Santander Consumer Bank

Polaków Portfel Własny

Test z cyberbezpieczeństwa

Spis treści

Wstęp

Życie w cyfrowym świecie przynosi liczne korzyści, ale stawia również przed nami wyzwania, które wymagają większej ostrożności. W czasach, gdy dostęp do internetu i nowoczesnych technologii jest powszechny, dysponujemy niemal nieograniczonymi możliwościami zdobywania wiedzy, komunikacji oraz korzystania z rozrywki. Jednak rośnie również zagrożenie ze strony cyberprzestępców, którzy wykorzystują zaawansowane techniki, aby uzyskać dostęp do danych osobowych, finansowych i poufnych informacji. Według raportu Force Threat Intelligence Index firmy IBM Europa była najczęściej atakowanym regionem na świecie w 2023 roku i odpowiadała za niemal jedną trzecią wszystkich globalnych cyberataków. Trzy główne cele ataków na europejskie organizacje to pozyskiwanie danych uwierzytelniających, które stanowiło 28 proc., wymuszenia obejmujące 24 proc. oraz wycieki danych, stanowiące 16 proc. wszystkich incydentów. Najczęściej atakowanym sektorem w Europie okazała się produkcja, która przesunęła się z drugiego miejsca zajmowanego w 2022 roku i odnotowała 28 procent wszystkich incydentów. Kolejną najbardziej narażoną branżą były usługi profesjonalne, biznesowe i konsumenckie, z udziałem 25 procent, a następnie sektory finansów i ubezpieczeń, stanowiące 16 procent oraz sektor energetyczny, obejmujący 14 procent cyberataków.

Podobne zjawisko można zaobserwować również w Polsce. Liczba cyberataków wzrosła gwałtownie z 50 incydentów w 1996 roku do ponad 80,2 tysiąca w 2023 roku. Według danych CERT Polska, liczba zgłoszeń i incydentów związanych z cyberbezpieczeństwem rośnie systematycznie, co świadczy o coraz większej świadomości zagrożeń w społeczeństwie. W ubiegłym roku CERT Polska zarejestrowało ponad 210 tys. zgłoszeń dotyczących naruszeń bezpieczeństwa, co stanowi ponad dwukrotny wzrost w porównaniu do roku 2022.

W raporcie „Test z cyberbezpieczeństwa" postanowiliśmy przyjrzeć się podejściu Polaków do kwestii cyberbezpieczeństwa – ich obawom oraz poczuciu pewności, że ich dane są odpowiednio zabezpieczone. Z pierwszego rozdziału dowiecie się, czego Polacy najbardziej obawiają się w sieci, jakie mają zdanie na temat zabezpieczeń stosowanych przez banki oraz jakie zaufanie pokładają w nowoczesnych rozwiązaniach chroniących ich dane.

Druga część raportu skupia się na stosowaniu oprogramowania antywirusowego przez Polaków. Analizujemy, w jakim stopniu są świadomi zagrożeń związanych z różnymi formami cyberataków oraz jak często korzystają z dodatkowych zabezpieczeń.

Kolejny rozdział dotyczy prób oszustw internetowych, w tym fałszywych wiadomości od osób podszywających się pod bliskich lub instytucje. W tekście przedstawiono skalę zjawiska oraz najczęstsze sytuacje, w których Polacy padają ofiarą cyberoszustw.

Ostatnia część raportu poświęcona jest weryfikacji informacji, które Polacy pozyskują z mediów społecznościowych i serwisów informacyjnych. Analizujemy, jakie metody najczęściej stosują, aby chronić się przed cyberzagrożeniami, oraz jak oceniają swoją wiedzę na temat cyberbezpieczeństwa.

Zespół Santander Consumer Banku

Kluczowe dane z raportu:

78%	badanych obawia się o bezpieczeństwo swoich danych
70%	Polaków najczęściej wymienia utratę środków finansowych wśród największych zmartwień
76%	uważa, że ich banki zapewniają im wystarczające zabezpieczenia i ochronę
79%	Polaków chroni swoje komputery lub laptopy za pomocą programów antywirusowych
49%	nie stosuje dodatkowego oprogramowania antywirusowego na smartfonach
87%	słyszało o phishingu
55%	otrzymało e-mail, SMS lub wiadomość w mediach społecznościowych od oszusta
18%	padło ofiarą cyberprzestępstw
40%	badanych nie weryfikuje prawdziwość treści
80%	unika otwierania podejrzanych linków i załączników
57%	ocenia swój poziom wiedzy na temat bezpieczeństwa w internecie jako średni

Czego Polacy obawiają się najbardziej w sieci

Internet jest dziś nierozerwalnie związany z naszym codziennym życiem. Badania pokazują, że wielu Polaków spędza w sieci nawet kilka godzin dziennie. Choć korzystanie z internetu przynosi liczne korzyści, wiąże się również z różnorodnymi zagrożeniami. W związku z tym w raporcie postanowiliśmy przyjrzeć się głównym obawom Polaków dotyczącym bezpieczeństwa w sieci.

Wyniki badania pokazują, że niemal 80 proc. respondentów odczuwa niepokój o bezpieczeństwo swoich danych online, podczas gdy jedynie 20 proc. nie wykazuje większych obaw w tej kwestii.

Czy obawia się Pan/i o bezpieczeństwo swoich danych w Internecie?

28%	Zdecydowanie tak
49%	Raczej tak
18%	Raczej nie
2%	Zdecydowanie nie

Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Warto zaznaczyć, że poziom ten jest najniższy wśród najmłodszej grupy, tj. osób w wieku 18-29 lat, z których 66 proc. odczuwa obawy. Może to wynikać z ich wysokiej znajomości technologii, większej biegłości w poruszaniu się po sieci oraz lepszej orientacji w metodach zabezpieczeń, które często towarzyszy ich codziennej aktywności online. Wraz z wiekiem poziom niepokoju wyraźnie rośnie, co sugeruje, że starsi użytkownicy mogą mieć mniejszą pewność w zakresie ochrony swoich danych lub mogą być bardziej świadomi ryzyka związanego z ich naruszeniem. Ten wzrost jest szczególnie widoczny w grupie pięćdziesięciolatków, gdzie blisko 90 proc. wyraża obawy o bezpieczeństwo swoich danych.

Czy obawia się Pan/i o bezpieczeństwo swoich danych w Internecie?

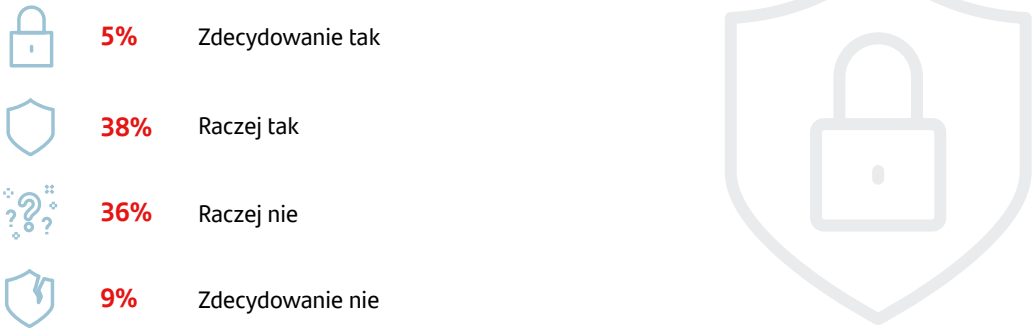
	18-29 lat	30-39 lat	40-49 lat	50-59 lat	60+ lat
Zdecydowanie tak	30%	28%	29%	32%	24%
Raczej tak	36%	52%	55%	54%	49%

Odpowiedzi nie sumują się do 100. Wybrane odpowiedzi przedstawiają stwierdzenia twierdzące „raczej tak" i zdecydowanie tak".

Zaufanie do technologii oraz instytucji bankowych stanowi jeden z kluczowych elementów w dobie cyfryzacji. W miarę jak coraz więcej codziennych czynności przenosi się do internetu, bankowość online staje się standardem dla wielu użytkowników. Zarządzanie finansami online jest wygodne i szybkie, jednak wymaga pełnej ochrony danych osobowych i finansów, co wzbudza potrzebę skutecznych środków ochrony.

Z raportu wynika, że 42 proc. Polaków uważa obecne technologie zabezpieczeń za wystarczające do ochrony swoich danych. Natomiast 45 proc. respondentów wyraża sceptycyzm i nie ma pewności, że same technologie mogą skutecznie chronić ich przed cyberzagrożeniami. Największy brak zaufania wykazują osoby w wieku 50-59 lat, spośród których 55 proc. ma wątpliwości co do bezpieczeństwa systemów. Z kolei najwyższy poziom zaufania odnotowano w grupie wiekowej 40-49 lat, gdzie 46 proc. respondentów uznaje technologie zabezpieczeń za adekwatne.

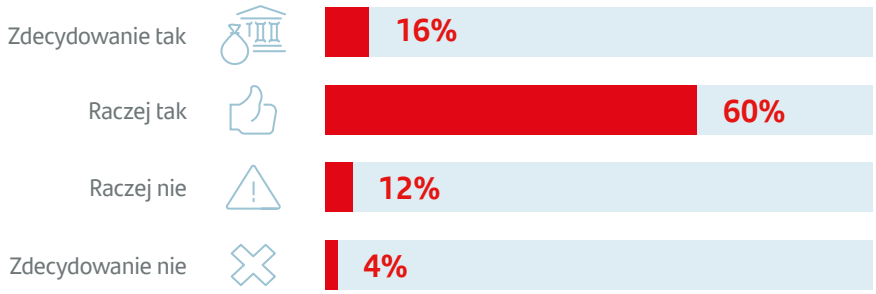
Czy według Pana/i **obecne technologie** zabezpieczeń są wystarczające, aby chronić Pańskie dane?



Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Użytkownicy pragną mieć pewność, że ich dane i pieniądze są zabezpieczone przed nieautoryzowanym dostępem i atakami hakerskimi. Banki wychodzą naprzeciw tym oczekiwaniom i nieustannie modernizują swoje systemy bezpieczeństwa poprzez wprowadzanie rozwiązań takich jak dwuetapowa weryfikacja, tokenizacja oraz zaawansowane szyfrowanie danych. Jak wynika z raportu, 76 proc. Polaków wyraża wysokie zaufanie do zabezpieczeń stosowanych przez banki i oceniają je jako wystarczające.

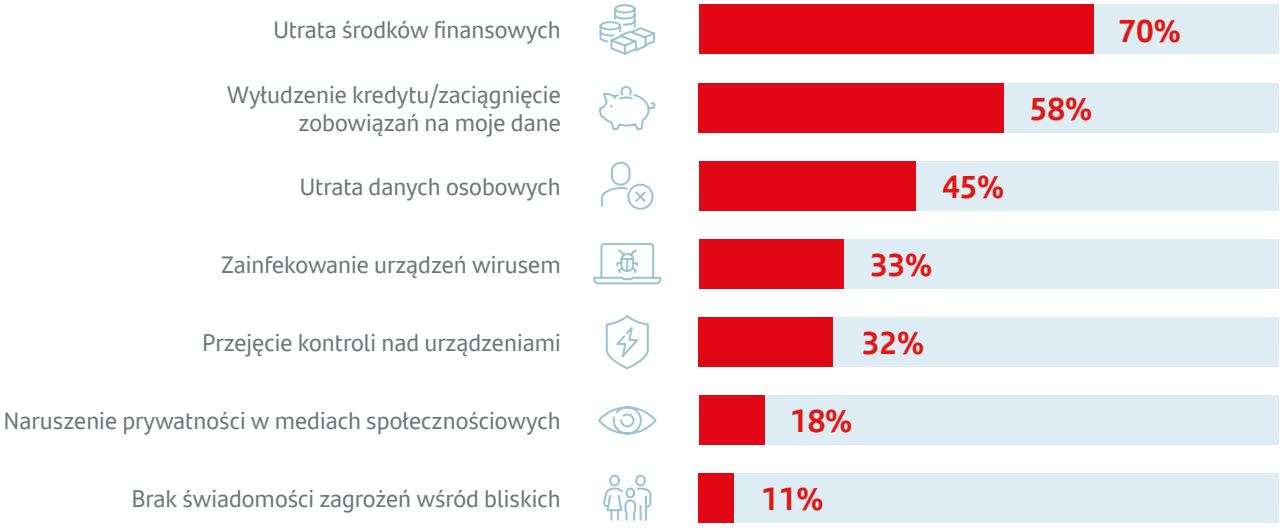
Czy uważa Pan/i, że Pana/i **bank zapewnia** wystarczające zabezpieczenia?



Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Na pytanie o największe obawy związane z cyberbezpieczeństwem Polacy najczęściej wskazują ryzyko utraty środków finansowych – aż 70 proc. badanych wyraża lęk przed możliwością utraty pieniędzy w wyniku cyberataków. Drugą największą obawą jest możliwość wyłudzenia kredytów lub zaciągnięcia zobowiązań na skradzione dane, co niepokoi 58 proc. respondentów. Kolejne zagrożenia to utrata danych osobowych, na którą zwraca uwagę 45 proc. uczestników badania. Infekcji urządzeń wirusami obawia się 33 proc. osób, a przejęcia nad nimi kontroli – 32 proc. badanych.

Jakie są Pana/i **największe obawy** związane z cyberbezpieczeństwem?



Pytanie wielokrotnego wyboru. Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Kiedy przyjrzymy się odpowiedziom w podziale na wiek, to wynika, że starsze pokolenia bardziej koncentrują się na zagrożeniach finansowych i bezpieczeństwie danych. Młodsi respondenci, w wieku 18-29 lat częściej wyrażają obawy dotyczące prywatności. Dla 30 proc. osób z tej grupy największe zagrożenie stanowi naruszenie prywatności w mediach społecznościowych.

	18-29 lat	30-39 lat	40-49 lat	50-59 lat	60+ lat
Utrata danych osobowych	47%	44%	43%	47%	46%
Wyłudzenie kredytu/ zaciągnięcie zobowiązań na moje dane	55%	56%	55%	71%	56%
Utrata środków finansowych	62%	74%	73%	76%	66%
Naruszenie prywatności w mediach społecznościowych	30%	19%	19%	14%	11%
Przejęcie kontroli nad urządzeniami	31%	35%	33%	33%	28%
Zainfekowanie urządzeń wirusem	28%	31%	34%	40%	35%
Brak świadomości zagrożeń wśród bliskich	16%	12%	11%	4%	9%

Pytanie wielokrotnego wyboru. Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Polacy na straży swoich urządzeń

Świat cyfrowy stwarza wiele możliwości zarówno w życiu prywatnym, jak i zawodowym. Jednak wraz ze wzrostem liczby cyberataków, zabezpieczenie urządzeń, których używamy na co dzień, staje się coraz bardziej istotne. Regularne aktualizacje systemów operacyjnych i aplikacji są jednym z kluczowych elementów zapobiegania zagrożeniom, ponieważ eliminują luki, które mogą być wykorzystane przez hakerów. Dodatkowo, niezwykle ważne jest stosowanie zaufanego oprogramowania antywirusowego, które zwiększa poziom ochrony przed potencjalnymi zagrożeniami.

Wyniki badania pokazują, że coraz więcej osób zdaje sobie sprawę z potrzeby zabezpieczania swoich urządzeń. Aż 79 proc. respondentów deklaruje, że chroni swoje komputery lub laptopy, co świadczy o wysokim poziomie wiedzy w tym zakresie. Jednak 16 proc. badanych wciąż nie korzysta z żadnych dodatkowych środków, co wskazuje na potrzebę dalszej edukacji w zakresie cyberbezpieczeństwa.

Czy posiada Pan/Pani **dodatkowe zabezpieczenia** jak program antywirusowy na swoim komputerze lub laptopie?

TAK 79%

NIE 16%

Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Zabezpieczenia smartfonów wypadają słabiej niż komputerów – niemal połowa badanych (49 proc.) nie instaluje żadnego programu ochronnego na swoich telefonach, mimo że korzystamy z nich codziennie. Na tych urządzeniach zawarte są nasze dane osobowe, aplikacje bankowe oraz dają dostęp do mediów społecznościowych. Tylko 45 proc. użytkowników decyduje się chronić swój telefon dodatkowymi zabezpieczeniami antywirusowymi. W związku z tym, że smartfony mamy zawsze na wyciągnięcie ręki i nieustannie z nich korzystamy, cyberprzestępcy coraz częściej kierują na nie swoje ataki. Poprzez stosowanie socjotechniki próbują wyłudzać dane do logowania lub informacje o kartach płatniczych.

W kwestii ochrony komputerów i smartfonów, najlepiej radzi sobie grupa wiekowa 40-49 lat – aż 87 proc. osób z tej grupy zabezpiecza swoje komputery, a 51 proc. dba o ochronę swoich smartfonów.

Czy zabezpiecza Pan/Pani swój telefon dodatkowym oprogramowaniem antywirusowym?

Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Konsekwencje cyberataków mogą być nie tylko kosztowne, ale również długotrwałe. Hakerzy często wykorzystują socjotechnikę, aby nakłonić użytkowników do odwiedzenia fałszywych stron internetowych. Takie przekierowania są zazwyczaj ukryte w postach i komentarzach w mediach społecznościowych, phishingowych e-mailach, wiadomościach w komunikatorach lub w reklamach internetowych. Dlatego ograniczone zaufanie oraz umiejętność rozpoznawania zagrożeń są kluczowe dla zachowania bezpieczeństwa online.

Jak pokazuje raport „Test z cyberbezpieczeństwa", phishing jest najczęściej rozpoznawanym przez Polaków rodzajem cyberataku. Aż 9 na 10 respondentów zna tę formę oszustwa, polegającą na podszywaniu się pod instytucje lub osoby w celu wyłudzenia poufnych danych albo nakłonienia ofiary do podjęcia określonych działań.

Innym powszechnie znanym zagrożeniem jest spoofing, czyli fałszowanie tożsamości, adresu e-mail lub IP w celu wyłudzenia danych lub pieniędzy. Ten rodzaj ataku rozpoznaje 73 proc. badanych. Podobny odsetek, 73 proc., słyszało również o deepfake — technologii wykorzystującej sztuczną inteligencję do tworzenia realistycznych, lecz fałszywych obrazów lub filmów, które mogą służyć do oszustwa lub dezinformacji.

Jednym z mniej rozpoznawalnych zagrożeń jest ransomware, czyli forma ataku polegająca na szyfrowaniu danych w celu uzyskania okupu. Tylko 44 proc. respondentów słyszało o tej formie ataku, podczas gdy połowa badanych nie zna tego zagrożenia.

Osoby w wieku 18-39 lat najczęściej rozpoznają wszystkie cztery rodzaje cyberataków, natomiast w grupie powyżej 60. roku życia świadomość tych zagrożeń jest najniższa.

Proszę powiedzieć, czy **słyszał/a Pan/i o poniższych formach cyberataków?**


87% **Phishing** (podszywanie się pod instytucje lub osoby w celu wyłudzenia poufnych informacji czy też nakłonienia ofiary do określonych działań)


73% **Spoofing** (fałszowanie tożsamości, adresu e-mail lub IP celem wyłudzenia danych lub pieniędzy)


73% **Deepfake** (Technologia, która wykorzystuje sztuczną inteligencję do tworzenia fałszywych, realistycznych obrazów lub filmów celem dezinformacji, oszustw lub szantażu)


44% **Ransomware** (szyfrowanie danych dla uzyskania okupu)

Pytanie wielokrotnego wyboru. Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Podszywanie się pod bliskich – pułapka cyfrowych oszustów

Próby oszustwa ze strony cyberprzestępców dotykają coraz większej liczby Polaków, którzy korzystają z popularnych kanałów komunikacji. E-maile, SMS-y oraz wiadomości przesyłane przez komunikatory, takie jak Messenger czy WhatsApp, są najczęściej wykorzystywane przez oszustów. Według danych CERT Polska liczba zgłoszonych incydentów cyberbezpieczeństwa pozostaje wysoka – w 2022 roku odnotowano 217 tys. przypadków, z kolei w 2023 roku liczba ta wzrosła do 221 tys. Wskazuje to na stałe, wysokie zagrożenie ze strony cyberprzestępców. Co więcej, aż jedna trzecia zgłoszeń (prawie 85 tys.) została zarejestrowana w grudniu, co sugeruje, że przestępcy szczególnie intensywnie działają w okresie świątecznym.

Liczba zgłoszeń dotyczących prób wyłudzenia wzrosła do 119 tys., co oznacza wzrost o 37 tys. w porównaniu z rokiem poprzednim. W efekcie, na listę ostrzeżeń CERT Polska dodano 8346 podejrzanych domen. Na przestrzeni ostatnich lat zauważono, że okres od Black Friday do Nowego Roku to czas, kiedy zgłaszanych jest najwięcej incydentów. W tym czasie oszuści często wykorzystują scenariusze związane z dostawami kurierskimi, na przykład wysyłają fałszywe wiadomości o konieczności dopłaty za paczkę. Takie metody okazują się wciąż bardzo skuteczne.

Badanie pokazuje, że aż 55 proc. Polaków otrzymało wiadomość od osoby podszywającej się pod znajomego, członka rodziny lub przedstawiciela znanej instytucji. Większość tych działań opiera się na socjotechnikach – metodach manipulacji, które wykorzystują naszą nieuwagę i brak świadomości. Jedną z najczęściej stosowanych strategii jest podszywanie się pod firmy kurierskie poprzez przesyłanie SMS-ów z prośbą o dopłatę za paczkę, co często kończy się kliknięciem w złośliwy link. Dlatego kluczowe jest, aby każdą podejrzaną wiadomość dokładnie przeanalizować i nie reagować pod wpływem impulsu. Chwila refleksji i uważności może uchronić przed oszustwem.

Jak wynika z badania, z takimi sytuacjami najczęściej spotykają się osoby w wieku 30-39 lat – aż 66 proc. z tej grupy miało do czynienia z próbą oszustwa. Dla porównania, w grupie osób powyżej 60. roku życia odsetek ten wynosi 36 proc.

Czy kiedykolwiek otrzymał/a Pan/i wiadomość (email, SMS, wiadomość w social mediach) od osoby, która podawała się za Pana/i znajomego, członka rodziny lub znaną Panu/i instytucje, a w rzeczywistości była oszustem?

55% Tak

39% Nie

Odpowiedzi nie sumują się do 100 proc. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć"

Oszustwa internetowe stają się coraz bardziej powszechne i dotykają użytkowników w różnym wieku – od młodzieży po osoby starsze. Według wyników raportu, co piąty ankietowany doświadczył wyłudzenia pieniędzy lub poufnych informacji przez cyberprzestępców. Jednak, świadomość dotycząca taktyk stosowanych przez oszustów stopniowo wzrasta, co sprawia, że coraz więcej osób potrafi unikać zagrożeń. Wyniki badania pokazują, że blisko trzy czwarte (73 proc.) respondentów nie padło ofiarą cyberprzestępców, co jest pozytywnym sygnałem wskazującym na rosnącą ostrożność i lepsze zabezpieczenia.

Czy kiedykolwiek padł/a Pan/i ofiarą cyberprzestępców (np. ktoś wyłudził od Pana/i pieniądze lub poufne informacje)?

18% Tak

73% Nie

Odpowiedzi nie sumują się do 100 proc. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć"

Warto jednak zauważyć, że choć osoby starsze często postrzega się jako bardziej podatne na takie zagrożenia, faktycznie ofiarą cyberoszustwa padło jedynie 11 proc. seniorów. Z kolei w grupie najmłodszych respondentów, w wieku 18-29 lat, odsetek ten wyniósł 24 proc., co może wynikać z częstszego korzystania z internetu przez młodsze pokolenia.

Czy kiedykolwiek padł/a Pan/i ofiarą cyberprzestępców (np. ktoś wyłudził od Pana/i pieniądze lub poufne informacje)?

	18-29 lat	30-39 lat	40-49 lat	50-59 lat	60+ lat
Tak	24%	23%	16%	18%	11%
Nie	66%	73%	72%	71%	80%

Odpowiedzi nie sumują się do 100. Pominięto odpowiedzi „Inne" oraz „Nie wiem/Trudno powiedzieć".

Rozwój internetu znacząco ułatwił przestępcom podszywanie się pod inne osoby i dotarcie do szerokiego grona potencjalnych ofiar. Cyberprzestępcy masowo wysyłają wiadomości i liczą, że przynajmniej część odbiorców da się oszukać. Co więcej, ataki phishingowe są coraz bardziej zaawansowane i precyzyjnie dopasowane do określonych grup. Przestępcy personalizują treści nie tylko pod kątem tematów, lecz także analizują profile odbiorców, aby zwiększyć skuteczność. Wykorzystują dane z mediów społecznościowych, geolokalizację i aktywność online, dzięki czemu lepiej profilują swoje ofiary. Z raportu wynika, że najczęściej fałszywe wiadomości trafiały do osób z dochodami netto w przedziale 5000–5999 zł – aż dwie trzecie respondentów z tej grupy. Z kolei wśród osób zarabiających do 3000 zł oraz od 3000 do 3999 zł co drugi badany padł ofiarą takich prób oszustwa.

Czy kiedykolwiek otrzymał/a Pan/i wiadomość (email, SMS, wiadomość w social mediach) od osoby, która podawała się za Pana/i znajomego, członka rodziny lub znaną Panu/i instytucje, **a w rzeczywistości była oszustem?**

51%
Do 3000 zł

50%
3000 – 3.999 zł

57%
4000 – 4999 zł

64%
5000 – 5999 zł

55%
6000 i więcej zł

Odpowiedzi nie sumują się do 100. Pominięto odpowiedź „Nie wiem/Trudno powiedzieć”.

Fałszywe informacje w sieci: czy Polacy potrafią je rozpoznać

Internet jest dziś podstawowym źródłem informacji, jednak nie wszystkie dostępne tam treści są rzetelne. Z przeprowadzonego badania wynika, że czterech na dziesięciu Polaków przyznaje, że nie podejmuje działań mających na celu weryfikację wiarygodności informacji publikowanych w sieci.

Czy ostatnim miesiącu **sprawdzał/a, weryfikował/a Pan/i prawdziwość treści** znalezionych w mediach społecznościowych lub w serwisach informacyjnych?

TAK 51%

NIE 40%

Odpowiedzi nie sumują się do 100. Pominięto odpowiedź „Nie wiem/Trudno powiedzieć".

Co więcej, w grupie osób powyżej 60. roku życia odsetek ten wynosi aż 54 proc., co oznacza, że seniorzy rzadziej sprawdzają rzetelność treści, które napotykają w Internecie. Weryfikacja informacji jest bardziej powszechna wśród młodszych użytkowników sieci. W grupie wiekowej 18-29 lat aż 71 proc. respondentów deklaruje, że regularnie sprawdza autentyczność wiadomości, zarówno w mediach społecznościowych, jak i na portalach informacyjnych. Dodatkowo zauważalne są różnice w podejściu do weryfikacji między płciami – 56 proc. mężczyzn oraz 46 proc. kobiet angażuje się w sprawdzanie źródeł informacji.

Santander Consumer Bank

Czy ostatnim miesiącu **sprawdzał/a, weryfikował/a Pan/i prawdziwość treści** znalezionych w mediach społecznościowych lub w serwisach informacyjnych?

	18-29 lat	30-39 lat	40-49 lat	50-59 lat	60+ lat
Tak	71%	56%	49%	44%	38%
Nie	18%	35%	44%	47%	54%

Odpowiedzi nie sumują się do 100. Pominięto odpowiedź „Nie wiem/Trudno powiedzieć".

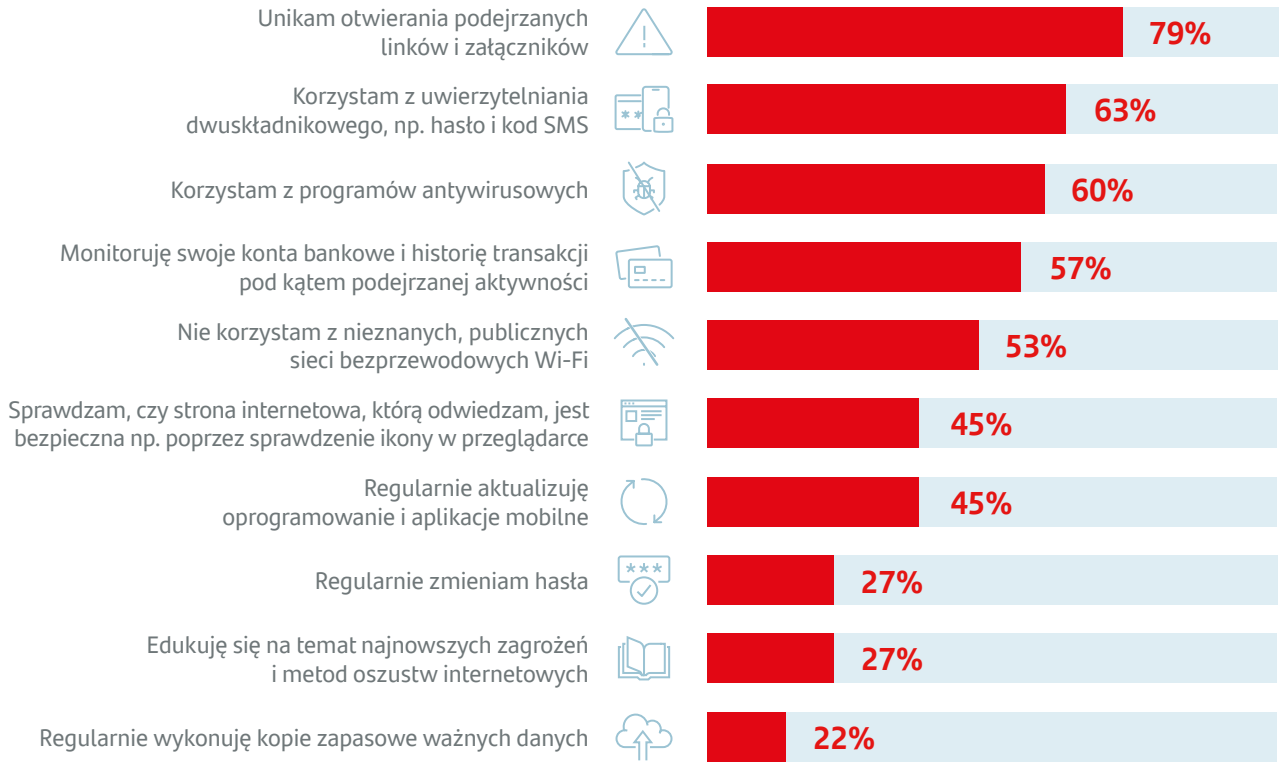
Wielu Polaków korzysta z różnorodnych praktyk, aby chronić swoje dane w internecie. Najczęściej wybieraną metodą ochrony jest unikanie podejrzanych linków i załączników, co deklaruje 79 proc. respondentów. Wskazuje to na wysoki poziom ostrożności wobec potencjalnych ataków phishingowych. Uwierzytelnianie dwuskładnikowe to kolejna powszechnie stosowana metoda ochrony, z której korzysta 63 proc. badanych. Polega ona na tym, że oprócz hasła użytkownik musi potwierdzić swoją tożsamość za pomocą drugiego elementu, na przykład jednorazowego kodu SMS, przesyłanego na zarejestrowany numer telefonu. Dzięki temu nawet jeśli cyberprzestępca pozna hasło użytkownika, to bez dostępu do drugiego czynnika – np. telefonu – nie uda mu się zalogować.

Równie dużą popularnością cieszą się programy antywirusowe, z których korzysta 60 proc. respondentów, co pozwala skutecznie blokować złośliwe oprogramowanie.

Unikanie publicznych hotspotów Wi-Fi również stanowi ważny element zabezpieczeń – 53 proc. ankietowanych rezygnuje z korzystania z tych sieci, aby zminimalizować ryzyko przechwycenia danych. Dodatkowo, 45 proc. respondentów sprawdza bezpieczeństwo odwiedzanych stron internetowych. Regularne monitorowanie kont bankowych, które pomaga szybko wykryć podejrzane transakcje, deklaruje 57 proc. badanych.

Choć większość respondentów stosuje różne metody ochrony, jedynie 27 proc. aktywnie pogłębia swoją wiedzę na temat najnowszych zagrożeń i metod internetowych oszustw. Tymczasem rozwijanie wiedzy w tym zakresie również pełni funkcję ochronną – pozwala szybciej rozpoznawać potencjalne ryzyka i lepiej chronić się przed atakami. Samoświadomość w obszarze cyberbezpieczeństwa działa jak tarcza, która wspiera inne zabezpieczenia i czyni je bardziej skutecznymi w obliczu coraz bardziej zaawansowanych zagrożeń.

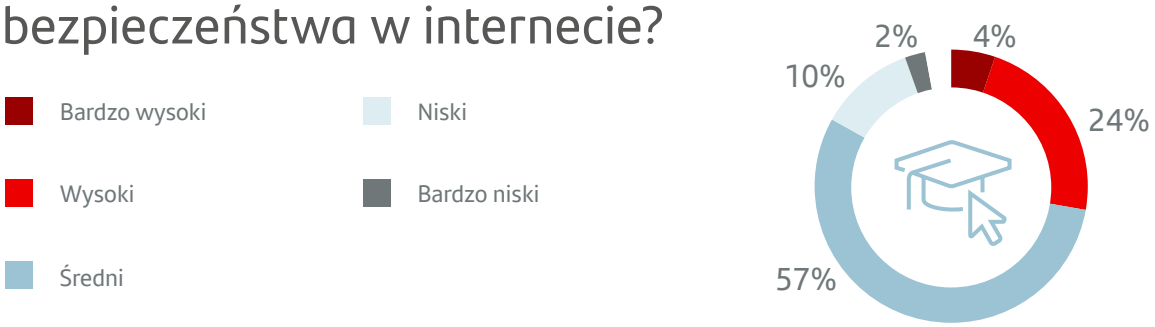
Jakie działania podejmuje Pan/i, aby dbać o zabezpieczenie swoich danych w internecie?



Pytanie wielokrotnego wyboru. Odpowiedzi nie sumują się do 100. Pominięto odpowiedź „Nie wiem/Trudno powiedzieć".

Wśród respondentów znaczna część ocenia swoją wiedzę na temat bezpieczeństwa w internecie jako umiarkowaną, co może zwiększać podatność na cyberzagrożenia. Tylko 29 proc. badanych określa swoje kompetencje w tym zakresie jako wysokie lub bardzo wysokie. Ponad połowa ankietowanych (57 proc.) ocenia swoją wiedzę jako średnią, co oznacza znajomość podstawowych zagrożeń internetowych, ale jednocześnie brak głębszej świadomości w zakresie bardziej zaawansowanych metod ataków. 12 proc. respondentów uznaje swoje kompetencje w zakresie cyberbezpieczeństwa za niskie lub bardzo niskie.

Jak ocenia Pan/i **swój poziom wiedzy** w zakresie bezpieczeństwa w internecie?



Odpowiedzi nie sumują się do 100. Pominięto odpowiedź „Nie wiem/Trudno powiedzieć".

Dane te wyraźnie podkreślają konieczność ciągłego podnoszenia świadomości na temat cyberzagrożeń. Wraz ze wzrostem liczby ataków w sieci, rośnie także potrzeba regularnego aktualizowania wiedzy oraz doskonalenia umiejętności w zakresie ochrony danych. Skuteczna obrona przed cyberprzestępczością nie ogranicza się jedynie do znajomości podstawowych zasad bezpieczeństwa, ale wymaga również zdolności do rozpoznawania coraz bardziej zaawansowanych technik stosowanych przez przestępców.

Zakończenie

Raport „Test z cyberbezpieczeństwa" ukazuje aktualny poziom świadomości Polaków w kwestii zagrożeń w sieci oraz ich podejście do ochrony danych. Wyniki badania pokazują, że chociaż Polacy coraz lepiej rozumieją znaczenie cyberbezpieczeństwa, wiele osób wciąż zmaga się z obawami, głównie związanymi z potencjalną utratą środków finansowych i prywatnych informacji.

Badanie wskazuje, że choć popularność zabezpieczeń, takich jak uwierzytelnianie dwuskładnikowe i programy antywirusowe, rośnie, wielu użytkowników stosuje je tylko na wybranych urządzeniach. Zdecydowana większość chroni swoje laptopy i komputery stacjonarne, natomiast rzadziej zabezpiecza smartfony, które gromadzą coraz więcej wrażliwych danych.

Jednocześnie, pomimo rosnącej świadomości zagrożeń internetowych, część użytkowników nadal nie podejmuje działań w celu weryfikacji informacji dostępnych online. W efekcie coraz więcej osób jest narażonych na kontakt z fałszywymi wiadomościami oraz phishingiem – techniką oszustwa, która polega na podszywaniu się pod zaufane źródła, której celem jest wyłudzenie danych osobowych lub finansowych.

Raport podkreśla również, że w miarę jak cyberzagrożenia ewoluują, kluczowe znaczenie ma dalsza edukacja w zakresie metod ochrony danych. Wzrost świadomości na temat działań cyberprzestępców oraz stosowanie odpowiednich środków ostrożności mogą znacząco ograniczyć skalę zagrożeń i pomóc lepiej przystosować się do wyzwań współczesnej przestrzeni cyfrowej.

Informacja o badaniu

Badanie zostało zrealizowane na zlecenie Santander Consumer Banku – banku od kredytów metodą telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI), przeprowadzonych przez Instytut Badań Rynkowych i Społecznych (IBRiS) w dniach 2-7 września 2024 r. W badaniu wzięła udział reprezentatywna grupa dorosłych Polaków korzystających z internetu. Próba n = 1000

Santander Consumer Bank – bank od kredytów jest jednym z liderów rynku consumer finance w Polsce. Oferuje klientom szeroki zakres produktów obejmujący kredyty gotówkowe, kredyty na nowe i używane samochody, kredyt celowy oraz internetowy limit odnawialny, karty kredytowe oraz lokaty i rachunki oszczędnościowe. Produkty dystrybuowane są online oraz poprzez sieć oddziałów, salony i komisy samochodowe, sklepy i punkty usługowe. Jest także wydawcą TurboKARTY.

Więcej na https://www.santanderconsumer.pl/