CHRONPESEL.PL

URZĄD OCHRONY DANYCH OSOBOWYCH

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków – raport z badań

I kwartał 2021 r.

Spis treści

Jan Nowak
prezes Urzędu Ochrony Danych Osobowych

Publikacja raportu „Zagrożenia dla bezpieczeństwa i ochrony danych zdaniem Polaków" zbiega się z trzecią rocznicą stosowania ogólnego rozporządzenia o ochronie danych osobowych (RODO). Rozporządzenie to bezpośrednio obowiązuje od 25 maja 2018 roku we wszystkich państwach członkowskich Unii Europejskiej, regulując prawa obywateli i obowiązki administratorów danych.

Mimo że w Polsce regulacje w zakresie ochrony danych osobowych obowiązują od ponad 20 lat, a RODO nie zmieniło ich w sposób istotny, to wprowadziło pewne nowe rozwiązania, które podniosły poziom ochrony danych osobowych.

Doświadczenia zebrane przez UODO w ciągu trzech lat stosowania RODO uwidoczniły, że świadomość obywateli i administratorów danych osobowych jest na coraz wyższym poziomie. Potwierdza to ilość skarg na administratorów danych. W 2017 roku, czyli jeszcze przed RODO, było ich około 2,9 tys. Rok później było już ponad 5,5 tys. skarg, a w 2019 roku ponad 9,3 tys. Rok 2020 był szczególnym. Pomimo ogólnoświatowej pandemii i skierowania wszystkich sił na walkę z rozprzestrzenianiem się koronawirusa, liczba skarg kierowanych do UODO co prawda zmalała, ale była nadal bardzo wysoka (ponad 6,4 tys. skarg). Ponadto w całym 2020 roku do UODO wpłynęło łącznie ponad 7,5 tys. naruszeń od administratorów danych. Wśród nich odnotowano m.in. wycieki danych np., które nastąpiły w skutek zastosowania niewystarczających zabezpieczeń czy błędów ludzkich.

Wyniki raportu pokazują, że pomimo, iż co czwarty Polak boi się ataku cyberprzestępców, a ponad 43 proc. ankietowanych uważa, że największe zagrożenie dla danych osobowych w czasie pandemii stanowi działalność oszustów, to jednocześnie, aż 84 proc. respondentów z tej grupy zadeklarowało, że potrafi rozpoznać fałszywą wiadomość, której nadawca chce wyłudzić dane osobowe. Cieszy również fakt, że ponad 61 proc. badanych deklaruje, że wie, jakie działania należy podjąć w przypadku kradzieży danych osobowych.

Niestety, z przeprowadzonych badań wynika, że 22 proc. nigdy nie zmienia hasła do konta bankowego. Ponadto sporo osób nie wie, co robić, gdy doszło do wycieku ich danych.

Niniejszy raport pokazuje, że wiele w zakresie ochrony danych osobowych i podnoszenia świadomości społeczeństwa zostało już zrobione, ale uświadamia też, że wiele pracy nadal jest przed nami.

Zapraszam do zapoznania się z publikacją.

Adam Łącki
prezes Zarządu Krajowego Rejestru Długów
Biura Informacji Gospodarczej SA

Od początku pandemii obserwujemy wzmożoną aktywność oszustów próbujących wyłudzić nasze dane osobowe. Przestępcy stosują przeróżne metody, żeby osiągnąć swój cel. Dlatego oprócz zadbania o swoje zdrowie, powinniśmy również zrobić wszystko, żeby zapewnić bezpieczeństwo naszym danym osobowym. Jak się okazuje, wiele z potrzebnych działań, które pomogą nam lepiej się chronić, możemy podjąć sami. Można więc powiedzieć, że bezpieczeństwo danych osobowych jest w naszych rękach.

Serwis ChronPESEL.pl i Krajowy Rejestr Długów przeprowadzili pod patronatem Urzędu Ochrony Danych Osobowych badanie sprawdzające stan wiedzy Polaków na temat zagrożeń związanych z bezpieczeństwem w cyberprzestrzeni. Poniższy raport prezentuje jego wyniki.

Jak się okazuje, nadal bardzo duża część społeczeństwa ma problemy z podjęciem właściwych działań w przypadku ataku hakerów na nasze komputery lub telefony oraz wycieku danych z serwisów, w których mamy konto. Zastanawiające jest również lekkomyślne podejście do zabezpieczeń haseł do logowania. Wiele osób rzadko lub wcale ich nie zmienia oraz, co bardziej niepokojące, nie przykłada dużego znaczenia do trudności haseł i używa ich wielokrotnie do logowania w kilku serwisach na raz.

Podobnie, jak w pierwszym naszym raporcie poświęconym tematowi bezpieczeństwa danych osobowych w czasie pandemii, również i tym razem widać lepsze przygotowanie młodszych grup respondentów, którzy wiedzą, jak powinni zareagować w sytuacji wycieku lub ataku hakerów. Wśród nich widać także wysoką świadomość zagrożenia, co zawsze pomaga w przedsięwzięciu potrzebnych środków ochrony. Dlatego młodsze pokolenie, które ma odpowiednią wiedzę i umiejętności, powinno zadbać o swoich bliskich, pomóc im identyfikować zagrożenie i właściwie reagować w sytuacjach, w których ktoś będzie próbował ich oszukać. Tylko w ten sposób, dzięki współpracy międzypokoleniowej, będziemy w stanie ograniczyć skutki działalności oszustów wyłudzających dane osobowe.

Poniższa publikacja oprócz analizy wyników badania zawiera również komentarze i wskazówki ekspertów na co dzień zajmujących się ochroną danych osobowych.

Zachęcam do lektury.

O badaniu

Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych zostało przeprowadzone w marcu 2021 roku metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International.

Główne wnioski

25%

Blisko co czwarty Polak
boi się, że w czasie pandemi padnie ofiarą hakerów wyłudzających dane osobowe. Dotyczy to nawet 32,5 proc. najmłodszych respondentów.

33%

Ponad 33 proc. respondentów
uważa, że największym zagrożeniem dla bezpieczeństwa ich danych osobowych są wycieki danych z firm prywatnych i instytucji publicznych.

61%

61,2 proc. badanych
deklaruje, że wie, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych. Najlepiej przygotowani do takich sytuacji są ludzie młodzi w wieku między 18 a 24 lata.

54%

53,8 proc. ankietowanych
nie wie lub nie jest pewna, jakie działania należy podjąć w przypadku wycieku danych z serwisu internetowego, w którym mają konto.

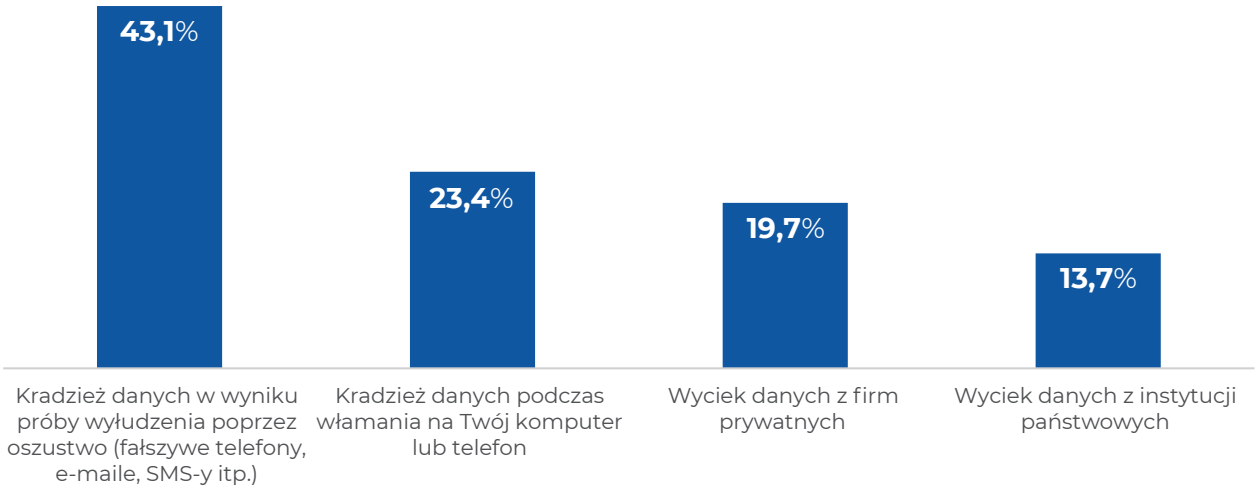
64%

63,9 proc. osób badanych
deklaruje, że używa bardzo trudnych lub trudnych haseł dostępu do serwisów. Równocześnie 22 proc. respondentów nigdy nie zmieniło hasła do konta bankowego.

Co czwarty Polak boi się ataku cyberprzestępców

Ponad 43 proc. ankietowanych uważa, że największe zagrożenie dla danych osobowych w czasie pandemii stanowi działalność oszustów próbujących wyłudzić dane osobowe. Równocześnie aż 84 proc. respondentów z tej grupy zadeklarowało w przeprowadzonym badaniu, że potrafi rozpoznać fałszywą wiadomość. Jednocześnie blisko co czwarty ankietowany (23,4 proc.) najbardziej obawia się tego, że padnie ofiarą ataku hakerów na komputer lub telefon oraz wycieku danych z bazy instytucji państwowej lub prywatnej firmy.

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



Ataku hakerów znacznie częściej obawiają się najmłodsi respondenci (32,5 proc.). Włamania na komputer lub telefon rzadziej obawiają się z kolei osoby w wieku 55–64 lata (19,5 proc.) oraz najstarsza grupa ankietowanych (17 proc.). Ta statystyka obrazuje stan świadomości istnienia takich zagrożeń. W tym wypadku większe obawy oznaczają wiedzę na temat konsekwencji działalności cyberprzestępców.

Wycieku danych osobowych z bazy firmy prywatnej najbardziej boją się osoby w wieku 35–44 lata (23,4 proc.). Najmniejsze zaufanie do zabezpieczeń stosowanych w instytucjach publicznych mają z kolei respondenci między 55 a 64 r.ż. (20,5 proc.).

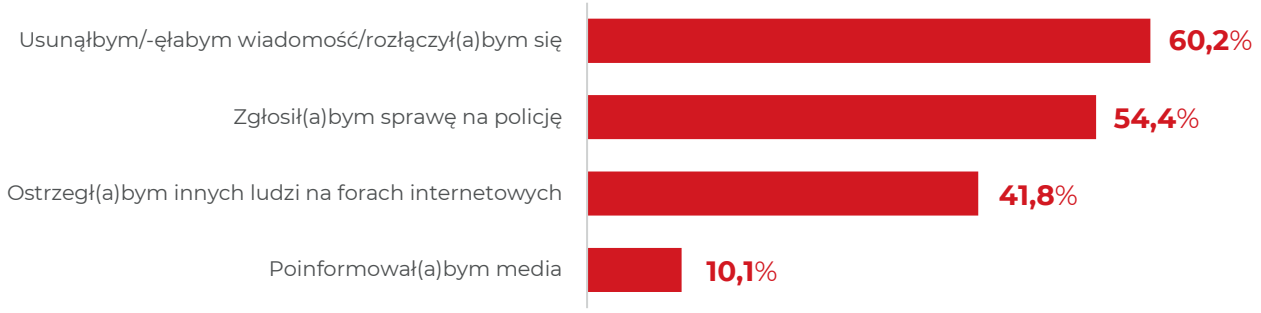
Zapytani o to, jak zareagowaliby w przypadku próby wyłudzenia danych osobowych, ankietowani najczęściej wskazywali na:

- usunięcie podejrzanej wiadomości lub rozłączenie się (60,2 proc.)
- głoszenie sprawy na policję (54,4 proc.)
- ostrzeżenie ludzi na forach internetowych (41,8 proc.).

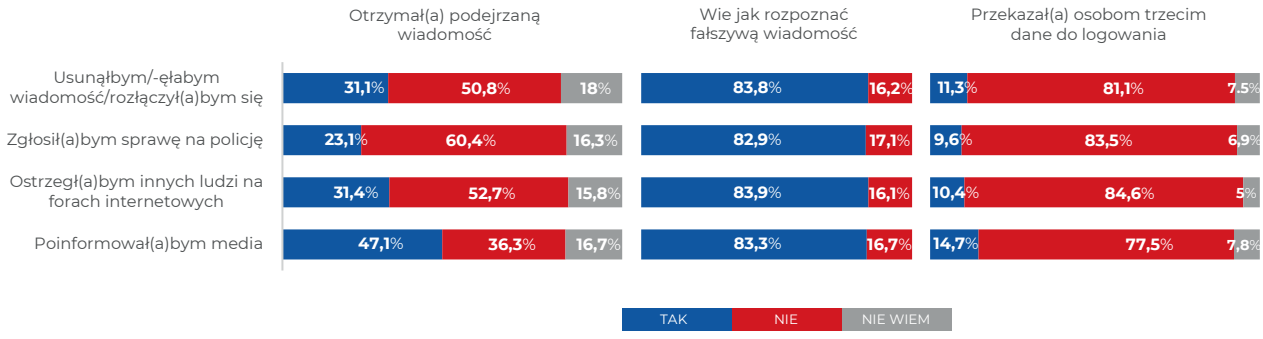
Na usunięcie podejrzanej wiadomości częściej zdecydowaliby się mężczyźni (64,8 proc. w stosunku do 55,9 proc. wśród kobiet) oraz najmłodsi (18–24 lata) i najstarsi respondenci (65–74 lat), gdzie odsetek pozytywnych odpowiedzi wyniósł odpowiednio 72,5 proc. oraz 70,9 proc.

Z deklaracji wynika, że na policję częściej zadzwonią osoby w wieku 45–54 lata (62 proc.), niż obywatele z najmłodszej grupy wiekowej (42,5 proc.). Z kolei na forach internetowych innych częściej ostrzegają kobiety (45,1 proc.) niż mężczyźni (38,3 proc.) i raczej rzadziej osoby z najstarszej grupy wiekowej (32,6 proc.).

Pytanie:
Jakie działania podjąłbyś/-ęłabyś, gdyby ktoś próbował wyłudzić Twoje dane osobowe?

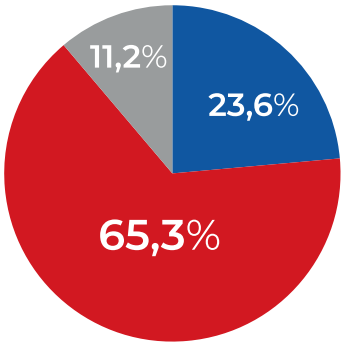


Jak wynika z przeprowadzonego badania, około 80 proc. osób z tych grup, deklaruje, że wie, jak rozpoznać fałszywą wiadomość oraz około 80 proc. z nich nie przekazuje osobom trzecim danych do logowania. Badani, którzy w czasie pandemii otrzymali podejrzaną wiadomość najczęściej deklarowali, że przy próbie wyłudzenia ich danych osobowych, usunęliby wiadomość (64,4 proc.), ostrzegliby innych na forach (45,1 proc.) oraz zgłosili sprawę na policję (43,4 proc.).

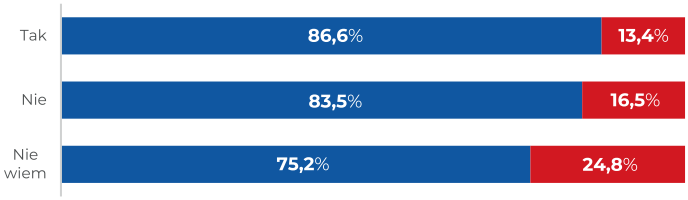


Prawie co czwarty badany (23,6 proc.) deklaruje, że podczas rozmowy telefonicznej został poproszony o swoje dane. Z udzielonych odpowiedzi wynika jednak, że większość tych osób (86,6 proc.) potrafi rozpoznać fałszywą wiadomość. Takie sytuacje najrzadziej zdarzały się osobom z najstarszej grupy wiekowej 65–74 lat (12,8 proc.).

Pytanie:
Czy zdarzyło się, że podczas rozmowy telefonicznej zostałeś/-aś poproszony/-a o Twoje dane, np. numer PESEL, numer i serię dowodu osobistego lub dane do logowania w bankowości elektronicznej?

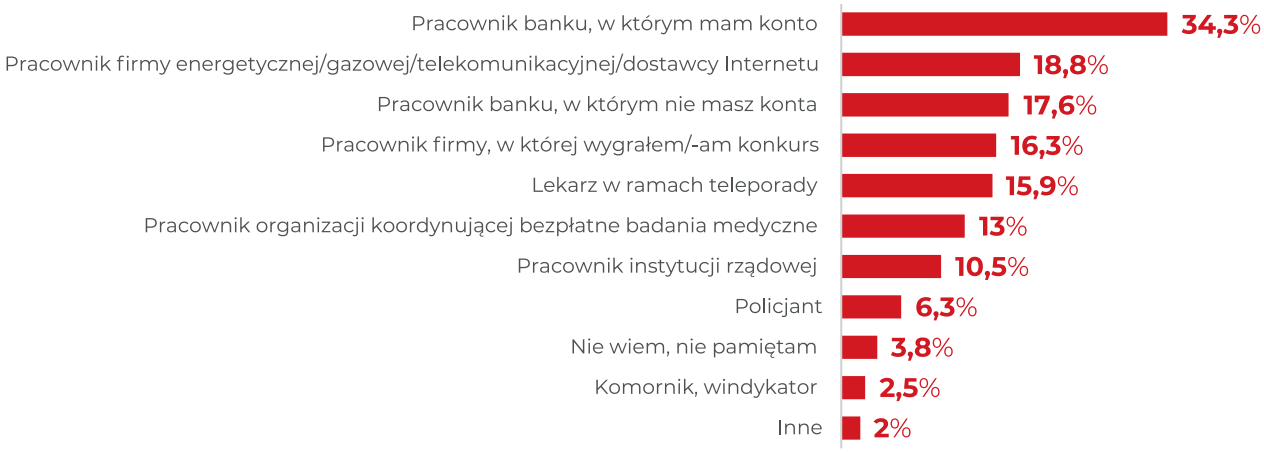


Wie, jak rozpoznać fałszywą wiadomość



Co trzeci ankietowany (34,3 proc.) wskazał, że sytuacja, w której został poproszony o dane osobowe dotyczyła rozmowy z pracownikiem banku, w którym ma konto. Jak wskazują badania, o takie informacje na temat rozmówcy w trakcie rozmowy telefonicznej prosili jeszcze m.in. przedstawiciele firm energetycznych, gazowych i telekomunikacyjnych oraz pracownicy banków, w których ankietowani nie mieli konta.

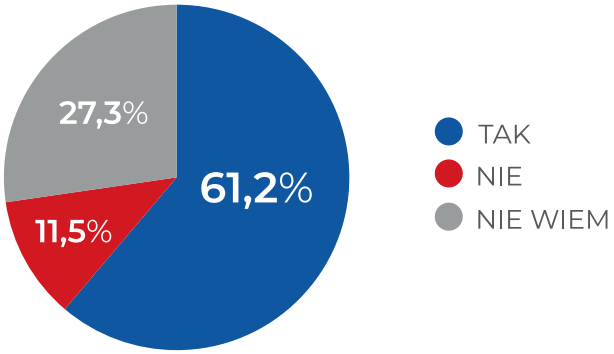
Pytanie:
Kto poprosił o Twoje dane, np. PESEL, numer i serię dowodu osobistego podczas rozmowy telefonicznej?



Polacy nie wiedzą, jak reagować w przypadku ataku hakerów lub wycieku danych

Blisko 2/3 dorosłych Polaków (61,2 proc.) deklaruje, że wie jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych. Jak wynika z przeprowadzonych badań, najlepiej przygotowani do takich sytuacji są ludzie młodzi w wieku między 18. a 24. r.ż. Blisko 74 proc. z nich zadeklarowało, że wie, jak zareagować w przypadku wyłudzenia lub kradzieży danych osobowych. Znacznie gorzej sytuacja wygląda wśród respondentów między 35. a 64. r.ż., wśród których niespełna 56 proc. wiedziałoby, jak się zachować.

Pytanie:
Czy wiesz, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych?



65,3 proc. osób, które zadeklarowały, że zostały poproszone o podanie danych osobowych, wie jakie działania należy podjąć w przypadku wyłudzenia danych. Jedna na pięć osób z tej grupy nie była pewna, jakie działania należy w takiej sytuacji podjąć. To pokazuje, że w edukacji nadal jest dużo do zrobienia.

Pytanie:
Czy zdarzyło się, że podczas rozmowy telefonicznej zostałeś/-aś poproszony/-a o Twoje dane?

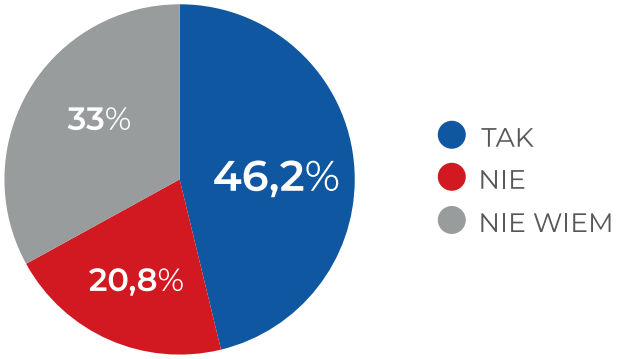
Najwięcej ankietowanych uważa, że w przypadku wyłudzenia lub kradzieży danych należy:
- zgłosić zdarzenia na policję (85,2 proc.)
- zgłosić zdarzenie w banku, w którym posiada się konto (69,7 proc.)
- zmienić dane do logowania (69,7 proc.).

Swojemu bankowi najbardziej ufają osoby w wieku 45–54 lata (74,7 proc.) oraz najstarsi respondenci (76,7 proc.).

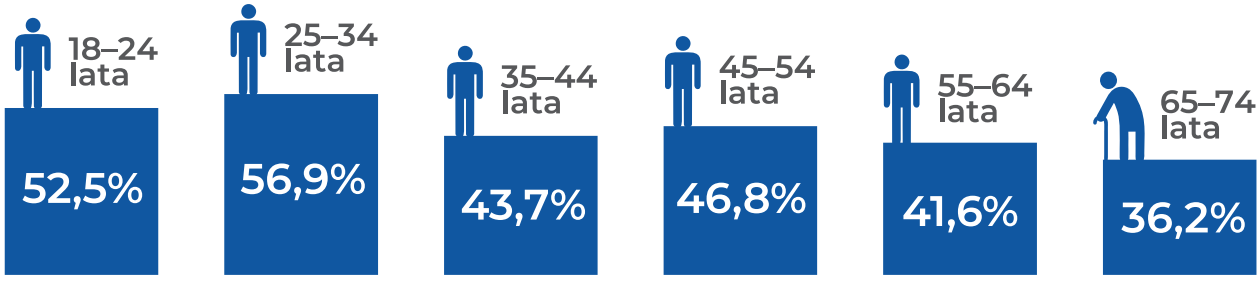
Pytanie:
Jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych?

Znacznie gorzej jesteśmy z kolei przygotowani do wycieków danych z serwisów internetowych, w których mamy konto. **Około połowy osób badanych (53,8 proc.) nie wie lub nie jest pewna, jakie działania należy podjąć w takim przypadku.** Swoją wiedzę na ten temat najlepiej oceniają osoby z najmłodszych grup, w których około połowa (52,6–56,9 proc.) uważa, że wie, jakie działania należy w takiej sytuacji podjąć. Poziom niezdecydowania w tej sprawie rośnie wraz z wiekiem.

Pytanie:
Czy wiesz, jakie działania należy podjąć w przypadku wycieku danych z serwisu, w którym miałeś konto?

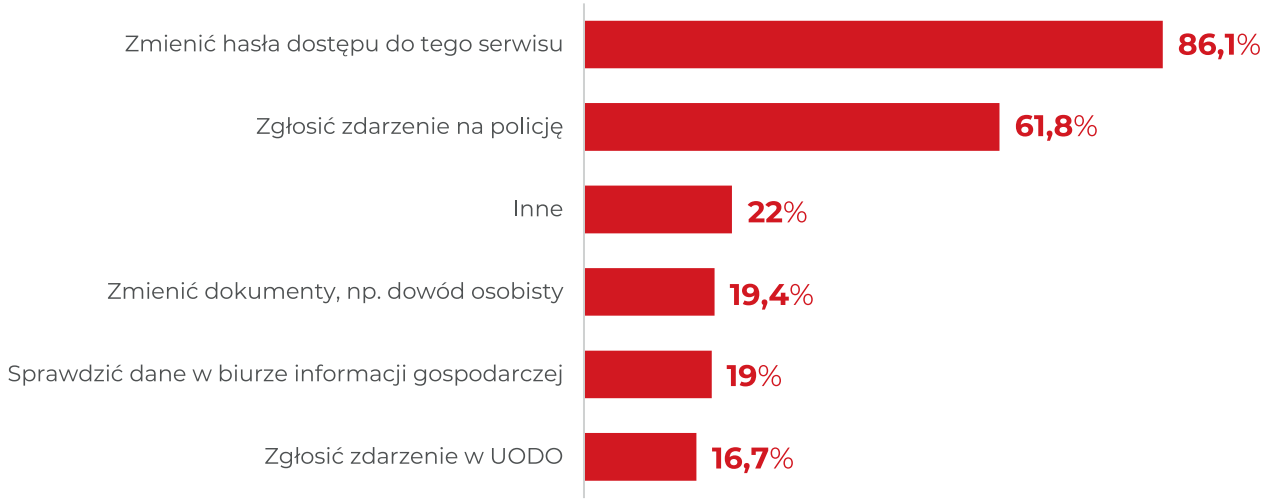


Wiem, co należy zrobić w przypadku wycieku danych z serwisu, w którym mam konto



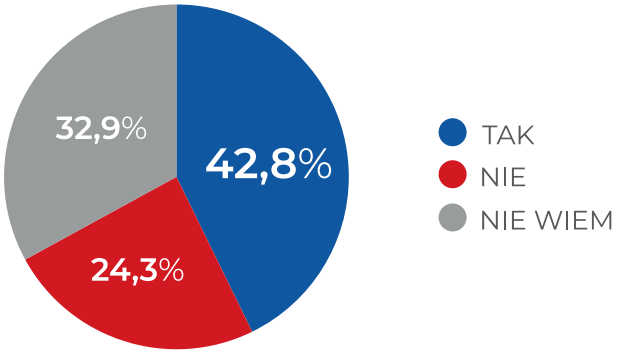
W przypadku wycieku lub kradzieży danych z serwisu większość badanych osób (86,1 proc.) zmieniłaby hasła dostępu do tego serwisu. Natomiast 61,8 proc. zgłosiłaby to zdarzenie na policję. Na taki ruch znacznie częściej zdecydowałyby się kobiety (68,4 proc. wobec 55,6 proc. wśród mężczyzn).

Pytanie:
Jakie działania należy podjąć w przypadku wycieku lub kradzieży danych z serwisu, w którym miałeś konto?

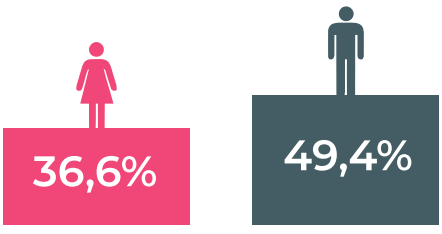


Problemów można się również spodziewać w sytuacji ataku cyberprzestępców, ponieważ **blisko 60 proc. (57,2 proc.) respondentów nie wie lub nie jest pewna, jakie działania należy podjąć w przypadku ataku hakerskiego.** W tym przypadku mężczyźni częściej niż kobiety wiedzą, jak powinni zareagować. Na taką sytuację lepiej przygotowane są również osoby młode. Pewność co do tego, jak powinno się zareagować spada wraz z wiekiem respondentów.

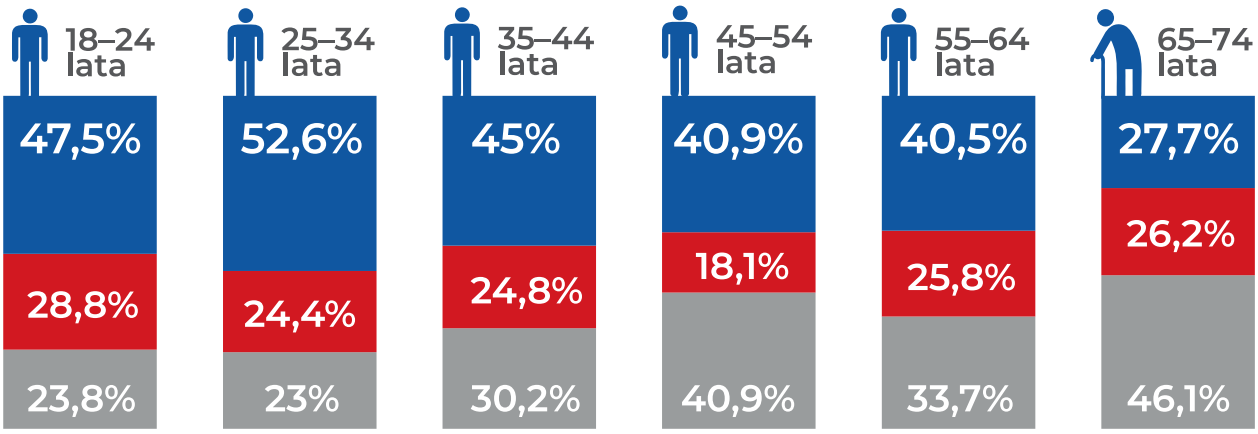
Pytanie:
Czy wiesz, jakie działania należy podjąć w przypadku ataku hakerskiego na komputer lub telefon?



Wiem, co należy zrobić w przypadku ataku hakerskiego



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



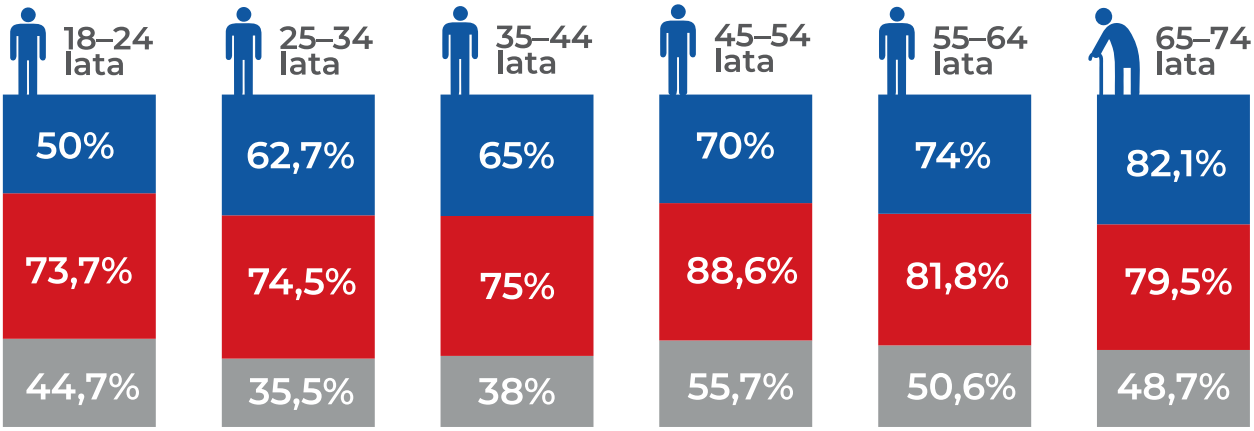
Najczęściej wybierane działania w przypadku ataku hakerskiego to:
- zmiana haseł (78,6 proc.)
- instalacja programu antywirusowego (67,1 proc.)
- zgłoszenie sprawy na policję (62,9 proc.).

Pytanie:
Jakie działania należy podjąć w przypadku ataku hakerskiego na komputer lub telefon?

Analizując odpowiedzi, można zauważyć różnice w podejściu do działań w zależności od płci oraz wieku osób badanych. Kobiety (68,9 proc.) częściej niż mężczyźni (58,2 proc.) zgłaszałyby takie zdarzenie na policję. Z kolei preferencja instalowania programu antywirusowego wzrasta wraz z wiekiem. Również zmianę hasła oraz zaktualizowanie systemu operacyjnego preferują w nieco większym stopniu osoby w średnim wieku i najstarsze.

Pytanie:
Jakie działania należy podjąć w przypadku ataku hakerskiego na komputer lub telefon?

- Zainstalować program antywirusowy
- Zmienić hasła do komputera lub telefonu
- Zaktualizować system operacyjny



Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL.pl

Wyniki przeprowadzonego badania jasno wskazują na to, że w edukacji o cyberbezpieczeństwie nadal mamy do wykonania wiele pracy. Za niepokojące należy uznać fakt, że ponad połowa respondentów nie wie, jak zareagować w przypadku wycieku danych z serwisu internetowego, w którym ma konto. Dodatkowo 1/3 społeczeństwa nie potrafi zareagować na inne próby wyłudzenia danych osobowych. Pozytywnym wyjątkiem są najmłodsze grupy ankietowanych, wśród których świadomość właściwych zachowań jest najwyższa. O tym, że działalność cyberprzestępców to realny problem, świadczą nie tylko ostrzeżenia specjalistów, ale również wyniki omawianego badania. Jak wynika z raportu, ataku hakerów na sprzęt elektroniczny w czasie pandemii boi się co czwarty Polak. 1/3 badanych jako największe zagrożenie wskazała z kolei wycieki z niewłaściwie zabezpieczonych baz danych. Potraktujmy to nie tylko jako wyraźne ostrzeżenie, ale także jako sygnał, w którym kierunku powinniśmy iść i jak rozłożyć akcenty w zakresie edukacji na temat ochrony danych osobowych.

Zdaniem eksperta

Monika Krasińska
Dyrektor Departamentu Orzecznictwa i Legislacji w UODO

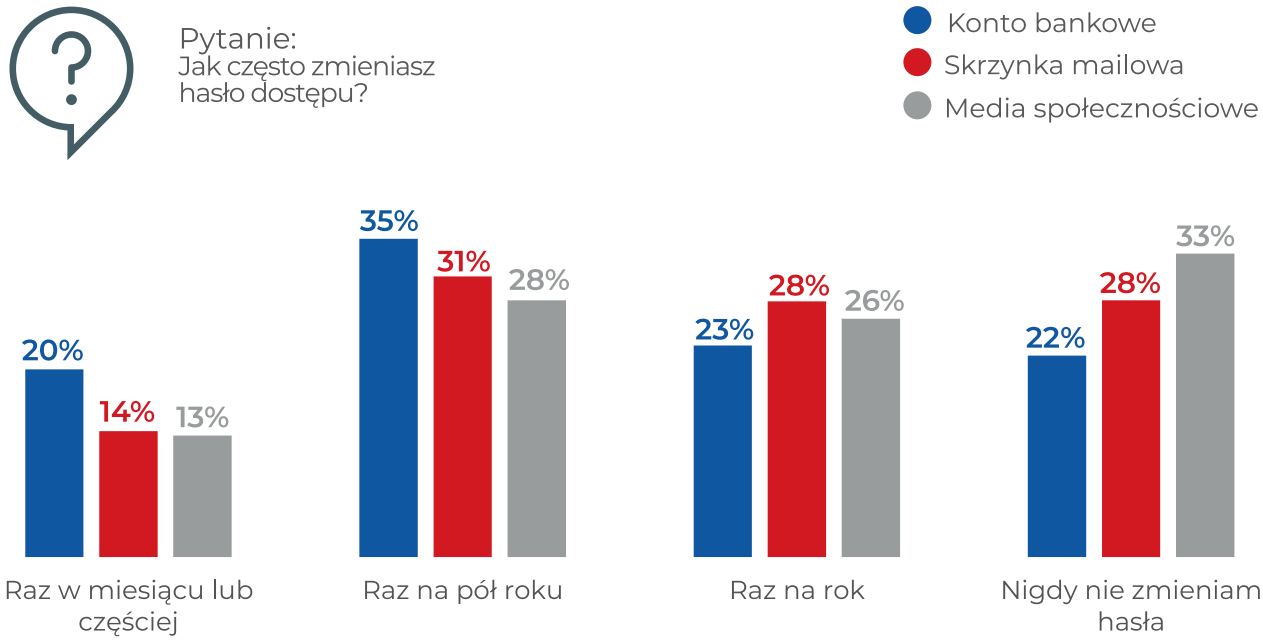
Część osób błędnie sądzi, że wówczas, gdy dojdzie do kradzieży ich tożsamości, powinny zgłaszać się do Urzędu Ochrony Danych Osobowych (UODO), który zajmie się ustaleniem i ukaraniem sprawcy, a także podejmie działania mające chronić ich przed negatywnymi konsekwencjami utraty danych. Tymczasem kradzież tożsamości to przestępstwo, które jak najszybciej należy zgłaszać na policję. UODO nie jest organem ścigania – nie ma ani uprawnień, ani odpowiednich narzędzi, aby ustalić, kto jest sprawcą tego typu działań. Jeżeli podmiot lub osoba, które w nielegalny sposób posługują się naszymi danymi, nie są nam znane, ich tożsamość powinna ustalić policja. Urząd Ochrony Danych Osobowych rozpatruje skargi, ale na działanie konkretnego, wskazanego w skardze administratora, który niewłaściwie przetwarza dane osoby skarżącej. UODO – gdy to niezbędne - może przeprowadzić u niego kontrole, a gdy stwierdzi naruszenie, skorzystać ze środków naprawczych czy nałożyć karę pieniężną. Kary finansowe nakładane przez Prezesa UODO to tylko jeden z wielu instrumentów oddziaływania, jakimi dysponuje organ nadzoru. Inne to m.in.: ostrzeżenia, upomnienia czy nakazy dostosowania określonych działań do obowiązujących przepisów. Korzystamy z nich stosownie do ustaleń poczynionych w toku prowadzonych postępowań.

Ponad 1/5 obywateli nie zmienia haseł do logowania w banku

Jedynie co piąta osoba (20,4 proc.) zmienia hasło do konta bankowego raz w miesiącu lub częściej, około 1/3 osób (34,6 proc.) zmienia tam hasło raz na pół roku. **Natomiast 22 proc. nigdy nie zmienia hasła do konta bankowego.**

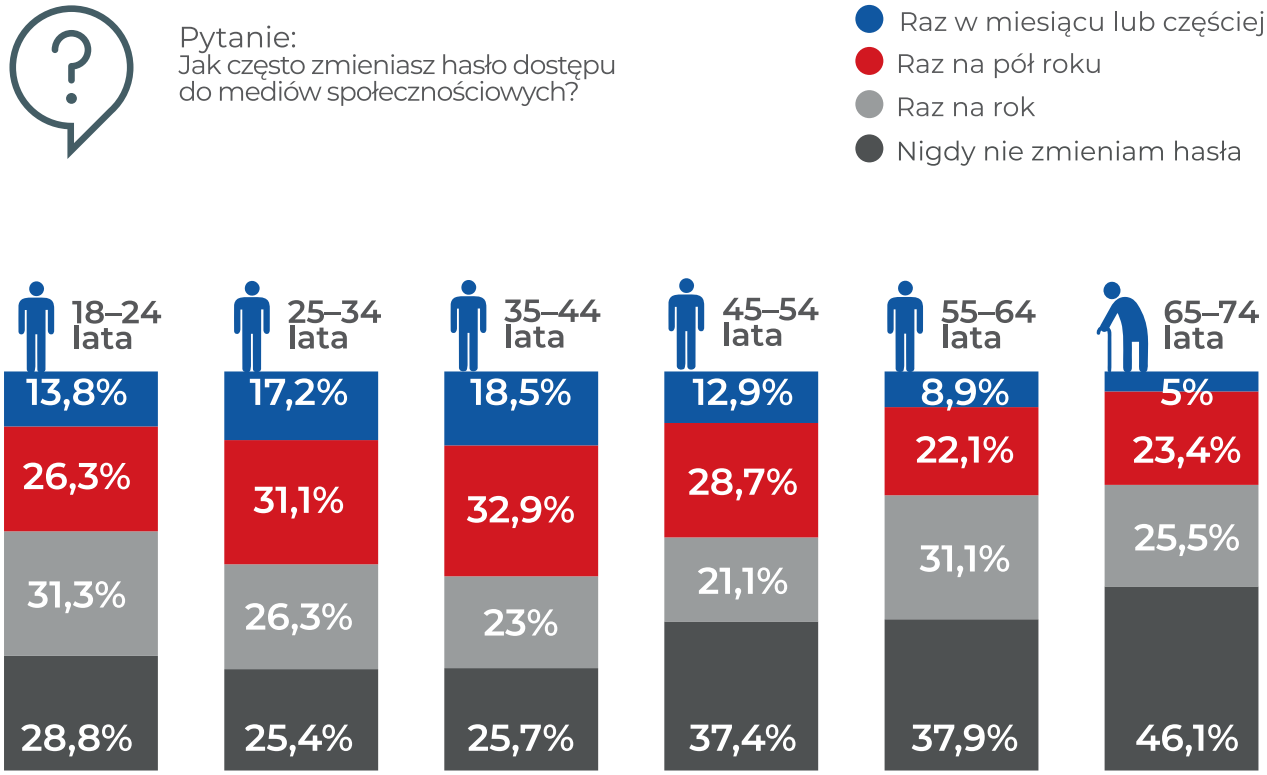
Jeszcze rzadziej robimy to w przypadku haseł do skrzynki mailowej i portali społecznościowych. Nieco mniej niż 1/3 osób zmienia hasło do swojej poczty elektronicznej raz na pół roku, podobny odsetek osób zmienia hasło raz na rok lub wcale. 33 proc. badanych nigdy nie zmieniło danych do logowania w serwisach społecznościowych. Nieco mniejszy odsetek zmienia hasło raz na pół roku lub raz na rok.

Pytanie:
Jak często zmieniasz hasło dostępu?



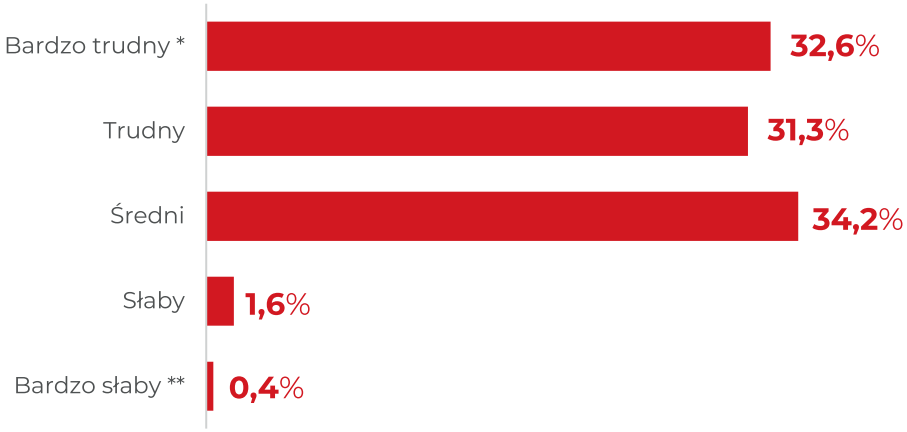
Analizując odpowiedzi, widać, że mężczyźni (53,6 proc.) nieco częściej niż kobiety (46,4 proc.) deklarują, że nigdy nie zmieniają hasła do mediów społecznościowych. Równocześnie osoby w średnim wieku proporcjonalnie częściej aktualizują dane dostępu do mediów społecznościowych. Najrzadziej, jak wynika z przeprowadzonego badania, hasła do logowania w serwisach społecznościowych zmieniają najstarsze osoby.

Pytanie:
Jak często zmieniasz hasło dostępu do mediów społecznościowych?



Blisko 2/3 badanych (63,9 proc.) deklaruje, że używa bardzo trudnych lub trudnych haseł dostępu do serwisów.

Pytanie:
Jak ocenił(a)byś stopień trudności Twoich haseł dostępu do, np.: komputera, portali internetowych, kont bankowych?



* co najmniej 8 liter, duże litery, cyfry, znaki specjalne

** bez dużych liter, cyfr, znaków specjalnych

Respondenci należący do dwóch najmłodszych grup wiekowych proporcjonalnie częściej deklarują używanie bardzo trudnych haseł dostępu:

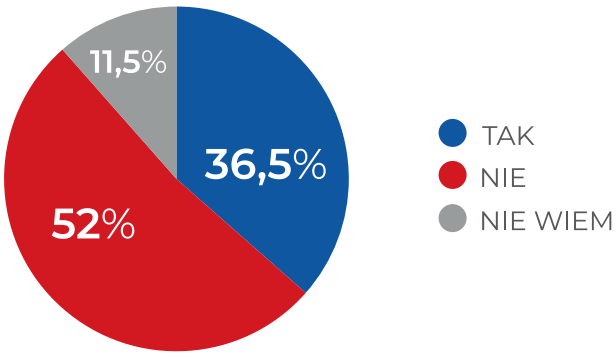
- 18–24 (50 proc.)
- 25–34 (38,8 proc.).

Mniej niż 1/3 osób z pozostałych grup wiekowych używa bardzo trudnych haseł. Osoby w wieku od 35 do 74 lat (35-40 proc.) częściej niż osoby od 18 do 34 r.ż. (20–25 proc.) używają średnich haseł dostępu.

Osoby, które nigdy nie zmieniają haseł do konta bankowego, poczty elektronicznej oraz portali społecznościowych, w około 60 proc. deklarują, że ich hasła są trudne lub bardzo trudne.

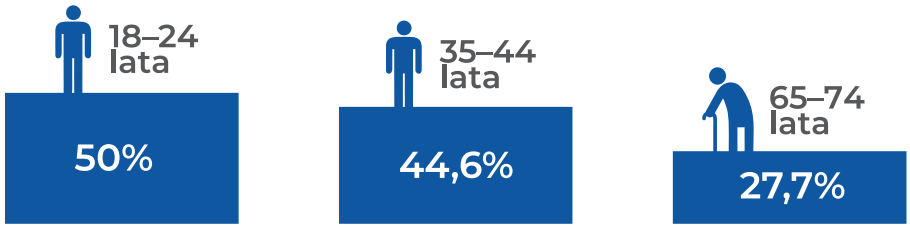
Niepokoić może z kolei fakt, że nieco ponad 1/3 (36,5 proc.) osób badanych wykorzystuje jednakowe hasła w różnych serwisach.

Pytanie:
Czy wykorzystujesz jednakowe hasło w kilku serwisach?



Najczęściej jednakowe hasła wykorzystuje najmłodsza grupa respondentów. Najrzadziej robią to osoby najstarsze w wieku 65–74 lata.

Wykorzystuję jednakowe hasło w kilku serwisach



Około 20 proc. osób, które korzystają z jednakowych haseł w różnych serwisach deklaruje, że przekazało kiedyś swoje dane do logowania osobom trzecim.

Wśród osób, które korzystają z jednakowych haseł w kilku serwisach 1/3 nigdy nie zmieniła hasła do konta bankowego, ponad 1/3 (37,3 proc.) nigdy nie zmieniła hasła skrzynki mailowej, a 40,3 proc. nie aktualizowało nigdy danych do logowania w mediach społecznościowych.

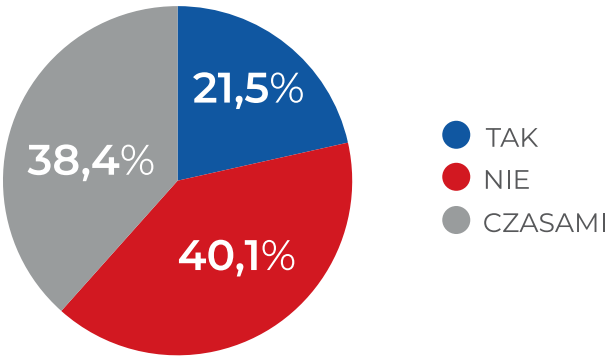
Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL.pl

Korzystanie z silnych haseł to warunek konieczny do tego, żeby chronić swoją tożsamość w sieci. Na szczęście jest kilka sprawdzonych sposobów na to, żeby utrudnić zadanie cyberprzestępcom próbującym włamać się na nasze konto. Tworząc silne hasło, powinniśmy przede wszystkim unikać zwrotów, które mogą być łatwe do odgadnięcia, np. „12345", „jedendwatrzy", „qwerty" oraz imion i nazwisk osób bliskich lub zwierząt domowych. Silne hasło powinno składać się z kilkunastu znaków i być odpowiednio złożone. Konstruując je, powinniśmy zadbać o to, by składało się z dużych i małych liter, liczb i znaków specjalnych. W ten sposób można zapisać łatwe do zapamiętania zwroty, np. „mam pomysł" jako „M@mP0my$1". Pamiętajmy, żeby nie używać jednego hasła do kilku witryn. W takim wypadku wystarczy bowiem złamać je raz, żeby zyskać dostęp do wszystkich naszych danych. Nie należy przesadzać z częstotliwością zmiany hasła, ponieważ trudno nam będzie co chwilę wymyślać coś skomplikowanego i będziemy bardziej skłonni do wybierania drogi na skróty lub zapisywania ich w niezabezpieczonych miejscach. Bezwzględnie należy je jednak zmienić w sytuacji, w której mamy chociaż cień podejrzenia, że ktoś mógł nam je wykraść.

Nieco ponad połowa respondentów (59,9 proc.) zapisuje hasła do komputera, telefonu lub serwisów.

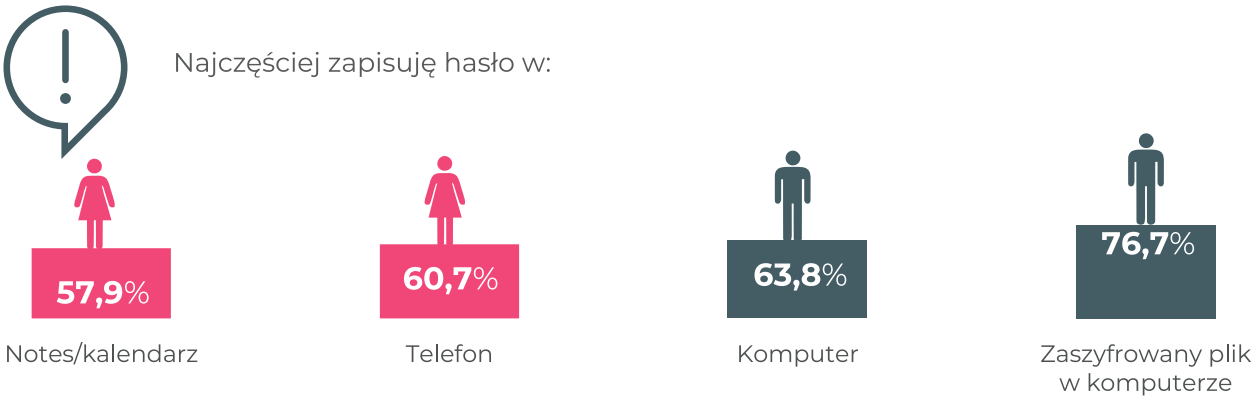
Pytanie:
Czy zapisujesz hasła dostępu do komputera, telefonu lub serwisów?

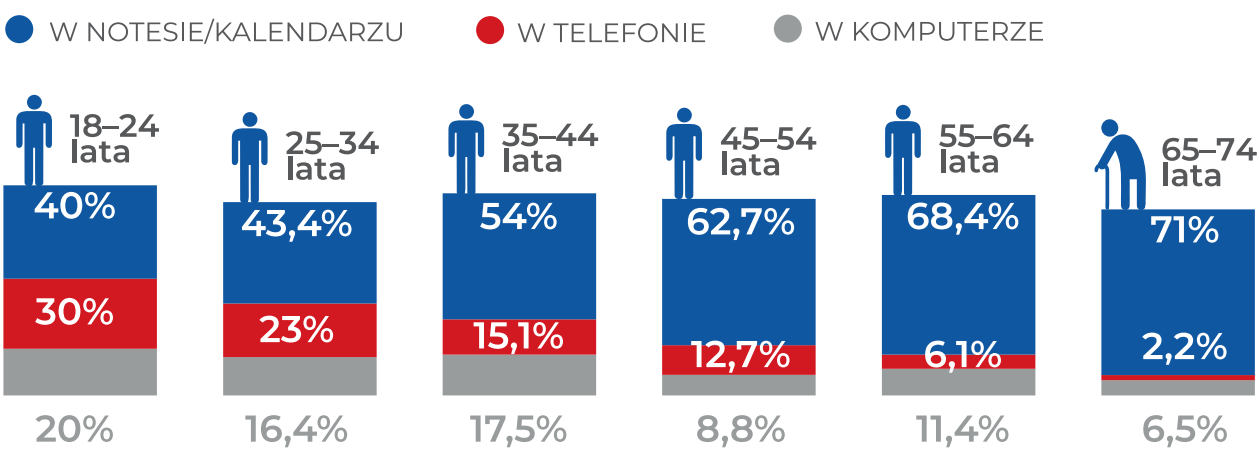


Blisko 60 proc. ankietowanych (57,5 proc.) swoje hasła do logowania zapisuje w notesie lub kalendarzu. Można zauważyć, że preferencja notesu lub kalendarza wzrasta wraz z wiekiem respondentów. Natomiast wybór telefonu lub komputera z wiekiem spada (co obrazuje tabela z wiekiem, przedstawiona niżej). Poza tym notes/kalendarz lub telefon nieco częściej wybierają kobiety. Z kolei mężczyźni nieco częściej preferują zapisanie hasła w komputerze oraz stanowią większość osób wybierających zaszyfrowany plik w komputerze.

Pytanie:
Gdzie zapisujesz hasła dostępu do komputera, telefonu lub serwisów?

Najczęściej zapisuję hasło w:





Zdaniem eksperta

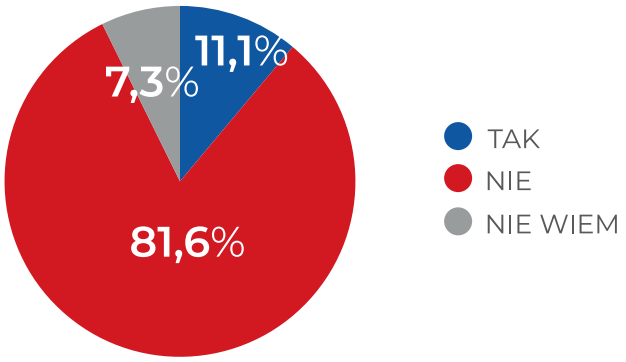
Monika Krasińska
Dyrektor Departamentu Orzecznictwa i Legislacji w UODO

Podawanie swoich danych do logowania, a więc także hasła, innym osobom to bardzo niebezpieczna praktyka. Tym bardziej gdy stosuje się jedno hasło w kilku miejscach, co również nie jest prawidłowe. Dla własnego bezpieczeństwa warto stosować różne hasła do różnych portali i systemów i nie udostępniać ich innym osobom. Nie powinno się też zapisywać ich na kartce papieru czy w notesie. Najlepiej jest je zapamiętywać, co jest dużą sztuką, gdy musimy logować się do wielu serwisów. Pomocne w tym zakresie mogą być tzw. menadżery haseł (także darmowe), które umożliwiają nie tylko generowanie odpowiednio trudnych do złamania haseł, ale i zapamiętują je za nas. Tym samym łatwiejsza jest częstsza zmiana haseł, a ryzyko, że ktoś je pozna maleje. Innym dobrym rozwiązaniem jest zapisywanie haseł w zaszyfrowanych plikach na swoich komputerach. Jednak to rozwiązanie może się sprawdzić po spełnieniu kilku warunków. Przede wszystkim komputer musi być chroniony silnym hasłem, które zapamiętamy, a do urządzenia nie mają dostępu inne osoby.

Nie daj się nabrać – jak się chronić?

Większość badanych (81,6 proc.) nie przekazuje swoich danych do logowania osobom trzecim. Najczęściej robią to osoby młodsze (28,8 proc.). Wraz z wiekiem ta tendencja spada. Najrzadziej swoje dane przekazują respondenci w najstarszych grupach wiekowych.

Pytanie:
Czy zdarzyło ci się przekazać osobom trzecim swoje dane do logowania?
(SMS, e-mail, Messenger lub ustnie)?



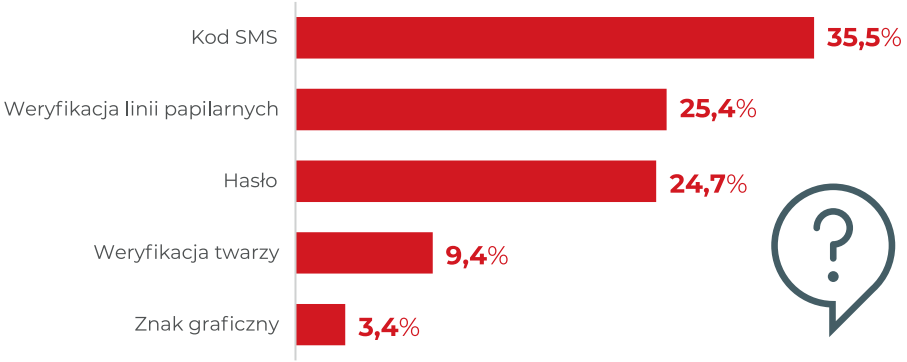
Zapytania o to, jaką formę logowania uważają za najbezpieczniejszą, respondenci najczęściej wskazują na:

- kod SMS (35,5 proc.)
- weryfikacja linii papilarnych (25,4 proc.)
- hasło (24,7 proc.).

Osoby badane niezależnie od różnic między sobą raczej zgadzają się względem tej hierarchii. Jednak analizując odpowiedzi, można zauważyć drobne różnice względem wieku i płci osób badanych. Na hasło jako najbezpieczniejszą formę logowania osoby w średnim wieku od 44 do 55 lat (29,2 proc.) wskazują częściej niż respondenci z dwóch najmłodszych grup wiekowych 18–24 (17,5 proc.) i 25–34 (19,1 proc.).

Spośród ankietowanych, którzy za najbezpieczniejszą formę uważają weryfikację twarzy 64,2 proc. stanowią kobiety.

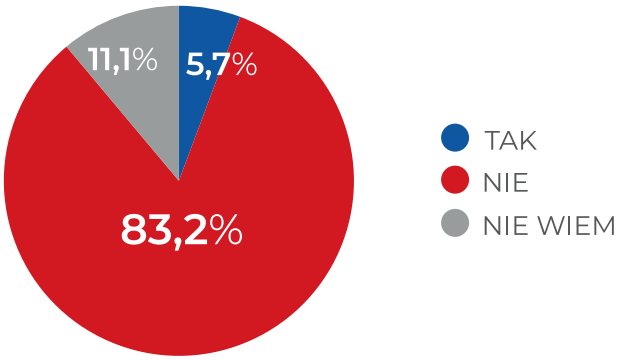
Z kolei weryfikację linii papilarnych wskazują raczej osoby młodsze w wieku 18–24 lata (35 proc.) niż z dwóch starszych grup 45–54 lata (22,8 proc.) i 65–74 lata (17,7 proc.) oraz badani w wieku od 55 do 64 lat (28,9 proc.).



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

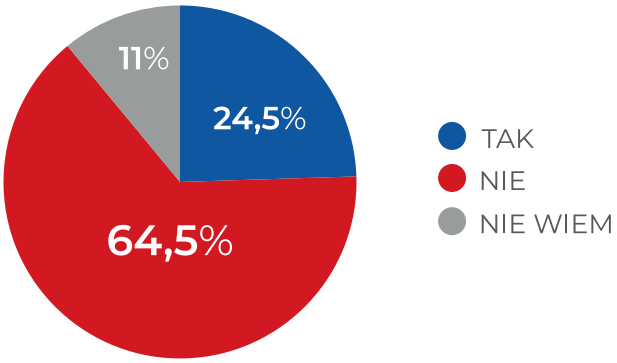
Sytuacje, w których w czasie zakupów w sieci sklep internetowy poprosił o numer PESEL zdarzają się bardzo rzadko (5,7 proc.). Częściej przytrafiły się mężczyznom (63,8 proc.) niż kobietom (36,2 proc.) oraz nieco częściej osobom młodszym od 18 do 24 lat (13,8 proc.) niż badanym z pozostałych grup wiekowych (od 3,5 proc. do 6,8 proc. z danej grupy).

Pytanie:
Czy spotkałeś/-aś się z sytuacją, gdy w czasie zakupów w sieci sklep internetowy poprosił o Twój numer PESEL?



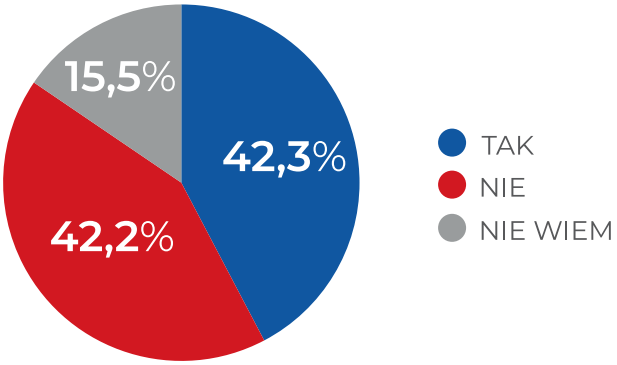
Jedynie 1/4 (24,5 proc.) osób badanych deklaruje, że zlikwidowała konto w nieużywanych przez siebie serwisach internetowych. W porównaniu z innymi, znacznie częściej zrobili to ankietowani z najmłodszej grupy 18–24 lata (36,3 proc.).

Pytanie:
Czy w okresie pandemii koronawirusa zlikwidowałeś konta w serwisach internetowych, z których od dawna nie korzystałeś?



Tyle samo osób (42,3 proc.) deklaruje uruchomienie i nie uruchomienie blokad antyspamowych w swoich prywatnych laptopach lub smartfonach w celu zwiększenia bezpieczeństwa swoich danych w czasie pandemii. Nieco częściej robili to mężczyźni (54,2 proc. względem 45,8 proc. wśród kobiet).

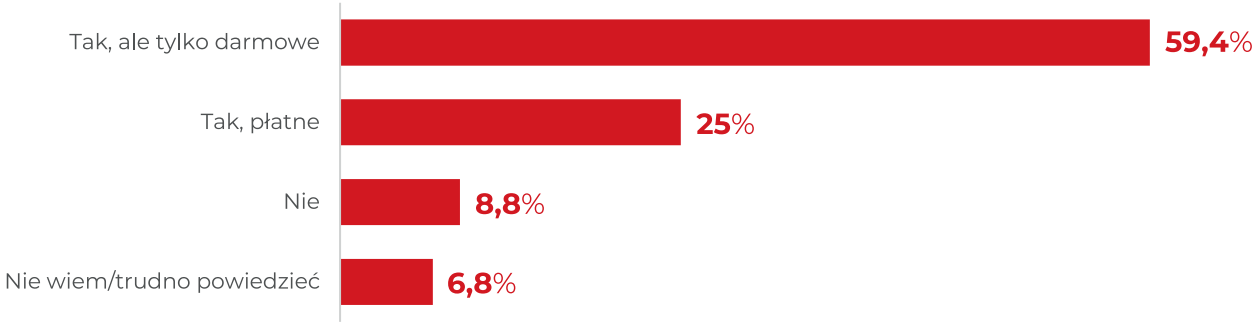
Pytanie:
Czy uruchomiłeś/-aś blokady antyspamowe w swoim prywatnym laptopie lub smartfonie w celu zwiększenia bezpieczeństwa swoich danych w czasie pandemii koronawirusa?



84,4 proc. badanych korzysta z aktualnego oprogramowania antywirusowego. Nieco ponad połowa respondentów wybiera jednak darmowe oprogramowanie, podczas gdy 1/4 badanych decyduje się na korzystanie z płatnych programów.

Różnice między respondentami najczęściej dotyczyły korzystania z darmowego lub płatnego oprogramowania antywirusowego. Na to drugie częściej decydowali się mężczyźni (55,7 proc.). Równocześnie blisko 2/3 ankietowanych (61,8 proc.), którzy nie używają aktualnego oprogramowania antywirusowego stanowią kobiety.

Pytanie:
Czy masz zainstalowane na komputerze osobistym aktualne oprogramowanie antywirusowe?



1/5 osób w wieku od 18 do 24 lat (20 proc.) nie korzysta z aktualnego oprogramowania. W innych grupach wiekowych ten odsetek jest o około 10 pp. niższy. Płatnego oprogramowania antywirusowego używa ponad 1/3 (37,5 proc.) osób z najstarszej grupy (65–74 lata) oraz 28,7 proc. ankietowanych w wieku 45–54 lat. W pozostałych grupach wiekowych to około 20 proc. respondentów.

Zdaniem eksperta

Bartłomiej Drozd
ekspert serwisu ChronPESEL.pl

Niestety, zapominając o podstawowych zasadach bezpieczeństwa, ułatwiamy cyberprzestępcom dostęp do naszych komputerów i narażamy na kradzież nasze dane osobowe. Odpowiednie zabezpieczenie komputera, tabletu lub telefonu, z którego na co dzień korzystamy, powinno być priorytetem. Musimy przy tym pamiętać, że ważniejsze od częstej zmiany haseł jest jego moc oraz to, żeby nie powtarzać go w innych serwisach. Nie wolno zapomnieć również o zachowaniu czujności podczas obecności w sieci. Zatem nie klikajmy w podejrzane linki otrzymane w e-mailach lub SMS-ach, a zakupy i transakcje bankowe róbmy tylko za pośrednictwem oficjalnych stron lub aplikacji. Nie stosując się do tych zasad, możemy narazić się na poważne konsekwencje. Korzystajmy również z programów antywirusowych, które zapewnią bezpieczeństwo w przypadku podstawowych zagrożeń, wysyłając ostrzeżenie przed pobraniem niebezpiecznym plików i informując o niezweryfikowanych stronach.

Zdaniem eksperta

Monika Krasińska
Dyrektor Departamentu Orzecznictwa i Legislacji w UODO

Oprócz silnych i unikatowych haseł bardzo ważna dla zapewnienia bezpieczeństwa naszych danych osobowych jest stała aktualizacja oprogramowania zarówno komputera, jak i telefonu. Wiele aktualizacji czy poprawek dotyczy bezpieczeństwa systemów operacyjnych zainstalowanych na takich urządzeniach, a także posiadanych przez nas aplikacji. Równie ważne jest nie tylko posiadanie programu antywirusowego, ale i jego uaktualnianie. Złośliwe oprogramowanie, przed którym chronią nas takie narzędzia, powstaje codziennie. Dlatego bez aktualnej bazy wirusów i bazy złośliwych aplikacji program antywirusowy nie będzie w pełni spełniał swojej roli. Nieaktualne oprogramowanie może zaś narazić nas na atak hakerów, którzy mogą wykorzystać podatność danego programu na niebezpieczeństwo. Istnieje też ryzyko zainfekowania naszego komputera oprogramowaniem szpiegującym czy też takim, które zaszyfruje nasze dane, przez co de facto je utracimy. To bardzo ważne szczególnie teraz, gdy w czasie pandemii COVID-19 wiele osób pracuje zdalnie i często wykorzystuje w tym celu prywatne komputery. Nieaktualne oprogramowanie naraża nas wówczas zarówno na utratę danych przetwarzanych w związku z realizowanymi zadaniami służbowymi, jak również na utratę naszych danych prywatnych, danych członków naszej rodziny czy innych osób.

Specjaliści zwracają uwagę na to, że nawet zachowanie wszystkich zasad bezpieczeństwa może nie wystarczyć, żeby uchronić się przed wykorzystaniem naszych danych osobowych. Nie wiemy, w jaki sposób zabezpieczone są bazy danych sklepów internetowych lub portali społecznościowych, z których korzystamy. Dlatego żeby minimalizować negatywne skutki kradzieży tożsamości Urząd Ochrony Danych Osobowych rekomenduje m.in. założenie konta w systemie informacji gospodarczej, aby monitorować swoją aktywność kredytową.

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