CHRONPESEL.PL

URZĄD OCHRONY DANYCH OSOBOWYCH

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Cyberzagrożenia – czego boją się Polacy?

Raport z badania
czerwiec 2022 r.

Spis treści

Adam Łącki
Prezes Zarządu Krajowego Rejestru Długów Biura Informacji Gospodarczej SA

Szanowni Państwo,

tematy związane z cyberbezpieczeństwem od dłuższego czasu są przedmiotem analizy ekspertów i dziennikarzy. Na stałe przeniknęły także do naszych codziennych rozmów. Z jednej strony to dobrze, ponieważ im więcej o tym mówimy, tym bardziej zagadnienia związane z zagrożeniami w sieci stają się dla nas zrozumiałe. Równocześnie, jak wynika z przeprowadzonego badania, Polacy nadal mniej pewnie czują się w sytuacjach związanych z wyciekami danych osobowych lub działalnością hakerów.

Wynika to z tego, że sposoby działania cyberprzestępców stale się zmieniają. Oszuści starają się bowiem dostosować do bieżących wydarzeń. Tak jest na przykład z tematem wojny, która toczy się za naszą wschodnią granicą i która od samego początku wykorzystywana jest przez różnych oszustów chcących zarobić na naszym strachu lub chęci pomocy poszkodowanym.

Drugim czynnikiem wpływającym na brak zdecydowanych deklaracji w sprawie reagowania na zagrożenia w sieci jest fakt, że w tej przestrzeni nie wszystko zależy od nas. Możemy korzystać z najnowocześniejszego oprogramowania i systemów antywirusowych oraz stosować wszystkie zasady bezpieczeństwa, a nasze dane wpadną w ręce cyberprzestępców w wyniku wycieku z bazy serwisu, z którego korzystamy. Tym bardziej ważna jest świadomość wszystkich zagrożeń oraz tego, co i w jakim momencie możemy zrobić, żeby się przed nimi uchronić lub zminimalizować ich skutki.

W tym celu chciałbym zachęcić do przeczytania raportu, który pod patronatem Urzędu Ochrony Danych Osobowych przygotowali eksperci serwisu ChronPESEL.pl i Krajowego Rejestru Długów. Znajdziecie w nim Państwo odpowiedzi na pytania, co jako społeczeństwo wiemy na temat cyberzagrożeń oraz wskazówki, jak powinniśmy reagować w konkretnych sytuacjach.

Nie brakuje także wątków dotyczących przyszłości. Wraz z rozwojem technologicznym obserwujemy również wzrost zainteresowania wykorzystania danych biometrycznych. Z przeprowadzonego badania wynika, że respondenci widzą korzyści ze zastosowania środków bezpieczeństwa opartych na unikalnych dla każdego z nas cechach.

Zapraszam do lektury.

Jan Nowak
Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo,

przyspieszenie transformacji cyfrowej oraz rozwój nowoczesnych technologii przyczyniły się do zastosowania w życiu codziennym wielu innowacyjnych rozwiązań. Świadczenie pracy w trybie zdalnym, nauczanie dzieci i młodzieży metodami na odległość, użycie e-usług w większości branż czy łatwiejszy dostęp do usług zdrowotnych dzięki popularyzacji telemedycyny – to tylko wybrane przykłady z życia codziennego, gdzie nowoczesne rozwiązania, m.in. oparte na danych, dały nam bardzo wiele korzyści. Niestety, spowodowały również wzmożoną aktywność cyberprzestępców, dla których niezwykle cenne są nasze dane osobowe. Z kolei brak prawidłowych nawyków osób fizycznych, dzięki którym mogą zabezpieczyć swoje dane osobowe czy mało odpowiedzialne traktowanie przez administratorów zasad ochrony danych osobowych, może prowadzić nas do kosztownych i uciążliwych w skutkach strat. Naszym wspólnym wyzwaniem staje się zatem zapewnienie cyfrowego bezpieczeństwa. Jego podstawowymi elementem powinny być wiedza oraz świadomość użytkowników Internetu, jaką profilaktykę cyberzagrożeń zastosować.

Ufam, że wnioski płynące z badania pt. „Cyberzagrożenia – czego boją się Polacy?" przyczynią się do podniesienia świadomości w obszarze ochrony danych osobowych wielu grup społecznych i zawodowych, o zróżnicowanym przekroju wiekowym. Jest to niezbędny czynnik w procesie kształtowania postaw obywateli, dzięki którym można odpowiednio zidentyfikować zagrożenie i postąpić adekwatnie do sytuacji, aby przeciwdziałać lub zminimalizować negatywne skutki ich wystąpienia.

Z przeprowadzonych badań wynika, że wielu Polaków wie, jak zareagować w przypadku utraty danych w związku z naruszeniem ochrony danych osobowych. Cieszy też, że wiele osób jest w stanie przewidzieć negatywne konsekwencje takiego zdarzenia. Pokrzepiające jest także to, że wiele osób ma świadomość, że naruszenia ochrony danych osobowych np. w postaci wycieku danych należy zgłosić policji, a także do UODO.

Badanie potwierdziło, że na profilaktykę cyberzagrożeń składają się także upowszechnianie wśród obywateli wiedzy o ochronie danych osobowych, o bezpieczeństwie naszych danych czy przysługujących nam prawach. Mam nadzieję, że lektura tego raportu wzmocni tę praktykę.

O badaniu

Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych zostało przeprowadzone w marcu 2022 roku metodą CAWI na reprezentatywnej grupie 1010 respondentów przez IMAS International.

Główne wnioski

1/3 Polaków boi się utraty danych na skutek wycieku z bazy serwisu lub aplikacji, w której ma konto. Więcej z nas ma obawy o bezpieczeństwo danych przetwarzanych przez prywatne firmy.

46%

Tylko niespełna połowa badanych wie, jak zareagować w takim przypadku.

30%

2 na 3 Polaków jest w stanie przewidzieć negatywne konsekwencje takiego zdarzenia, a tylko niewiele ponad **30 proc. ankietowanych** wie, kto powinien się zająć neutralizacją skutków wycieku.

23%

Blisko **co czwarty ankietowany** za największe zagrożenie dla bezpieczeństwa swoich danych osobowych uważa działalność hakerów.

40%

Zaledwie **niewiele ponad 40 proc**. osób wie, jak zareagować w przypadku włamania na komputer lub telefon.

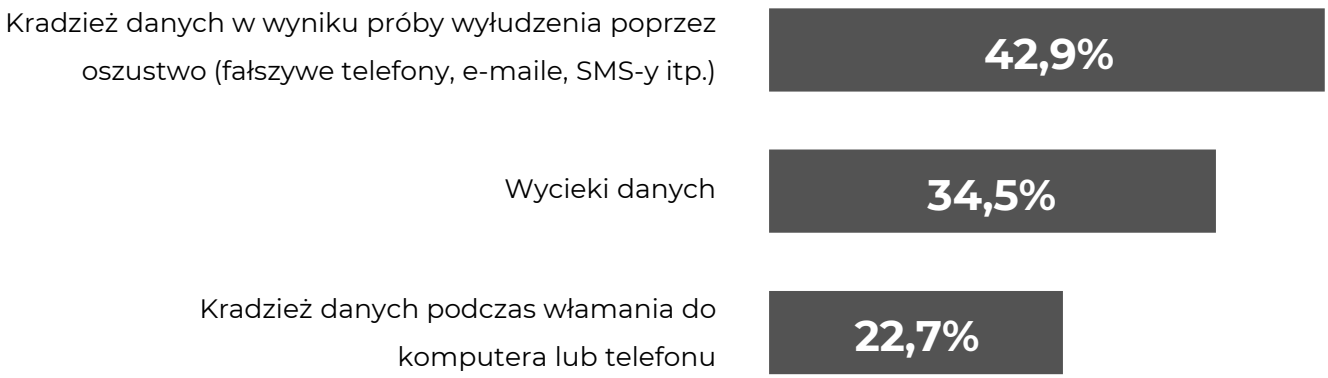
1/3 ankietowanych uważa logowanie z wykorzystaniem danych biometrycznych za najbezpieczniejszą metodę.

Wycieki danych osobowych wysoko na liście zagrożeń

Zapytani o to, skąd pochodzi zagrożenie dla naszych danych, Polacy najczęściej wskazują na oszustów, którzy próbują je wyłudzić. Na drugim miejscu znalazły się jednak wycieki danych. Obawia się ich co trzeci ankietowany (34,5 proc.).

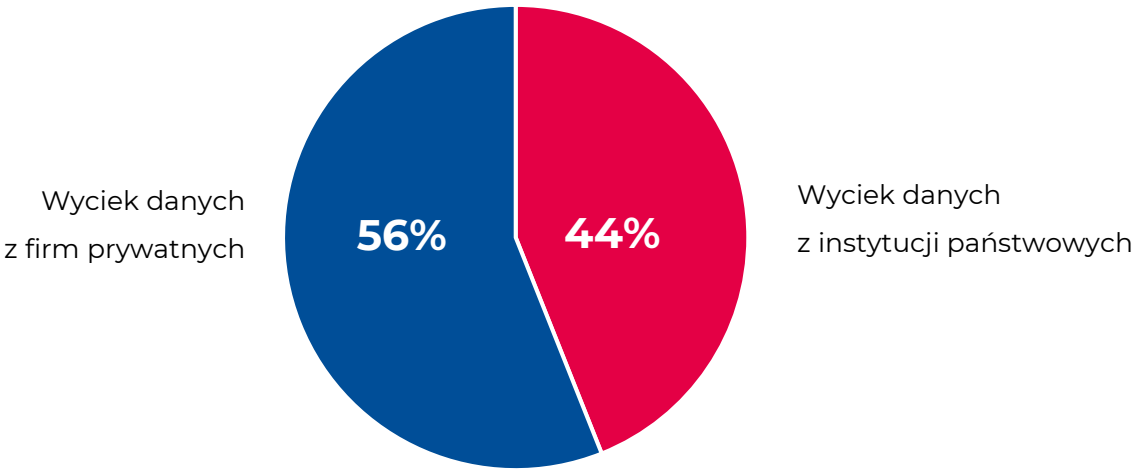
Wykres 1

Skąd, Twoim zdaniem, pochodzi największe zagrożenie dla Twoich danych?



Wykres 2

Skąd, Twoim zdaniem, pochodzi największe zagrożenie dla Twoich danych — ankietowani, którzy wskazali wyciek danych



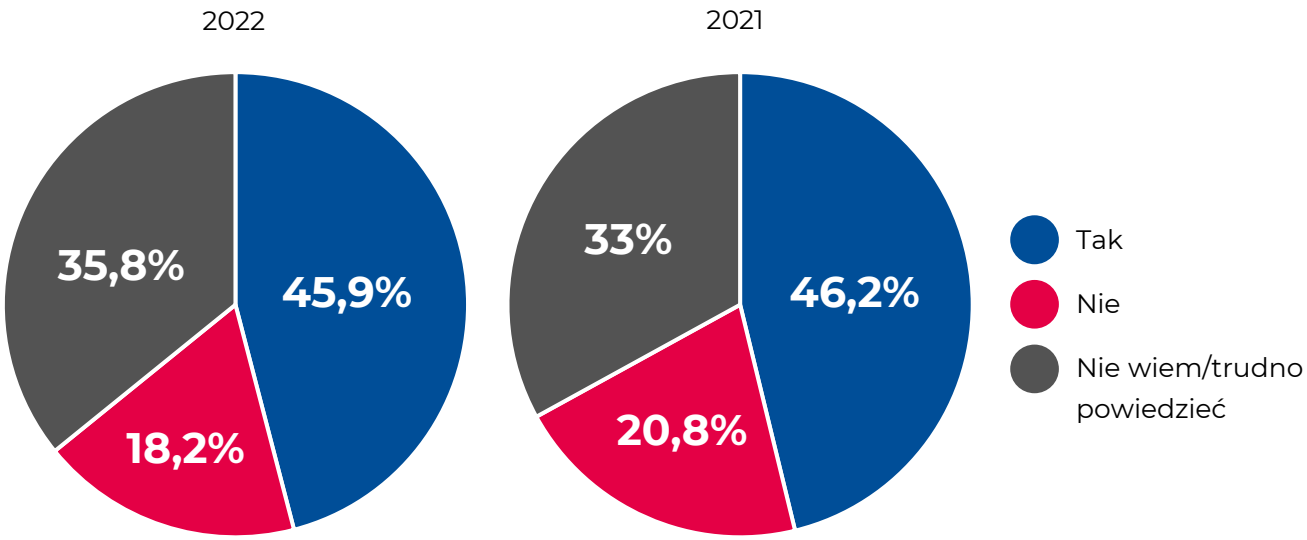
Co ciekawe, badani częściej wskazywali na wycieki z baz firm prywatnych. Za największe zagrożenie uznało je blisko 1/5 społeczeństwa (19,3 proc.). Nieznacznie lepiej wypadły instytucje publiczne. Wycieku danych z baz, którymi zarządza administracja publiczna obawia się 15 proc. ankietowanych. Tegoroczne wyniki nie różnią się w znaczący sposób od ubiegłorocznych odpowiedzi respondentów.

Jak wynika z deklaracji, tylko niespełna połowa z nas (46 proc.) wiedziałaby, jak należy zareagować w przypadku wycieku danych osobowych. Najpewniej czują się ludzie młodzi. Ponad 57 proc. ankietowanych w wieku 25–34 lata deklaruje, że wiedziałoby, co zrobić w takiej sytuacji. Największe problemy mieliby z tym z kolei seniorzy. Jak wynika z przeprowadzonego badania, 2/3 osób powyżej 65. r.ż. nie wiedziałoby, jak należy zareagować w sytuacji wycieku danych osobowych.

Porównując te wyniki z ubiegłorocznymi, nie widać znaczących zmian. Jeśli jednak przeanalizować to, jak odpowiadali ankietowani w poszczególnych grupach wiekowych, można zauważyć pewne różnice. Na pewno, względem 2021 roku, w widoczny sposób zmniejszył się odsetek osób, które deklarują, że nie wiedzą, co należy zrobić w przypadku wycieku danych. Dotyczy to ankietowanych w wieku 18–44 lata oraz 65–74 lata. W większości zmiany te dotyczyły osób niezdecydowanych lub takich, które mają wątpliwości.

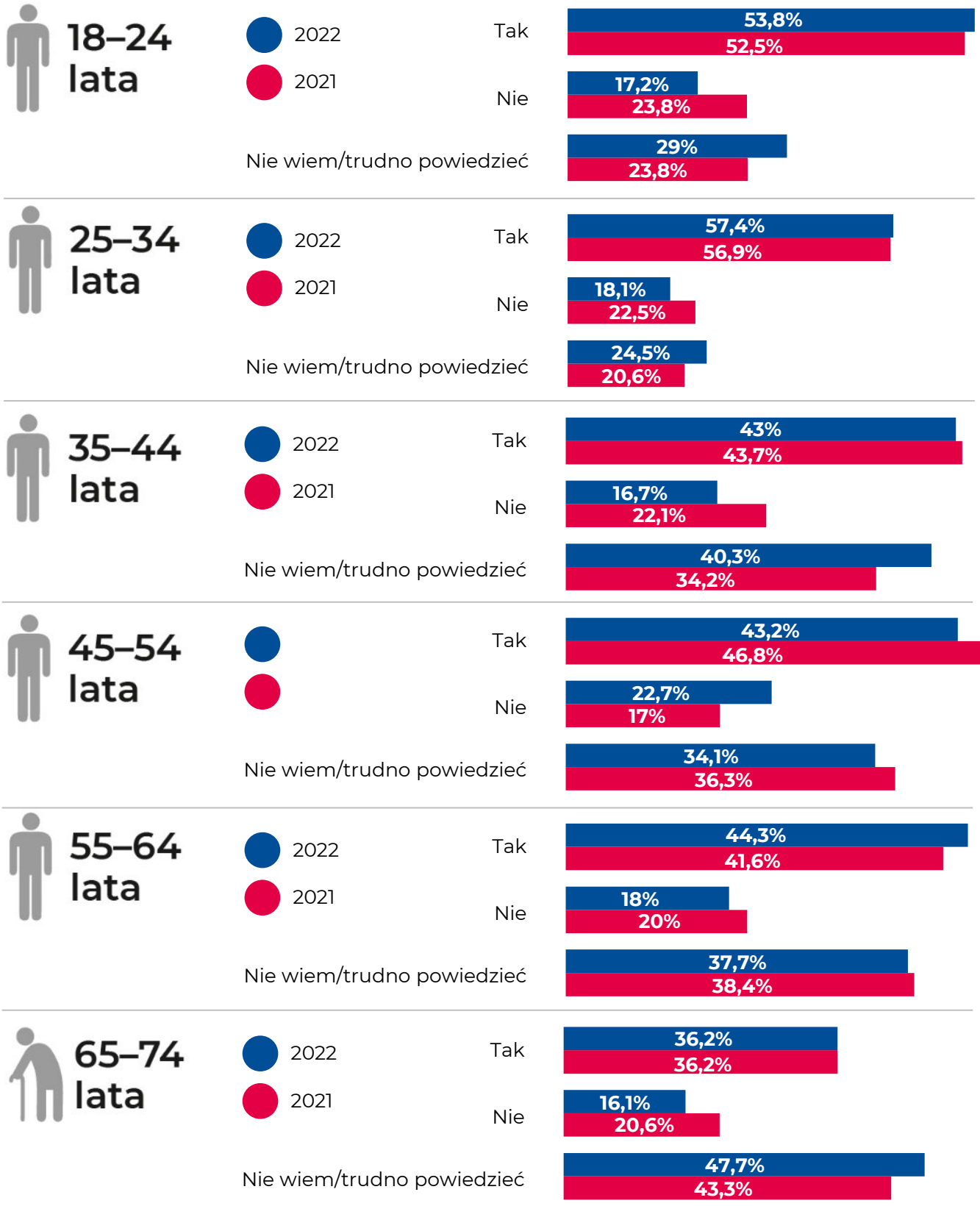
Wykres 3

Czy wiesz, jakie działania należy podjąć w przypadku wycieku danych z serwisu lub aplikacji, w których miałeś konto?



Wykres 4

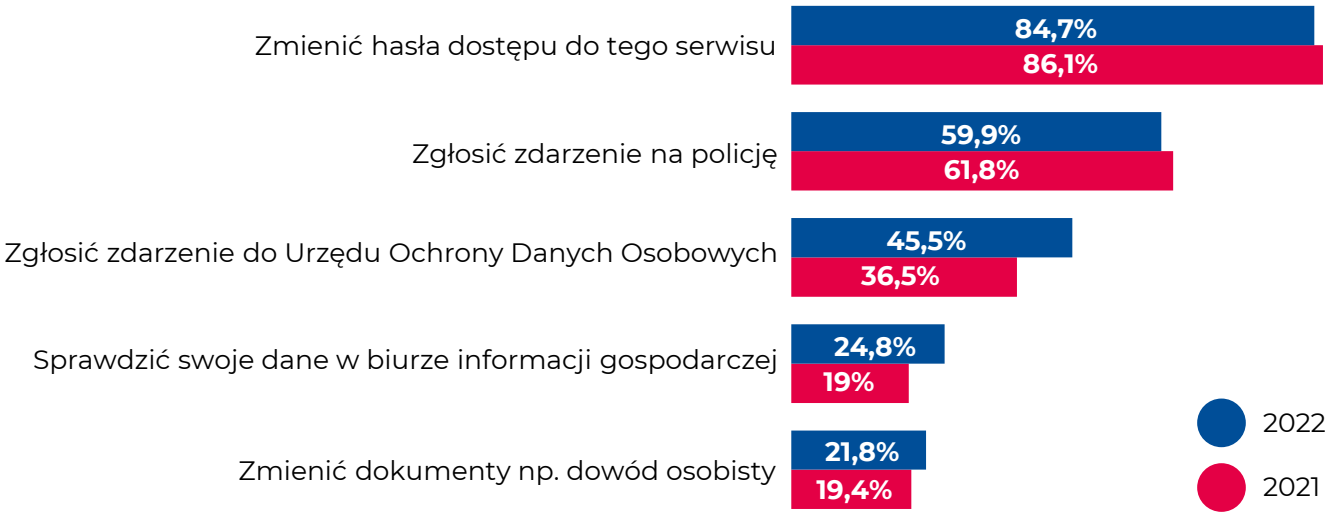
Wiem, jak zareagować w przypadku wyłudzenia danych osobowych



85 proc. ankietowanych zmieniłoby hasło dostępu do serwisu, z którego wyciekły dane. 60 proc. zgłosiłby zdarzenie na policję, a 45 proc. do UODO. Co czwarty badany sprawdziłby swoje dane z biurze informacji gospodarczej. Porównując udzielone odpowiedzi z 2021 rokiem, widzimy, że wzrósł odsetek osób, które zgłosiłby zdarzenie do UODO (36,5 proc.) i sprawdziły swoje dane w biurze informacji gospodarczej (19 proc.).

Wykres 5

Jakie działania należy podjąć w przypadku wycieku danych z serwisu lub aplikacji, w których miałeś konto?

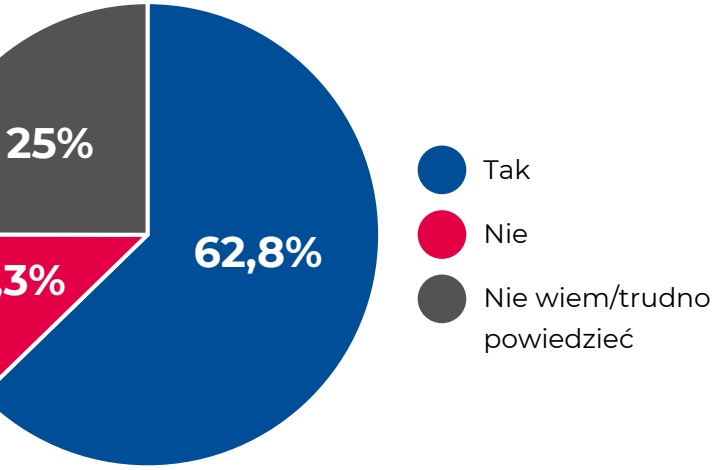


Konsekwencja wycieków

Blisko 2/3 ankietowanych wie, z czym może się wiązać wyciek danych osobowych. Wśród potencjalnych konsekwencji takiego zdarzenia najczęściej wskazujemy na zaciągnięcie zobowiązań finansowych w postaci, np. umowy kredytowej lub leasingowej (86 proc.), wykorzystanie danych do tego, by podszywając się pod nas oszukać naszych bliskich (75 proc.), sprzedaż danych osobowych (68 proc.) lub założenie firmy na skradzione dane (64 proc.).

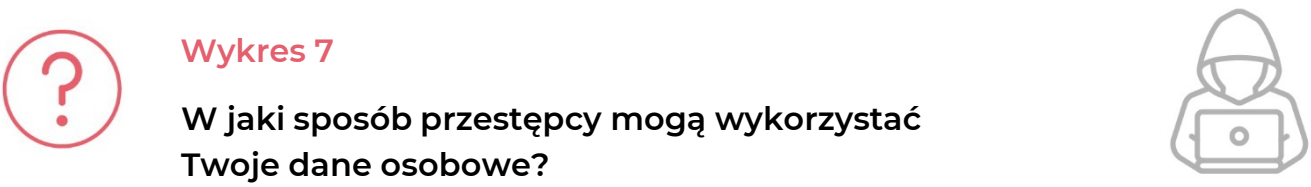
Wykres 6

Czy wiesz, jakie mogą być konsekwencje wycieku danych z serwisu/aplikacji, w których miałeś konto?



Wykres 7

W jaki sposób przestępcy mogą wykorzystać Twoje dane osobowe?



Jak poradzić sobie z konsekwencjami wycieków

Tylko niewiele ponad 30 proc. ankietowanych wie, kto powinien się zająć przeciwdziałaniem wystąpienia negatywnych skutków wycieku. W przypadku osób powyżej 65. r.ż. twierdząco na to pytanie odpowiedziało tylko niewiele ponad 20 proc. badanych.

Zdaniem 70 proc. ankietowanych to zadanie policji i innych służb ścigania, np. prokuratury. 60 proc. wskazuje na firmę lub instytucję będącą administratorem bazy danych, z której te wyciekły. Ponad 56 proc. wskazuje na UODO, a 44 proc. na inspektorów ochrony danych z instytucji i firm, z których te wyciekły.

Co trzeci ankietowany uważa, że neutralizacją skutków powinna zająć się osoba, której dane wyciekły. Najczęściej dotyczy to osób powyżej 35. r.ż., wśród których ten odsetek wynosi ok. 40 proc., a wśród badanych w wieku 55–64 lata nawet ponad 45 proc. Innego zdania są osoby młode. W grupie 25–34 lata tylko co piąty ankietowany uważa, że neutralizacją skutków wycieku danych powinna się zająć osoba, której dane dotyczą.

Zdaniem eksperta

Jacek Młotkiewicz
dyrektor Departamentu Kontroli i Naruszeń, UODO

Ogólne rozporządzenie o ochronie danych osobowych (RODO) stanowi, że każdy podmiot, który decyduje o celu przetwarzania danych osobowych i jego sposobach jest administratorem. Zgodnie z RODO, na takim administratorze ciąży wiele obowiązków. Dla przykładu, pozyskując dane osobowe od osoby, której one dotyczą, będzie zobowiązany poinformować ją m.in. o tym, kto jest administratorem, w jakim celu i na jakiej podstawie prawnej będzie je przetwarzał, a także komu ma zamiar je udostępniać. Innym obowiązkiem jest zapewnienie bezpieczeństwa przetwarzanych danych osobowych. Takie bezpieczeństwo pozwalają zachować wprowadzone środki, czy to techniczne, jak np. podwójne uwierzytelnianie przy wpisywaniu haseł lub szyfrowanie plików, czy także organizacyjne, jak cykliczne szkolenie pracowników. To dzięki wprowadzeniu odpowiednich środków, ale także ich regularnemu testowaniu, administrator może zapewnić bezpieczeństwo danych osobowych. RODO nakłada na administratorów także obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych. Taki rejestr to nic innego jak zbiór informacji na temat przetwarzanych danych osobowych. Pozwala on usystematyzować wykonywane czynności oraz całościowo spojrzeć jak wyglądają procesy przetwarzania danych osobowych w organizacji. Dzięki zebranym w tych rejestrach informacjom, administratorzy mogą również ocenić jakie dane są niezbędne do pozyskiwania.
Trzeba pamiętać, że administrator zawsze odpowiada za prawidłowe przetwarzanie danych osobowych.

Zapytani o to, co w przypadku wycieku danych powinien zrobić podmiot odpowiedzialny za ich gromadzenie i przetwarzanie najczęściej wskazujemy na informację o tym, że doszło do wycieku (2/3 ankietowanych) oraz jakie dane dokładnie wyciekły (60 proc.). Blisko 57 proc. oczekiwałoby także od instytucji wdrożenia działań zmniejszających ryzyko ponownego wycieku w przyszłości.

Ponad połowa ankietowanych oczekiwałaby od takiej firmy lub instytucji informacji, do kogo trafiły nasze dane, wsparcia prawnego oraz pokrycia kosztów pomocy prawnej i ewentualnych konsekwencji wycieku. 48 proc. badanych chciałaby także otrzymać informację na temat możliwych skutków wycieku.

Około 40 proc. ankietowanych oczekiwałoby rekomendacji działań, które należy podjąć, żeby zminimalizować ryzyko wycieku oraz przyznania rekompensaty w postaci odszkodowania lub rabatu na usługi danej firmy.

Zdaniem eksperta

Jacek Młotkiewicz
dyrektor Departamentu Kontroli i Naruszeń, UODO

Instytucje, podmioty, firmy, które przetwarzają dane osobowe, a więc administratorzy, muszą zapewnić ochronę danych osobowych. Zasady na jakich powinno się odbywać przetwarzanie danych określa RODO. Konieczne jest zapewnienie poufności tych danych. Każdy administrator powinien przetwarzać dane osobowe z należytą dbałością o ich bezpieczeństwo. W sytuacji, w której dochodzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia lub ujawnienia danych, mamy do czynienia z naruszeniem ochrony danych osobowych.

Wówczas administrator powinien zgłosić do UODO fakt wystąpienia naruszenia ochrony danych osobowych w terminie 72 godzin. Zgłoszenie naruszenia pozwala UODO na właściwą reakcję mogącą ograniczyć negatywne skutki takich naruszeń. Administrator ma obowiązek podjęcia skutecznych działań, które zapewnią ochronę osobom fizycznym i ich danym osobowym.

W sytuacji kiedy zachodzi wysokie ryzyko dla praw i wolności osoby, której dane dotyczą, wynikające z naruszenia, administrator jest zobowiązany bez zbędnej zwłoki zawiadomić osobę o incydencie. To bardzo ważne, ponieważ takie informacje umożliwią tej osobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać m.in. opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co trzeba zrobić, aby zminimalizować potencjalnie niekorzystne skutki. Informacje o incydencie należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to możliwe. Trzeba mieć na uwadze, że nie każde zgłaszane naruszenie jest utożsamiane z wyciekiem danych osobowych.

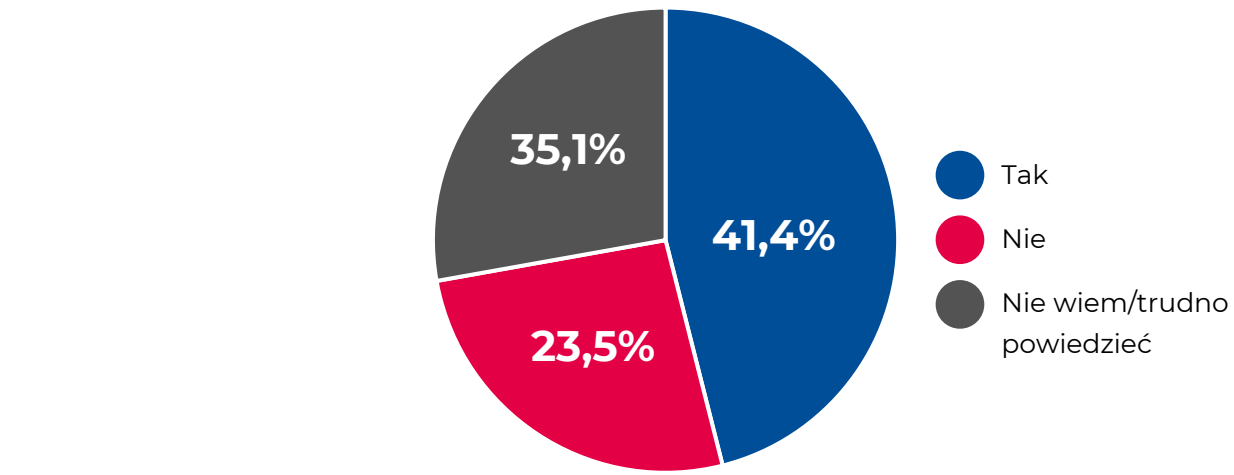
Starsi Polacy czują się coraz pewniej w starciu z hakerami

Jak wynika z przeprowadzonego badania, prawie co czwarty Polak obawia się utraty danych osobowych w wyniku włamania na komputer lub telefon. Dodatkowo tylko niewiele ponad 40 proc. z nas wie, jakie kroki należy podjąć w przypadku takiego ataku hakerskiego. Najpewniejsi swojej wiedzy są mężczyźni (prawie 50 proc.) i osoby w wieku 18–24 lata (ponad 47 proc.). Najmniej ankietowani między 35. a 44. r.ż. i seniorzy powyżej 65. r.ż. W tych grupach odsetek wynosi mniej niż 40 proc.

W tym przypadku również trzeba przeanalizować odpowiedzi udzielone w poszczególnych grupach wiekowych, żeby zaobserwować zmiany względem ubiegłorocznego raportu. Na pewno za niepokojącą informację należy uznać mniejszy niż w 2021 rok odsetek osób, które wiedzą, jak zareagować w przypadku ataku hakerskiego. Dotyczy to ankietowanych w wieku 25–44 lata. Spadek jest zauważalny – od 8 do 10 pp. w porównaniu do ubiegłego roku. Z drugiej strony, widać także budujący trend wśród najstarszych respondentów, wśród których istotnie (o 9 pp.) wzrósł odsetek osób, które wiedzą, jak poradzić sobie z atakiem hakerów.

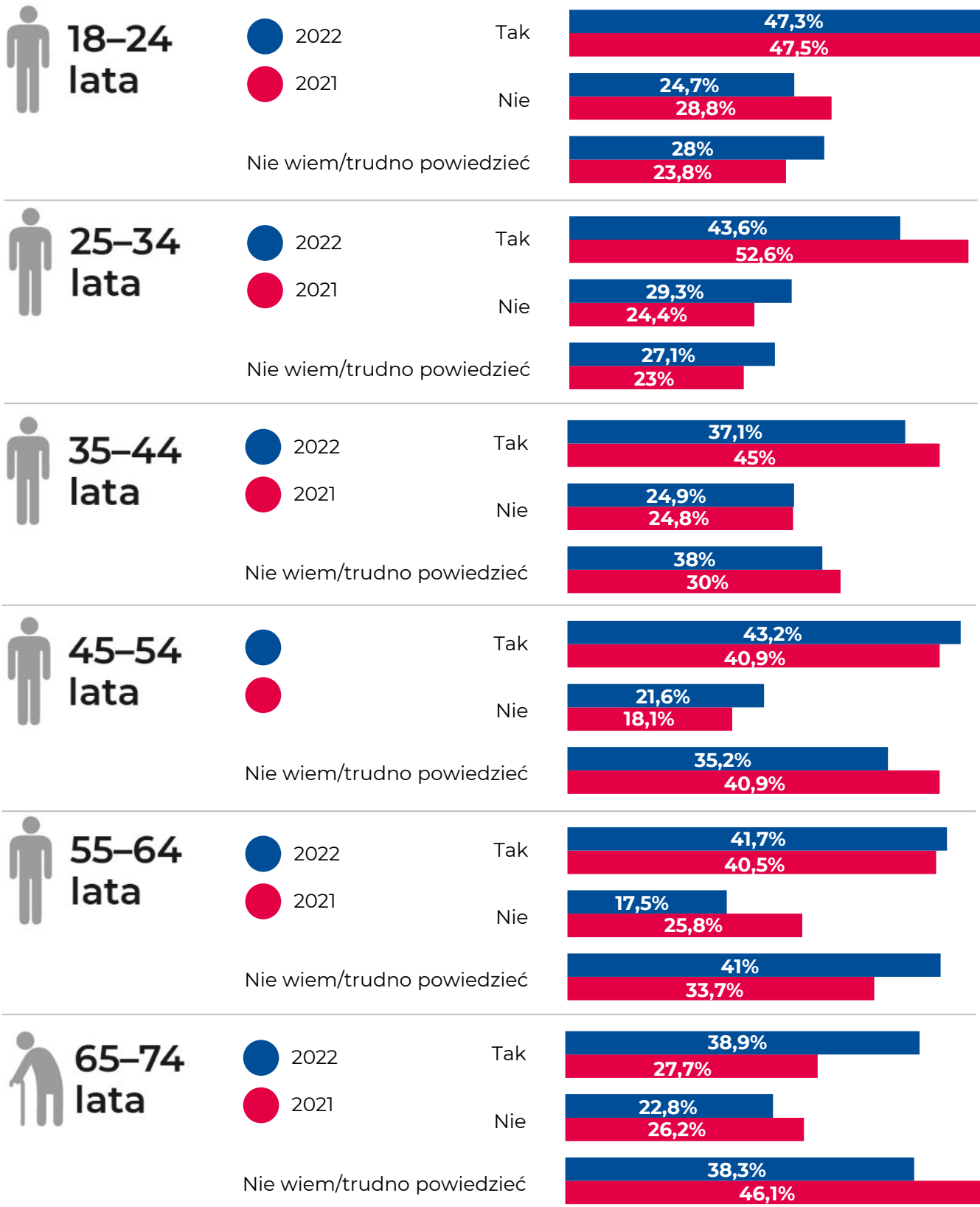
Wykres 8

Czy wiesz, jakie działania należy podjąć w przypadku ataku hakerskiego na komputer lub telefon?



Wykres 9

Wiem, jak zareagować w przypadku ataku hakerskiego na komputer lub telefon



Ponad 82 proc. badanych zmieniłaby hasła do komputera lub telefonu. 2/3 z nas zaktualizowałoby z kolei program antywirusowy, a prawie 59 proc. dopiero w przypadku ataku hakerskiego w ogóle by go zainstalowało. 63 proc. badanych zgłosiłoby sprawę na policję, a niespełna połowa sformatowałaby zaatakowane urządzenie.

Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL/PL

Zagrożenia związane z wyciekami danych osobowych oraz działalnością hakerów są ze sobą mocno powiązane. Dzięki zdobytym w ten sposób informacjom, cyberprzestępcy mogą próbować włamać się np. do naszych kont w serwisach lub skrzynek mailowych, które będą mogli następnie wykorzystać. W związku z tym powinniśmy pamiętać o kilku zasadach. Po pierwsze, bardzo ważne jest posiadanie odpowiednio złożonego i unikatowego hasła do logowania. Powinniśmy mieć także nawyk szybkiego zmieniania go w momencie, gdy wycieknią dane z serwisu, z którego korzystamy lub jeśli mamy chociaż cień podejrzenia, że ktoś włamał się do naszej skrzynki mailowej. Warto stosować także podwójne uwierzytelnienie przy logowaniu. Nie możemy też zapominać o aktualnym oprogramowaniu oraz zabezpieczeniom antywirusowym na naszym sprzęcie elektronicznym, również na telefonie, który aktualnie jest nośnikiem wielu danych. A jeśli już je stracimy, powinniśmy jak najszybciej zareagować, żeby ograniczyć negatywne skutki.

Bezpieczne metody logowania i wykorzystanie danych biometrycznych

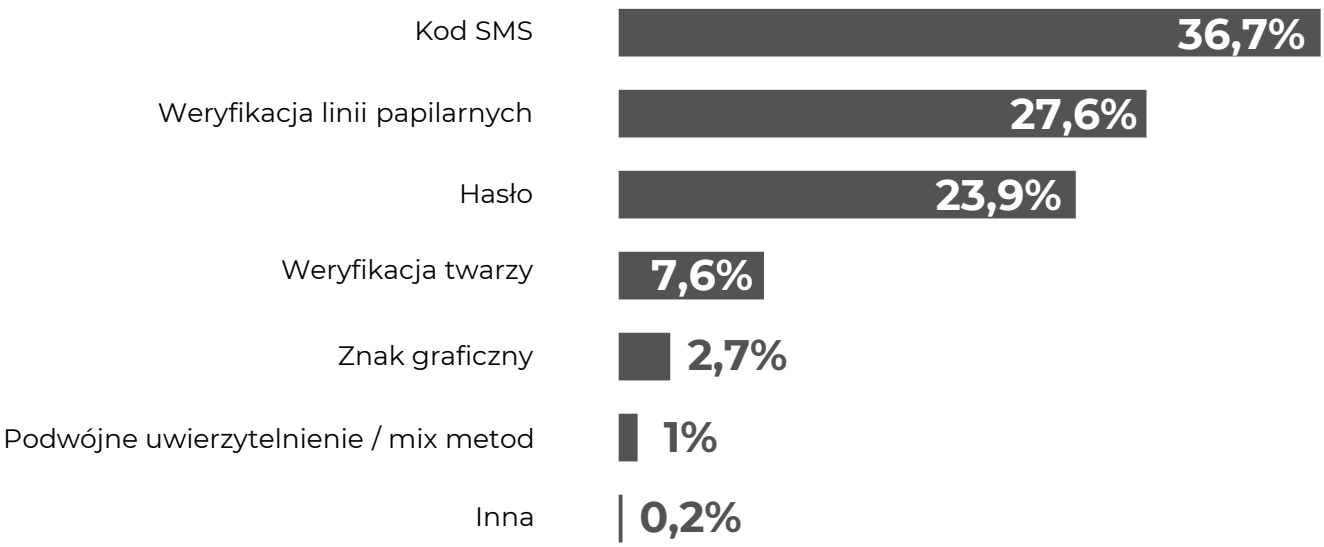
Za najbezpieczniejsze metody logowania do bankowości mobilnej lub serwisów internetowych uważamy kod SMS (37 proc.), weryfikację linii papilarnych (28 proc.) oraz hasło (24 proc.). Warto zwrócić też uwagę na wysokie zaufanie do logowania za pośrednictwem danych biometrycznych, jak odcisk palca, weryfikacja twarzy – tak deklaruje łącznie ponad 35 proc. ankietowanych.

Wykorzystanie danych biometrycznych podczas logowania za najbezpieczniejszą metodą uważają kobiety (37,5 proc.) oraz ankietowani w wieku 18–24 lata (45 proc.), 25–34 lata (39 proc.) i 35–44 lat (37,5 proc.). Stawiają ją nawet wyżej niż kod SMS i wymagane hasło.

Na podstawie tak udzielonych odpowiedzi przez ankietowanych można przypuszczać w jakim kierunku będą w najbliższym czasie rozwijać się zasady bezpieczeństwa.

Wykres 10

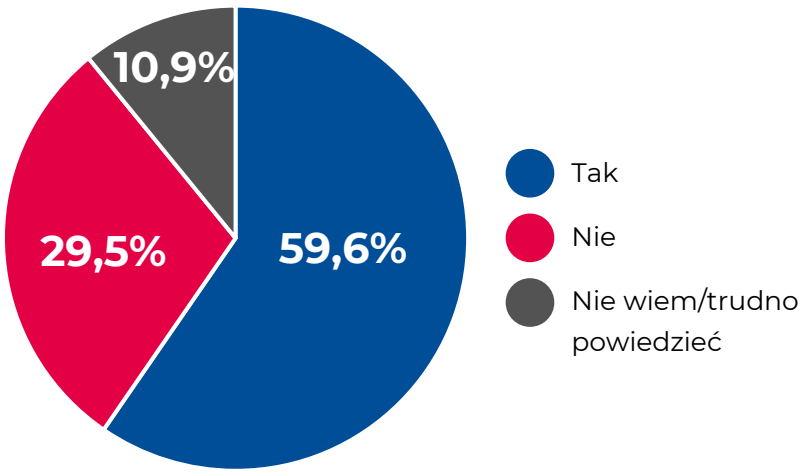
Jaka forma logowania do portali/bankowości internetowej jest, Twoim zdaniem, najbezpieczniejsza?



Prawie 60 proc. ankietowanych przy logowaniu korzysta z dodatkowych zabezpieczeń w postaci podwójnego uwierzytelnienia lub wykorzystania danych biometrycznych. Wśród młodych w wieku 18–34 lata ten odsetek wynosi prawie 70 proc.

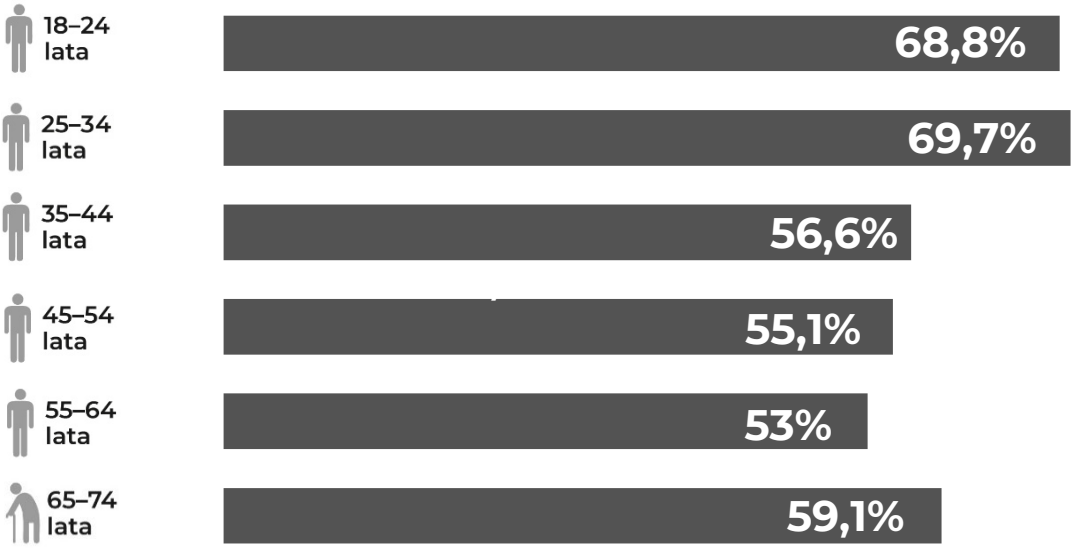
Wykres 11

Czy korzystasz z dodatkowych zabezpieczeń podczas logowania się do portali/bankowości internetowej, na przykład podwójnego uwierzytelniania lub wykorzystania danych biometrycznych?



Wykres 12

Korzystam z dodatkowych zabezpieczeń podczas logowania się do portali/bankowości internetowej, na przykład podwójnego uwierzytelniania lub wykorzystania danych biometrycznych



Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL/PL

Czasy, w których, żeby zabezpieczyć dane osobowe wystarczyło pilnować własnego portfela z dowodem osobistym już dawno minęły. Dzisiaj nośnikami wrażliwych informacji są prawie wszystkie urządzenia elektroniczne, z których korzystamy. Wraz z rozwojem technologii wyzwań w zakresie cyberbezpieczeństwa będzie tylko przybywać. Nie zmieniło się jedno. Nadal jedną z najważniejszych zasad, którą powinniśmy stosować jest zachowanie ostrożności i zdrowego rozsądku. Na nic bowiem zdadzą się skomplikowane hasła, aktualne oprogramowanie oraz narzędzia do podwójnego uwierzytelnienia podczas logowania, jeśli sami będziemy udostępniać nasze dane w sieci, np. poprzez publikacje zdjęć dokumentów lub jeśli w wyniku braku ostrożności pobierzemy i zainstalujemy szkodliwe oprogramowanie. Człowiek jest istotnym elementem systemu ochrony, niestety jednym z najbardziej zawodnych. Ostatecznie musimy zdawać sobie sprawę również, że nie wszystko, co dzieje się w przestrzeni wirtualnej mamy wpływ, np. na zabezpieczenia baz danych, w których gromadzone są nasze dane osobowe. Dlatego warto monitorować swoją aktywność kredytową w biurze informacji gospodarczej. Dzięki temu będziemy wiedzieć, gdy ktoś spróbuję wykorzystać nasze dane osobowe.

Autorzy raportu

ChronPESEL.pl – misją serwisu ChronPESEL.pl jest zwiększenie poziomu bezpieczeństwa i ograniczenie ryzyka wystąpienia negatywnych konsekwencji utraty danych osobowych oraz kradzieży tożsamości. Korzystając z najnowszych rozwiązań technologicznych, ChronPESEL.pl monitoruje w czasie rzeczywistym potencjalne próby wyłudzeń, dzięki czemu można im zapobiegać z dużo większą skutecznością. Prowadzi również aktywne działania edukacyjne mające na celu zwiększenie świadomości aktualnych zagrożeń oraz poznanie zasad bezpieczeństwa.

Krajowy Rejestr Długów Biuro Informacji Gospodarczej – najstarsze i największe biuro informacji gospodarczej w Polsce działające od 4 sierpnia 2003 roku pod nadzorem Ministerstwa Rozwoju i Technologii. Lider na rynku informacji gospodarczej, administrujący bazą danych o 2,7 mln dłużników. Z usług KRD korzysta blisko 930 tysięcy przedsiębiorców i konsumentów, którzy rocznie pobierają 34 miliony raportów gospodarczych. KRD BIG SA wchodzi w skład Kaczmarski Group, do którego należą również takie firmy i marki, jak: firma windykacyjna Kaczmarski Inkasso, Rzetelna Firma, Kancelaria Prawna VIA LEX, firma faktoringowa NFG, ChronPESEL.pl oraz Easy Check.

Prezes Urzędu Ochrony Danych Osobowych jest organem nadzorczym powołanym do przestrzegania przepisów RODO. Wykonuje swoje zadania przy pomocy Urzędu Ochrony Danych Osobowych. Niezależność Prezesa UODO i kierowanego przez niego Urzędu jest gwarantowana przez ogólne rozporządzenie o ochronie danych osobowych.

Zadania Prezesa UODO określa RODO, do których należy m.in.: monitorowanie i egzekwowanie stosowania rozporządzenia ogólnego o ochronie danych; upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych; upowszechnianie wśród administratorów i podmiotów przetwarzających wiedzy o obowiązkach spoczywających na nich na mocy RODO; rozpatrywanie skarg wniesionych przez osoby, których dane dotyczą; analiza naruszeń u administratorów; prowadzenie postępowań administracyjnych w związku z ochroną danych osobowych. Do uprawnień organu nadzorczego należy m.in. nakładanie kar pieniężnych (art. 58 RODO). Jednak karanie administratorów danych nie jest celem samym w sobie. Dlatego UODO w pierwszej kolejności – jeśli w ogóle jest taka potrzeba – korzysta z takich uprawnień, jak upomnienia, ostrzeżenia czy wezwania do przywrócenia stanu, w którym przetwarzanie danych odbywa się zgodnie z prawem.

Prezes Urzędu jest również członkiem Europejskiej Rady Ochrony Danych Osobowych.

Kontakt dla mediów:

ChronPESEL.pl **Jan Garnecki** | media@chronpesel.pl
Krajowy Rejestr Długów BIG SA **Andrzej Kulik** | media@krd.pl
Urząd Ochrony Danych Osobowych **Adam Sanocki** | rzecznikprasowy@uodo.gov.pl