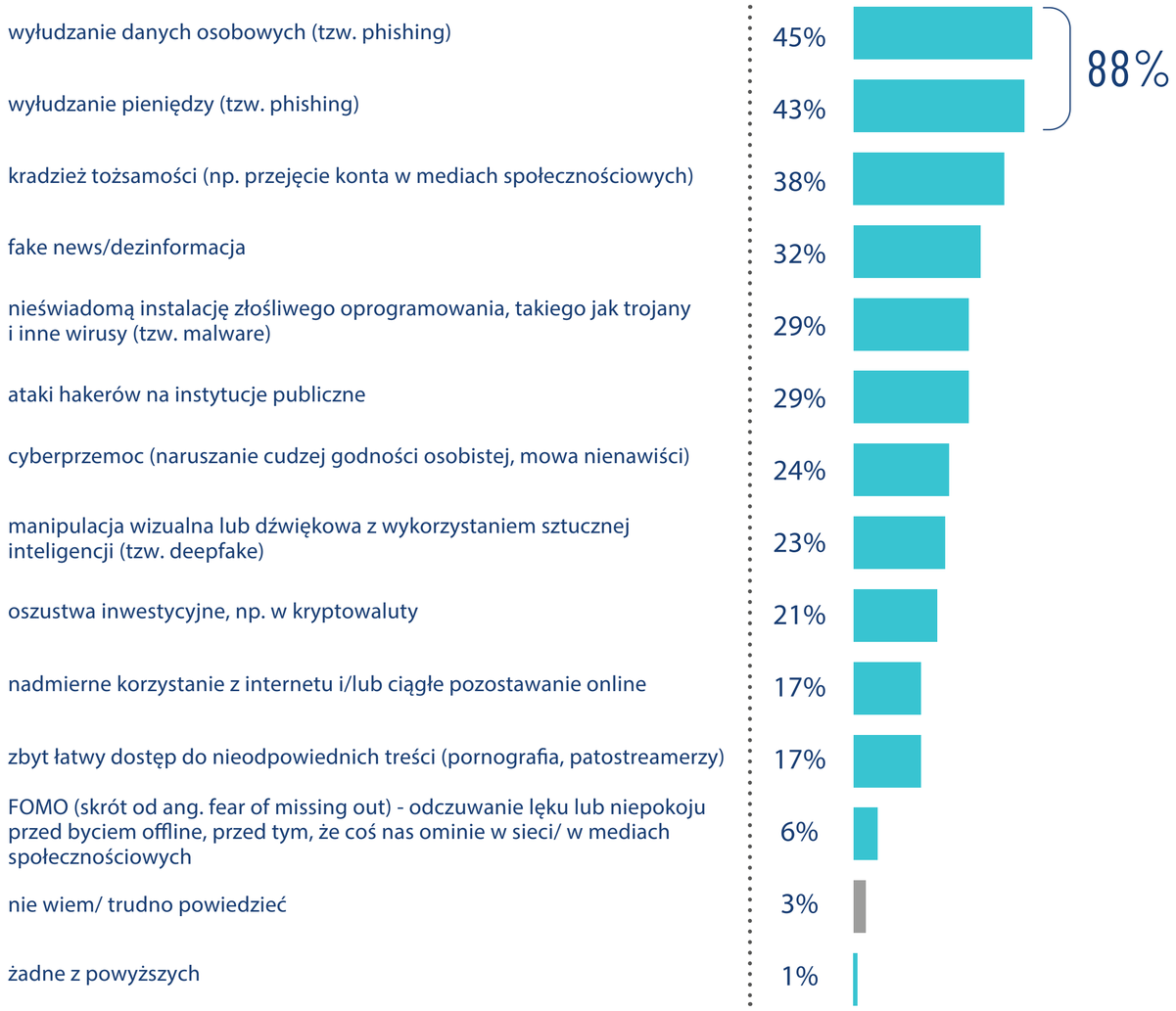
Phishing największym zagrożeniem w przestrzeni cyfrowej!

▶ TOP 3 najgroźniejszych oszustw w sieci to według badanych:

phishing	kradzież tożsamości	dezinformacja i fake newsy
(z ang.) – aż 88 proc. Polaków za największe zagrożenie w cyfrowym świecie uznaje phishing; respondenci obawiają się, że w wyniku tego oszustwa zostaną wyłudzone ich dane (45 proc.) i pieniądze (43 proc.).	(w tym w social mediach): 38 proc. respondentów uważa atak na wirtualną tożsamość za niebezpieczną.	32 proc. badanych uważa, że zjawisko dezinformacji jest groźne.

Warto zauważyć, że prawie co trzeci badany (29 proc.) obawia się ataków hakerów na instytucje publiczne oraz zagrożeń typu malware, (nieświadoma instalacja złośliwego oprogramowania, np. trojany lub inne wirusy). Respondenci zwracają również uwagę na zagrożenie w postaci mowy nienawiści i naruszania cudzej godności osobistej – 24 proc. uznało cyberprzemoc za groźne zjawisko. Badani dostrzegają także zagrożenia związane z oszustwami z wykorzystaniem sztucznej inteligencji – blisko co czwarty (23 proc.) uznaje deepfake w internecie za zagrożenie. Ponadto za pośrednictwem deepfake'ów mogą być również realizowane mistyfikacje inwestycyjne, np. w kryptowaluty – 21 proc. respondentów uważa oszustwa inwestycyjne za niebezpieczne.

Pytanie:
Wskaż obszary, które uważasz obecnie za największe zagrożenia w przestrzeni cyfrowej *(możliwość 4 wskazań)*



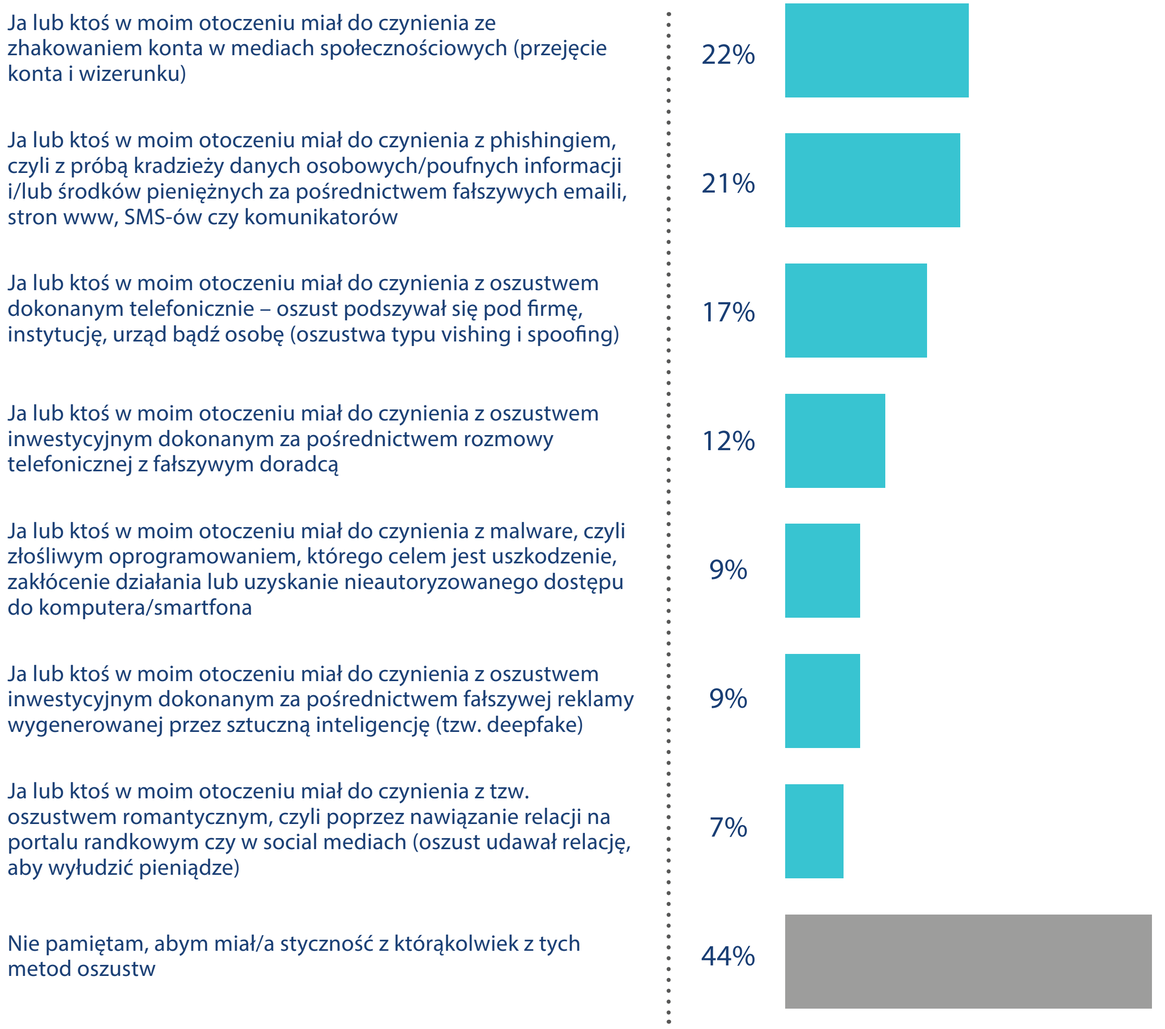
Polacy najczęściej atakowani w social mediach

- **Badani, którzy doświadczyli oszustwa na własnej skórze (lub ktoś z ich otoczenia), deklarują, że najczęściej mają styczność z hakowaniem konta w mediach społecznościowych** – deklaruje tak 22 proc. respondentów. Częściej z takimi atakami muszą mierzyć się kobiety – 25 proc. doświadczyło przejęcia ich konta i wizerunku przez hakerów, w przypadku mężczyzn to 18 proc. badanych.

Co piąty badany (21 proc.) przyznał, że był ofiarą phishingu, a 17 proc. miało do czynienia z oszustwami telefonicznymi za pośrednictwem tzw. spoofingu, czyli podszywania się pod dany numer telefonu (np. instytucji, banku, urzędu czy znanej osoby).

Co ciekawe, oszustw inwestycyjnych za pośrednictwem rozmowy telefonicznej z fałszywym doradcą doświadczają najczęściej osoby w wieku 35-44 lata (16 proc.), a poprzez deepfake (np. fałszywe reklamy intratnej i szybkiej inwestycji) - najmłodsi badani w wieku 18-24-lat (17 proc.).

Pytanie:
Czy w ciągu ostatnich 12 miesięcy spotkałeś/aś się (osobiście lub w Twoim otoczeniu) z następującymi oszustwami? *(wielokrotność odpowiedzi)*



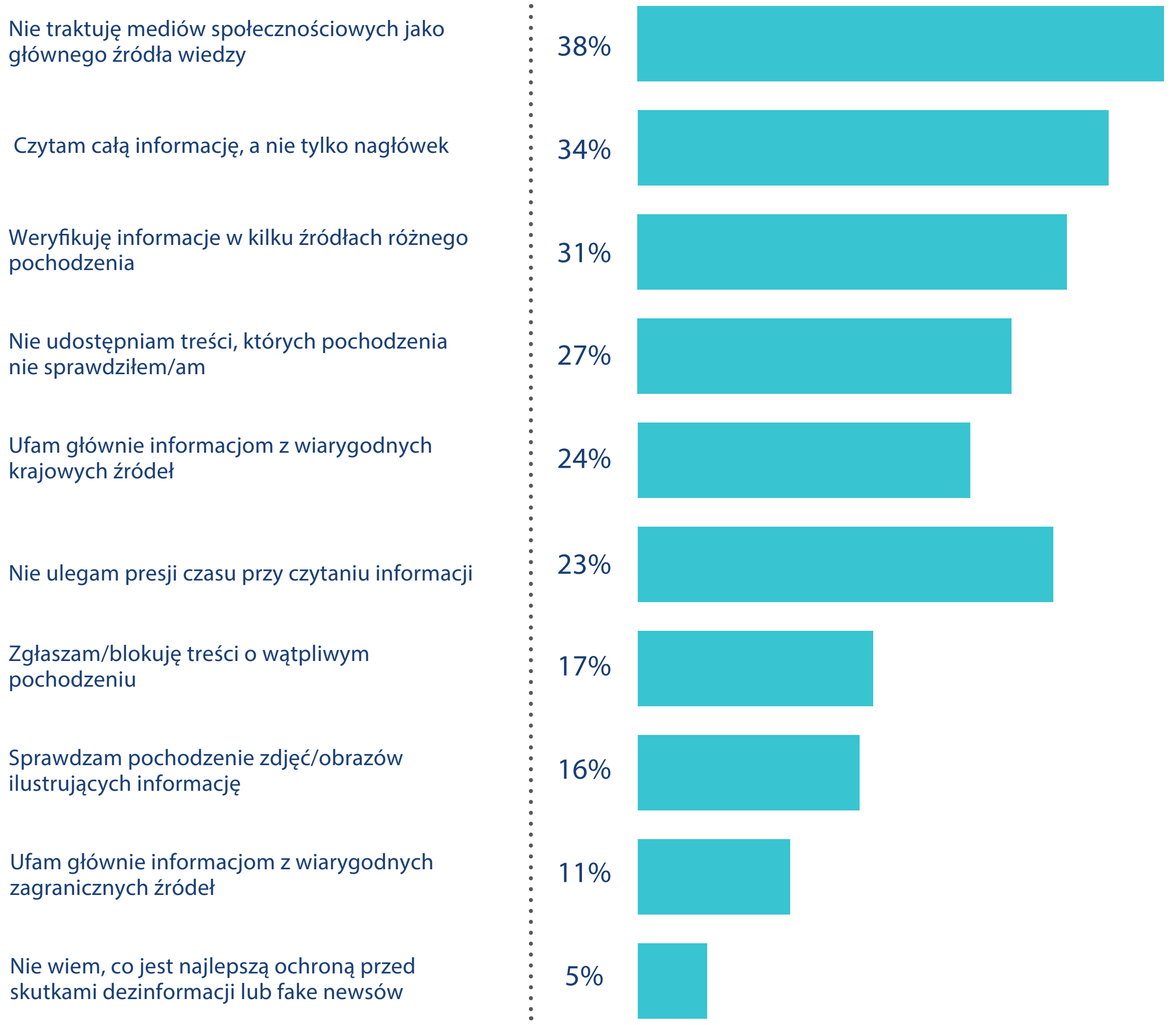
Polacy wskazali dezinformację i fake newsy jako 3. największe zagrożenie w sieci, ale zbyt rzadko je zgłaszają

- **Badani deklarują, że wiedzą jak asekurować się przed dezinformacją i fake newsami – 38 proc. ma dystans do informacji prezentowanych w mediach społecznościowych** (nie traktuje ich jako głównego źródła wiedzy), 34 proc. czyta treści w całości (a nie tylko clickbaitowe tytuły), a 23 proc. nie ulega przy tym presji czasu, zaś 27 proc. nie udostępnia ich bez weryfikacji.

Z drugiej strony tylko **16 proc. badanych sprawdza pochodzenie zdjęć/obrazów ilustrujących informację, co może przyczyniać się do rozprzestrzeniania dezinformacji poprzez udostępnianie deepfake'ków.**

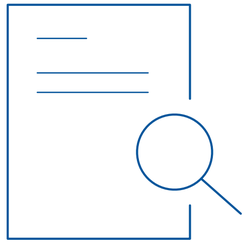
Zdecydowanie za mało Polaków (tylko 17 proc.) zgłasza i/lub blokuje treści o wątpliwym pochodzeniu.

Pytanie:
Jakie sposoby Twoim zdaniem są najlepszą ochroną przed skutkami dezinformacji lub fake newsów?
(możliwość 3 wskazań)

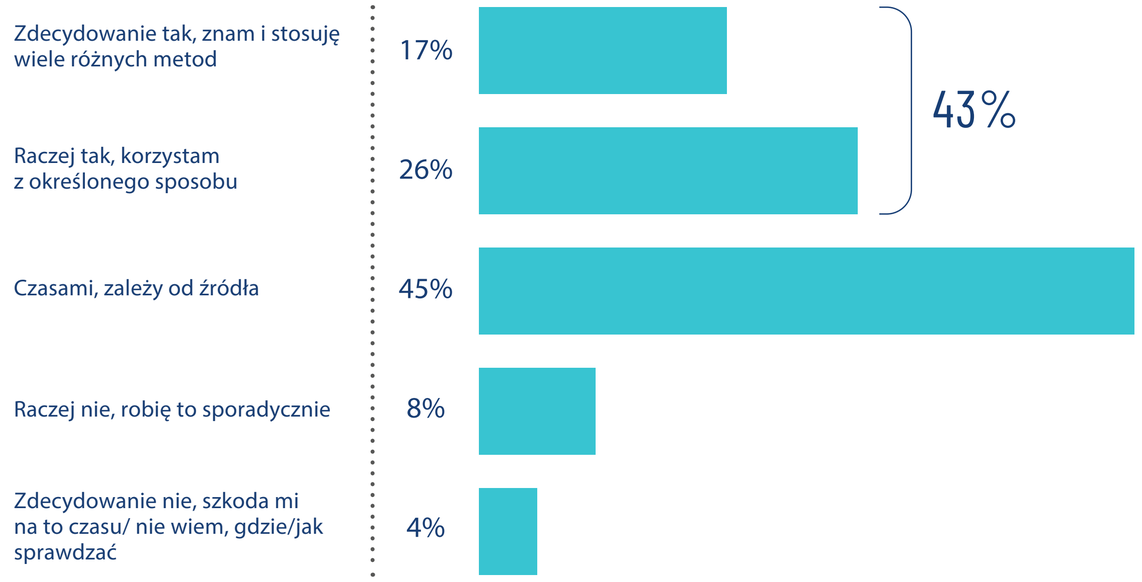


Niestety mniej niż połowa Polaków regularnie weryfikuje informacje pojawiające się w Internecie

- 43 proc. Polaków twierdzi, że sprawdza wiarygodność informacji w przestrzeni cyfrowej, w tym tylko 17% z nich weryfikuje je kilkoma różnymi metodami, a 26% tylko w jeden sposób, natomiast **45 proc. badanych przyznaje, że robi to nieregularnie i w zależności od źródła**. Najczęściej czujność w odniesieniu do weryfikowania informacji i ich źródeł zachowują osoby z wykształceniem wyższym.



Pytanie:
Czy w jakikolwiek sposób sprawdzasz wiarygodność informacji, które przeczytałeś/aś w Internecie? *(jedno wskazanie)*

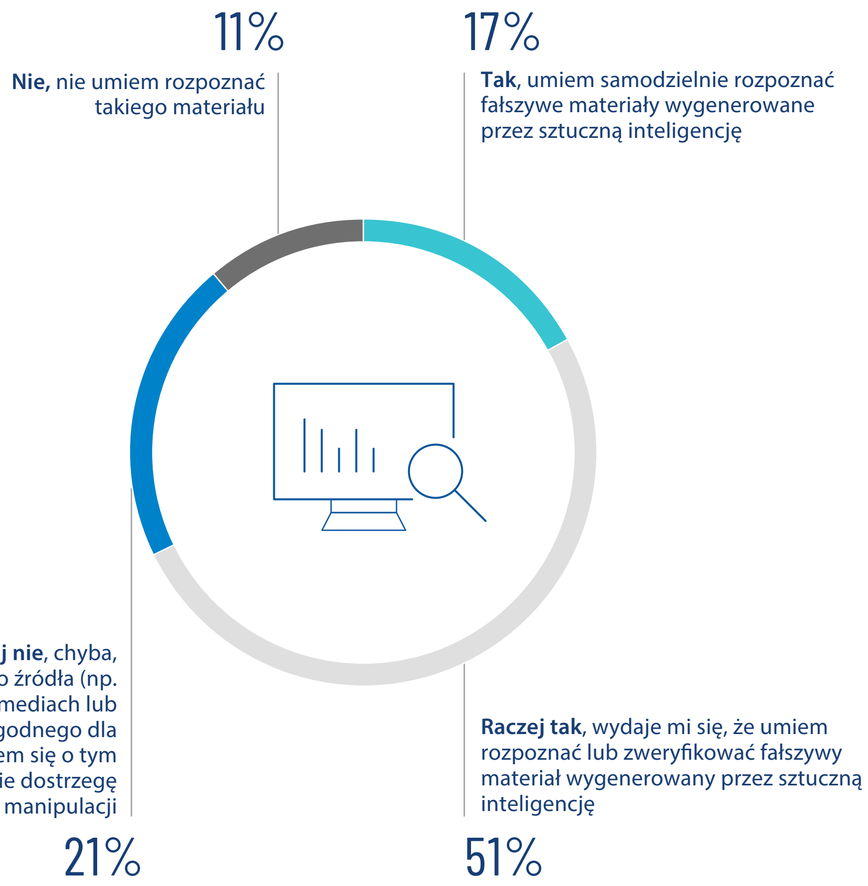


Ponad połowie Polaków wydaje się, że potrafią rozpoznać deepfake'i

Spostrzegawczość Polaków silniejsza od zdolności AI? Ponad połowie Polaków (51 proc.) wydaje się, że potrafi rozpoznać fałszywe nagrania i zdjęcia stworzone przy użyciu AI (tzw. deepfake'i), które mogą służyć m.in. rozprzestrzenianiu dezinformacji. Deklarowana zdolność do weryfikacji deepfake'ów dominuje wśród osób w wieku 35-44 lata z wykształceniem wyższym.

Co piąty respondent (21 proc.) miałby problem ze wskazaniem deepfake'a, chyba, że miałby informacje z innego źródła, że może mieć z nim do czynienia. **Co ciekawe, aż 39 proc. młodych dorosłych w wieku 18-24 lat twierdzi, że umie samodzielnie rozróżnić fałszywe materiały audiowizualne wytworzone przez sztuczną inteligencję.**

Pytanie:
Czy umiesz rozpoznać tzw. deepfake, czyli nieprawdziwe materiały audiowizualne (fałszywe nagrania i zdjęcia) wytworzone przy użyciu technik sztucznej inteligencji? – deepfake'i wykorzystywane są m.in. do oszustw finansowych, dyskredytowania osób publicznych, rozprzestrzeniania dezinformacji. *(jedno wskazanie)*

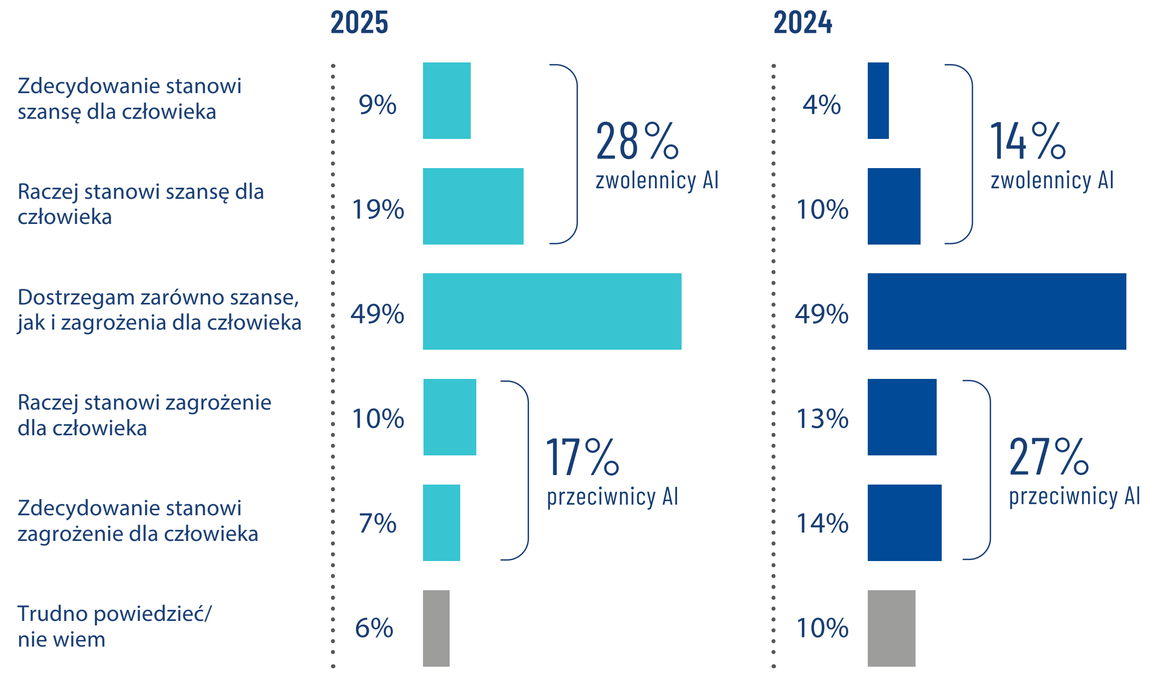


Polacy oswajają się ze sztuczną inteligencją

Jeszcze rok temu (w lipcu 2024) badanie WIB wskazało więcej przeciwników AI niż zwolenników (odpowiednio 27 proc. i 14 proc.), w tym roku tendencja ta się odwróciła – dwukrotnie więcej (28 proc.) Polaków widzi w AI szansę, a nie zagrożenie.

Jednocześnie badani starają się nie lekceważyć niebezpieczeństwa, które wiąże się z niewłaściwym zastosowaniem technologii, stąd podchodzą do niej w sposób ambiwalentny – blisko połowa badanych (49 proc.) uważa, że AI ma zarówno zalety, jak i wady.

Pytanie:
Jaki jest Twój stosunek do AI (tj. sztucznej inteligencji)? *(jedno wskazanie)*

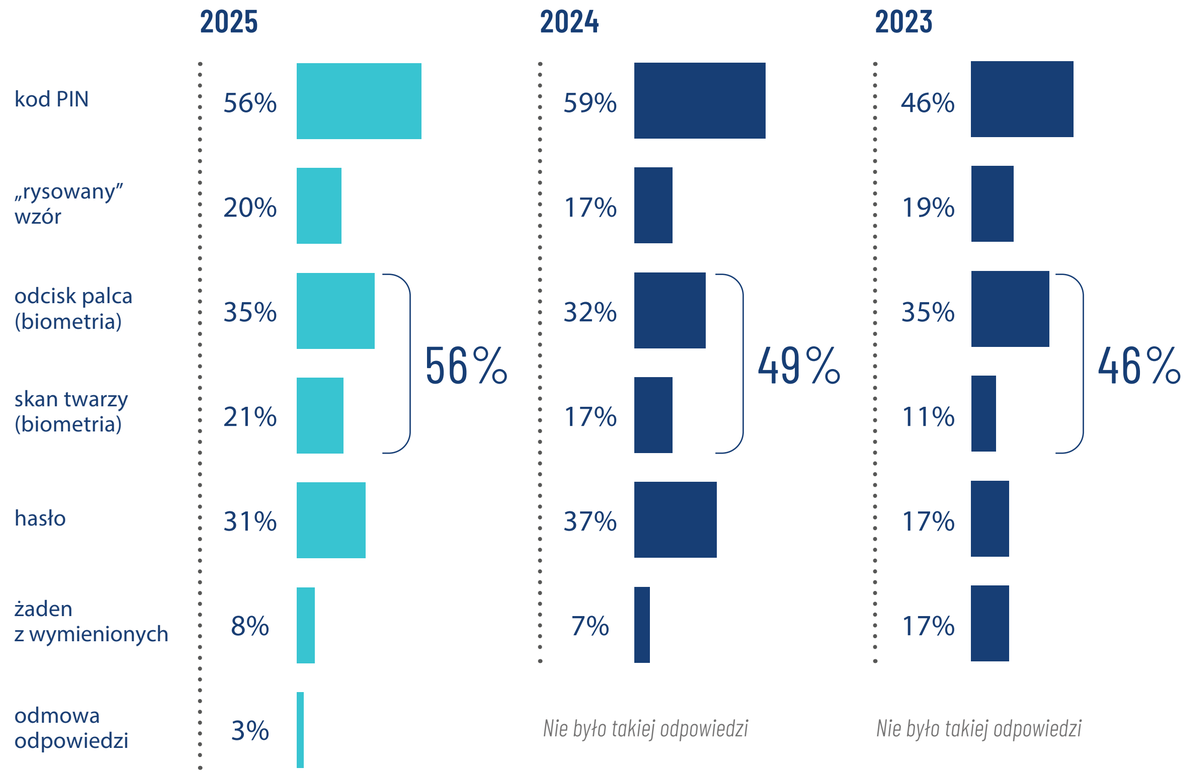


Nowe technologie w służbie bezpieczeństwa – biometria rozpoznawania twarzy coraz bardziej popularna

- Mimo, że Polacy nadal najczęściej wybierają kod PIN jako zabezpieczenie dostępu do swoich smartfonów (56 proc. badanych stosuje taką metodę), to w tegorocznym badaniu okazuje się, że tyle samo odblokowuje je za pomocą technologii biometrycznych (zarówno odciskiem palca jak i skanem twarzy). **W perspektywie ostatnich 3 lat korzystanie z biometrii, w celu zabezpieczania telefonów, staje się coraz bardziej atrakcyjne – szczególnie na popularności zyskuje skanowanie twarzy** (w porównaniu z 2023 rokiem wzrost jest prawie dwukrotny).

Technologie biometryczne najczęściej stosują młodzi dorośli (89 proc.) – prawie połowa (45 proc.) tegorocznych badanych w wieku 18-24 lata odblokowuje telefon odciskiem palca, a 44 proc. skanem twarzy.

Pytanie:
Jaki typ zabezpieczenia blokady/ dostępu do ekranu telefonu stosujesz? *(wielokrotność odpowiedzi)*

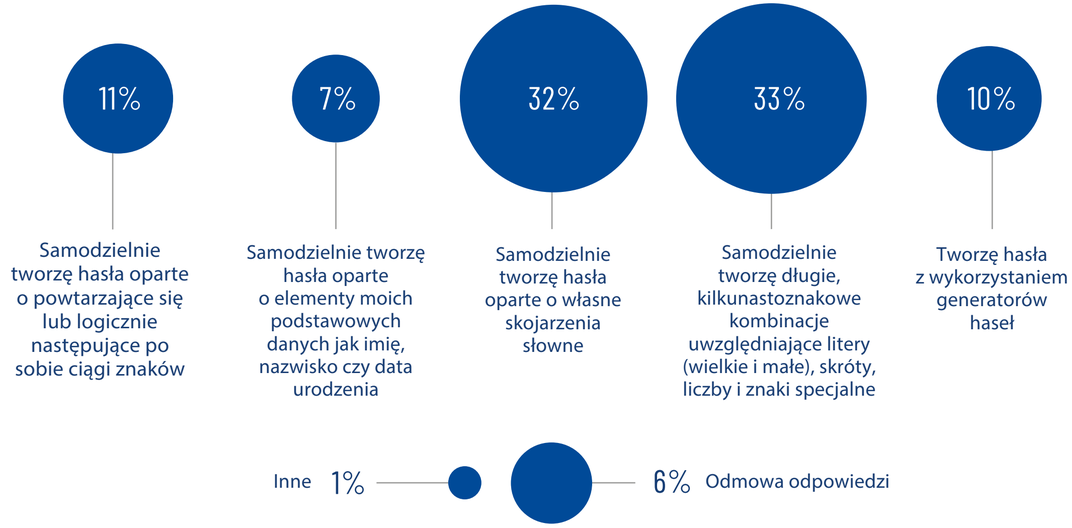


W tworzeniu i zabezpieczaniu haseł ciągle wolimy stawiać na własną kreatywność niż wspomagać się technologią

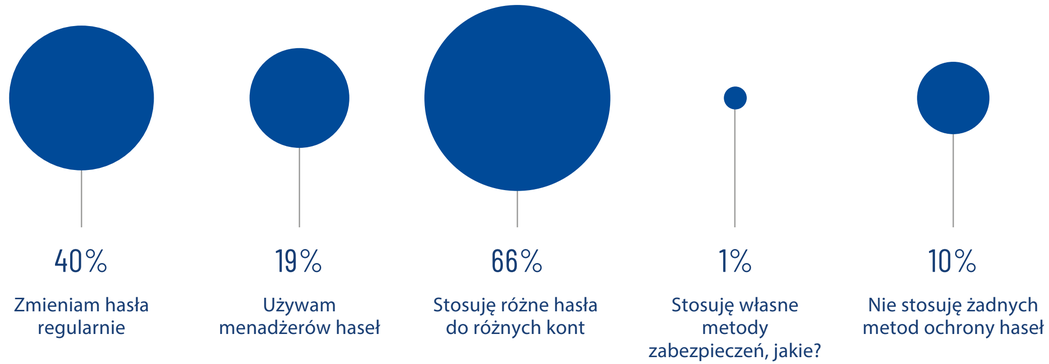
Co ciekawe, nie każde rozwiązania technologiczne są dla nas atrakcyjne, np. zbyt rzadko używamy programów (tzw. generatorów), które w sekundę stworzą losowe i trudne do złamania hasła – zaledwie 10 proc. badanych korzysta z takich rozwiązań. Wolimy postawić na pomysłowość i samodzielnie tworzymy hasła oparte o własne kombinacje oraz skojarzenia słowne – co trzeci badany stosuje taką metodę (32%).

Niewiele lepiej jest w przypadku ochrony za pośrednictwem menadżera haseł (np. Googla) – tylko co piąty badany (19 proc.), najczęściej w wieku 18-34 lat deklaruje, że zabezpiecza je w tym programie.

Pytanie:
Jakiego typu hasła najczęściej tworzysz? *(jedna odpowiedź)*



Pytanie:
Co robisz, żeby zabezpieczać swoje hasła (np. do poczty e-mail, banku, mediów społecznościowych)?
wiele odpowiedzi



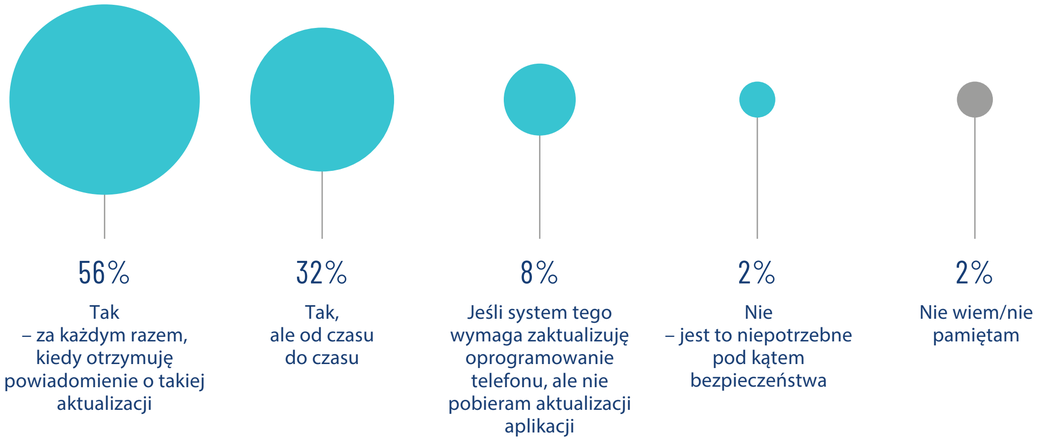
Doceniamy programy antywirusowe jako zabezpieczenie komputera i telefonu, ale za mało uwagi przywiązujemy do ich aktualizacji

Ponad połowa Polaków deklaruje, że ma aktualne oprogramowanie antywirusowe na swoim smartfonie (56 proc.) i komputerze (53 proc.), ale równocześnie co trzecia osoba aktualizuje antywirusa od czasu do czasu, czym naraża się na ataki typu malware.

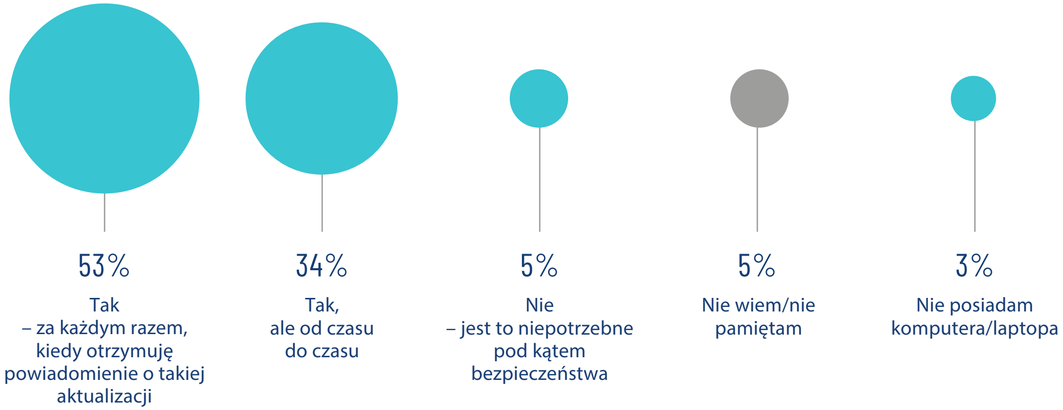
Warto również zwrócić uwagę, że młodzi dorośli w wieku 18-24 lata wolą bardziej zabezpieczyć swój telefon niż komputer – 45 proc. młodych aktualizuje smartfon za każdym razem, kiedy otrzymuje powiadomienie, a tylko 35 proc. robi tak w przypadku laptopa.

O zabezpieczenie komputera dbają bardziej seniorzy – 61 proc. osób w wieku 65+ pobiera aktualizacje systemu zawsze, gdy jest to wymagane.

Pytanie:
Czy aktualizujesz oprogramowanie i aplikacje na swoim osobistym telefonie komórkowym/ smartfonie? *(jedno wskazanie)*



Pytanie:
Czy aktualizujesz system na swoim osobistym komputerze/laptopie? *(jedno wskazanie)*



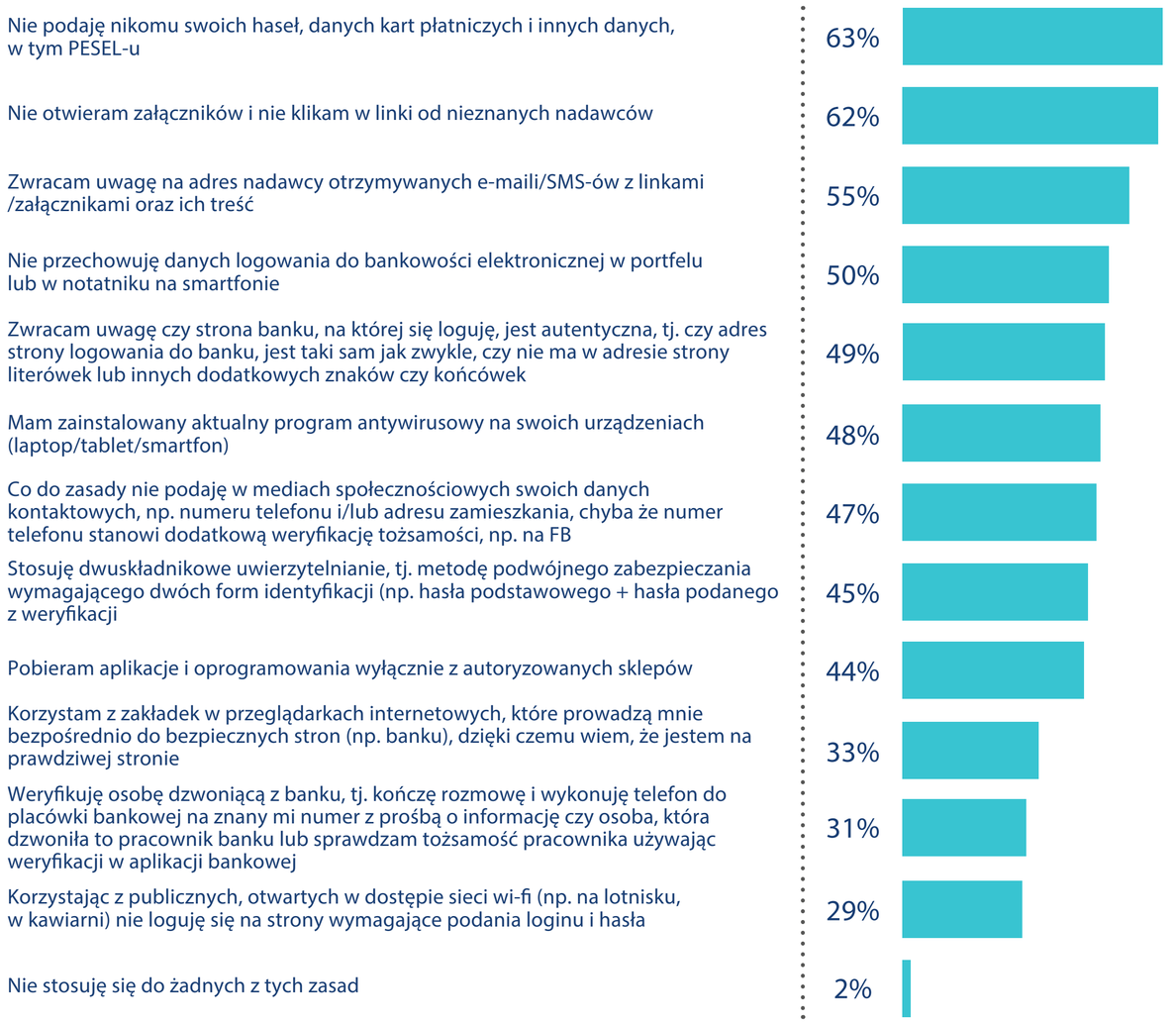
Najczęściej stosujemy 2 podstawowe zasady cyberbezpieczeństwa, a czujność tracimy, gdy dzwoni telefon lub korzystamy z publicznego wi-fi!

Większość respondentów (63 proc.) dba o ochronę swoich danych (hasła, karty płatnicze, PESEL) oraz nie otwiera załączników i nie klika w linki od nieznanych nadawców (62 proc.). Połowa Polaków prawidłowo chroni dostęp do swojej bankowości elektronicznej, ale już mniej niż połowa dba o prywatność w social mediach (47 proc.), stosuje dwuskładnikowe uwierzytelnianie (45 proc.) i pobiera aplikacje czy oprogramowanie wyłącznie z autoryzowanych sklepów (44 proc.).

Niestety Polacy zbyt rzadko weryfikują dzwoniącą osobę, która przedstawia się jako pracownik banku, przez co mogą być narażeni na oszustwa typu vishing i spoofing (z ang.), które grożą wyłudzeniem danych potrzebnych do zhakowania elektronicznego konta bankowego. Tylko 31 proc. respondentów sprawdza tożsamość takiej osoby, dzwoniąc samodzielnie do placówki bankowej.

Niepokojący jest również brak obaw, co do korzystania z publicznych sieci wi-fi – w takiej sytuacji tylko 29 proc. badanych dba o bezpieczeństwo i nie korzysta ze stron www wymagających podania loginu i hasła.

Pytanie:
Zaznacz, do których zasad w zakresie cyberbezpieczeństwa się stosujesz. *(wielokrotny wybór)*

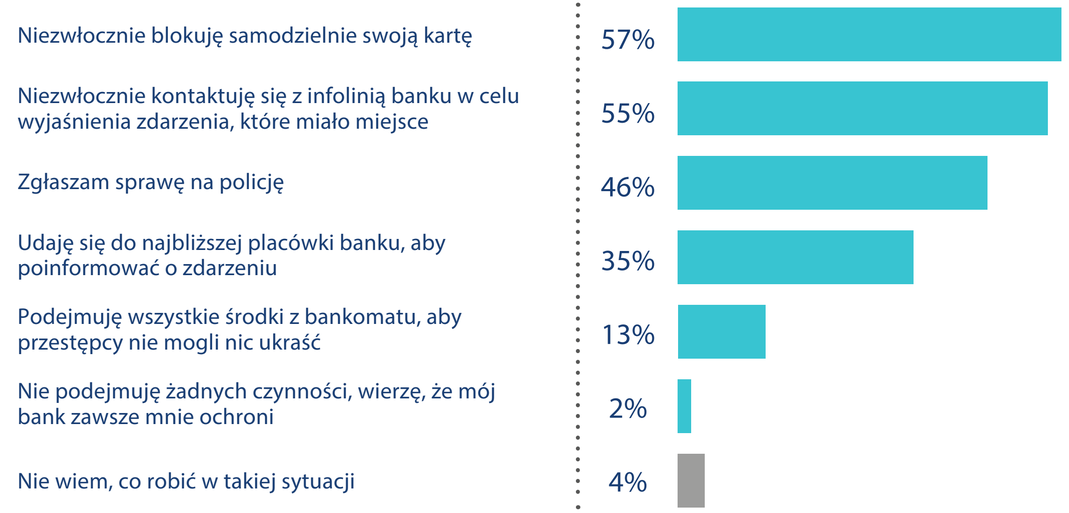


Wiemy jak postąpić i gdzie zgłosić cyberoszustwo, gdy staniemy się jego ofiarą

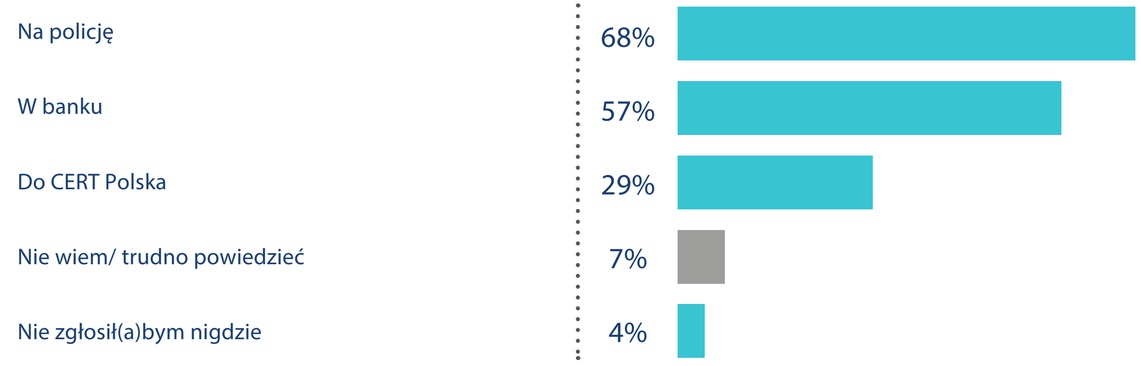
Podejrzewając, że haker/oszust zdobył dane, które umożliwią mu np. wyłudzenie pieniędzy lub zalogowanie się do bankowości internetowej lub mobilnej, 57 proc. respondentów od razu blokuje kartę płatniczą, a 55 proc. informuje telefonicznie swój bank w celu wyjaśnienia zdarzenia i ewentualnej blokady konta. 68 proc. badanych zgłosiłoby oszustwo phishingowe w pierwszej kolejności na policję, zaś 57 proc. wybrałoby powiadomienie banku.

Tylko niespełna co trzecia osoba (29 proc.) zdecydowałaby się na powiadomienie CERT Polska, czyli instytucji, która przyjmuje zgłoszenia phishingu.

Pytanie:
Co robisz, jeśli podejrzewasz, że padłeś/aś ofiarą oszustwa i Twoje konto bankowe jest zagrożone?
(wielokrotny wybór)



Pytanie:
Gdzie zgłosiłbyś/zgłosiłabyś próbę wyłudzenia pieniędzy i/lub Twoich danych, które zostało dokonane za pośrednictwem fałszywej strony www, wiadomości email/SMS i/lub połączenia telefonicznego? *(trzy wskazania)*

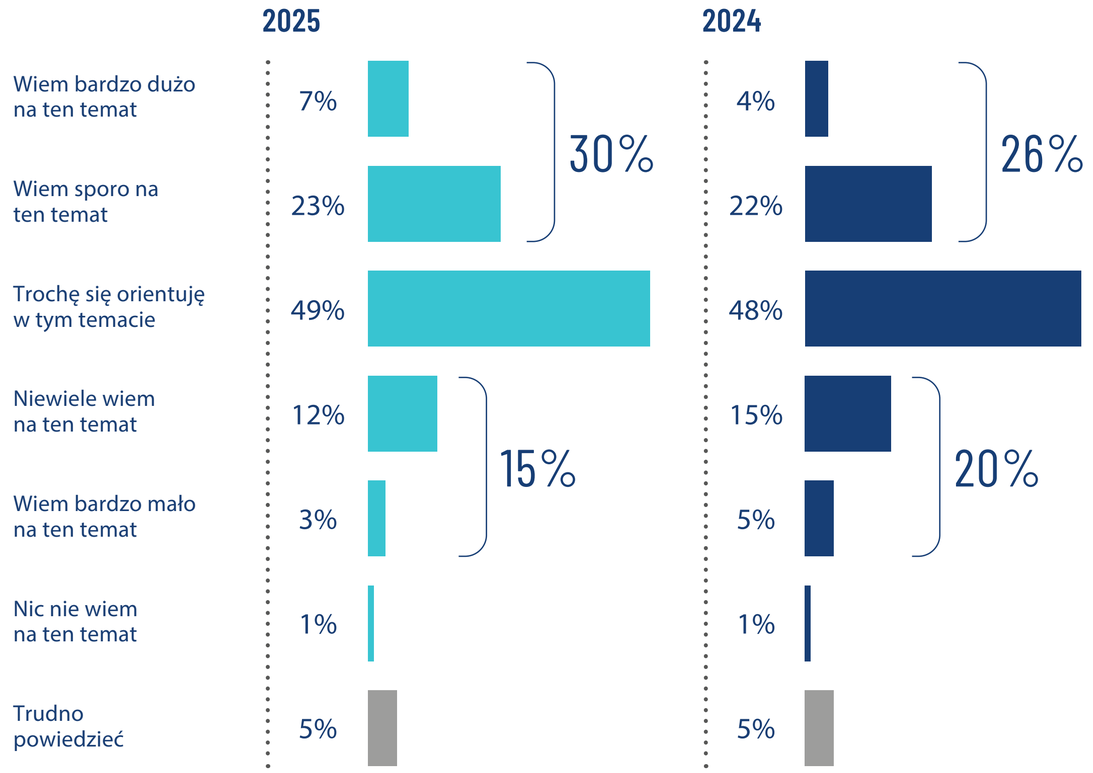


Wiedza polaków o cyberbezpieczeństwie powoli rośnie

- 30 proc. badanych Polaków deklaruje, że bardzo dobrze zna się na bezpieczeństwie w przestrzeni cyfowej (najczęściej są to soby z dużych miast z wykształceneim wyższym) – to o 4 p.p. więcej niż w zeszłym roku, gdy 26 proc. respondentów deklarowało doskonałą znajomość zasad cyberbezpieczeństwa.

Mimo to prawie połowa badanych (49 proc.) posiada wciąż tylko orientacyjną wiedzę w tym temacie. To pokazuje, że niezbędnę są systemowe i ciągłe działania edukacyjne, które podnosić będą wiedzę i umiejętności społeczeństwa w tym zakresie.

Pytanie:
Jak ogólnie oceniasz swoją wiedzę w zakresie cyberbezpieczeństwa? *(jedno wskazanie)*

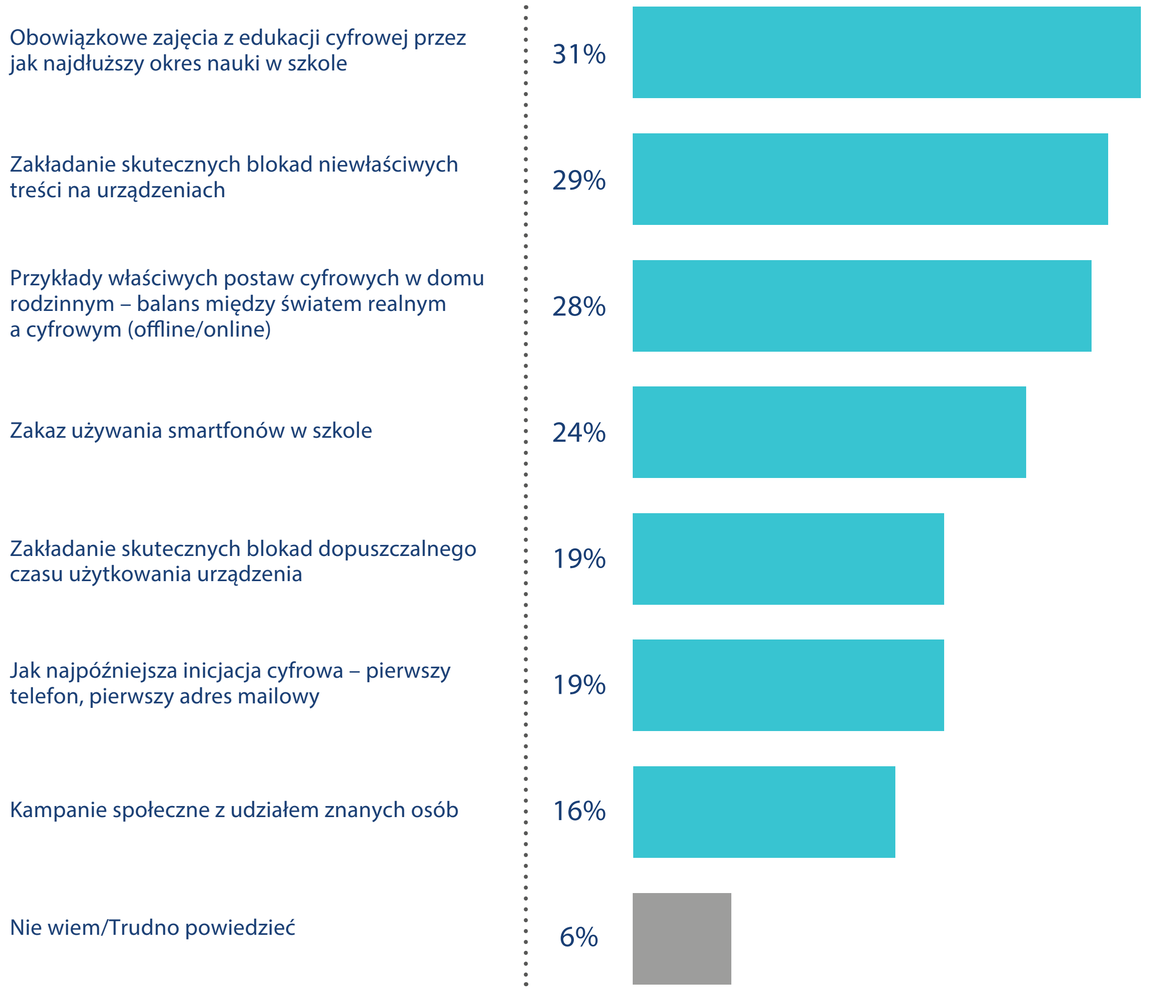


Bardziej wyedukowani dorośli stawiają na edukację cyfrową dzieci zarówno w szkole, jak i w domu

Edukacja i poszerzanie wiedzy w zakresie cyberbezpieczeństwa są zdaniem Polaków niezbędne w dynamicznie zmieniającym się świecie. **Co trzeci badany (31 proc.) uważa, że świadomość młodzieży na temat bezpiecznego i zdrowego korzystania z sieci powinni kształtować nauczyciele, wprowadzając obowiązkowe zajęcia z edukacji cyfrowej oraz rodzice, którzy na własnym przykładzie mogliby pokazywać dzieciom właściwe postawy cyfrowe oraz uczyć balansu pomiędzy byciem online i offline** (uważa tak 28 proc. respondentów).

Z drugiej strony, **część badanych jest zwolennikami bardziej rygorystycznych działań, które miałyby chronić dzieci i młodzież przed cyfrowymi zagrożeniami** – 29 proc. jest za zakładaniem blokad przed niewłaściwymi treściami na urządzeniach, a 24 proc. za wprowadzeniem zakazu używania smartfonów w szkołach. W odniesieniu do dbałości o higienę cyfrową młodych, 19 proc. Polaków wskazuje za właściwą ochronę jak najpóźniejszą inicjację cyfrową dziecka oraz ograniczanie czasu, który spędza przez komputerem czy telefonem.

Pytanie:
Które z działań wspierających ochronę dzieci i młodzieży oraz poprawę ich świadomości na temat bezpiecznego i zdrowego korzystania z sieci uważasz za kluczowe? *(wielokrotny wybór)*

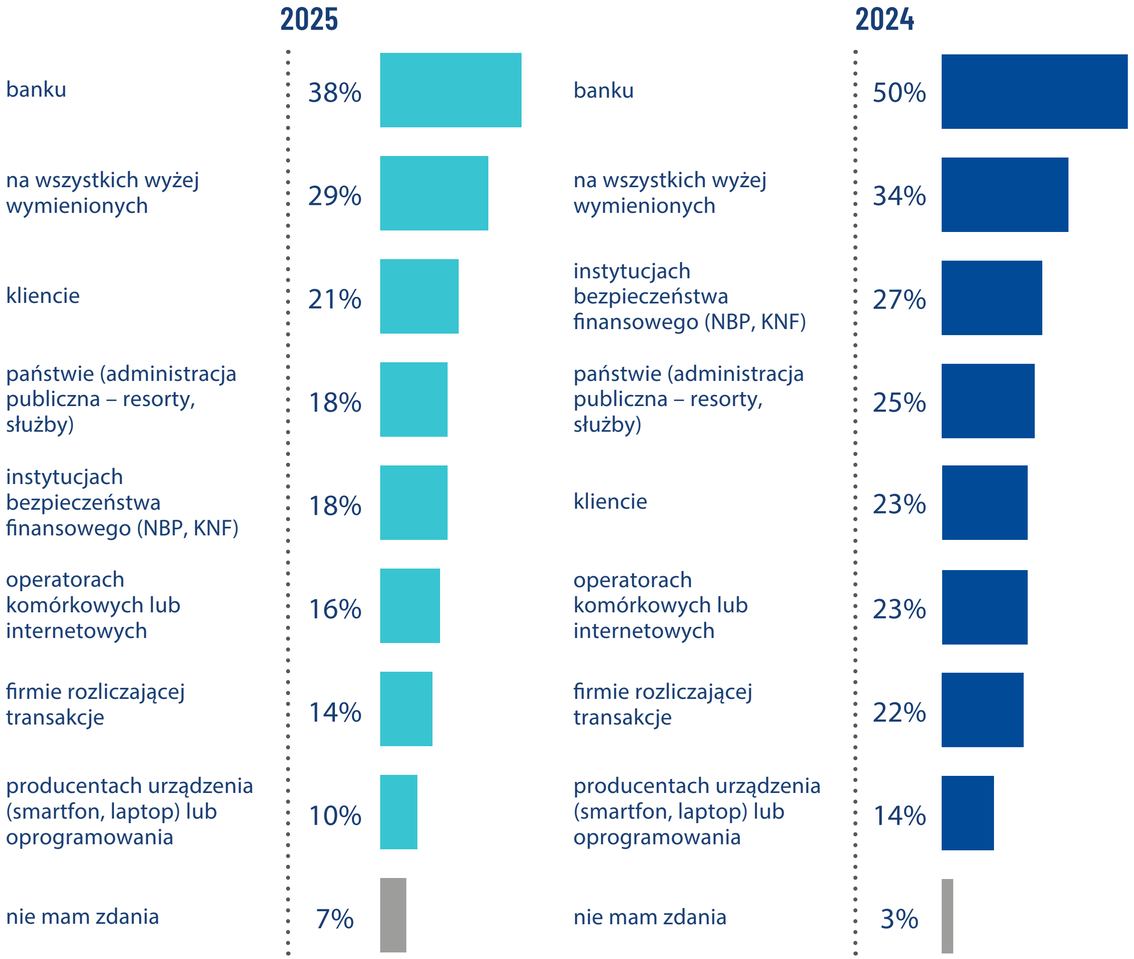


Zaczynamy dostrzegać siebie jako ważne ogniwo bezpieczeństwa w cyfrowym świecie usług finansowych

Blisko czterech na dziesięciu badanych (38 proc.) wskazuje, że za bezpieczeństwo elektronicznych usług finansowych odpowiadają głównie banki. **Warto zauważyć**, że w rzeczywistości, w której coraz więcej usług finansowych przenosi się do cyfrowego świata, **Polacy zauważają, że odpowiedzialność za nasze cyberbezpieczeństwo staje się coraz bardziej rozproszona – 29 proc. badanych twierdzi, że finansowa ochrona powinna płynąć z różnych źródeł jednocześnie - od państwa, operatorów komórkowych i internetowych, producentów urządzeń czy firm rozliczających transakcje.**

Instytucje bankowe przestają być traktowane jako jedyna tarcza ochronna elektronicznych finansów. Bardziej wyedukowane społeczeństwo zaczyna dostrzegać również swój wpływ na cyberbezpieczeństwo **– Polacy już na trzecim miejscu (21 proc.) stawiają siebie jako ogniwo bezpieczeństwa w cyfrowym świecie usług finansowych (rok temu w hierarchii odpowiedzialności klienci uplasowali się na piątym miejscu).**

Pytanie:
Odpowiedzialność za bezpieczeństwo usług finansowych dokonywanych w formie elektronicznej Twoim zdaniem spoczywa na *(wielokrotny wybór)*

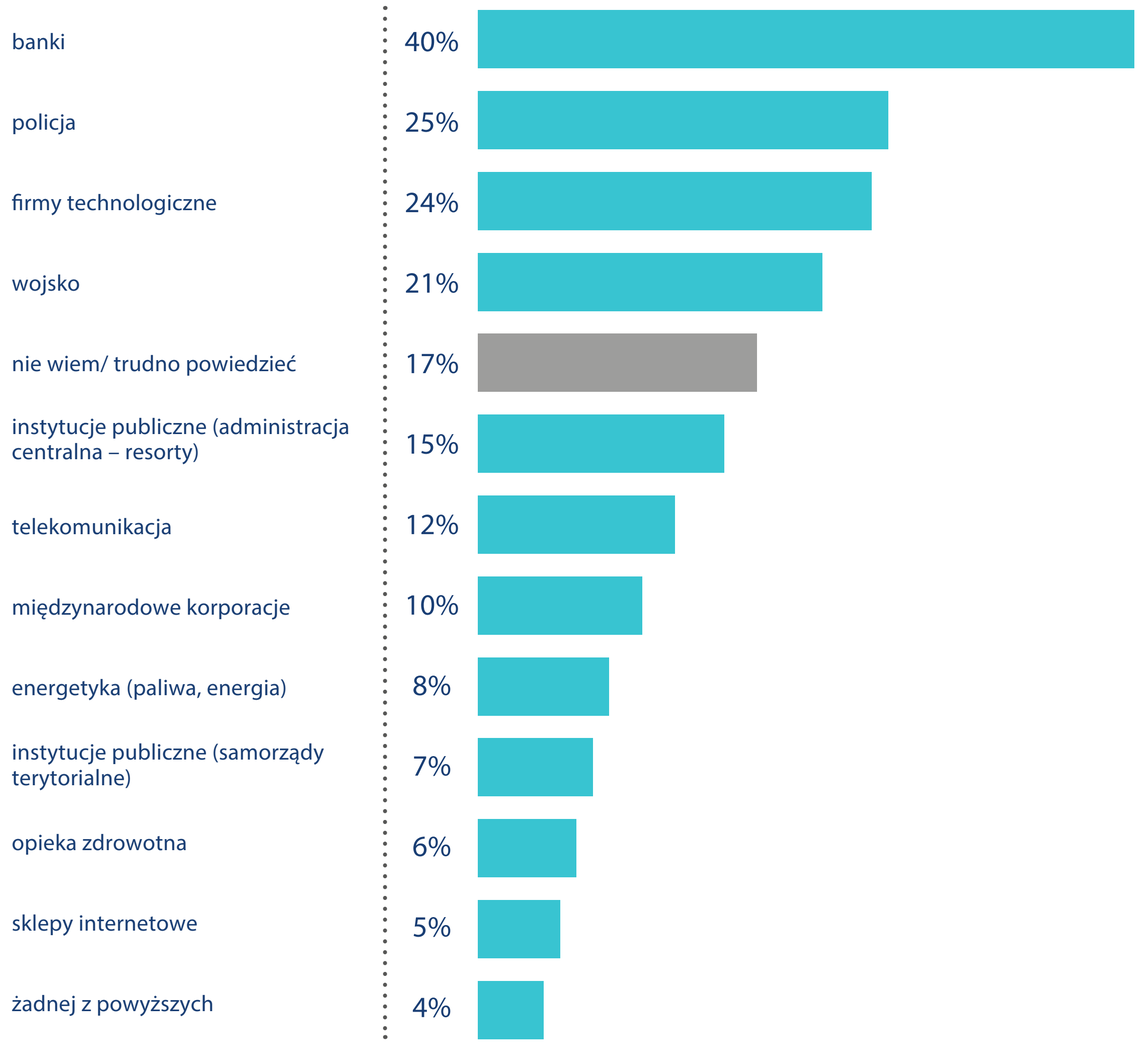


Polacy uważają banki za liderów cyberbezpieczeństwa

- Najwięcej badanych (40 proc.) wskazuje, że to banki są najlepszym gwarantem bezpieczeństwa w przestrzeni cyfrowej i najbardziej rozwijają się w zakresie cyberbezpieczeństwa. Respondenci doceniają również zabezpieczenia służb mundurowych (policji – 25 proc., wojska – 21 proc.) oraz firm technologicznych (24 proc.).

  Najmniejsze zaufanie, co do cyfrowego bezpieczeństwa, mamy w stosunku do: sklepów internetowych (5 proc.), ochrony zdrowia (6 proc.), samorządów terytorialnych (7 proc.), ale niestety również do ważnego sektora energetycznego – tylko 8 proc. badanych uważa firmy energetyczne za dbające o cyberbezpieczeństwo.

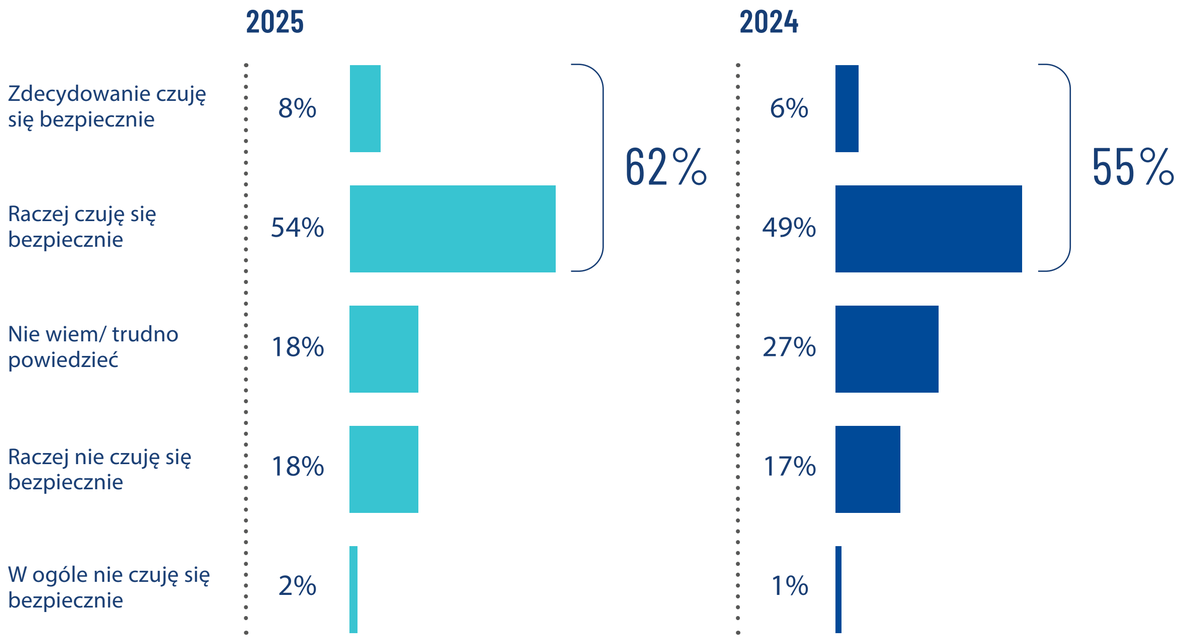
Pytanie:
Którą z poniższych branż lub instytucji postrzegasz jako liderów w zakresie cyberbezpieczeństwa?
(trzy wskazania)



A nasze poczucie cyberbezpieczeństwa?
Polacy w większości czują się bezpiecznie w cyfrowym świecie

- Polacy dostrzegają zagrożenia w cyberprzestrzeni na różnych polach, np. w e-usługach (w tym finansowych) czy w internecie i social mediach, mimo to poziom ich poczucia bezpieczeństwa w tym zakresie wrasta – już 62 proc. respondentów czuje się bezpiecznie w cyfrowym świecie, to o 7 p.p. więcej niż w ubiegłym roku. Coraz mniej osób odczuwa niepewność w tym zakresie, co może wskazywać na wyższy poziom świadomości zagrożeń. W przestrzeni cyfrowej bardziej bezpiecznie czują się panowie niż panie oraz osoby w wieku 45+ z dużych miast (na poczucie bezpieczeństwa nie ma wpływu wykształcenie).
- **Podsumowując wyniki tegorocznego badania, postawy Polaków wobec cyberbezpieczeństwa są coraz bardziej świadome, dostrzegamy wiele różnych zagrożeń, ale twierdzimy, że tylko niektórych z nich doświadczamy. Coraz więcej osób wie, jak się przed nimi bronić, choć ciągle stosunkowo za mało Polaków zna różne zasady bezpiecznych zachowań. Doceniamy nowe technologie jako tarczę ochronną w cyfrowym świecie, a z drugiej strony nie wystarczająco z nich korzystamy. Posiadanie nawet minimalnie większej wiedzy w zakresie cyberbezpieczeństwa i świadomości, że swoim zachowaniem w sieci możemy narazić się lub uniknąć niebezpieczeństw, sprawia, że w cyfrowym świecie czujemy się bardziej bezpieczni.**

Pytanie:
Na ile bezpiecznie czujesz się w cyfrowym świecie, tj. w usługach, internecie, social mediach, komunikatorach itp.? *(jedno wskazanie)*



Raport z badania powstał w ramach projektu edukacyjnego Fundacji Warszawski Instytut Bankowości pn. „**Bezpieczeństwo w Cyberprzestrzeni**" realizowanego wspólnie z Partnerami

Projekt "Bezpieczeństwo w Cyberprzestrzeni"

realizowany jest od 2017 roku przez Fundację Warszawski Instytut Bankowości.
Celem projektu jest edukowanie społeczeństwa (uczniów, studentów, dorosłych i seniorów) oraz przekazywanie wiedzy i kształtowanie kompetencji na temat:

- ROZPOZNAWANIA I UNIKANIA CYBERZAGROŻEŃ
- AKTYWNEGO I BEZPIECZNEGO KORZYSTANIA Z NOWOCZESNYCH TECHNOLOGII, W TYM NARZĘDZI GOSPODARKI ELEKTRONICZNEJ
- WŁAŚCIWYCH POSTAW W OBSZARZE OCHRONY TOŻSAMOŚCI I WIZERUNKU
- PRZECIWDZIAŁANIA DEZINFORMACJI I OGRANICZANIA CYBERPRZEMOCY

Projekt dotarł do blisko 2 mln bezpośrednich beneficjentów w zasięgu różnych aktywności, w tym:

- >600 tys. UCZNIÓW
- >200 tys. STUDENTÓW
- >220 tys. SENIORÓW

Patron honorowy:

Ministerstwo Cyfryzacji

Partner merytoryczny:

NASK

Partnerzy wspierający projekt Bezpieczeństwo w Cyberprzestrzeni:

allegro, blik, VISA, DAGMA BEZPIECZEŃSTWO IT, eset Digital Security Progress. Protected., ING, Santander, Santander Fundacja

WARSZAWSKI INSTYTUT BANKOWOŚCI

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

ZWIĄZEK BANKÓW POLSKICH

Masz pytania ws. raportu

– napisz do Koordynatorki projektu:

Aleksandra Czyrkowska – aczyrkowska@wib.org.pl

Więcej materiałów o cyberbezpieczeństwie i informacji o projekcie „Bezpieczeństwo w Cyberprzestrzeni” znajdziesz na stronie internetowej:
cyber.wib.edu.pl

Zapraszamy również na strony:

- Warszawskiego Instytutu Bankowości:
  www.wib.org.pl
- Programu „Bankowcy dla Edukacji”:
  www.bde.wib.org.pl

Zachęcamy do obserwowania naszych profili:

Warszawski Instytut Bankowości

WarszawskiInstytutBankowosci