

Informujemy, iż w celu optymalizacji treści dostępnych w naszym serwisie i dostosowania ich do Państwa indywidualnych potrzeb korzystamy z informacji zapisanych za pomocą plików cookies na urządzeniach końcowych użytkowników. Pliki cookies użytkownik może kontrolować za pomocą ustawień swojej przeglądarki internetowej. Dalsze korzystanie z naszego serwisu internetowego bez zmiany ustawień przeglądarki internetowej oznacza, iż użytkownik akceptuje stosowanie plików cookies.

[Akceptuję pliki cookies](#)

MENU

[Instrukcja korzystania z BIP](#)

[Nabór](#)

[Zamówienia publiczne](#)

[Organizacja przyjmowania i załatwiania skarg i wniosków](#)

[Podstawa prawna powstania Centrum Usług Informatycznych w Białymstoku](#)

[Plan zamówień publicznych](#)

[Sprawozdania finansowe](#)

[Dostęp do informacji publicznej nieudostępnionej w BIP](#)

[Ochrona danych osobowych](#)

[Cyberbezpieczeństwo](#)

[Zarządzenia](#)

[Petycje](#)

[Sygnałista](#)

[Raport o stanie zapewnienia dostępności podmiotu publicznego
zgłoszeń naruszeń prawa](#)

Cyberbezpieczeństwo w przestrzeni - raport z 2025 r.

Czy Polacy są gotowi na cyfrowe zagrożenia? Wnioski z raportu „*Postawy Polaków wobec cyberbezpieczeństwa 2025*”

Raport „*Postawy Polaków wobec cyberbezpieczeństwa 2025*”, zrealizowany został w ramach projektu Bezpieczeństwo w Cyberprzestrzeni przez firmę badawczą SW Research na zlecenie Warszawskiego Instytutu Bankowości. Raport stanowi kompleksową analizę świadomości i oczekiwań obywateli wobec zagrożeń cyfrowych. Dokument bazuje na reprezentatywnym badaniu opinii publicznej, przeprowadzonym w II kwartale 2025 roku, i dostarcza istotnych danych dla ustawodawcy, instytucji publicznych oraz sektora prywatnego.

Phishing największym zagrożeniem w przestrzeni cyfrowej

Aż 88 proc. Polaków za największe zagrożenie w cyfrowym świecie uznaje phishing; respondenci obawiają się, że w wyniku tego oszustwa zostaną wyłudzone ich dane osobowe i pieniądze.

Pytanie:

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



Warto zauważyć, że prawie co trzeci badany (29%) obawia się ataków hakerów na instytucje publiczne oraz zagrożeń typu malware, (nieświadoma instalacja złośliwego oprogramowania, np. trojany lub inne wirusy).

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. 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 etc.)

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

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

Badania deklarują, że 38 proc. Polaków 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 udostępnienie 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)

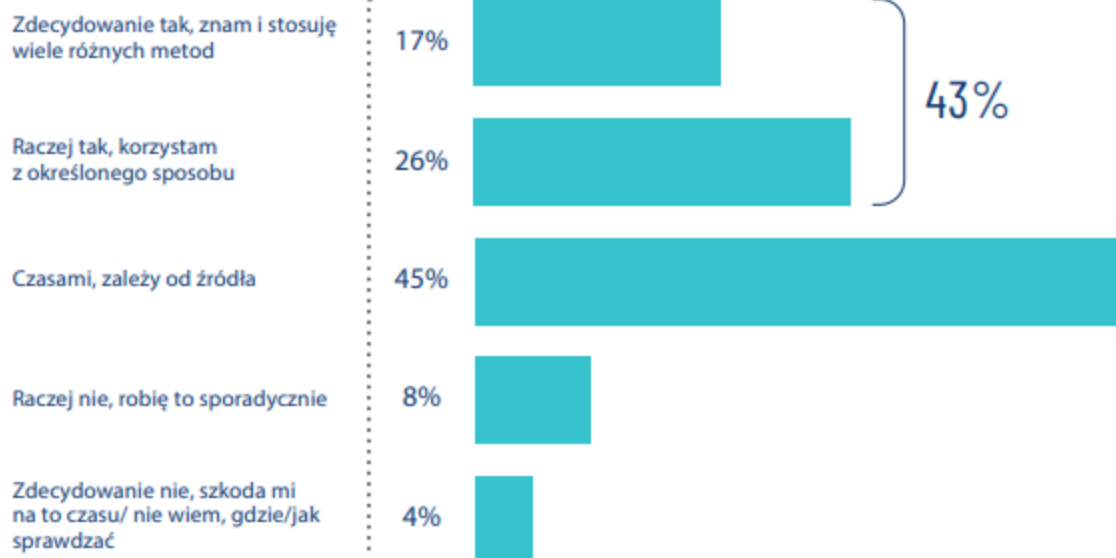


Mniej niż połowa Polaków regularnie weryfikuje informacje pojawiające się w Internecie

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.

Pytanie:

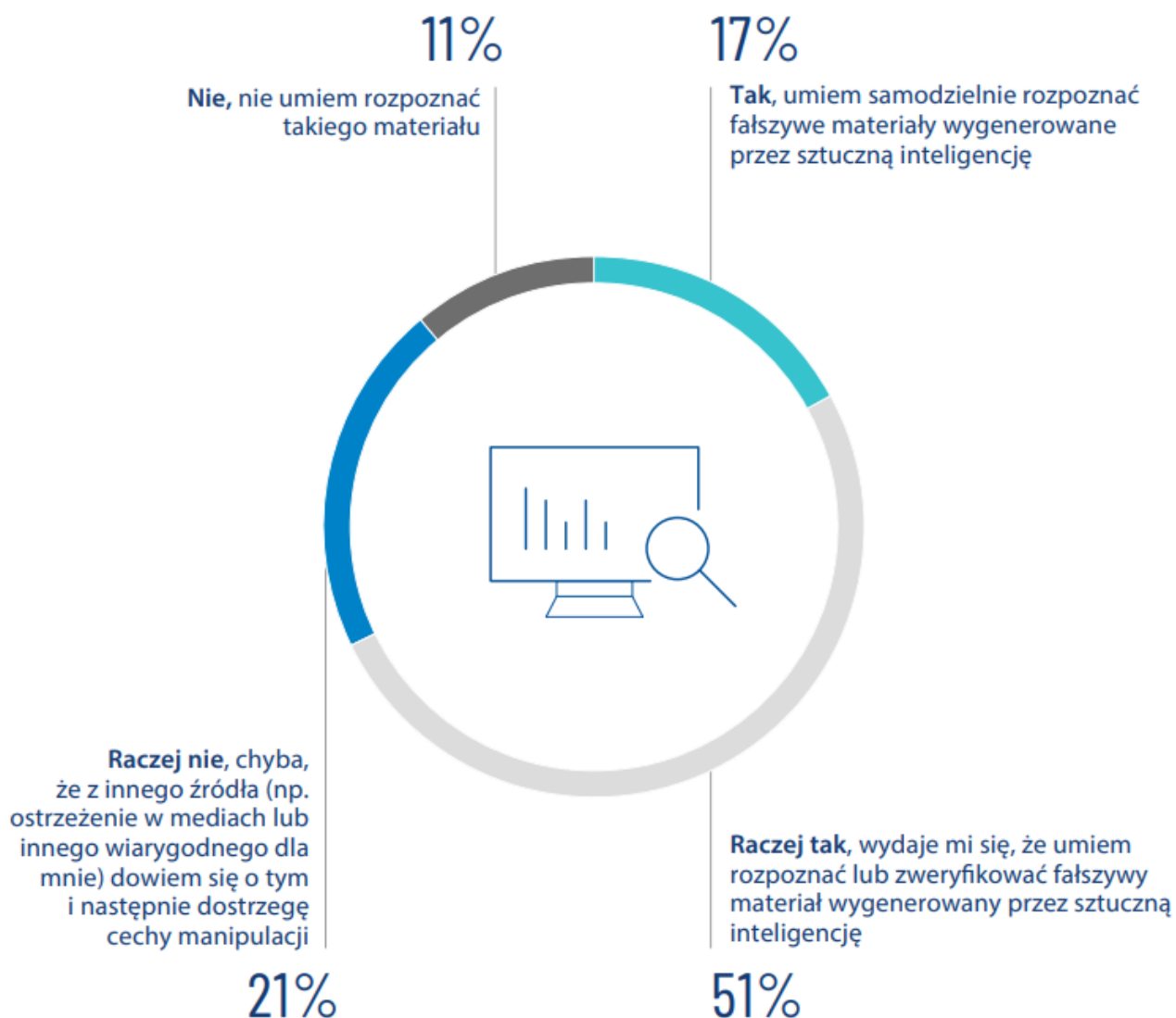
**Czy w jakikolwiek sposób sprawdzasz wiarygodność informacji,
które przeczytałeś/aś w Internecie? (jedno wskazanie)**



Ponad połowie Polaków wydaje się,
że potrafią rozpoznać deepfake'i.
Spostrzegawczość Polaków silniejsza
od zdolności AI?

Pytanie:

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



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

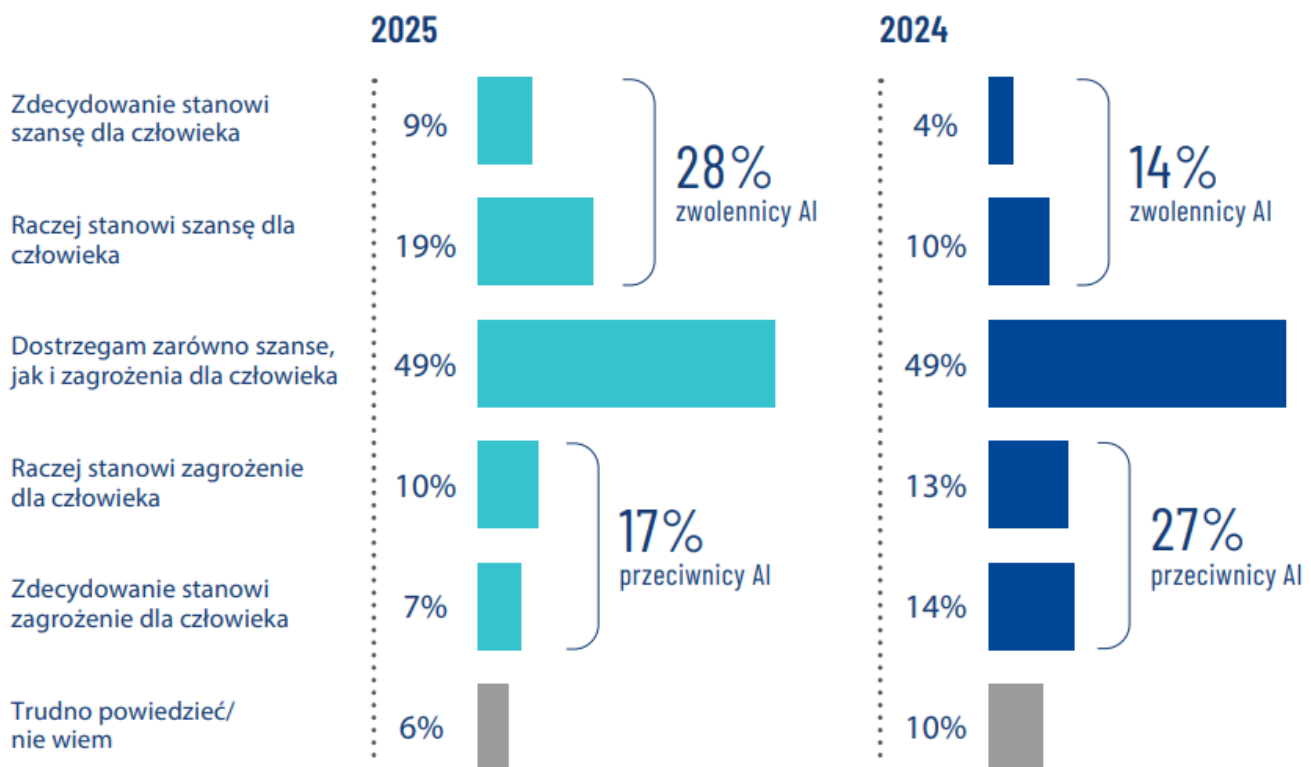
Sztuczna inteligencja zyskuje zaufanie – Polacy widzą w niej szansę, nie zagrożenie

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

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

Kreatywność ponad algorytmy – Polacy wciąż wolą wymyślać hasła po swojemu

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. Google) – tylko co piąty badany (19 proc.) najczęściej w wieku 18-34 lat deklaruje, że zabezpiecza je w tym programie.

Antywirus zainstalowany – i zapomniany? Aktualizacje wciąż poza uwagą

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

Publiczne Wi-Fi i rozmowy telefoniczne – momenty, w których zapominamy

o bezpieczeństwie

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, stosuje dwuskładnikowe uwierzytelnianie, pobiera aplikacje czy oprogramowanie wyłącznie z autoryzowanych sklepów.

Niestety Polacy zbyt rzadko weryfikują dzwoniącą osobę, która przedstawia się jako pracownik banku, przez co mogą być narażeni na oszustwa typu phishing i spoofing, które grożą wyłudzeniem danych potrzebnych do zhakowania elektronicznego konta bankowego.

Niepokojący jest 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!

Cyberoszustwo? Polacy coraz lepiej wiedzą, co robić

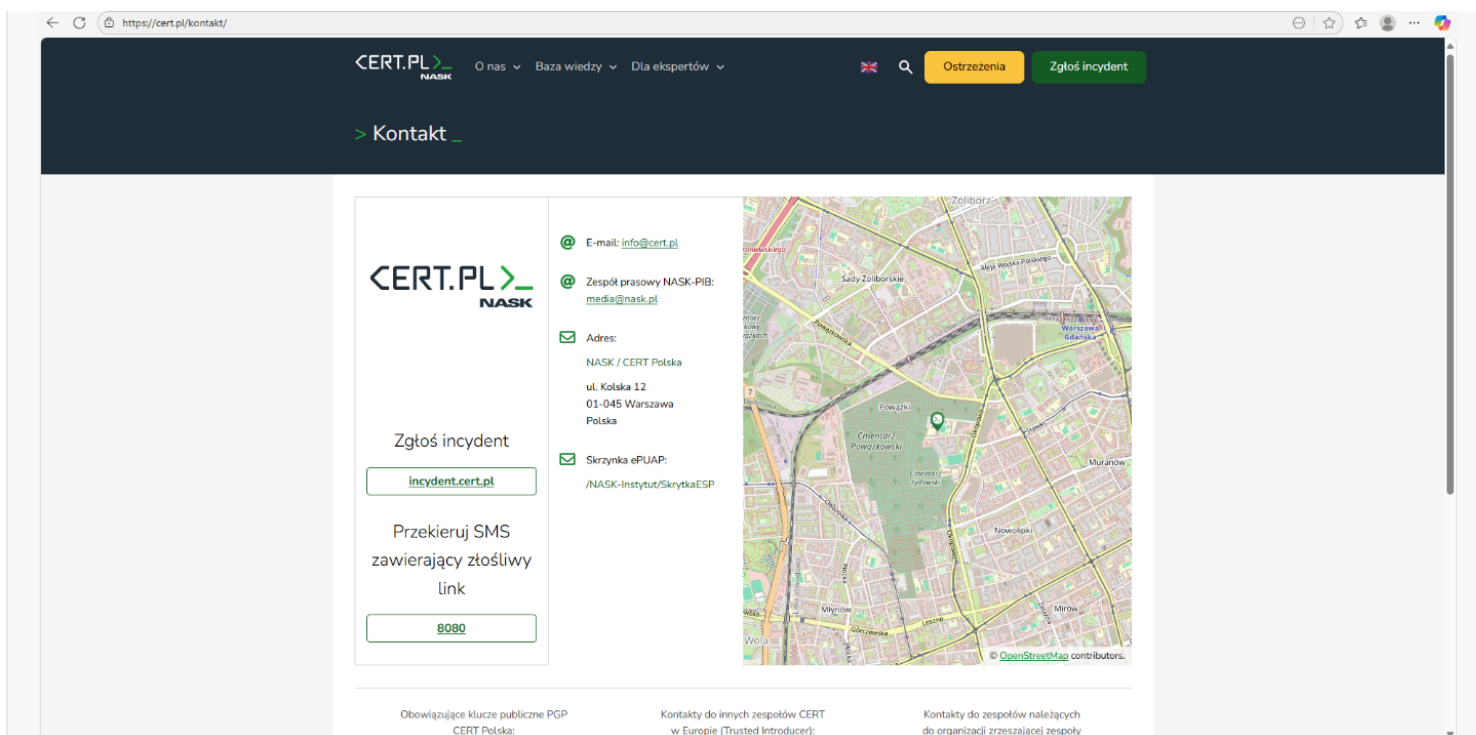
Podejrzewając, że haker/oszust zdobył dane, które umożliwiają mu np. wyłudzenie pieniędzy lub zalogowanie się do bankowości internetowej lub mobilnej, 57 proc. respondentów od razu blokuje kartę płatniczą, a 55 proc. informuje telefonicznie bank w celu wyjaśnienia zdarzenia i ewentualnej blokady konta.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

Pytanie:

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



Tylko niespełna co trzecia osoba (29 proc.) zdecydowałaby się na powiadomienie CERT Polska, czyli instytucji, która przyjmuje zgłoszenia phishingu. W razie jakichkolwiek wątpliwości, bądź chęci powiadomienia CERT Polska o możliwym cyberoszustwie, wystarczy skontaktować się z instytucją poprzez wskazaną poniżej stronę internetową (CERT Polska).



Wiedza Polaków o cyberbezpieczeństwie powoli rośnie

30 proc. badanych Polaków deklaruje, że bardzo dobrze zna się na bezpieczeństwie w przestrzeni cyfrowej – to o 4 p.p. więcej niż w zeszłym roku. Mimo to prawie połowa badanych (49 proc.) posiada wciąż tylko orientacyjną wiedzę w tym temacie. To pokazuje, że niezbędne są systemowe i ciągłe działania edukacyjne, które podnosić będą wiedzę i umiejętności społeczeństwa w tym zakresie.

Cyfrowa mądrość dorosłych buduje kompetencje dzieci – w domu i w szkole

Edukacja i poszerzenie 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 pokazać dzieciom właściwe postawy cyfrowe oraz uczyć balansu pomiędzy byciem online i offline.

Z drugiej strony, część badanych jest zwolennikami bardziej rygorystycznych działań, które miałyby chronić dzieci i młodzież przed cyfrowymi zagrożeniami (zakładanie blokad przed niewłaściwymi treściami na urządzeniach, czy wprowadzenie zakazu używania smartfonów w szkołach).

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

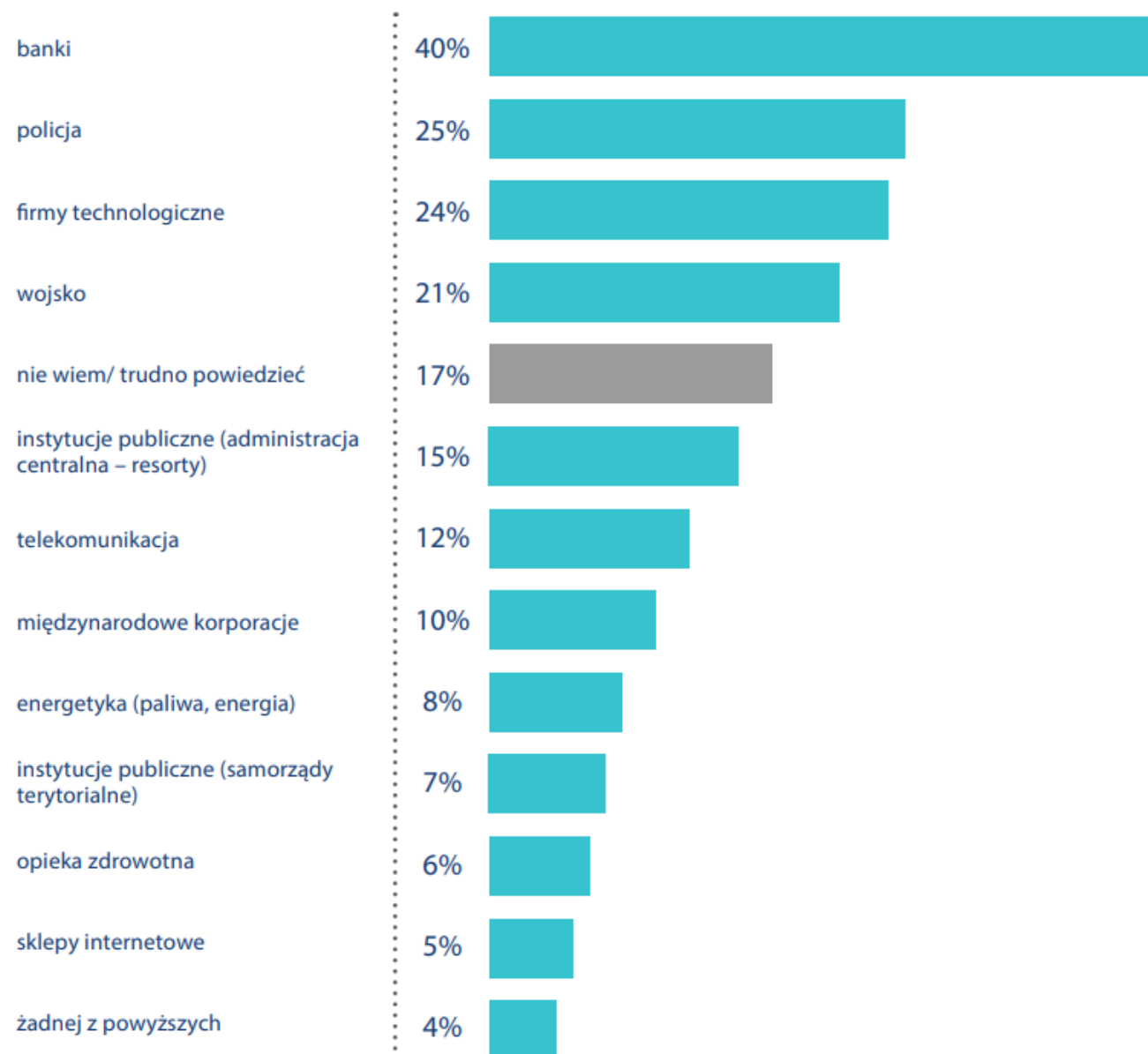
Blisko czterech na dziesięciu badanych (38 proc.) wskazuje, że za bezpieczeństwo elektronicznych usług finansowych odpowiadają głównie banki. Warto zauważyć, że w rzeczywistości, w której coraz więcej usług finansowych przenosi się do cyfrowego świata, Polacy zauważają, że odpowiedzialność za nasze cyberbezpieczeństwo 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. Społeczeństwo zaczyna dostrzegać również swój wpływ na cyberbezpieczeństwo.

Cyberbezpieczeństwo? Najpierw bank – Polacy wskazują lidera

Pytanie:

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



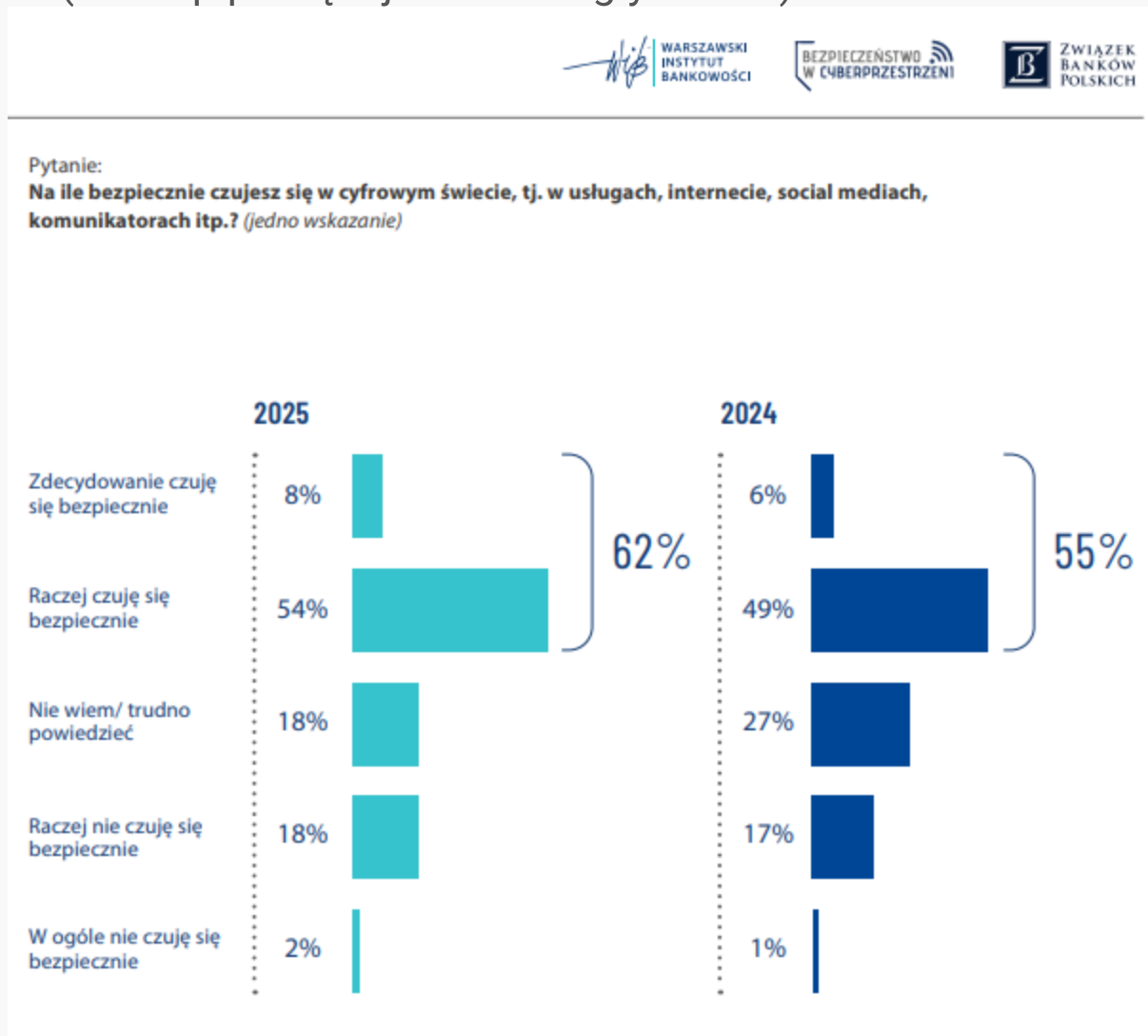
Najwięcej badanych (40 proc.) wskazuje, że to banki są najlepszym gwarantem bezpieczeństwa w przestrzeni cyfrowej i najbardziej rozwijają się w zakresie cyberbezpieczeństwa. Respondenci doceniają również zabezpieczenia służb mundurowych (policji – 25 proc., wojska – 21 proc.) oraz firm technologicznych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

Poczucie bezpieczeństwa obywateli? 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 wzrasta – już 62 proc. respondentów czuje się bezpiecznie w cyfrowym świecie (to o 7 p.p. więcej niż w ubiegłym roku).



Raport „*Postawy Polaków wobec cyberbezpieczeństwa 2025*” stanowi ważny głos w debacie nad kształtem polityki cyfrowej państwa. Z punktu widzenia socjologii prawa, widoczna jest rozbieżność między

świadomością zagrożeń a rzeczywistymi praktykami ochronnymi. Raport wskazuje na potrzebę intensyfikacji działań edukacyjnych, wzmocnienia zaufania do instytucji oraz wdrożenia skuteczniejszych mechanizmów ochrony danych. W obliczu rosnącej liczby zagrożeń cyfrowych, konieczne jest zintegrowane podejście, łączące regulacje prawne, edukację społeczną i odpowiedzialność instytucjonalną.

METRYKA STRONY

REJESTR ZMIAN