WARSZAWSKI INSTYTUT BANKOWOŚCI

RAPORT

CYBERBEZPIECZNY PORTFEL



edycja VI
październik 2026

Publikacja **Warszawskiego Instytutu Bankowości** pod patronatem Związku Banków Polskich

BEZPIECZEŃSTWO W CYBERPRZESTRZENI

BANKOWCY DLA EDUKACJI program sektorowy

ZWIĄZEK BANKÓW POLSKICH

SPIS TREŚCI

		strona
O raporcie „Cyberbezpieczny Portfel”		3
rozdział 1	Statystyka badania „Postawy Polaków wobec cyberbezpieczeństwa”	5
rozdział 2	Zagrożenia w cyfrowym świecie	8
rozdział 3	Zasady bezpieczeństwa w przestrzeni cyfrowej	17
rozdział 4	Cyberbezpieczny portfel – bezpieczeństwo finansowe Polaków	23
rozdział 5	Edukacja - wiedza to potęgi klucz	30
O projekcie edukacyjnym „Bezpieczeństwo w Cyberprzestrzeni”		32

O RAPORCIE

Raport „Cyberbezpieczny Portfel" to cykliczna publikacja Warszawskiego Instytutu Bankowości wydawana od 2016 r. pod patronatem Związku Banków Polskich, która przybliża postawy społeczne w cyfrowym świecie, ze szczególną uwagą na kwestie bezpieczeństwa finansowego i zagrożeń w cyberprzestrzeni.

Postępująca cyfryzacja usług wiąże się z coraz większą aktywnością społeczeństwa w przestrzeni online. Również sprawcy przestępstw dostosowują swoje metody działania do dynamicznie zmieniającego się środowiska cyfrowego, poszukując coraz bardziej zaawansowanych sposobów dokonywania oszustw internetowych. Omawiany raport przedstawia szeroki zakres tego rodzaju zagrożeń, wśród których szczególne miejsce zajmuje phishing, polegający na pozyskiwaniu poufnych informacji w celu osiągnięcia korzyści majątkowych. Publikacja porusza również zagadnienia związane z rozwojem sztucznej inteligencji, społecznym podejściem do jej wykorzystywania oraz narastającym problemem dezinformacji, w tym treści generowanych z zastosowaniem narzędzi opartych na AI.

Celem raportu jest nie tylko przedstawienie istotnych danych dotyczących cyfrowego bezpieczeństwa, lecz także zwiększanie świadomości społecznej w zakresie odpowiedzialnego korzystania z internetu. W związku z tym opracowanie zawiera również praktyczne wskazówki, których zastosowanie może przyczynić się do ograniczenia ryzyka związanego z cyberzagrożeniami, a tym samym do skuteczniejszej ochrony danych osobowych i zasobów finansowych użytkowników. Istotnym aspektem publikacji jest zatem upowszechnianie wiedzy na temat cyberbezpieczeństwa oraz zachęcanie do dzielenia się informacjami i wnioskami wynikającymi z analizy przedstawionych zagadnień.

dr Michał Polak,
Wiceprezes Fundacji Warszawski Instytut Bankowości



okładka Raportu z 2024 roku

Raport „Cyberbezpieczny Portfel" (edycja VI) powstał w oparciu o wyniki badania „Postawy Polaków wobec cyberbezpieczeństwa 2026", zleconego przez Fundację Warszawski Instytut Bankowości (WIB), a przeprowadzonego przez firmę badawczą SW Research. Badanie przeprowadzono we wrześniu 2026 roku w formie ankiety online na reprezentatywnej próbie 1001 osób (Polek i Polaków) w wieku 18–60+.

Raport i badanie zrealizowano w ramach projektu edukacyjnego WIB „Bezpieczeństwo w Cyberprzestrzeni", który jest częścią Programu sektorowego „Bankowcy dla Edukacji". Raport „Cyberbezpieczny Portfel" publikowany jest co dwa lata.

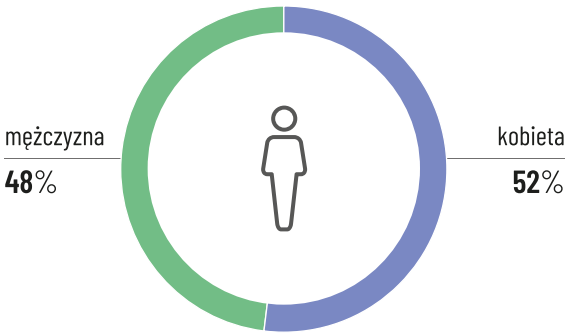
ROZDZIAŁ



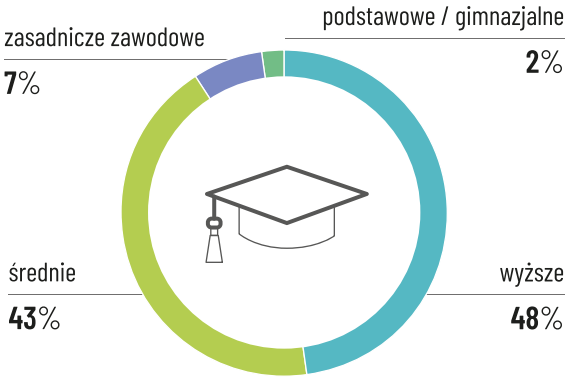
Statystyka badania *„Postawy Polaków wobec cyberbezpieczeństwa”*

METRYCZKA BADANIA[1]

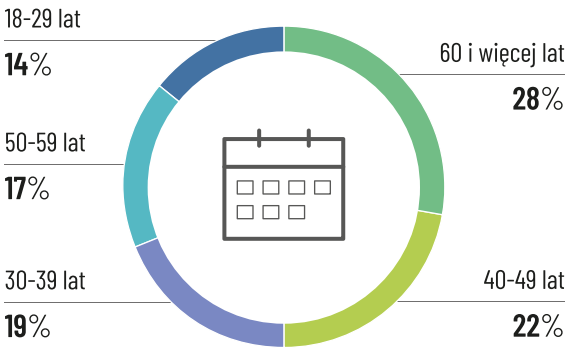
Płeć



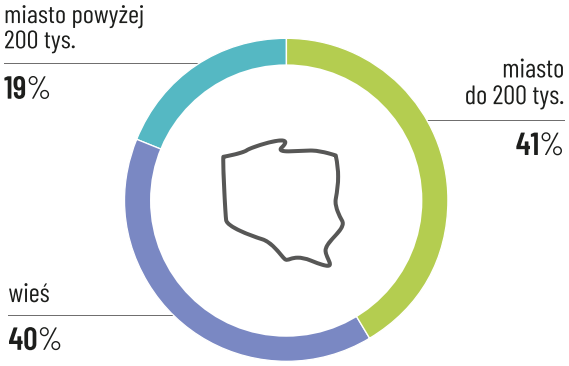
Wykształcenie



Kategoria wiekowa



Wielkości miejscowości

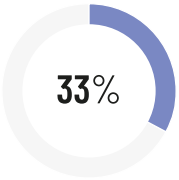


[1] W raporcie dane procentowe z badania „Postawy Polaków wobec cyberbezpieczeństwa" zostały odpowiednio zaokrąglone dla przejrzystości przekazu.

KLUCZOWE WNIOSKI I TRENDY[2]

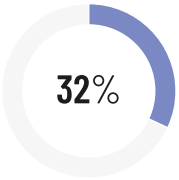
TOP 4 NAJWIĘKSZYCH ZAGROŻEŃ

1



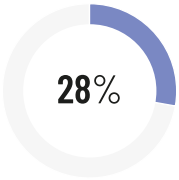
respondentów uznało **kradzież tożsamości w social mediach za najgroźniejsze zagrożenie w cyberprzestrzeni** (spośród 14 wytypowanych)

2



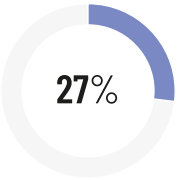
obawia się oszustwa tzw. phishingu, tj. wyłudzania pieniędzy i danych osobowych

3

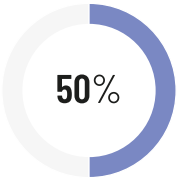


za 3 największe zagrożenie uznaje ataki hakerów na instytucje publiczne

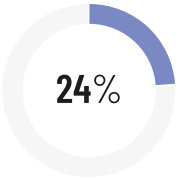
4



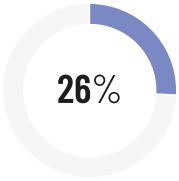
badanych obawia się fake newsów i dezinformacji, ale tylko 44% czasami weryfikuje przeglądane materiały w sieci



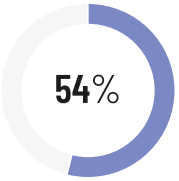
Polaków dostrzega w AI zarówno sprzymierzeńca, jak i wroga



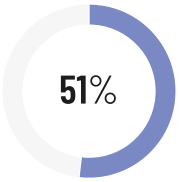
niepokoi zbyt szybki rozwój sztucznej inteligencji



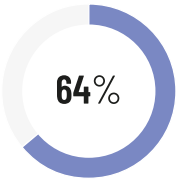
badanych obawia się wykorzystania AI do działań przestępczych wycelowanych w bezpieczeństwo finansowe



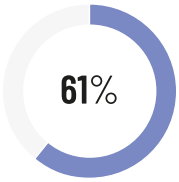
nie umie rozpoznać lub zweryfikować fałszywego materiału wygenerowanego przez AI (tzw. deepfake'a)



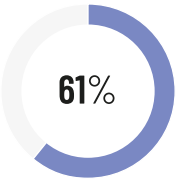
Polaków czuje się w miarę bezpiecznie w cyfrowym świecie



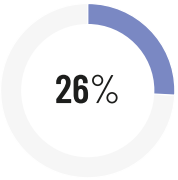
stosuje różne hasła do różnych kont, ale tylko 10% korzysta z generatorów haseł



nie podaje haseł do bankowości, danych kart płatniczych, czy nr PESEL



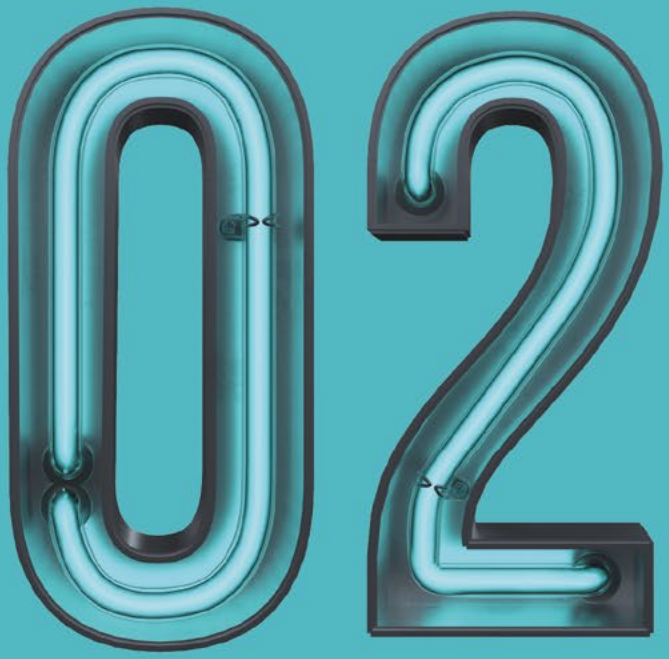
Polaków nigdy nie zgłosiło próby wyłudzenia pieniędzy i danych (tj. phishingu) dokonanych przez fałszywą stronę www / email / SMS / połączenie telefoniczne!



prawie co czwarty Polak dostrzega coraz większą rolę firm technologicznych w wyścigu o cyfrowe bezpieczeństwo Polaków, choć banki nadal pozostają liderem w zakresie cyberbezpieczeństwa

[2] Wybrane liczby z badania „Postawy Polaków wobec cyberbezpieczeństwa 2026"

ROZDZIAŁ



Zagrożenia w cyfrowym świecie

ZAGROŻENIA W CYFROWYM ŚWIECIE

Współcześnie przestrzeń internetowa stanowi istotny element funkcjonowania człowieka, umożliwiając realizację wielu aspektów życia codziennego, takich jak wykonywanie obowiązków zawodowych, korzystanie z usług finansowych i bankowości elektronicznej, robienie zakupów, zdobywanie wiedzy, pozyskiwanie informacji czy nawiązywanie i podtrzymywanie relacji interpersonalnych. Jednocześnie cyfrowy świat jest środowiskiem, w którym podobnie jak w rzeczywistym, występują różnego rodzaju oszustwa, wykroczenia oraz przestępstwa. Stąd rozwijanie kompetencji cyfrowych, zdobywanie wiedzy o zagrożeniach i bezpiecznym poruszaniu się w cyberprzestrzeni powinno stanowić ważną część funkcjonowania współczesnego, coraz bardziej zdigitalizowanego społeczeństwa.

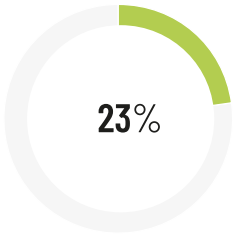
NAJWIĘKSZE ZAGROŻENIA

Badanie Fundacji Warszawski Instytut Bankowości pt. „Postawy Polaków wobec cyberbezpieczeństwa 2026" wskazuje, że obecnie spośród 14 wytypowanych niebezpieczeństw w przestrzeni cyfrowej za najgroźniejsze uznano kradzież tożsamości w mediach społecznościowych - wskazał tak co trzeci badany (33%). Natomiast prawie co piąta osoba (21%) osobiście lub w swoim otoczeniu doświadczyła zhakowania konta w social mediach - zazwyczaj była to kobieta w wieku od 18 do 49 lat. Co ciekawe za zagrożenie uznaje to cyberprzestępstwo więcej pań w wieku senioralnym, tj. 60+.

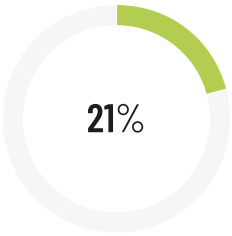
Drugim sporym zagrożeniem w sieci jest tzw. z ang. phishing – uważa tak 32% respondentów, którzy za pośrednictwem tego oszustwa obawiają się wyłudzania pieniędzy i danych osobowych. W ciągu ostatnich 12 miesięcy z próbą kradzieży poufnych informacji i/lub środków pieniężnych (za pośrednictwem fałszywych emaili, stron www, SMS-ów czy komunikatorów) zetknęło się osobiście lub w swoim otoczeniu 18% badanych. Natomiast 19% osób miało do czynienia z tym procederem poprzez tzw. spoofing, tj. w sytuacji gdy oszust dzwoniąc, podszywał się pod firmę/instytucję/urząd za pośrednictwem fałszywego numeru telefonu.

Kolejnymi dużymi zagrożeniami wzbudzającymi niepokój wśród Polaków są również ataki hakerów na instytucje publiczne (28%) oraz rozpowszechniane w przestrzeni cyfrowej fake newsy i dezinformacja (27%).

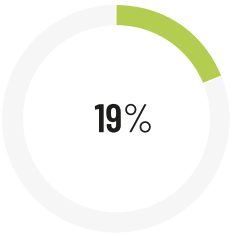
Respondenci zwrócili także uwagę na inne szkodliwe działania występujące w cyfrowym świecie, takie jak:



wskazało tzw. malware (z ang.), tj. nieświadomą instalację złośliwego oprogramowania, takiego jak trojany i inne wirusy – zetknięcie się z takim zagrożeniem deklaruje więcej panów w wieku 18-29 lat



oszustwa inwestycyjne, np. w kryptowaluty – największe obawy wzbudza u 30-letnich mężczyzn

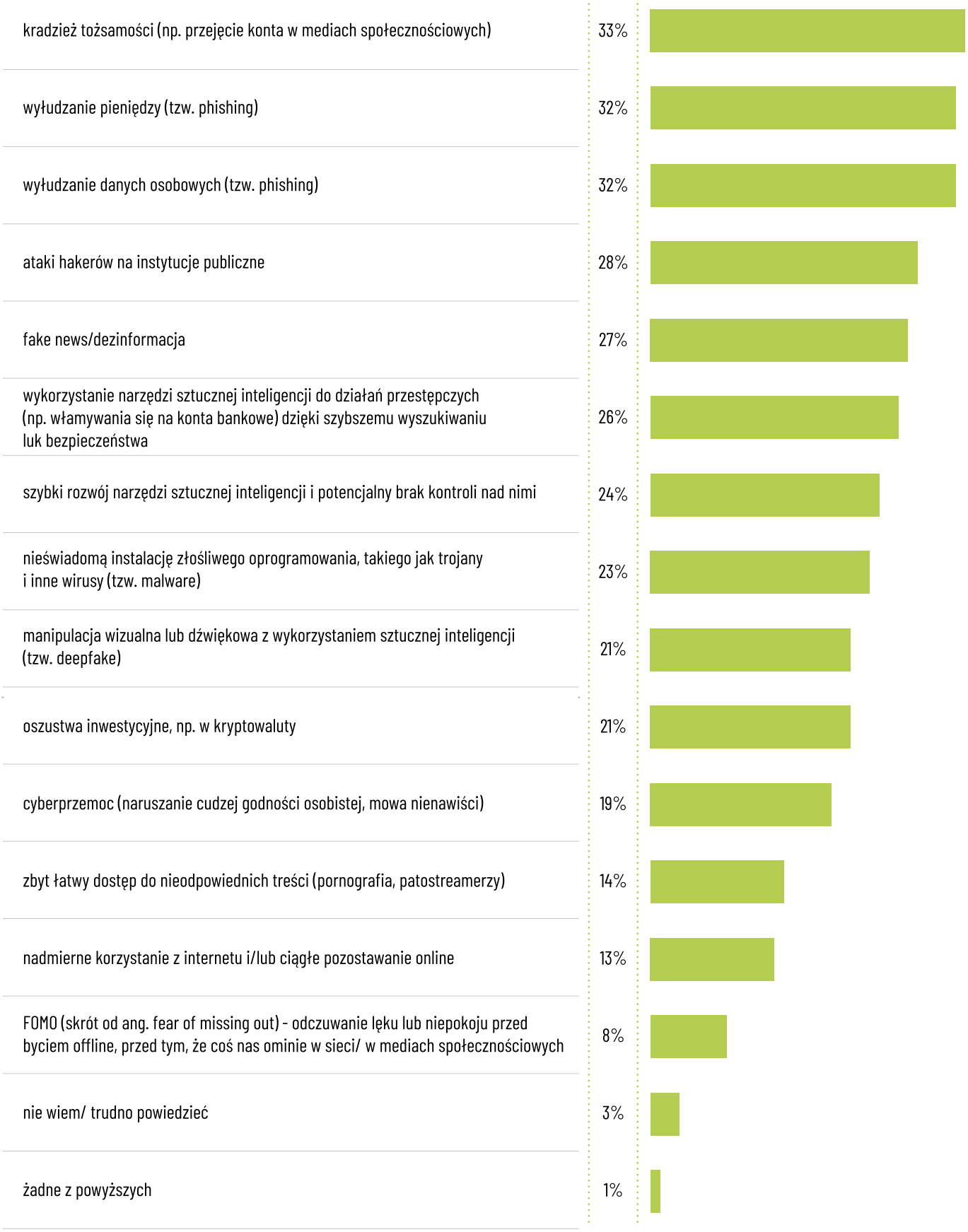


cyberprzemoc, naruszanie cudzej godności osobistej i mowa nienawiści – najbardziej niepokoi kobiety w wieku 40-59 lat

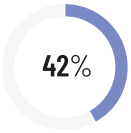
Warto zwrócić uwagę, że obawy Polaków wzbudza także szybki rozwój sztucznej inteligencji – o potencjalny brak kontroli nad AI boi się co czwarty badany (24%). Natomiast 21% Polaków zauważa wykorzystywanie tej technologii do tworzenia fikcji i manipulacji poprzez tzw. deepfake'i, czyli wygenerowane przez AI fałszywe obrazy, treści i filmy, które mogą być użyte m.in. do oszustw finansowych, dyskredytowania osób publicznych czy rozprzestrzeniania dezinformacji. Natomiast 26% respondentów niepokoi się wykorzystaniem sztucznej inteligencji do działań przestępczych wycelowanych stricte w bezpieczeństwo finansowe, np. w przypadku włamania się na konta bankowe, dzięki szybszemu wyszukiwaniu przez AI luk w systemach ochronnych.



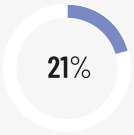
Wskaż obszary, które uważasz obecnie za największe zagrożenia w przestrzeni cyfrowej?



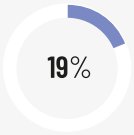
Czy w ciągu ostatnich 12 miesięcy spotkałeś/aś się (osobiście lub w Twoim otoczeniu) z następującymi oszustwami?



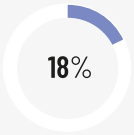
Nie pamiętam, abym miał/a styczność z którąkolwiek z tych metod oszustw



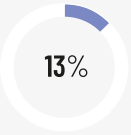
Ja lub ktoś w moim otoczeniu miał do czynienia ze **zhakowaniem konta w mediach społecznościowych** (przejęcie konta i wizerunku)



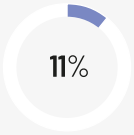
Ja lub ktoś w moim otoczeniu miał do czynienia **z oszustwem dokonanym telefonicznie** – oszust podszywał się pod firmę, instytucję, urząd bądź osobę (tzw. spoofing)



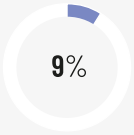
Ja lub ktoś w moim otoczeniu miał do czynienia z **phishingiem**, czyli z próbą kradzieży danych osobowych/poufnych informacji i/lub środków pieniężnych za pośrednictwem fałszywych emaili, stron www, SMS-ów czy komunikatorów



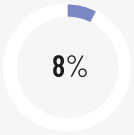
Ja lub ktoś w moim otoczeniu miał do czynienia **z oszustwem inwestycyjnym dokonanym za pośrednictwem rozmowy** telefonicznej z fałszywym doradcą



Ja lub ktoś w moim otoczeniu miał do czynienia z **malware**, czyli złośliwym oprogramowaniem, którego celem jest uszkodzenie, zakłócenie działania lub uzyskanie nieautoryzowanego dostępu do komputera / smartfona



Ja lub ktoś w moim otoczeniu miał do czynienia **z oszustwem inwestycyjnym dokonanym za pośrednictwem fałszywej reklamy** wygenerowanej przez sztuczną inteligencję (tzw. deepfake)



Ja lub ktoś w moim otoczeniu miał do czynienia z tzw. **oszustwem romantycznym**, czyli poprzez nawiązanie relacji na portalu randkowym czy w social mediach (oszust udawał relację, aby wyłudzić pieniądze)

PRZYDATNE DEFINICJE

Phishing (powiązane z ang. słowem „fishing", czyli łowieniem ryb) - przestępcy, podobnie jak wędkarze stosują przynętę, tj. podszywają się np. pod osobę zaufania publicznego lub instytucję/ firmę za pośrednictwem fałszywych e-maili, stron www lub SMS-ów, aby zdobyć poufne informacje (takie jak login i hasło do banku, PESEL itp.) w celu kradzieży pieniędzy. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych.

Vishing (z ang. voice phishing, tj. rodzaj phishingu przez telefon) - przestępcy dzwonią z nieznanych numerów i podszywają się zazwyczaj pod osobę zaufania publicznego (np. policjanta, lekarza, pracownika ZUS) w celu wyłudzenia danych lub pieniędzy.

Spoofing – to fałszowanie numeru telefonicznego w połączeniu przychodzącym. Na ekranie telefonu odbiorca rozmowy widzi np. numer swojego banku, policji lub urzędu, podczas gdy dzwoni oszust.

AI A FAKE NEWSY I DEZINFORMACJA. JAK SIĘ CHRONIĆ?

Rozwój sztucznej inteligencji umożliwia tworzenie coraz bardziej zaawansowanych i trudnych do wykrycia fałszywych treści. Stąd tworzone przez AI deepfake'i służą m.in. do rozpowszechniania dezinformacji i stają się jednym ze skutecznych narzędzi manipulacji informacją, mogąc wpływać na emocje, decyzje czy nawet na przekonania odbiorców.

Dane z 2025 roku wskazane przez NASK-PIB we współpracy z KNF CSIRT informują o ponad 13 tysiącach deepfake'ów w sieci (głównie reklamowych), gdzie niemal 60% z nich dotyczyło fałszywych instrumentów finansowych i programów rządowych, w których wykorzystano ponad 280 wizerunków znanych osób.[3]

Biorąc pod uwagę tak dużą skalę deepfake'ów krążących w przestrzeni cyfrowej, zadziwiające jest, że ponad połowie Polaków (głównie z wykształceniem wyższym w przedziale wiekowym 30-49 lat) wydaje się, że rozpozna i zweryfikuje fałszywy materiał wygenerowany przez sztuczną inteligencję, podczas gdy tylko 16% ogółu badanych sprawdza pochodzenie zdjęć i obrazów ilustrujących informację.[4]

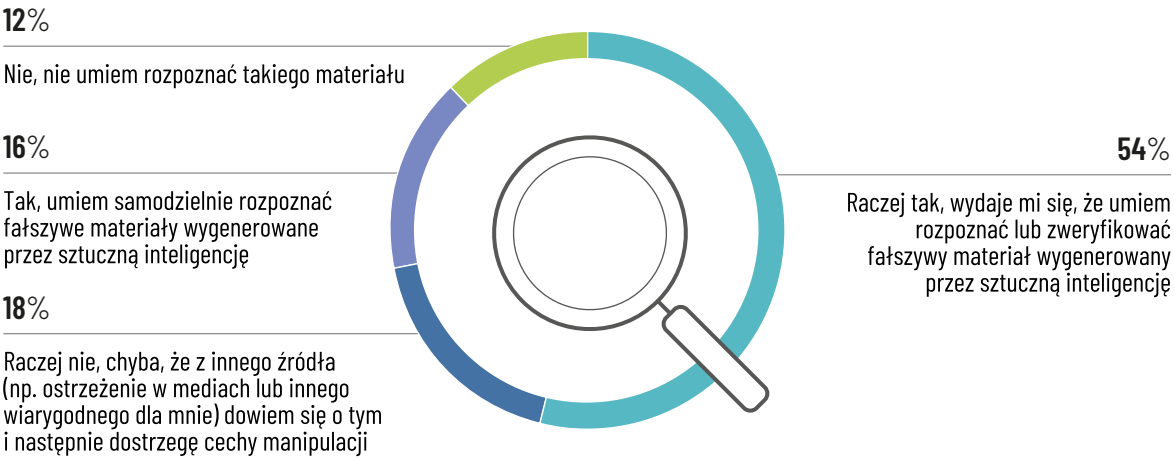
Natomiast co piąty respondent badania WIB (18%) zadeklarował trudności z rozpoznaniem materiałów typu deepfake, wskazując, że identyfikacja tego rodzaju treści byłaby łatwiejsza w przypadku posiadania wcześniejszych informacji o możliwości zetknięcia się z taką manipulacją. Tylko 12% osób przyznaje, że w ogóle nie potrafiłoby rozpoznać deepfake'a stworzonego przez AI.

KATARZYNA GRABOWSKA
starszy specjalista ds. edukacyjno-informacyjnych, NASK-PIB

„Na materiały stworzone przy użyciu sztucznej inteligencji można trafić w wielu miejscach: media społecznościowe, serwisy internetowe, reklamy w wyszukiwarkach czy strony internetowe. Powszechność oraz dostępność narzędzi AI sprawia, że tworzenie różnego rodzaju zdjęć, materiałów audio i wideo stało się nie tylko bardzo proste, ale i wraz z rozwojem technologii doskonalsze. Jakość generowanych materiałów jest coraz lepsza przez co coraz trudniej na pierwszy rzut oka rozpoznać, że to, co widzimy może nie być prawdą. Dlatego nie warto bezkrytycznie ufać temu, co widzimy i słyszymy w internecie. Nawet osoby posiadające wiedzę na temat nowych technologii i zagrożeń cyfrowych mogą mieć trudność z rozpoznaniem treści wygenerowanych przez zaawansowane systemy AI. Kluczowe znaczenie ma zachowanie krytycznego myślenia, weryfikowanie informacji w wiarygodnych źródłach oraz ostrożne podejście do materiałów, które wywołują silne emocje lub wydają się zaskakujące."

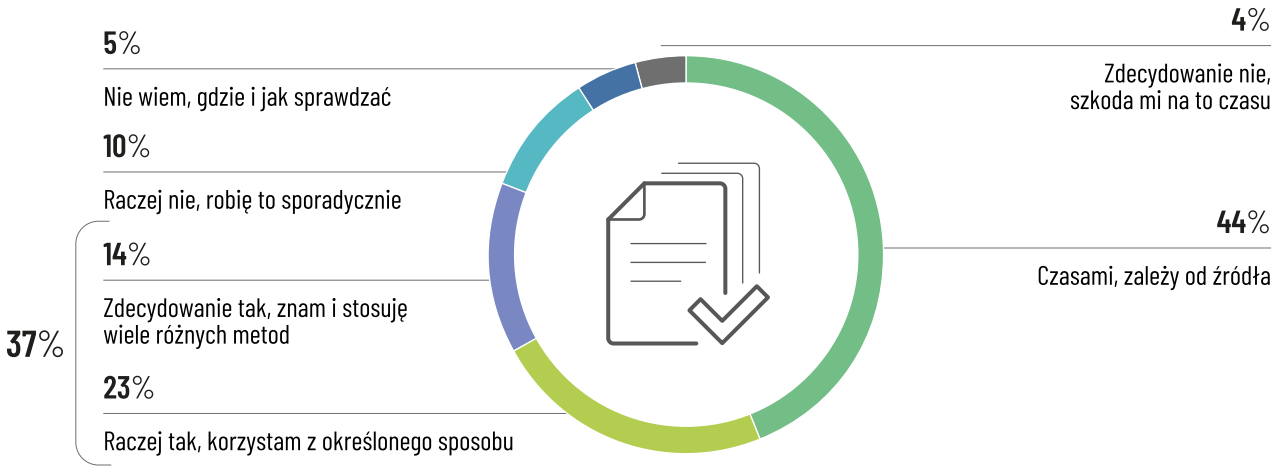
[3] Źródło: strona internetowa gov.pl - https://www.gov.pl/web/ai/techniki-manipulacji-w-swiecie-deepfakeow---jak-sztuczna-inteligencja-zmienia-oblicze-dezinformacji
[4] Dane z badanie WIB „Postawy Polaków wobec cyberbezpieczeństwa 2026"

Czy umiesz rozpoznać tzw. deepfake, czyli nieprawdziwe materiały audiowizualne (fałszywe nagrania i zdjęcia) wytworzone przy użyciu technik sztucznej inteligencji?



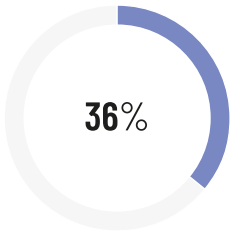
Do rozpoznawania fake newsów lub innych fałszywych materiałów w przestrzeni cyfrowej potrzebne jest zatem sprawdzanie wiarygodności informacji. Jedynie 37% Polaków kontroluje autentyczność wiadomości w internecie, przy czym 23% badanych stosuje w tym celu tylko jeden określony sposób weryfikacji. Niestety większość respondentów (44%) tylko czasami sprawdza przeglądane materiały w sieci, uzależniając to również od źródła, w jakim odnajduje daną informację.

Czy w jakikolwiek sposób sprawdzasz wiarygodność informacji, które przeczytałeś/aś w Internecie?

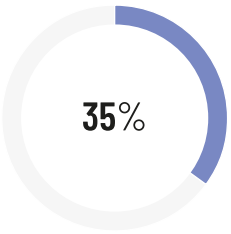


Najnowsza edycja raportu pt. „Dezinformacja oczami Polaków" (z czerwca 2026 r., wydanego przez Fundację Digital Poland wspólnie ze Stowarzyszeniem Demagog - członkiem koalicji Razem Przeciw Dezinformacji) wskazuje, że aż 77% Polaków deklaruje styczność z fake newsami. Stąd tak ważna dla społeczeństwa powinna być wiedza, jak się chronić przed dezinformacją i wpływem fake newsów.

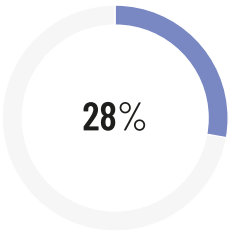
Badanie WIB pokazuje, że Polacy asekurują się przed powyższymi szkodliwymi zjawiskami na kilka sposobów:



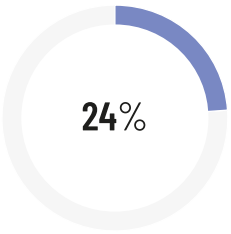
badanych ma dystans do treści prezentowanych w mediach społecznościowych i nie traktuje ich jako głównego zasobu wiedzy



weryfikuje wiadomości z internetu w kilku niezależnych od siebie źródłach - co ciekawe Polacy ufają bardziej krajowym informacjom (25%) niż zagranicznym (tylko 8% ma zaufanie do wiarygodnych mediów z zagranicy)



zapoznaje się z całymi artykułami, a nie tylko clickbaitowymi tytułami, przy czym 25% nie ulega presji czasu podczas czytania



nie rozpowszechnia niesprawdzonych informacji

Jednakże zdecydowanie za mało respondentów (18%) zgłasza lub blokuje cyfrowe treści o wątpliwym pochodzeniu.

Jakie sposoby Twoim zdaniem są najlepszą ochroną przed skutkami dezinformacji lub fake newsów?



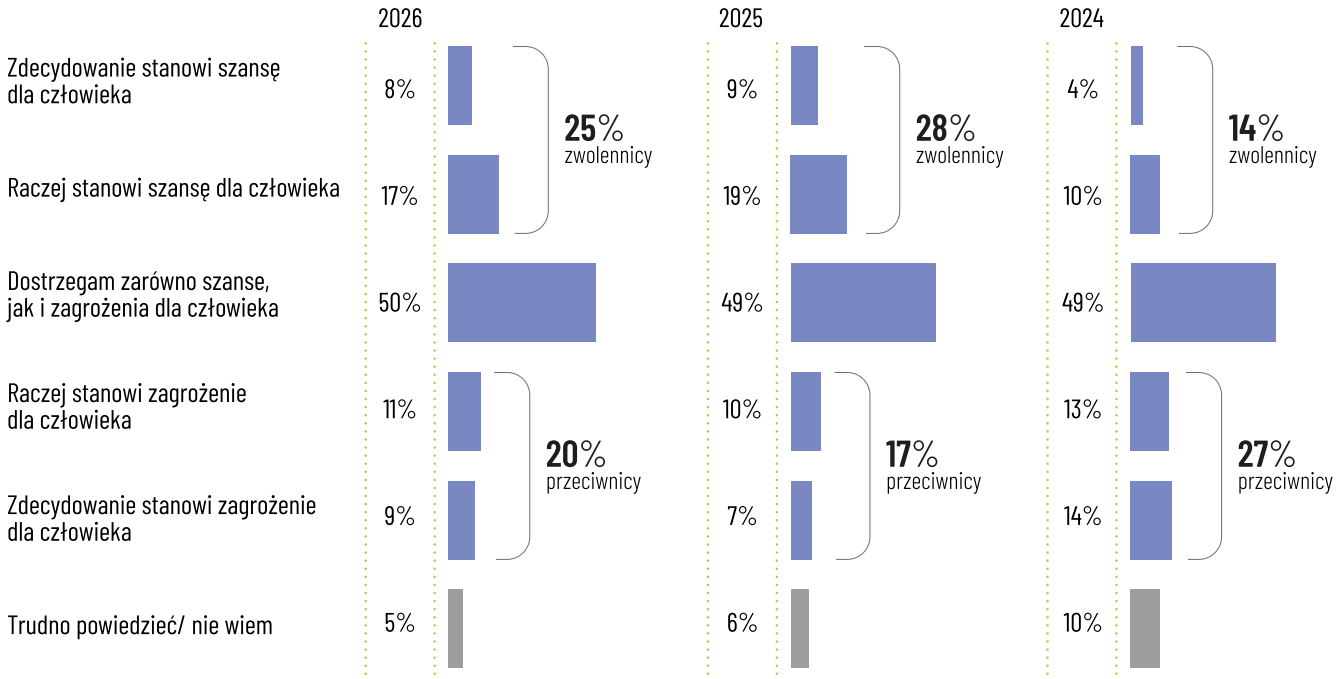
SZTUCZNA INTELIGENCJA – PRZYJACIEL CZY WRÓG?

Pomimo obaw Polaków o wykorzystywanie narzędzi AI w sposób zagrażający człowiekowi, z badania WIB wynika, że zwolenników sztucznej inteligencji jest więcej (tj. 25%) niż przeciwników (20%). Aczkolwiek porównując wyniki sprzed roku, antagonizmy w kwestii AI zacierają się i różnica procentowa pomiędzy sprzymierzeńcami tej technologii a jej wrogami maleje – w 2026 r. różnica pomiędzy tymi grupami wyniosła 5 punktów procentowych, zaś w 2025 r. było to aż 11 punktów procentowych.

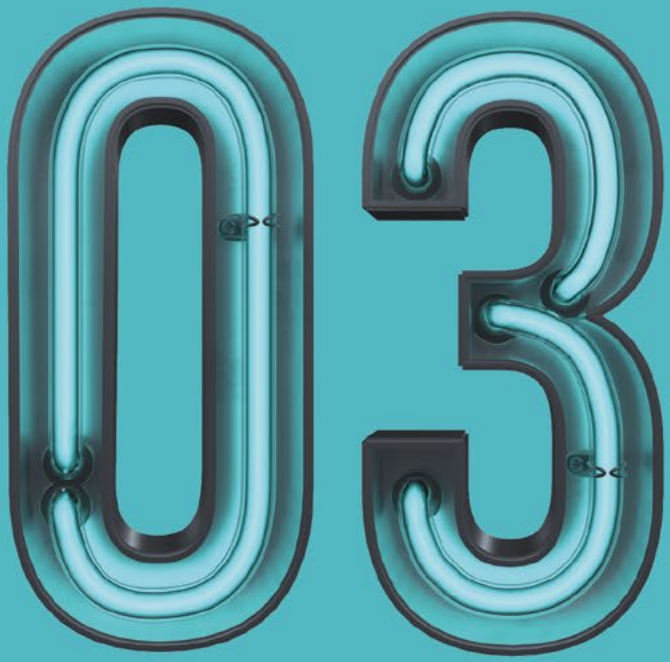
Warto również zauważyć, że jeszcze 2 lata temu (w 2024 roku) to samo badanie wykazało więcej przeciwników AI (27%) niż zwolenników (których było 14%), podczas gdy w 2025 roku tendencja odwróciła się i więcej Polaków widziało w AI szansę (28%), a 17% zagrożenie.

Od trzech lat dominuje jednak ambiwalentny stosunek Polaków do sztucznej inteligencji, tj. większość respondentów (tj. 50%) dostrzega zarówno szanse jak i zagrożenia, jakie daje ta stale rozwijająca się technologia.

Jaki jest Twój stosunek do AI?



ROZDZIAŁ



Zasady bezpieczeństwa w przestrzeni cyfrowej

ZASADY BEZPIECZEŃSTWA W PRZESTRZENI CYFROWEJ

Polacy dostrzegają zagrożenia w życiu online w różnych jego aspektach: od e-usług (w tym finansowych), po korzystanie z social mediów i internetu, aż do szybkiego rozwoju sztucznej inteligencji. Jednocześnie, jak wynika z badania WIB, większość respondentów (51%) czuje się w miarę bezpiecznie w cyfrowym świecie, choć tylko 8% ogółu badanych ma zdecydowanie wysokie odczucie w tym zakresie.

ZNAJOMOŚĆ OGÓLNYCH ZASAD CYBERBEZPIECZEŃSTWA

Umiarkowane poczucie bezpieczeństwa w cyberprzestrzeni zapewne jest wynikiem znajomości różnych metod ochrony przed niebezpieczeństwami tam czyhającymi. Jak wynika z danych WIB, top 3 „złotych" zasad zna i stosuje większość badanych:

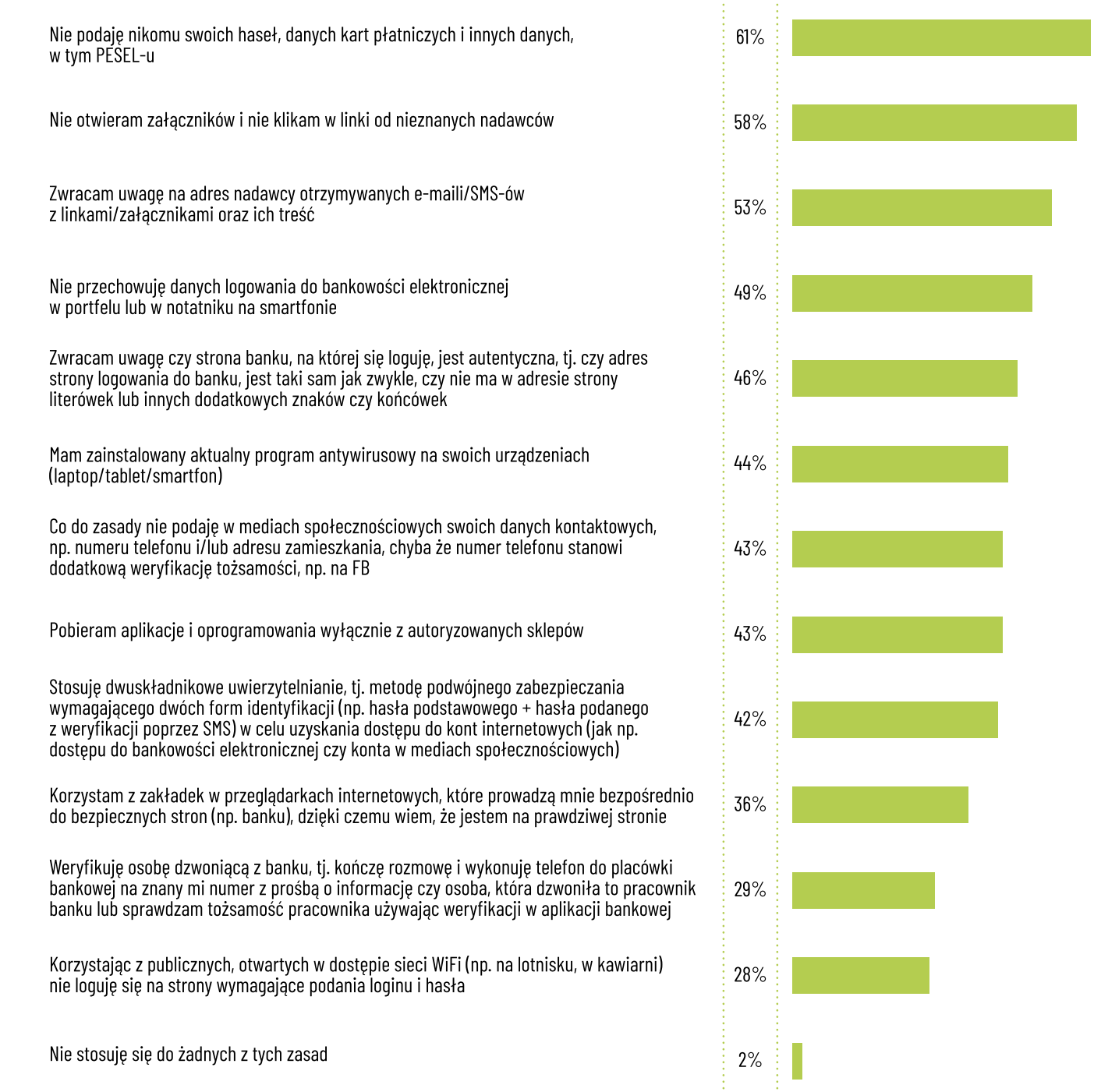


Ponadto co drugi respondent korzysta z kolejnych czterech wytycznych cyberbezpieczeństwa:

- posiadania zainstalowanego aktualnego programu antywirusowego na urządzeniach (laptop/tablet/smartfon);
- pobierania aplikacji i oprogramowania wyłącznie z autoryzowanych sklepów;
- ochrony danych kontaktowych w mediach społecznościowych, tj. nieujawniania numeru telefonu i/lub adresu zamieszkania (chyba, że numer telefonu stanowiłby dodatkową kontrolę tożsamości);
- stosowania dwuskładnikowego uwierzytelniania,
- - tj. metody podwójnego zabezpieczania wymagającego dwóch form identyfikacji (przykładowo złożonej z hasła podstawowego oraz drugiego, podanego w weryfikacji np. poprzez SMS) w celu uzyskania dostępu do kont internetowych, jak np. do wybranej platformy społecznościowej czy do bankowości elektronicznej.

Niestety zbyt mało Polaków dba o bezpieczeństwo korzystając z publicznych połączeń wi-fi. W takiej sytuacji, w której sieć internetowa nie jest odpowiednio zabezpieczona, zaleca się nielogowanie na strony www wymagające wpisania loginu i hasła – postępuje tak 28% badanych. Za rzadko stosujemy również narzędzia online wspomagające ochronę, na przykład niespełna co trzeci respondent (36%) używa zakładek w przeglądarkach internetowych, dzięki którym od razu zostałby przekierowany na właściwą (tj. prawdziwą), wybraną stronę, np. swojego banku.

Zaznacz, do których zasad w zakresie cyberbezpieczeństwa się stosujesz:



ZASADY DOTYCZĄCE SPRZĘTU: BLOKADY, AKTUALIZACJE I HASŁA

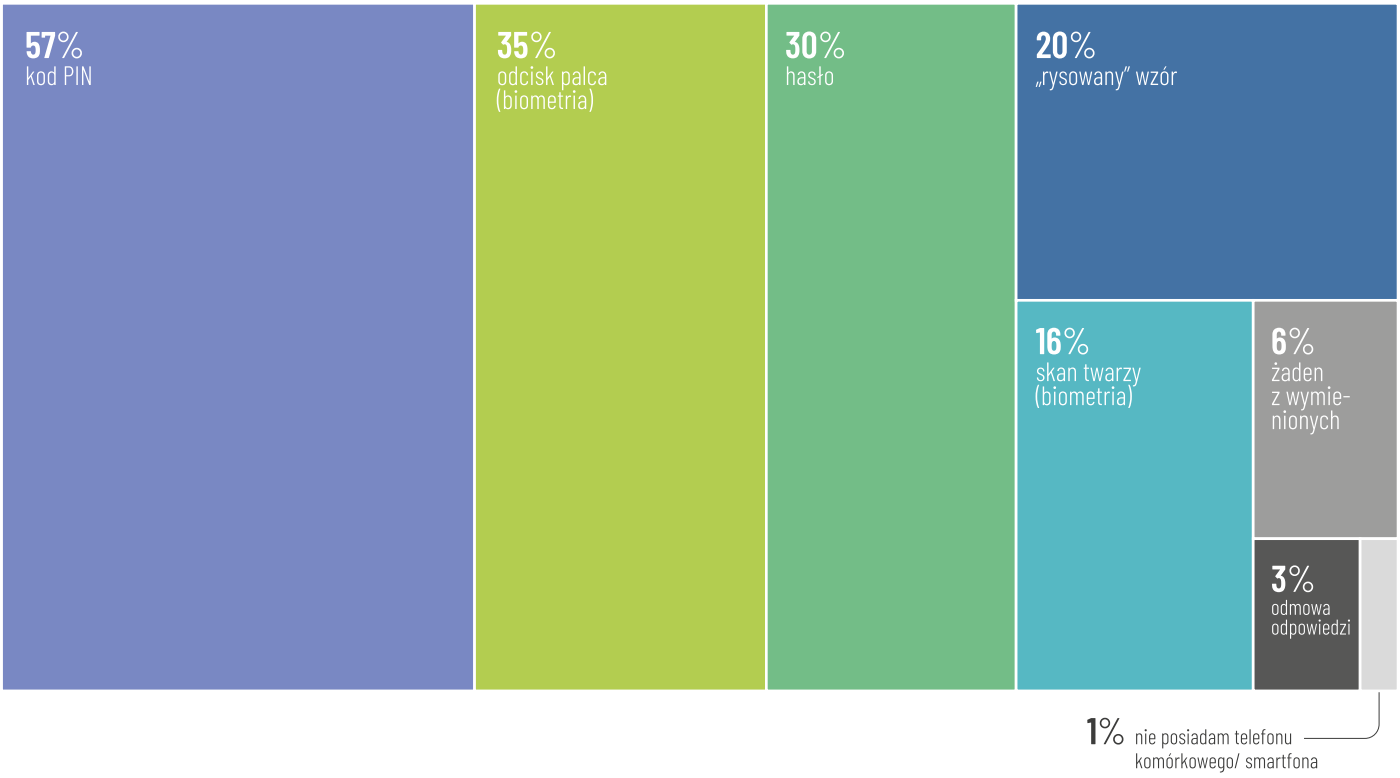
Oprócz znajomości metod na temat bezpiecznego poruszania się w cyfrowym świecie, Polacy dbają o bezpieczeństwo swoich urządzeń, choć bardziej chronią swój telefon niż komputer.

Dostęp do telefonu komórkowego zabezpieczamy w większości kodem PIN (57%), ale chętnie sięgamy również po szybsze sposoby, oparte na technologii biometrycznej - prawie co trzeci respondent (35%) odblokowuje swój smartfon odciskiem palca (taką metodę wolą panowie w wieku 18-39 lat). Natomiast zabezpieczenie łączące pokolenie młodych dorosłych w wieku 18-29 lat i osób 50+ to hasło. Dodatkowo ponad połowa badanych (56%) aktualizuje oprogramowanie i aplikacje na swoim telefonie za każdym razem, kiedy otrzymuje powiadomienie o takiej potrzebie. Co ciekawe niewielka grupa osób (8%), w większości kobiet, dokona update'u oprogramowania, ale nie pobierze aktualizacji aplikacji.

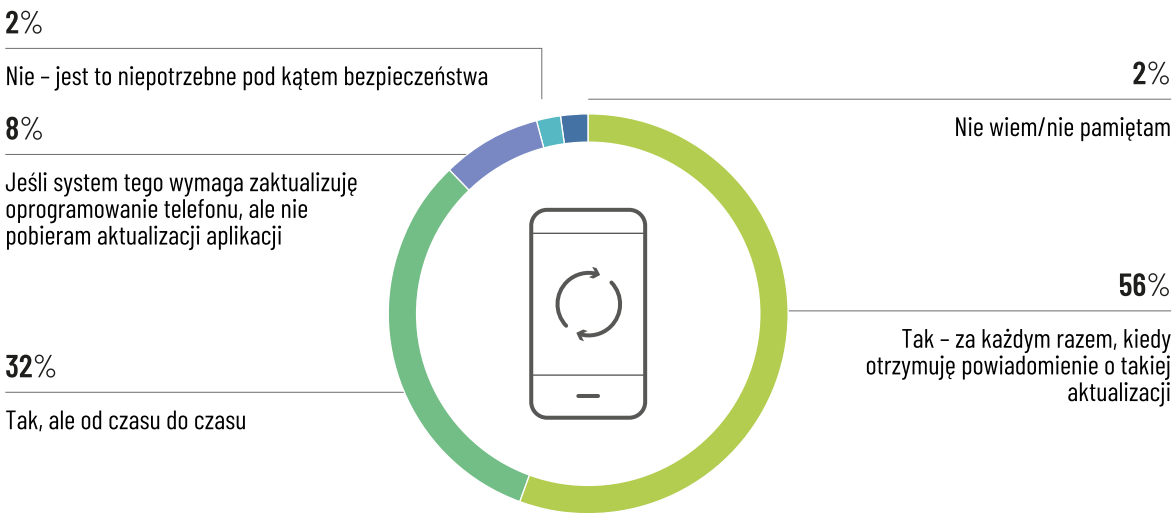
Natomiast zdecydowanie za mało Polaków chroni swój laptop lub komputer stacjonarny - połowa badanych zaktualizuje urządzenie wtedy, kiedy system tego wymaga, ale 36% pomimo wyskakujących powiadomień, sporadycznie zrealizuje update - narażamy się w ten sposób na ataki typu malware.

Warto zwrócić uwagę, że największą dysproporcję pomiędzy ochroną telefonu a komputera można zaobserwować wśród młodych dorosłych w wieku 18-29 lat - połowa z nich dokona aktualizacji na smartfonie za każdym razem, kiedy pojawi się systemowa informacja o tej potrzebie, ale tylko 37% zrobi tak w przypadku laptopa.

Jaki typ zabezpieczenia blokady/dostępu do ekranu telefonu komórkowego/smartfona stosujesz?



Czy aktualizujesz oprogramowanie i aplikacje na swoim osobistym telefonie komórkowym/ smartfonie?



W tworzeniu i zabezpieczaniu haseł Polacy preferują własną kreatywność niż wspomaganie się technologią. Zaledwie 10% badanych korzysta ze specjalnych programów (tzw. generatorów), które w kilka sekund stworzą losowe i trudne do złamania hasła. Niewiele lepiej jest w przypadku ochrony za pośrednictwem menadżera haseł, np. Googla – tylko co piąty badany stosuje takie e-narzędzia (19%, częściej panowie niż panie).

Wolimy postawić na pomysłowość i samodzielnie układamy długie kilkunastoznakowe kombinacje, ale uwzględniające zalecane standardy bezpieczeństwa (tj. z wykorzystaniem wielkich i małych liter, liczb oraz znaków specjalnych, a także oparte na skojarzeniach słownych) – co trzeci badany stosuje taką metodę (32%).

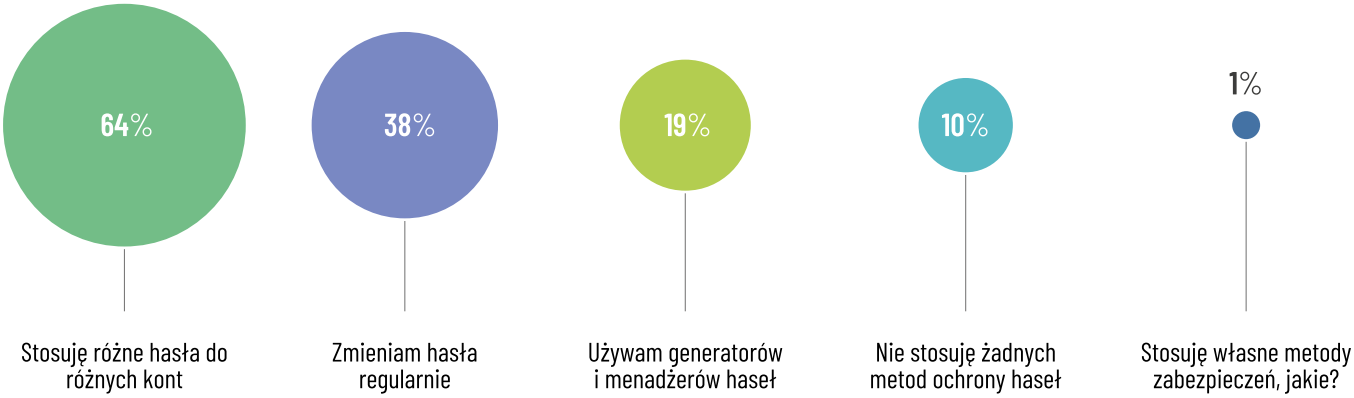
Pozytywnym aspektem w kontekście bezpiecznego korzystania z przestrzeni cyfrowej jest przestrzeganie „złotej" zasady nieużywania tego samego hasła do różnych kont (np. do poczty e-mail, banku czy mediów społecznościowych), którą praktykuje większość respondentów (64%).



Jakiego typu hasła najczęściej tworzysz?

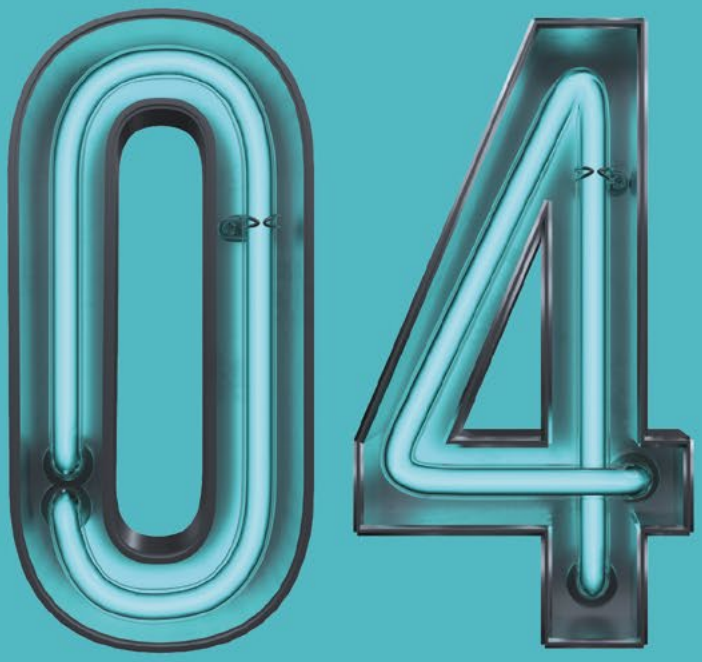


Co robisz, żeby zabezpieczać swoje hasła (np. do poczty e-mail, banku, mediów społecznościowych)?





ROZDZIAŁ



Cyberbezpieczny portfel – bezpieczeństwo finansowe Polaków

CYBERBEZPIECZNY PORTFEL – BEZPIECZEŃSTWO FINANSOWE POLAKÓW

ZASADY BEZPIECZEŃSTWA W BANKOWOŚCI ELEKTRONICZNEJ

Polacy w większości znają i stosują ogólne wytyczne cyberbezpieczeństwa, ale w świecie cyfrowych finansów nie czują się już tak pewnie. Jak wynika z danych WIB, tylko prawie połowa badanych prawidłowo chroni dostęp do swojej bankowości elektronicznej, nie przechowując danych do logowania w portfelu lub w notatniku na smartfonie. Natomiast mniej niż połowa (46%) zwraca uwagę na autentyczność strony internetowej banku podczas logowania, pilnując czy adres strony jest taki sam jak zwykle, czy nie ma literówek lub innych dodatkowych znaków i końcówek. Sami stwarzamy też ryzyko narażenia się na takie oszustwa jak vishing i spoofing, których celem jest wyłudzenie danych umożliwiających zhakowanie elektronicznego konta bankowego. Przykładowo dzieje się tak podczas rozmowy telefonicznej, kiedy zbyt mało z nas samodzielnie weryfikuje osobę dzwoniącą, która podaje się za pracownika banku. Zaledwie 29% badanych potwierdza tożsamość rozmówcy, wykonując samodzielnie połączenie telefoniczne do placówki bankowej.[5]

„Vishing to cyberoszustwo, w którym przestępcy wykorzystują rozmowę telefoniczną, by wyłudzić pieniądze lub poufne dane. Podszywają się np. pod pracownika banku czy policjanta i stosując techniki manipulacji, skłaniają ofiarę do określonych działań: instalacji oprogramowania, wykonania przelewu na „bezpieczne konto" czy przekazania gotówki. Budują zaufanie, a jednocześnie wywierają presję, by utrudnić spokojną ocenę sytuacji. Z raportu „Cyberbezpieczny Portfel" wynika, że tylko 29% badanych samodzielnie kontaktuje się z placówką bankową, by potwierdzić tożsamość rozmówcy. To pokazuje, jak ważne jest budowanie nawyków bezpiecznego korzystania z usług finansowych. Dlatego w Fundacji Erste i banku zachęcamy klientów do weryfikowania pracowników za pomocą aplikacji mobilnej. To proste i wygodne rozwiązanie. Warto pamiętać o podstawowej zasadzie: jeśli rozmowa budzi wątpliwości, rozłącz się i samodzielnie zadzwoń na oficjalny numer banku, np. z jego strony internetowej lub karty. Nie oddzwaniaj na numer z historii połączeń ani nie podawaj haseł czy kodów autoryzacyjnych."

MARZENA ATKIELSKA
prezes zarządu, Fundacja ERSTE Bank Polska im. Ignacego Jana Paderewskiego

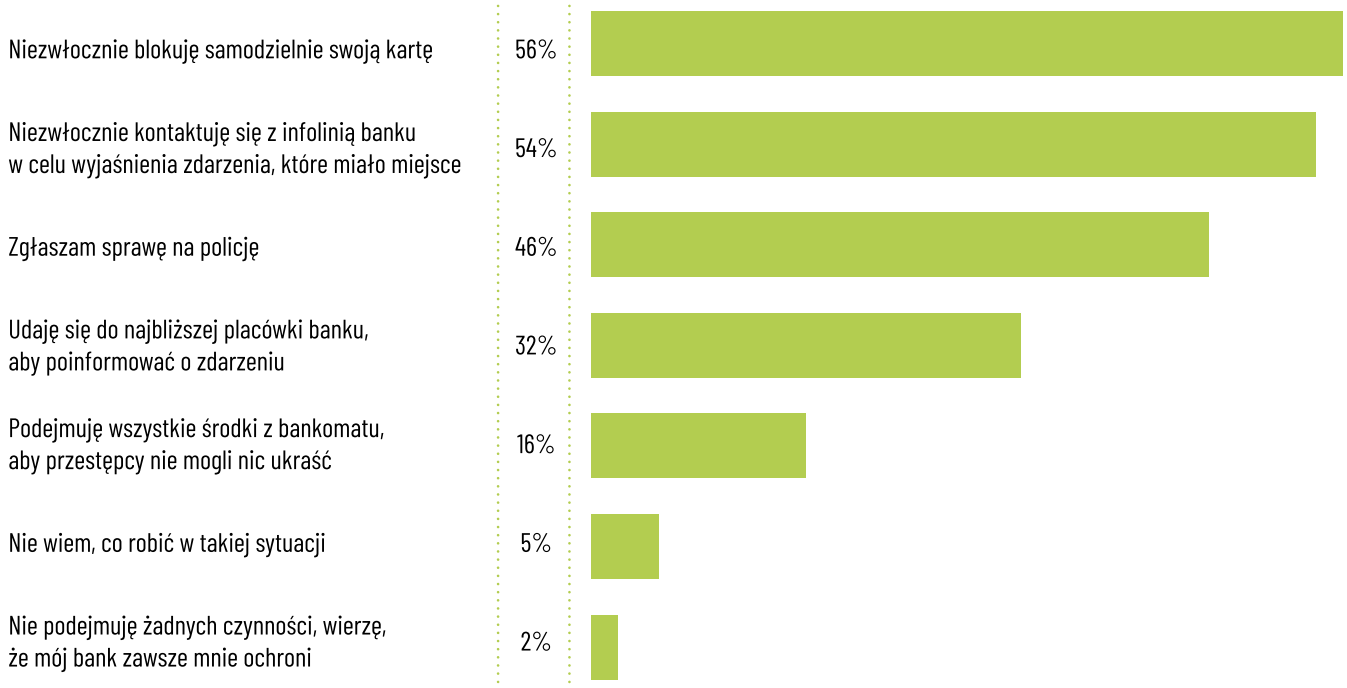
[5] Dane z wykresu ze str. 18, badanie „Postawy Polaków wobec cyberbezpieczeństwa"

POSTĘPOWANIE W PRZYPADKU OSZUSTWA FINANSOWEGO

Potrafimy jednak właściwie zachować się w sytuacji, kiedy nasze konto bankowe jest zagrożone i wiemy, gdzie zgłosić cyberoszustwo dotyczące wyłudzenia pieniędzy i/lub naszych danych, tj. na przykład za pośrednictwem fałszywej strony www, wiadomości email, SMS lub połączenia telefonicznego.

Kiedy zostajemy oszukani i nasze środki finansowe zostały wyłudzone, to większość Polaków podejmuje natychmiastowe i konkretne działania w celu ochrony swoich środków. Ponad połowa respondentów postępuje zgodnie z zalecaną wytyczną, którą jest niezwłoczne zablokowanie karty płatniczej (56%) oraz szybki kontakt z infolinią banku w celu wyjaśnienia zdarzenia (54%), zaś co trzecia osoba (częściej panie) udałaby się również do najbliższej placówki banku. Warta uwagi jest także szybsza reakcja kobiet w takich sytuacjach - 60% pań niezwłocznie zablokowałby kartę i 56% z nich skontaktowałoby się z infolinią banku (na 52% panów). Niewiele mniej badanych (46%) zgłosiłoby sytuację na policję.

Co robisz, jeśli podejrzewasz, że padłeś/aś ofiarą oszustwa i Twoje konto bankowe jest zagrożone?

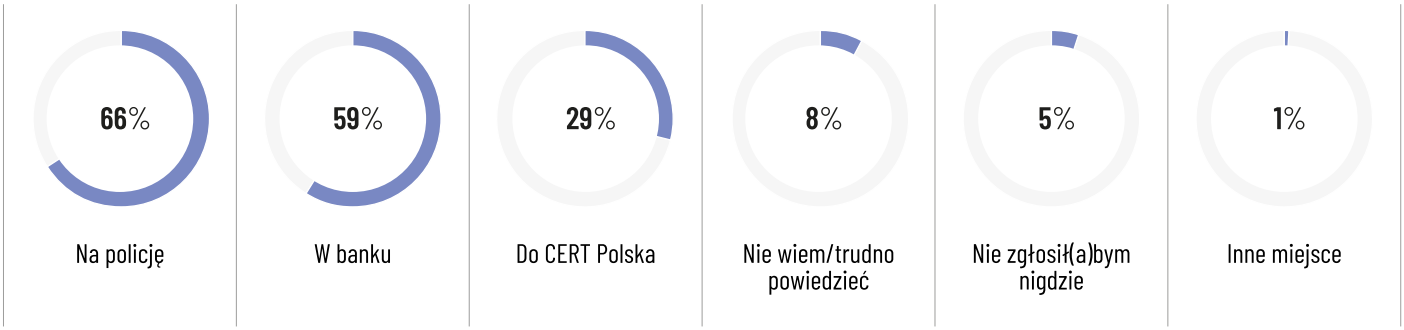


W kontekście zagrożenia wyłudzenia pieniędzy lub danych bankowych i osobowych ważna jest również wiedza o tym, gdzie i w jaki sposób należy je zgłosić. Wyniki badania pokazują, że badani najczęściej wskazywali instytucje, które na co dzień kojarzą się z ochroną obywateli i bezpieczeństwem finansowym. Około dwóch na trzech respondentów (66%) zawiadomiłoby o próbie ataku phishing-owego najpierw policję. Niewiele mniej badanych (59%) - swój bank, natomiast w dalszej kolejności -CERT Polska (29%).

Ciekawą zależność widać także w odpowiedziach kobiet i mężczyzn. Kobiety wskazywały częściej policję (71%) oraz bank (61%), natomiast mężczyźni częściej wybierali CERT Polska (34%).



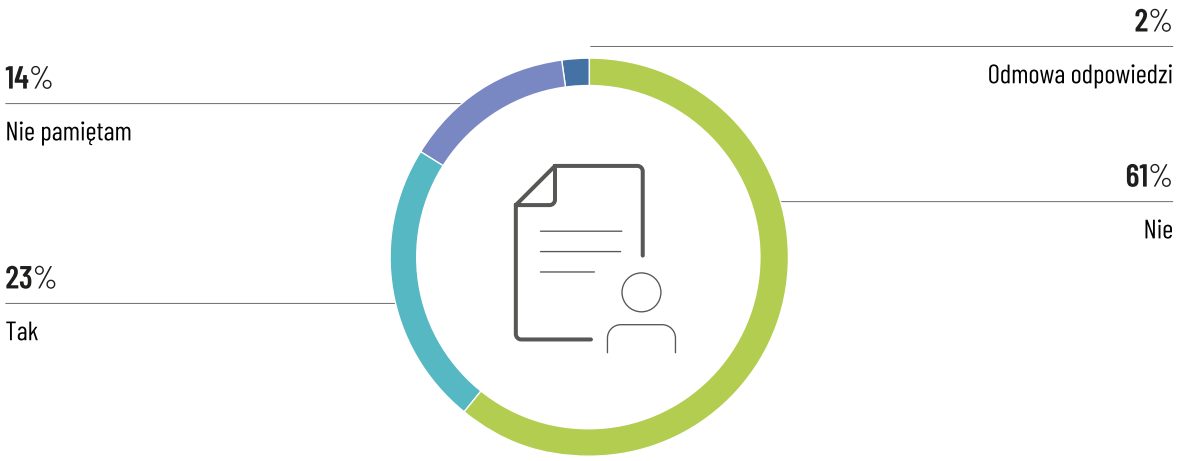
Gdzie zgłosiłbyś/zgłosiłabyś próbę oszustwa wyłudzenia pieniędzy i/lub Twoich danych?



Świadomość Polaków na temat postępowania w przypadku zagrożenia finansowego (utraty pieniędzy) jest względnie na wysokim poziomie. Stąd dziwi deklaracja respondentów, że sami nie powiadamiają organów ścigania o oszustwie dokonanym za pośrednictwem fałszywej strony www, wiadomości czy połączenia telefonicznego - aż 61% przyznało, że nigdy nie zgłosiło takiej sytuacji. Tylko 23% badanych przyznało się do złożenia zawiadomienia o próbie wyłudzenia pieniędzy i/lub danych osobowych. Różnica między tymi odpowiedziami wynosi aż 38 punktów procentowych.

Warto również zwrócić uwagę na zależność między wiekiem a skłonnością do zgłaszania ww. cyberoszustwa. Z przedstawionych danych wynika, że im starsze są poszkodowane osoby, tym mniej skore do informowania o takich incydentach. W najmłodszej grupie badanych, obejmującej osoby w wieku 18–29 lat, taką postawę zadeklarowało 50% respondentów, a wśród osób powyżej 60. roku życia - 66%.

Czy kiedykolwiek zgłosiłaś/eś próbę wyłudzenia pieniędzy i/lub Twoich danych, które zostało dokonane za pośrednictwem fałszywej strony www, wiadomości email/SMS i/lub połączenia telefonicznego?



ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO CYFROWYCH USŁUG FINANSOWYCH

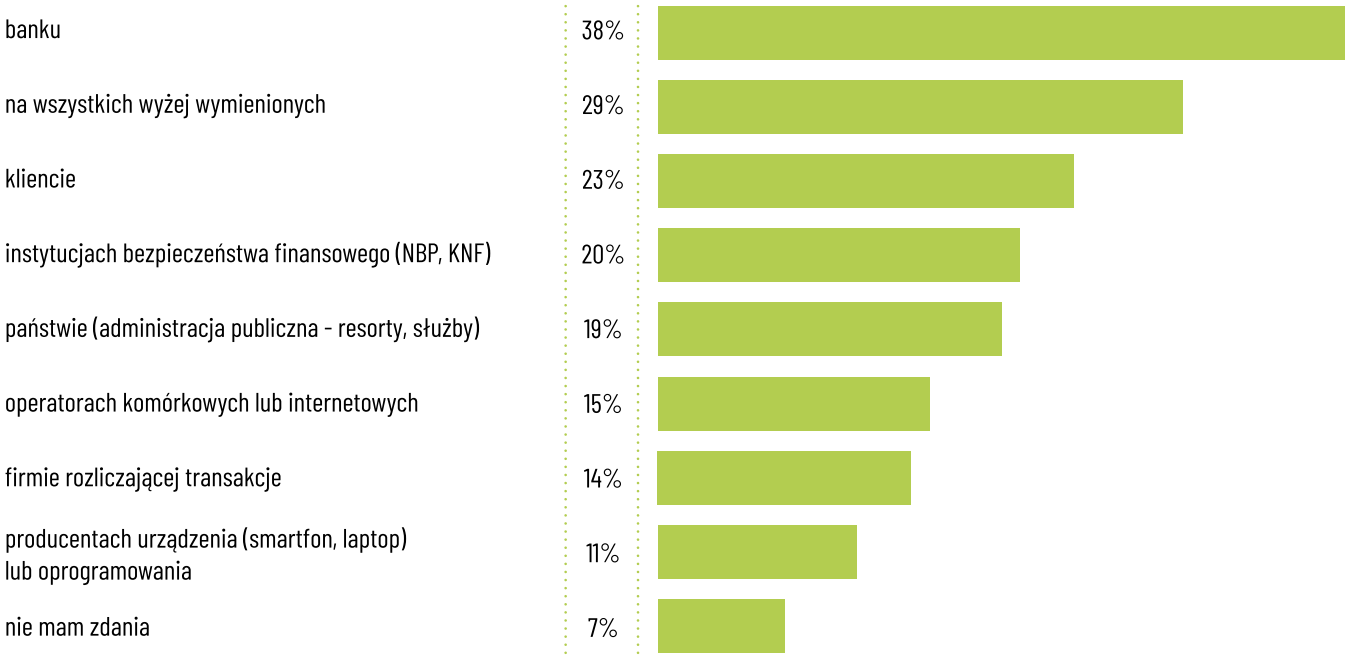
W tym zakresie kształtuje się ciekawy trend, który wskazuje, że klienci zaczynają dostrzegać swoją rolę w zapewnianiu bezpieczeństwa cyfrowych usług finansowych. Już co czwarty respondent (23%) wskazuje samego siebie jako trzecią w kolejności tarczę ochronną dla elektronicznych finansów. Niemniej, według Polaków główną osią bezpieczeństwa są nadal banki - blisko czterech na dziesięciu respondentów (38%) uważa, że w głównej mierze to instytucje bankowe są odpowiedzialne za ochronę naszych pieniędzy w cyberprzestrzeni.

Coraz częściej dostrzegamy również, że ochrona przed finansowymi cyberzagrożeniami wymaga zaangażowania wielu podmiotów jednocześnie. Zdaniem co trzeciego badanego odpowiedzialność w tym zakresie powinna być dzielona pomiędzy: instytucje bezpieczeństwa finansowego, takie jak NBP czy KNF - wskazało tak 20% badanych, 19% na państwo (w szczególności w odniesieniu do administracji publicznej), 15% na operatorów telekomunikacyjnych i internetowych, 14% na podmioty obsługujące płatności, a 11% na producentów urządzeń i oprogramowania.

„W Visa łączymy sztuczną inteligencję, analizę danych i odporną infrastrukturę, aby możliwie wcześnie wychwytywać nietypowe zachowania i reagować, zanim zagrożenie przerodzi się w stratę. Przykładem jest Visa A2A Protect, które wykorzystuje AI, by w czasie rzeczywistym oceniać ryzyko przelewów i wykrywać odstępstwa od typowych zachowań klienta. Równie ważna jak technologia jest współpraca całego ekosystemu płatniczego. Banki, firmy technologiczne, sprzedawcy i instytucje publiczne widzą różne fragmenty tej samej sytuacji, dlatego wymiana wiedzy i sygnałów pomaga budować pełniejszy obraz ryzyka. Globalne doświadczenie Visa łączymy z lokalnymi kompetencjami i inwestycjami w Europie, opracowując rozwiązania, które działają w tle i wspierają bezpieczne, szybkie oraz wygodne płatności. Konsument nie musi znać wszystkich mechanizmów ochrony – najważniejsze, by działały one stale, na wielu poziomach i we współpracy z partnerami."

MATEUSZ OLEKSY
dyrektor generalny Visa w Polsce

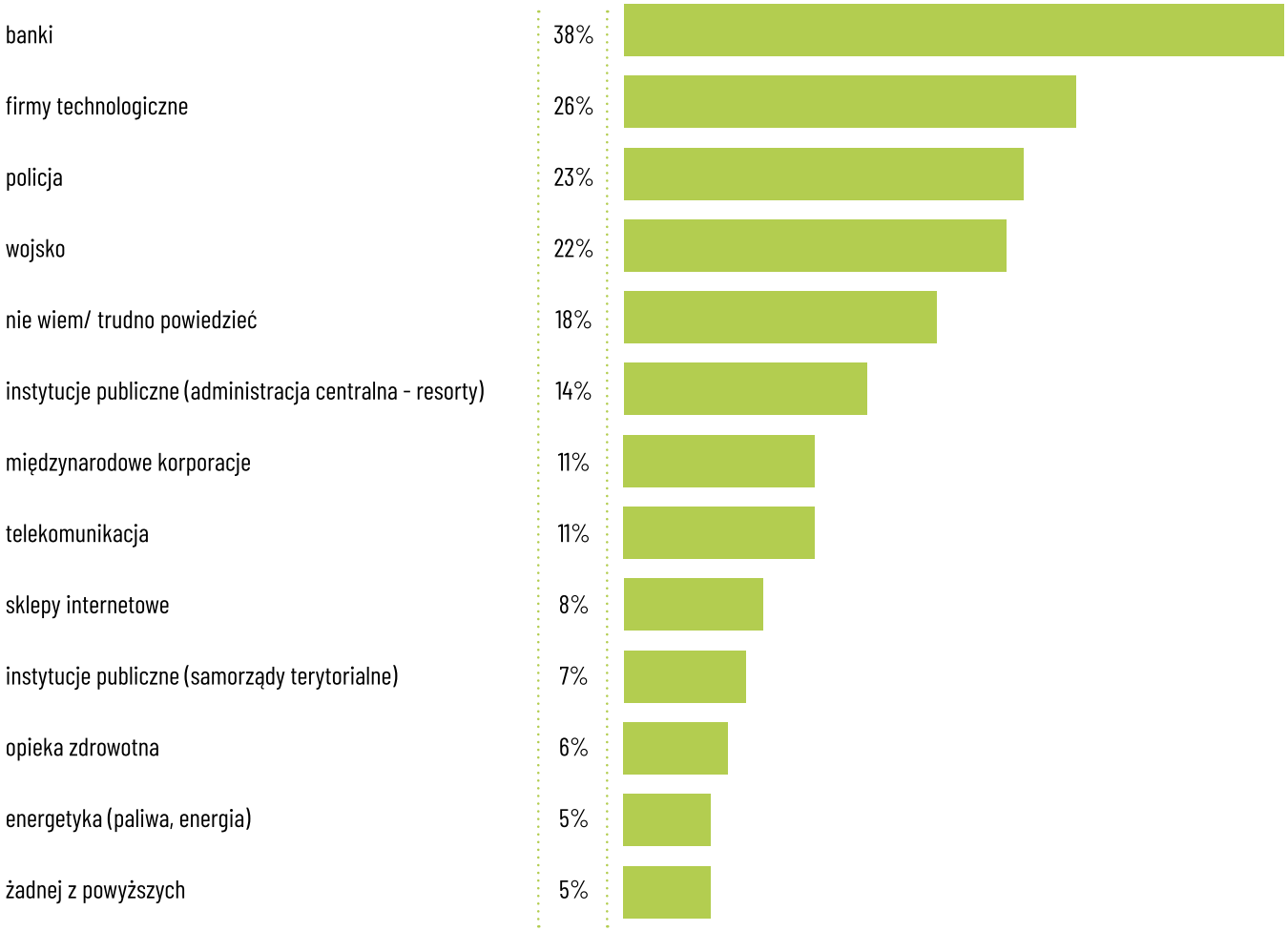
Odpowiedzialność za bezpieczeństwo usług finansowych dokonywanych w formie elektronicznej Twoim zdaniem spoczywa na:



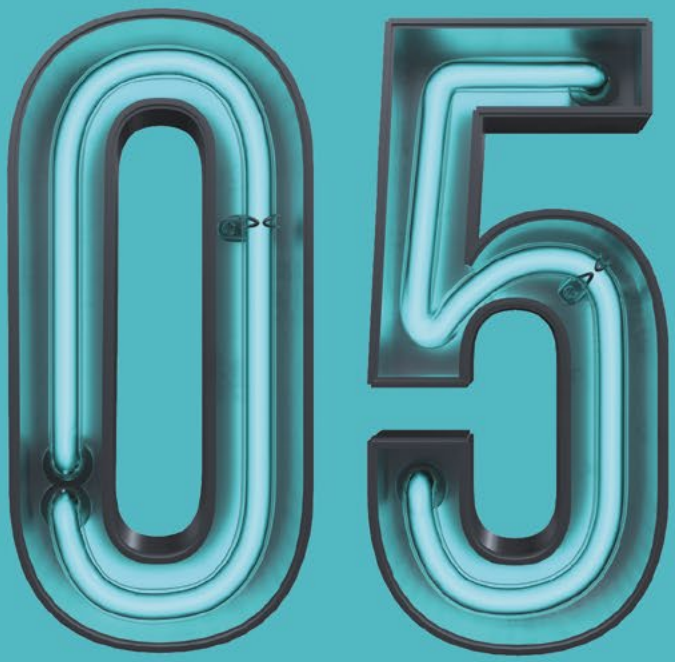
Jednak najwięcej badanych (38%) uważa, że to banki najbardziej dbają o rozwój narzędzi i systemów stanowiących cybertarczę, tym samym zachowując nadal pozycję lidera w tym zakresie. Jednocześnie, w obliczu postępującej cyfryzacji, prawie co czwarty respondent (26%) dostrzegł coraz większą rolę firm technologicznych w wyścigu o cyfrowe bezpieczeństwo Polaków. Badani doceniają również zabezpieczenia służb mundurowych: policji – 23%, wojska – 22%.

Najmniejsze zaufanie do podmiotów, które są ważne dla społeczeństwa w kontekście zapewnienia cyberbezpieczeństwa, mamy w stosunku do sektora energetycznego (5%), ale także do ochrony zdrowia (6%), samorządów terytorialnych (7%) i niestety również do sklepów internetowych (8%).

Którą z poniższych branż lub instytucji postrzegasz jako liderów w zakresie cyberbezpieczeństwa?



ROZDZIAŁ



Edukacja – wiedza to potęgi klucz

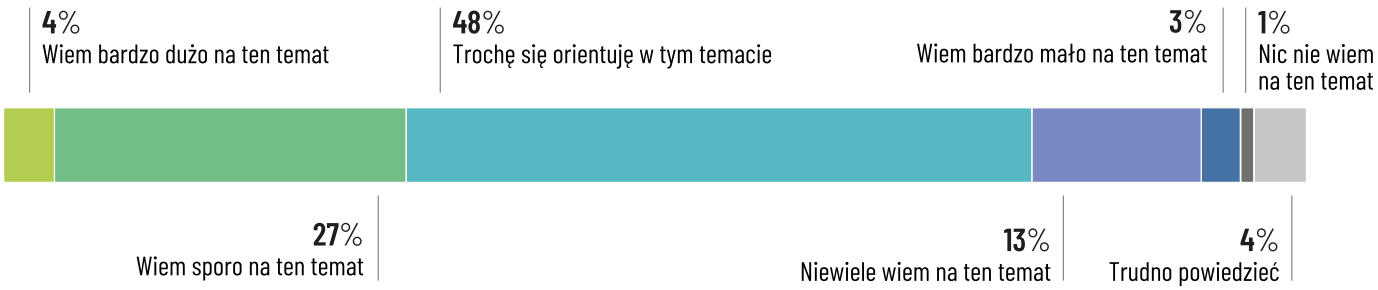
EDUKACJA - WIEDZA TO POTĘGI KLUCZ

Wiedza Polaków o cyberbezpieczeństwie rośnie, choć powoli - stąd nadal potrzebne są systemowe działania edukacyjne podnoszące kompetencje społeczeństwa w tym zakresie, a szczególnie wśród dzieci i młodzieży.

Obecnie możemy znaleźć wiele informacji o bezpiecznym korzystaniu z przestrzeni cyfrowej. Coraz częściej poruszane są tematy związane z cyberbezpieczeństwem, dezinformacją czy ochroną danych osobowych. Mimo rosnącej dostępności takich treści, poziom erudycji społeczeństwa w zakresie cyberbezpieczeństwa, pozostaje ciągle na niewystarczającym poziomie.

Z tegorocznego badania WIB wynika, że prawie połowa badanych (48%) nadal posiada tylko orientację w tym temacie. Natomiast już co trzeci z nas (31%) uważa, że jego wiedza jest na dość wysokim poziomie - porównując z zeszłym rokiem to raptem tylko 1 punkt procentowy wzwyż. Aczkolwiek warto zauważyć, że wśród osób, które wiedzą sporo w zakresie bezpieczeństwa w cyberprzestrzeni (najczęściej to panowie w wieku 18-29 lat z wykształceniem wyższym), nastąpił wzrost o 4 punkty procentowe. Z drugiej strony niewielu respondentów (13%) odpowiedziało, że niewiele wiedzą o cyberbezpieczeństwie - najczęściej wskazywały tak kobiety po 60-tce z wykształceniem średnim.

Jak ogólnie oceniasz swoją wiedzę w zakresie cyberbezpieczeństwa?



Mimo zróżnicowania, wyniki badania potwierdzają, że edukacja dotycząca cyberbezpieczeństwa wciąż powinna być ważnym elementem rozwoju użytkowników internetu, zwłaszcza wśród tych najmłodszych, którzy dopiero kształtują swoją cyfrową świadomość. Bezpieczne korzystanie z cyberprzestrzeni, jest szczególnie istotne w kontekście dzieci i młodzieży. W związku z ich coraz większą obecnością w cyfrowym świecie, ważnym staje się kształtowanie właściwych nawyków online, w tym wpływ rodziców na ich cyfrowy dobrostan oraz podnoszenie edukacji w szkołach na temat zagrożeń, z jakimi mogą spotkać się w sieci.

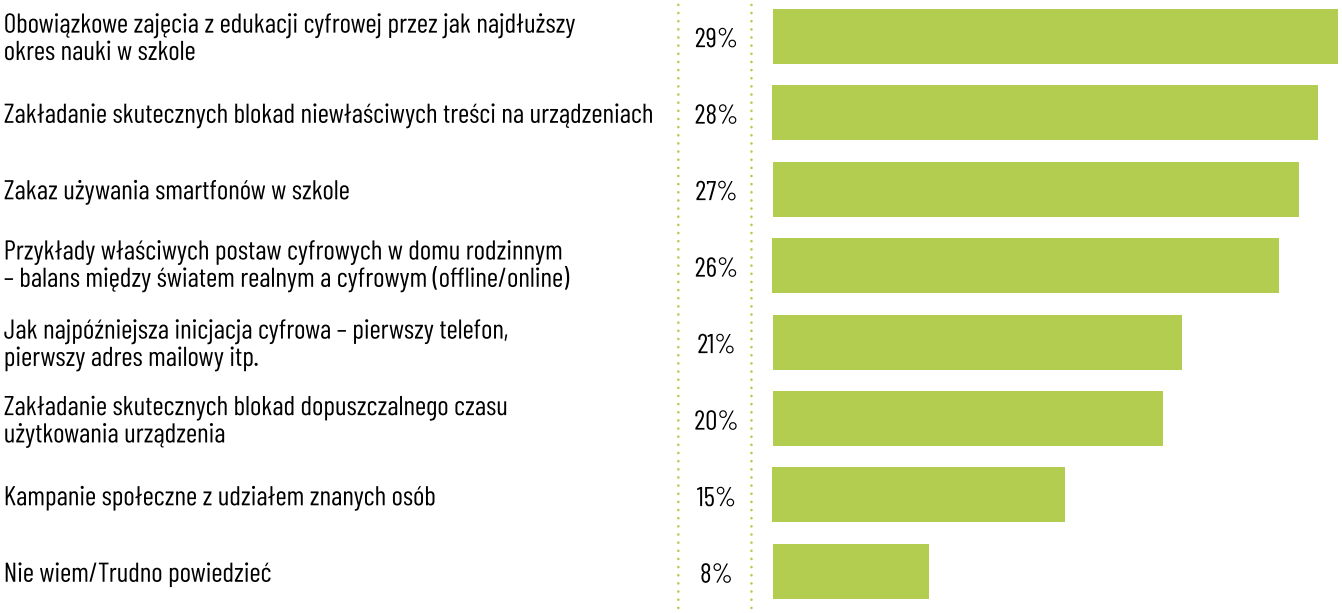
Wśród najważniejszych działań systemowych, które mają wspierać ochronę uczniów, najwięcej respondentów wskazało przede wszystkim wprowadzenie w szkole obowiązkowych zajęć z edukacji cyfrowej – najlepiej przez cały okres nauki (29%) oraz zakaz używania telefonów w placówkach szkolnych (27%). Dla Polaków istotnym środowiskiem, który powinien wpływać na właściwe postawy cyfrowe najmłodszych, jest dom rodzinny – 26% badanych jest zdania, że to rodzice powinni dbać o cyfrowy dobrostan dzieci i młodzieży. Z pozostałych aktywności wspierających ochronę, prawie co czwarty respondent (28%) wskazał blokowanie niewłaściwych treści na urządzeniach, które użytkują najmłodsi, a także 21% badanych było za nakładaniem blokad dopuszczalnego czasu użytkowania smartfonu lub komputera. Dla respondentów istotnym wydaje się również jak najpóźniejsza inicjacja cyfrowa – prawie co piąty badany (21%) uważa, że dzieciom powinno się opóźniać wejście do cyfrowego świata. Najmniej Polaków (15%) widzi potencjał w edukacji cyfrowej poprzez kampanie społeczne, w których biorą udział znane osoby. Poparcie dla tego rozwiązania wyraźnie maleje wraz wiekiem - wśród młodych dorosłych (18-29-latkowie) wskazało je 20% badanych, natomiast w grupie 60+ lat już tylko 12%.

DEPARTAMENT BEZPIECZEŃSTWA BLIK

„Szczególną rolę w procesie budowania wiedzy o bezpieczeństwie odgrywa świadomość, że najmłodsze pokolenia wychowują się w świecie opartym o technologię. Świat cyfrowy jest naturalnym przedłużeniem ich rzeczywistości. Młodzi ludzie sprawnie korzystają z technologii, ale brak doświadczenia i dopiero kształtująca się umiejętność krytycznej oceny sytuacji sprawiają, że są bardziej narażeni na manipulację i dezinformację. Jako dorośli musimy zdać sobie sprawę, że w bardzo wczesnym wieku są oni już zagłębieni w meandrach cyfrowego świata. Zablokowanie dostępu do strony czy aplikacji nie sprawi, że młodzi ludzie nigdy się z nimi nie zetkną. Kluczowa więc pozostaje edukacja samodzielnego rozpoznawania zagrożeń i właściwego reagowania. Skuteczność edukacji, istotnej też dla zawierania znajomości oraz zachowania higieny cyfrowej rosną wraz z procesem kształcenia. Jeżeli młody człowiek będzie potrafił rozróżnić treści wartościowe od szkodliwych, w odpowiednim momencie powie „STOP"

#StopPodszywaczom to hasło kampanii edukacyjnej „Metoda na Podszywacza", realizowanej przez BLIKw celu zwiększania bezpieczeństwa w internecie. Celem inicjatywy jest podnoszenie świadomości użytkowników przestrzeni cyfrowej na temat mechanizmów oszustw, polegających na podszywaniu się przestępców pod znajomych, członków rodziny lub inne zaufane osoby. Oszuści wykorzystują przejęte konta w serwisach społecznościowych i kontaktują się z bliskimi ofiary za pośrednictwem komunikatorów internetowych. Wywierają presję czasu i manipulują odbiorcami aby skłonić ich do przekazania pieniędzy. W ramach inicjatywy odbiorcy uczą się, jak rozpoznawać próby oszustwa, chronić się przed nimi oraz właściwie reagować w sytuacji, gdy padną ich ofiarą. Wykorzystywane są w tym celu materiały edukacyjne, filmy oraz praktyczne wskazówki.

Które z działań wspierających ochronę dzieci i młodzieży oraz poprawę ich świadomości na temat bezpiecznego i zdrowego korzystania z sieci uważasz za kluczowe?



O PROJEKCIE EDUKACYJNYM „BEZPIECZEŃSTWO W CYBERPRZESTRZENI"

Projekt "Bezpieczeństwo w Cyberprzestrzeni" realizowany jest od 2017 roku przez Fundację Warszawski Instytut Bankowości w ramach sektorowego Programu „Bankowcy dla Edukacji" – największego programu edukacji finansowej w Europie. Celem projektu jest edukowanie społeczeństwa poprzez różne aktywności szkoleniowo-edukacyjne dopasowane do potrzeb różnych grup odbiorców oraz przekazywanie wiedzy i kształtowanie kompetencji na temat:

- Rozpoznawania i unikania cyberzagrożeń
- Aktywnego i bezpiecznego korzystania z nowoczesnych technologii, w tym narzędzi gospodarki elektronicznej
- Kształtowania właściwych postaw w obszarze ochrony tożsamości i wizerunku
- Przeciwdziałania dezinformacji i cyberprzemocy

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

BEZPIECZEŃSTWO W CYBERPRZESTRZENI



>600 tys. UCZNIÓW

>200 tys. STUDENTÓW

>200 tys. SENIORÓW

Patron honorowy: Ministerstwo Cyfryzacji

Partner merytoryczny: NASK

Partnerzy wspierający: allegro, blik, ING, ERSTE Fundacja, VISA

Partner edukacyjny: Fundacja Digital University

Zespół redakcyjny raportu
*„**Cyberbezpieczny Portfel**”*

Aleksandra Czyrkowska
autorka i redaktor naczelna

Helena Florczak
współautorka

Patryk Gąsior
nadzór merytoryczny

Polska Grupa Infograficzna – **Karolina Wojciechowska**
opracowanie graficzne

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

Zapraszamy również na strony:
Warszawskiego Instytutu Bankowości: **www.wib.org.pl**
Programu „Bankowcy dla Edukacji”: **www.bankowcydlaedukacji.pl**


WARSZAWSKI
INSTYTUT
BANKOWOŚCI