DANE OSOBOWE – CZY WIEMY, JAK JE CHRONIĆ?

Raport z badania | Maj 2023 r.

CHRONPESEL.PL

KRAJOWY REJESTR DŁUGÓW www.krd.pl

URZĄD OCHRONY DANYCH OSOBOWYCH

Instytut Prawa Ochrony Danych Osobowych

SPIS TREŚCI

ADAM ŁĄCKI,
Prezes Zarządu Krajowego Rejestru Długów
Biura Informacji Gospodarczej SA

Szanowni Państwo!

Serdecznie zapraszam do lektury kolejnego raportu, który przygotowaliśmy wspólnie z ekspertami serwisu ChronPESEL.pl i Urzędu Ochrony Danych Osobowych. Pierwsze takie wspólne opracowanie na podstawie badania opublikowaliśmy w 2021 r., dlatego w tym roku możemy analizować nie tylko wyniki z maja 2023 r., ale także zmiany, które zaszły w świadomości Polaków na przestrzeni ostatnich 2 lat.

Za każdym razem staramy się jednak dodać nowe pytania, żeby badać kolejne zjawiska. Tym razem było to pytanie, wydawać by się mogło, oczywiste – co zdaniem Polaków zalicza się do zbioru „danych osobowych". Odpowiedzi są bardzo interesujące, więc już teraz zachęcam do ich analizy.

Przechodząc jednak do porównania z poprzednimi edycjami, pierwsze, co rzuca się w oczy to nadal wysoki, bo blisko 90-procentowy odsetek ankietowanych, którzy deklarują, że wiedzą, jak zadbać o bezpieczeństwo danych osobowych. Co prawda, dynamika wzrostu zwolniła, na co wpływ z pewnością miały wydarzenia ostatnich 12 miesięcy, np. trwająca wojna na terenie Ukrainy, którą wykorzystują cyberprzestępcy, jednak różnica między poziomem świadomości z 2021 r., a tym obecnym jest zauważalna.

Od kilku edycji pewnym znakiem szczególnym jest postawa młodych Polaków, których deklaracje na temat wiedzy o bezpieczeństwie danych nie zawsze szły w parze z postawami w konkretnych przypadkach. Tymczasem, jak wynika z przeprowadzonego badania, w 2023 r. znacznie ostrożniej podchodzą oni do tematu swojej wiedzy. Może to świadczyć o większej dojrzałości młodego pokolenia.

Na uwagę zasługuje również fakt rosnącego zaufania do Urzędu Ochrony Danych Osobowych oraz biur informacji gospodarczej, o czym świadczy znaczny wzrost liczby ankietowanych, którzy właśnie w tych instytucjach szukaliby wsparcia.

Oczywiście cały czas przed nami bardzo dużo pracy do wykonania na rzecz edukacji. Wciąż bowiem blisko połowa Polaków nie wie co zrobić w przypadku wycieku danych osobowych, a 40 proc. z nas nie potrafi wyobrazić sobie konsekwencji takiego zdarzenia. To z kolei może utrudnić odpowiednią reakcję. Dodatkowo 1 na 10 badanych deklaruje, że nie potrafiłby rozpoznać próby oszustwa. A tych nie brakuje, o czym świadczą wyniki przeprowadzonego przez nas badania.

Wszystkie te analizy, opracowania oraz porady ekspertów, którzy dzielą się swoją wiedzą, znajdziecie Państwo w poniższym raporcie.

Zapraszam do lektury.

JAN NOWAK,
Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo!

Oddajemy w Państwa ręce publikację przedstawiającą wnioski z kolejnej edycji badania „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce" przeprowadzonego pod patronatem Urzędu Ochrony Danych Osobowych. Cieszę się, że ponownie możemy zaprezentować informacje jak społeczeństwo rozumie ochronę danych osobowych, definiuje zasady ochrony danych osobowych oraz czy potrafi przewidzieć konsekwencje swojego zachowania w przypadku nadmiernego udostępniania danych osobowych.

Raport „Dane osobowe – czy wiemy jak je chronić?" daje nam wszystkim do myślenia. Z jednej strony świadomość społeczeństwa na temat ochrony danych osobowych jest nadal wysoka – tak zadeklarowało 89 proc. ankietowanych. Z drugiej strony potrzeba rozwagi, zachowania odpowiedniej postawy i przewidywania konsekwencji swojego działania, aby zachować ich bezpieczeństwo.

Obecnie żyjemy w czasach niezwykle dynamicznych, które determinują ogromne zmiany. Jesteśmy nie tylko świadkami, ale i uczestnikami postępu technologicznego. Wielu z nas na co dzień korzysta z e-usług, porad telemedycyny, czy świadczy swoją pracę w formie zdalnej. To tylko kilka przykładów z naszego życia codziennego, kiedy udostępniamy wiele informacji na swój temat. Niemal „całe nasze życie nosimy w jednym telefonie". To co do tej pory wydawało nam się zupełnie oczywiste i zrozumiałe, już takie nie jest. Dotychczas stosowane metody zabezpieczania się przed niepożądanymi działaniami innych okazują się niewystarczające. Nowe technologie bez wątpienia służą społeczeństwu. Jednak nie możemy zapomnieć, że „żyjąc w sieci" jesteśmy nieustannie monitorowani, sprawdzane są nasze preferencje zawodowe, dokonywane płatności czy nawet upodobania zakupowe. Kierowane są do nas komunikaty, w których trudno jednoznacznie określić, kto jest ich nadawcą i w jakim celu się z nami kontaktuje. Miewamy też wątpliwości, czy rozmawiamy z człowiekiem czy może jest to wirtualny konsultant. Społeczeństwo dostrzega, że liczba oszustw wzrasta, a metody cyberprzestępców są coraz bardziej wyrafinowane. Trudno się dziwić, że w czasie tak intensywnej aktywności złodziei danych, obywatele nie do końca są przekonani, że wiedzą, jak zadbać o swoje dane. Jak pokazało najnowsze badanie nieco ponad 18 proc. ankietowanych deklaruje, że jest absolutnie pewnych, że nie dadzą się nabrać oszustom. Jednak wynik ten jest trochę słabszy niż przed rokiem. Dlatego Urząd Ochrony Danych Osobowych, który ostrzega i systematycznie edukuje społeczeństwo w zakresie bezpieczeństwa danych osobowych jeszcze bardziej zamierza zintensyfikować działania w tym celu. Jednym z przykładów takiej aktywności jest powołany niedawno z naszej inicjatywy Instytut Prawa Ochrony Danych Osobowych, którego celem jest zwiększenie świadomości społeczeństwa na temat prawa ochrony danych oraz propagowanie najlepszych praktyk i rozwiązań w tym zakresie.

Wkroczyliśmy w cyfrową erę, od której nie ma odwrotu. Świadomi są tego i obywatele, i decydenci. Pojawiają się nowe akty prawne odnoszące się zarówno do ochrony danych osobowych, jak i do szeroko rozumianych nowych technologii, sztucznej inteligencji.

Wierzę, że niniejsza publikacja będzie stanowiła cenne źródło informacji i inspiracji dla wszystkich zainteresowanych ochroną danych osobowych.

NAJWAŻNIEJSZE WNIOSKI

Blisko 89 proc. ankietowanych deklaruje, że wie, jak zadbać o bezpieczeństwo danych osobowych. Jednak tylko co ósmy miał stuprocentową pewność.

Za największe zagrożenia dla bezpieczeństwa danych osobowych ankietowani uważają działalność przestępców, którzy wyłudzają je poprzez oszustwa (42 proc.) oraz wycieki danych (38 proc.). Co piąty badany najbardziej obawia się hakerów włamujących się na nasze komputery i telefony.

Ponad 89 proc. ankietowanych twierdzi, że potrafiłoby rozpoznać próbę oszustwa poprzez SMS, e-mail lub fałszywy telefon. Pewność w tym zakresie ma jednak 18,5 proc. badanych.

Co trzeci z nas doświadczył w ciągu ostatnich 12 miesięcy próby wyłudzenia danych poprzez fałszywy SMS, telefon lub e-mail. Zaledwie niewiele ponad połowa ankietowanych (55,5 proc.) wie, jak powinna zareagować w takiej sytuacji.

Tylko niewiele ponad 45 proc. badanych deklaruje, że wie, co powinni zrobić w przypadku wycieku danych osobowych. 3 na 4 Polaków nie potrafi powiedzieć, kto powinien się zająć neutralizacją negatywnych skutków takich zdarzeń. 40 proc. z nas nie potrafi sobie wyobrazić, jakie mogą być tego konsekwencje.

O BADANIU

Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych oraz Instytutu Prawa Ochrony Danych Osobowych zostało przeprowadzone w maju 2023 roku metodą CAWI na reprezentatywnej grupie 1007 respondentów przez IMAS International.

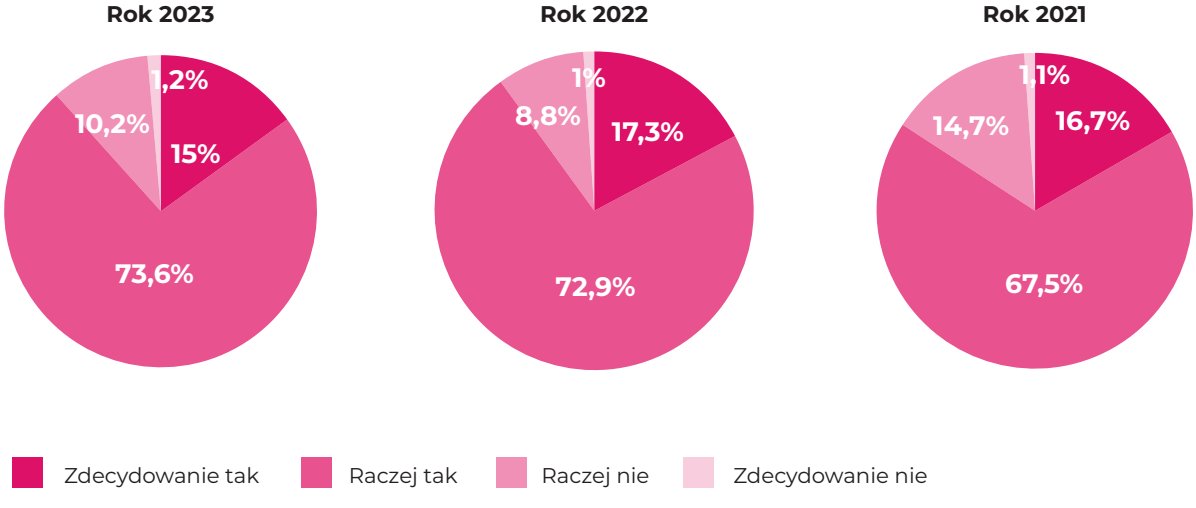
CO DZIESIĄTY ANKIETOWANY NIE WIE, JAK ZADBAĆ O BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Zapytani o to, czy wiedzą, jak zadbać o bezpieczeństwo swoich danych osobowych, blisko 89 proc. ankietowanych odpowiedziało twierdząco. Jednak tylko co ósmy miał stuprocentową pewność. Najwięcej wiary we własne możliwości tradycyjnie już przejawiają najmłodsi respondenci w wieku 18–24 lata oraz niewiele starsi badani między 25 a 34 r.ż. W tych grupach odsetek tych, którzy deklarują, że wiedzą, jak się zabezpieczyć wyniósł 20 proc.

Na drugim biegunie znaleźli się z kolei ankietowani w wieku 55–64 lata oraz ci między 65 a 74 r.ż. W obydwu grupach odsetek osób deklarujących pełne zaufanie do swojej wiedzy na temat zabezpieczania danych osobowych nie przekroczył 10 proc.

Porównując z poprzednimi edycjami raportów, widać, że po ubiegłorocznym wzroście względem 2021 roku, grupa respondentów, która deklaruje, że wie, jak zadbać o bezpieczeństwo danych osobowych ustabilizowała się na poziomie około 90 proc.

Czy wiesz, w jaki sposób dbać o bezpieczeństwo swoich danych osobowych?



Zauważalne przesunięcie można natomiast dostrzec wśród najmłodszych ankietowanych. Podczas gdy w 2022 roku co trzeci z nich (32,3 proc.) wydawał się być pewny swojej wiedzy i umiejętności, w tym roku ten odsetek wyniósł 20 proc. Na szczęście brakujących ponad 10 pp. należy szukać w grupie tych, którzy na pytanie odpowiedzieli „Raczej tak". Może to świadczyć o większej dojrzałości najmłodszych ankietowanych. Do tej pory bowiem eksperci zwracali uwagę na to, że deklaracje najmłodszych nie idą w parze z reakcją na konkretne zagrożenie.

Zdecydowanie wiem,
jak zadbać o bezpieczeństwo swoich danych osobowych

18-24 lata

Rok 2023

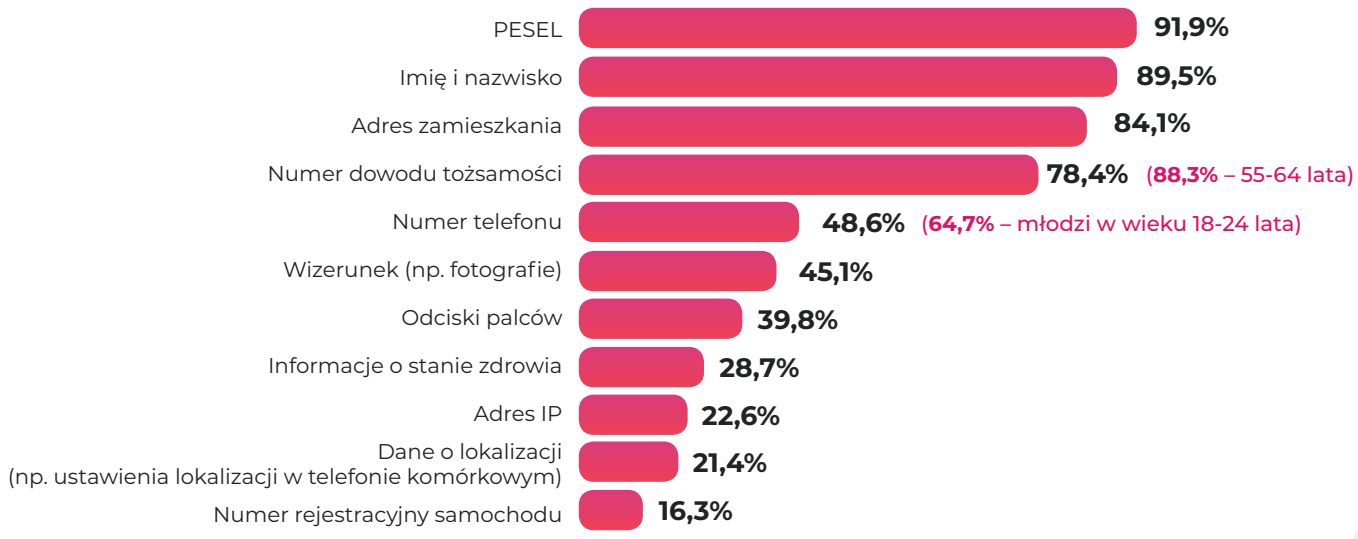
20%

Rok 2022

32,3%

Istotna w kontekście należytej ochrony i przyjęcia odpowiednich zasad bezpieczeństwa jest wiedza odnośnie do tego, które informacje na nasz temat możemy nazwać danymi osobowymi. Zapytani o to, ankietowani najczęściej wskazywali na numer PESEL (92 proc.), imię i nazwisko (89,5 proc.) oraz adres zamieszkania (84 proc.).

Co Twoim zdaniem
wchodzi w skład danych osobowych?



Jakub Groszkowski,
Zastępca Prezesa Urzędu
Ochrony Danych Osobowych

ZDANIEM EKSPERTA

Zgodnie z definicją dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Na podstawie imienia i nazwiska, numeru PESEL czy adresu miejsca zamieszkania, niezaprzeczalnie można zidentyfikować każdą osobę fizyczną. Istnieją też liczne inne dane, które pozwalają na naszą identyfikację. Wysoki procent ankietowanych, wymieniając dane osobowe wskazał na numer telefonu, który służy do kontaktu z osobą, do której ten numer należy, a więc do osoby skonkretyzowanej. To doskonały przykład, ponieważ nie ma znaczenia, czy dzwoniący posiada imię i nazwisko właściciela numeru. Choć numer telefonu nie określa bezpośrednio tożsamości osoby fizycznej, to jest on informacją, która umożliwia bezpośredni kontakt z tą osobą. Podobnie jest z numerami tablic rejestracyjnych, za pośrednictwem których możliwe jest zidentyfikowanie – w sposób pośredni – osoby fizycznej, będącej właścicielem pojazdu. Wyniki badań to doskonały przykład wzrostu świadomości potrzeby ochrony swoich danych wyrażony przez ankietowanych.

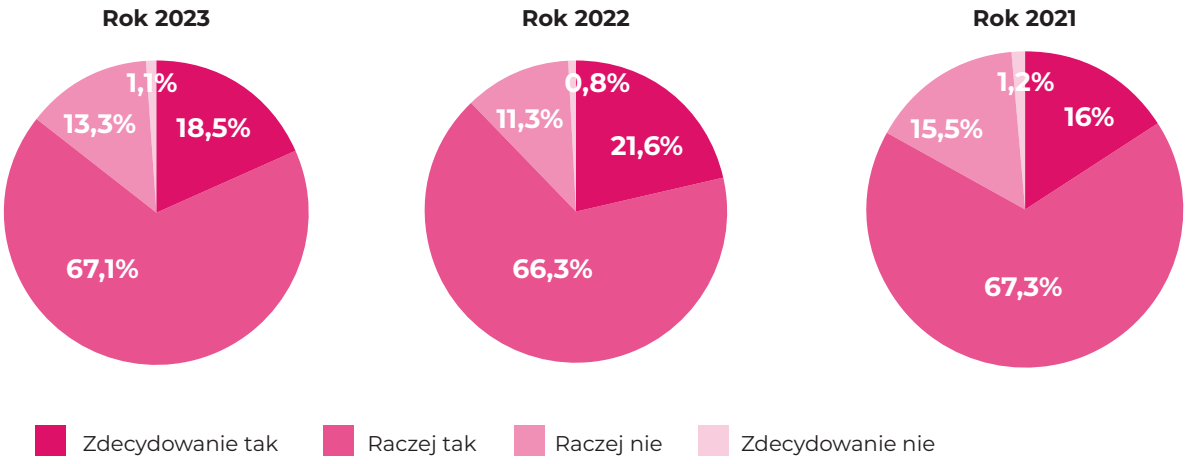
Badanie pokazało również, że wachlarz danych stanowiących dane osobowe jest bardzo szeroki, a w dobie tak szybkiego rozwoju technologicznego będzie jeszcze więcej możliwości na ustalenie i ewentualne naruszenie naszej prywatności. Im więcej informacji dotyczących człowieka będzie uznawanych za dane osobowe, tym bardziej zwiększy się skuteczność ochrony jego danych osobowych poprzez możliwość realizacji praw, które daje mu RODO, a także zwiększy się możliwość działania Prezesa UODO.

ROSNĄCA LICZBA OSZUSTÓW WPROWADZA KONSTERNACJĘ

Jedną z powszechnie stosowanych przez oszustów metod wyłudzania danych osobowych jest phishing. Przestępcy, którzy próbują nas w ten sposób nabrać, najczęściej podszywają się pod różne instytucje lub firmy.

Jak wynika z przeprowadzonego badania, odsetek osób, które deklarują, że wiedzą, jak rozpoznać fałszywą wiadomość lub telefon, utrzymała się na podobnym poziomie, jak w ubiegłym roku, tj. 89,2 proc. (w 2022 r. było to 91,4 proc.). Zauważalnie spadł jednak odsetek tych, którzy są absolutnie pewni, że nie dadzą się nabrać oszustom. Deklaruje to 18,5 proc. ankietowanych, o ponad 3 pp. mniej niż przed rokiem.

Czy wiesz, jak rozpoznać fałszywą wiadomość/fałszywy telefon, w którym ktoś powołuje się na bank, sklep internetowy, firmę kurierską lub instytucję publiczną?



Zmiany widoczne są także wśród najmłodszych i najstarszych badanych. Tych pierwszych opuściła pewność siebie – w grupie między 18 a 24 r.ż. blisko 31 proc. (30,6 proc.) jest przekonanych, że rozpoznałaby próbę oszustwa, a wśród niewiele starszych (25–34 lata) ten odsetek wynosi 25 proc. W ubiegłym roku było to odpowiednio 35,5 proc. oraz ponad 32 proc. (32,4 proc.).

Podobne zjawisko występuje wśród badanych między 55 a 64 r.ż. Tylko niespełna 10 proc. z nich deklaruje, że potrafiłoby rozpoznać fałszywą wiadomość od oszustów. To ponad dwa razy mniej niż w 2022 roku, kiedy to ten odsetek przekroczył 22 proc. (22,4 proc.). W przypadku najstarszej grupy respondentów w wieku 65–74 lata należy z kolei zwrócić uwagę na wzrost względem 2022 r. o ponad 5 pp. (z 12 proc. na 17,1 proc.) wśród ankietowanych, którzy deklarują, że w przypadku oszustwa nie potrafiliby rozpoznać z kim mają do czynienia.

Powodów takich zmian należy upatrywać w stale rosnącej liczbie coraz bardziej wymyślnych metod, po które sięgają przestępcy, żeby nas oszukać.

Wiem, jak rozpoznać fałszywą wiadomość/fałszywy telefon, w którym ktoś powołuje się na bank, sklep internetowy, firmę kurierską lub instytucję publiczną

18-24 lata

Rok 2023
30,6%

Rok 2022
35,5%

Rok 2021
26,3%

25–34 lata

Rok 2023

25%

Rok 2022

32,4%

Rok 2021

24,4%

55-64 lata

Rok 2023

9,9%

Rok 2022

22,4%

Rok 2021

11,1%

Nie wiem, jak rozpoznać fałszywą wiadomość/fałszywy telefon, w którym ktoś powołuje się na bank, sklep internetowy, firmę kurierską lub instytucję publiczną

65-74 lata

Rok 2023

17,1%

Rok 2022

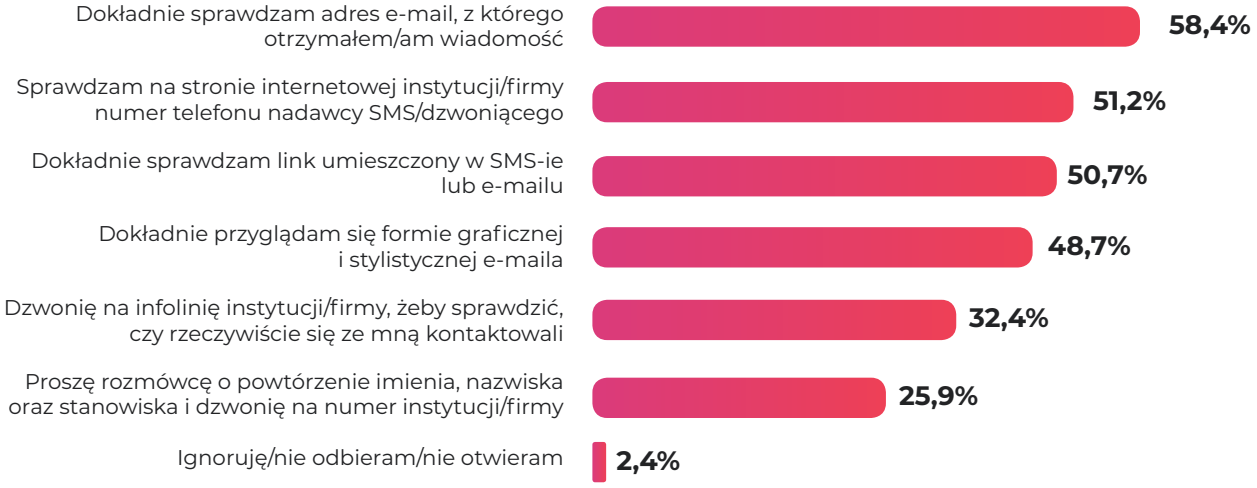
12%

Rok 2021

16,3%

Zapytani o to, w jaki sposób weryfikują, czy otrzymane wiadomości lub połączenia są autentyczne, badani najczęściej wskazują na dokładne sprawdzanie adresu e-mail (58,4 proc.), umieszczonego w wiadomości linku (50,7 proc.) oraz wejście na stronę firmy lub instytucji w celu potwierdzenia numeru, z którego otrzymali telefon (51,2 proc.).

W jaki sposób weryfikujesz autentyczność otrzymywanych wiadomości lub odbieranych połączeń?



Bartłomiej Drozd,
ekspert serwisu ChronPESEL.pl

ZDANIEM EKSPERTA

Powinniśmy przygotować się do tego, żeby jak najwcześniej wykryć próbę oszustwa. Pierwszą rzeczą, na którą warto zwrócić uwagę, jest styl, tytuł wiadomości i obecność lub brak identyfikacji wizualnej naszego banku, dostawcy prądu lub firmy, która rzekomo próbuje się z nami skontaktować. Należy również dokładnie sprawdzić, czy adres e-mail, z którego otrzymaliśmy wiadomość, nie zawiera literówek. Powinniśmy też regularnie śledzić ostrzeżenia publikowane w mediach i na stronach instytucji odpowiedzialnych za cyberbezpieczeństwo. Dzięki temu będziemy bardziej czujni na podejrzane komunikaty. Pamiętajmy również, żeby w przypadku jakichkolwiek wątpliwości zadzwonić na infolinię, zanim podejmiemy jakiekolwiek działania na podstawie otrzymanej wiadomości. Uważać powinniśmy także na rozmowy telefoniczne. Dzwoniący oszuści zazwyczaj próbują nas ostrzec przed rzekomym zagrożeniem, aby w ten sposób zmusić nas do szybkiej reakcji. Nigdy nie powinniśmy się na to godzić. W takiej sytuacji należy przerwać rozmowę i podobnie jak wcześniej, skontaktować się z rzekomą instytucją lub firmą, na którą osoba się powoływała, aby upewnić się, czy rzeczywiście jest jej pracownikiem.

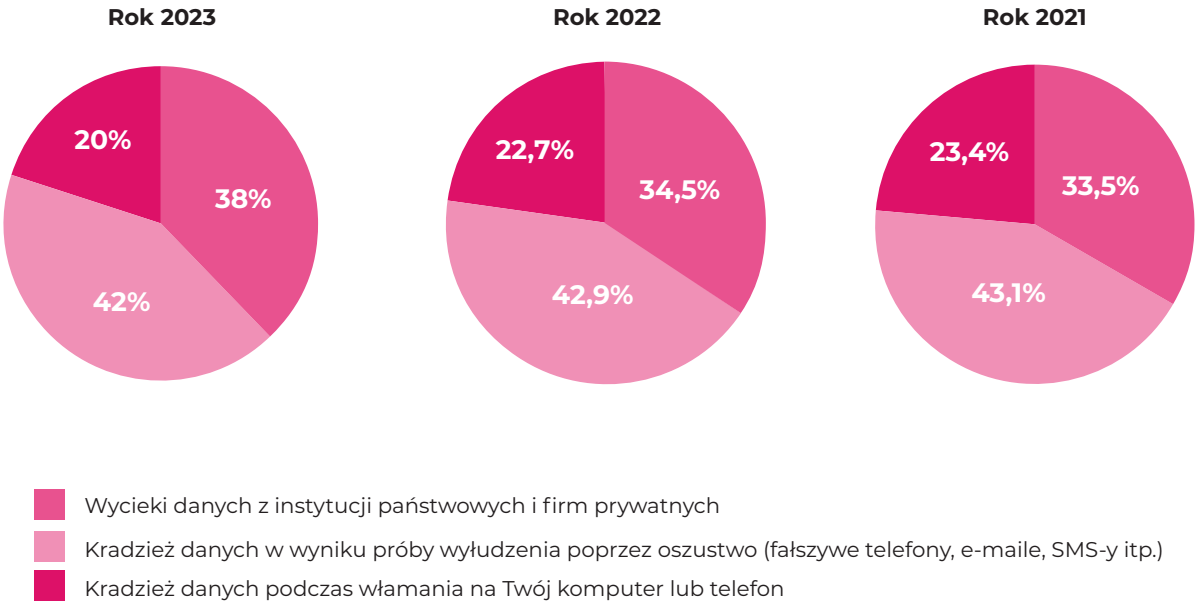
OSZUŚCI WYŁUDZAJĄCY DANE NAJWIĘKSZYM ZAGROŻENIEM

Za największe zagrożenie dla bezpieczeństwa danych osobowych (42 proc.) ankietowani uważają działalność przestępców, którzy wyłudzają je poprzez oszustwa. Na drugim miejscu znalazły się wycieki z baz instytucji publicznych (17 proc.) oraz firm prywatnych (21 proc.). To łącznie 38 proc. Co piąty badany najbardziej obawia się hakerów włamujących się na ich komputery i telefony.

Co ciekawe ta hierarchia różni się w zależności od wieku. **Dla najmłodszych (18–24 lata) znacznie bardziej niebezpieczni są hakerzy niż wycieki danych.** Z kolei dla badanych w wieku 55–64 lat największym zagrożeniem są właśnie te drugie.

Porównując te wyniki z poprzednimi edycjami badania, widać wyraźnie wzrost liczby osób, które za najbardziej niebezpieczne uznali wycieki danych osobowych.

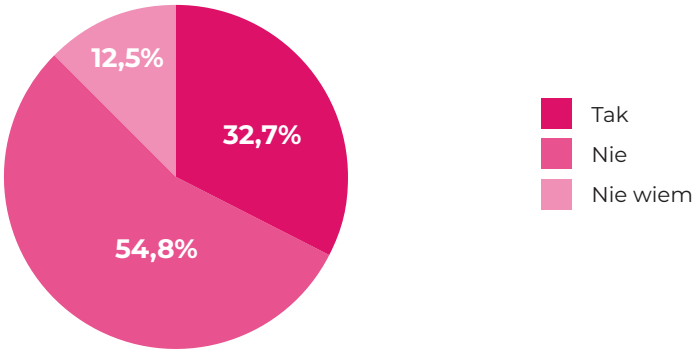
Skąd, Twoim zdaniem, pochodzi największe zagrożenie dla Twoich danych?



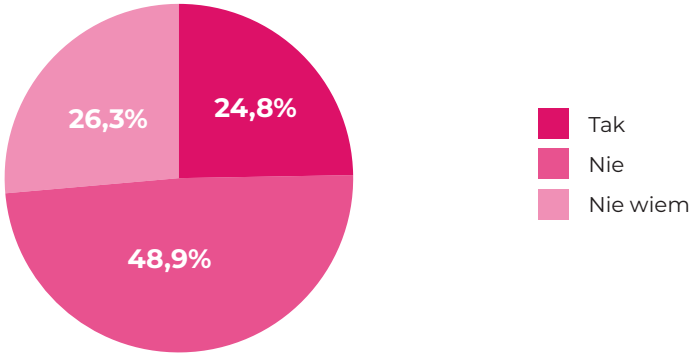
CO TRZECI ANKIETOWANY OTRZYMAŁ PRZEZ OSTATNI ROK PODEJRZANY TELEFON LUB SMS

O tym, że nie są to bezpodstawne obawy świadczą inne statystyki. Jak wynika bowiem z przeprowadzonego badania, **co trzeci z nas doświadczył w ciągu ostatnich 12 miesięcy próby wyłudzenia danych poprzez fałszywy SMS, telefon lub e-mail.** Ten odsetek mógłby być jeszcze wyższy, ponieważ równocześnie 12,5 proc. ankietowanych nie potrafiło udzielić jednoznacznej odpowiedzi na to pytanie. Dodatkowo co czwarty ankietowany deklaruje, że podobnej próby doświadczyli jego znajomi lub bliscy.

Czy w ciągu ostatnich 12 miesięcy doświadczyłeś/aś próby wyłudzenia Twoich danych poprzez fałszywy SMS, telefon lub e-mail?

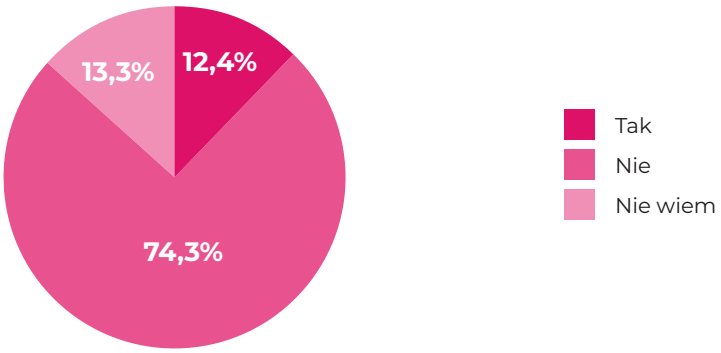


Czy w ciągu ostatnich 12 miesięcy Twoi znajomi bądź członkowie rodziny doświadczyli próby wyłudzenia danych poprzez fałszywy SMS, telefon lub e-mail

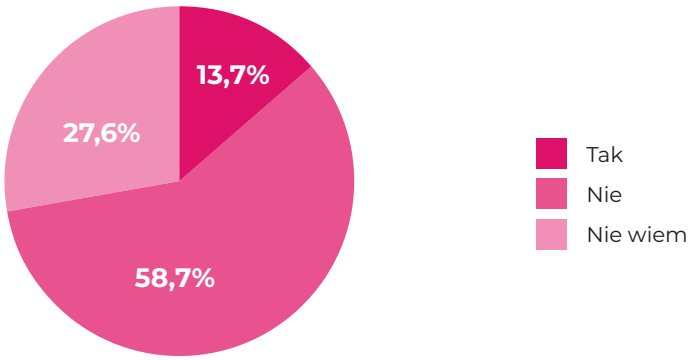


Jedna na 8 takich prób zakończyła się kradzieżą danych. Tak wynika z odpowiedzi ankietowanych. Dodatkowo co siódmy badany do dzisiaj nie ma pewności, czy przypadkiem nie dał się nabrać. Respondenci zauważyli także, że podobny problem z działalnością oszustów mieli ich bliscy.

Czy w ciągu ostatnich 12 miesięcy doświadczyłeś/aś kradzieży danych w wyniku próby wyłudzenia poprzez oszustwo (fałszywe telefony, e-maile, SMS-y)



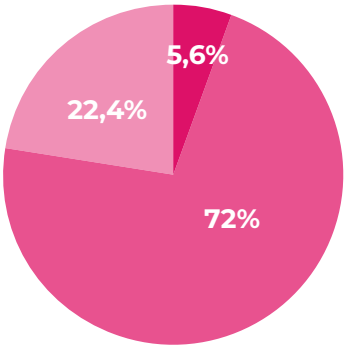
Czy w ciągu ostatnich 12 miesięcy Twoi znajomi bądź członkowie rodziny doświadczyli kradzieży danych w wyniku próby wyłudzenia poprzez oszustwo (fałszywe telefony, e-maile, SMS-y)



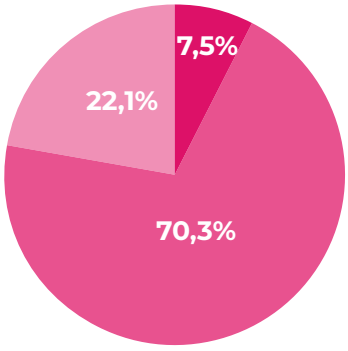
WYCIEKI DANYCH I DZIAŁANIA HAKERÓW – NASZE DOŚWIADCZENIA

Nieco inaczej wygląda sytuacja, jeśli chodzi o nasze doświadczenia z wyciekami. Co prawda odsetek ankietowanych, których dane w ciągu ostatnich 12 miesięcy wyciekły wydaje się niewielki – niespełna 6 proc. w przypadku instytucji publicznych oraz 7,5 proc. z firm prywatnych – jednak uwagę należy zwrócić na grupę tych, którzy nie potrafili jednoznacznie odpowiedzieć. To ponad 22 proc. badanych. Biorąc pod uwagę specyfikę wycieków, o których nie zawsze dowiadujemy się od razu, taki wynik należy uznać za alarmujący.

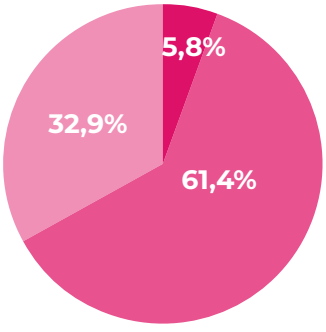
Czy w ciągu ostatnich 12 miesięcy doświadczyłeś/aś wycieku Twoich danych z instytucji publicznej?



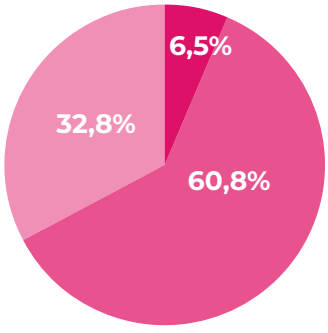
Czy w ciągu ostatnich 12 miesięcy doświadczyłeś/aś wycieku danych z firmy prywatnej?



Czy w ciągu ostatnich 12 miesięcy Twoi znajomi bądź członkowie rodziny doświadczyli wycieku danych z instytucji publicznej?



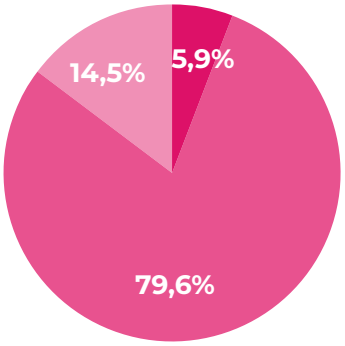
Czy w ciągu ostatnich 12 miesięcy Twoi znajomi bądź członkowie rodziny doświadczyli wycieku danych z firmy prywatnej?



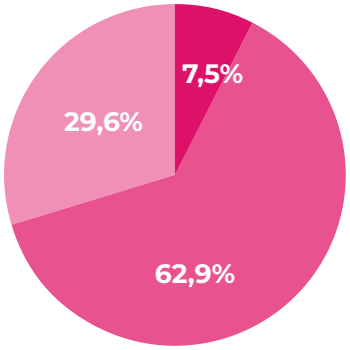
Tak Nie Nie wiem

Również 6 proc. z nas deklaruje, że w ciągu ostatnich 12 miesięcy padło ofiarą hakerów, którzy włamali się na ich komputer lub telefon.

Czy w ciągu ostatnich 12 miesięcy doświadczyłeś/aś kradzieży danych podczas włamania na Twój komputer lub telefon?



Czy w ciągu ostatnich 12 miesięcy Twoi znajomi bądź członkowie rodziny doświadczyli kradzieży danych podczas włamania na komputer lub telefon



Tak Nie Nie wiem

Bartłomiej Drozd,
ekspert serwisu ChronPESEL.pl

ZDANIEM EKSPERTA

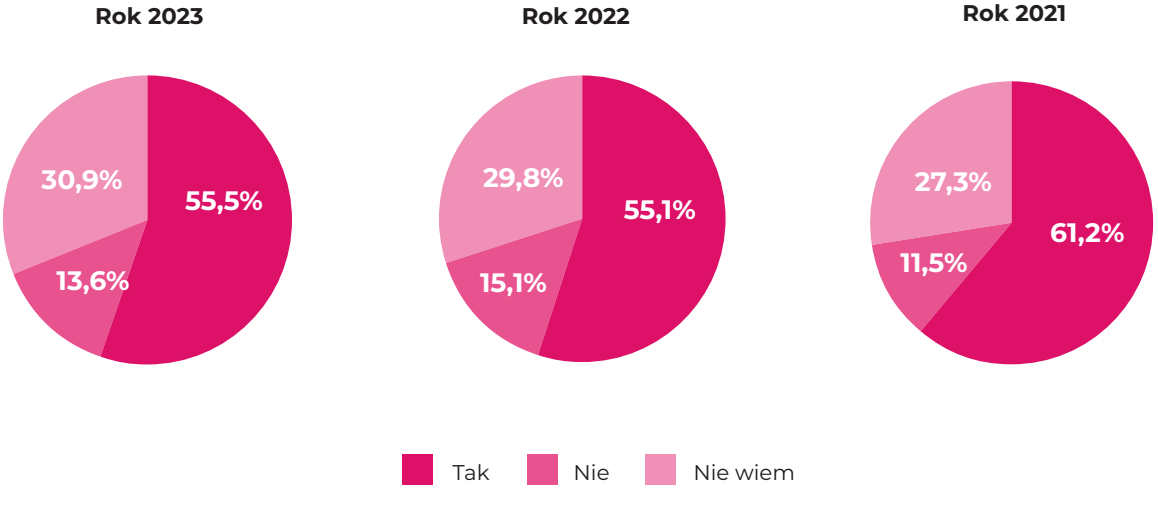
W przypadku takich sytuacji szybka reakcja ma dużą wagę. Dodatkowym utrudnieniem, jeśli chodzi o wycieki jest fakt, że bezpieczeństwo danych zgromadzonych w różnych instytucjach i firmach zależy nie tylko od nas, ale także od podmiotów, które nimi zarządzają. Dlatego ważne jest, aby znać odpowiednie osoby do kontaktu i wiedzieć, jakie kroki podjąć. Na przykład, jeśli wyciekły dane osobowe, takie jak numer PESEL, należy jak najszybciej sprawdzić, czy nie zostały one już wykorzystane przez niepowołane osoby. Rozważmy również uruchomienie monitoringu użycia naszego numeru PESEL, co pozwoli nam zauważyć próby wyłudzenia pożyczek lub innych zobowiązań finansowych w przyszłości.

JAK ZAREAGOWAĆ W PRZYPADKU WYŁUDZENIA LUB KRADZIEŻY DANYCH OSOBOWYCH

Ponad połowa respondentów (55,5 proc.) deklaruje, że wie, co powinna zrobić w przypadku wyłudzenia lub kradzieży danych osobowych. Przecząco na to pytanie odpowiedziało niespełna 14 proc. (13,6 proc.) ankietowanych. Znacznie więcej niepokoju powinna natomiast wzbudzić grupa tych, którzy nie potrafili odpowiedzieć na to pytanie. To prawie 1/3 badanych (30,9 proc.). W porównaniu z ubiegłym rokiem nie widać zatem znaczących różnic.

Najlepiej przygotowani do takich sytuacji wydają się być ankietowani w wieku 25–34 lata oraz ci między 65–74 r.ż. Ponad 60 proc. z nich zadeklarowało, że wiedziałoby, jak się zachować w przypadku wyłudzenia lub kradzieży danych osobowych. Na drugim biegunie znaleźli się najmłodsi (18–24 lata). Prawie co czwarty z nich (22,4 proc.) nie potrafiłby odpowiednio zareagować. To jedyna grupa, w której odsetek tych, którzy wiedzieliby, co zrobić jest niższy niż 50 proc. (47,1 proc.).

Czy wiesz, jakie działania należy podjąć w przypadku wyłudzenia lub kradzieży danych osobowych, takich jak: imię, nazwisko, adres, PESEL?



Odpowiedzią na pytanie, co w przypadku wyłudzenia lub kradzieży danych osobowych należałoby zrobić najczęściej jest zgłoszenie zdarzenia na policję (85,2 proc.), do banku, w którym posiada się konto (77,8 proc.) oraz zmiana danych do logowania (71,7 proc.).

Adam Sanocki,
dyrektor Departamentu Komunikacji Społecznej, rzecznik prasowy Urzędu Ochrony Danych Osobowych

ZDANIEM EKSPERTA

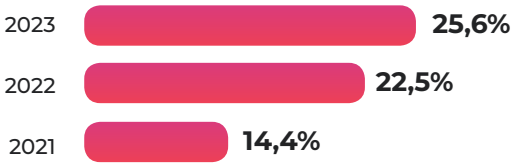
Wyniki badania jednoznacznie potwierdzają, że całkiem sporo osób zdaje sobie sprawę, że gdy dochodzi do kradzieży ich tożsamości, a więc przestępstwa z wykorzystaniem ich danych osobowych, to tego typu zdarzenie należy zgłosić na policję. Jednocześnie część osób błędnie wskazała, że takie działanie przestępców należy zgłaszać do Urzędu Ochrony Danych Osobowych, który jednak nie jest organem ścigania i nie jest w stanie ustalić sprawców takiej kradzieży. UODO może natomiast rozpatrzyć skargę na działanie konkretnego administratora, który narusza prawa osoby, której dane dotyczą lub niewłaściwie przetwarza jej dane.

Ponad połowa ankietowanych (51,5 proc.) skierowałaby tę sprawę do Urzędu Ochrony Danych Osobowych, a co czwarty sprawdziłby swoje dane w biurze informacji gospodarczej. Widać rosnące zaufanie do tych podmiotów na przestrzeni ostatnich 2 lat. Jeszcze w 2021 roku, jak wynika z deklaracji ankietowanych, sprawę do UODO zgłosiłby zaledwie co trzeci badany, zaś dane w biurze informacji gospodarczej sprawdziłoby niewiele ponad 14 proc. (14,4 proc.).

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

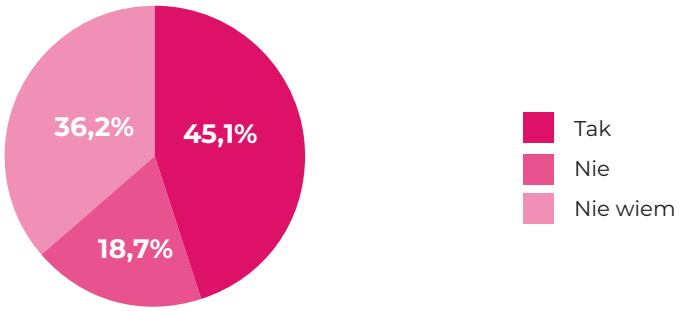
W przypadku wyłudzenia lub kradzieży danych osobowych: Zgłosił(a)bym sprawę do UODO

Sprawdził(a)bym swoje dane w biurze informacji gospodarczej



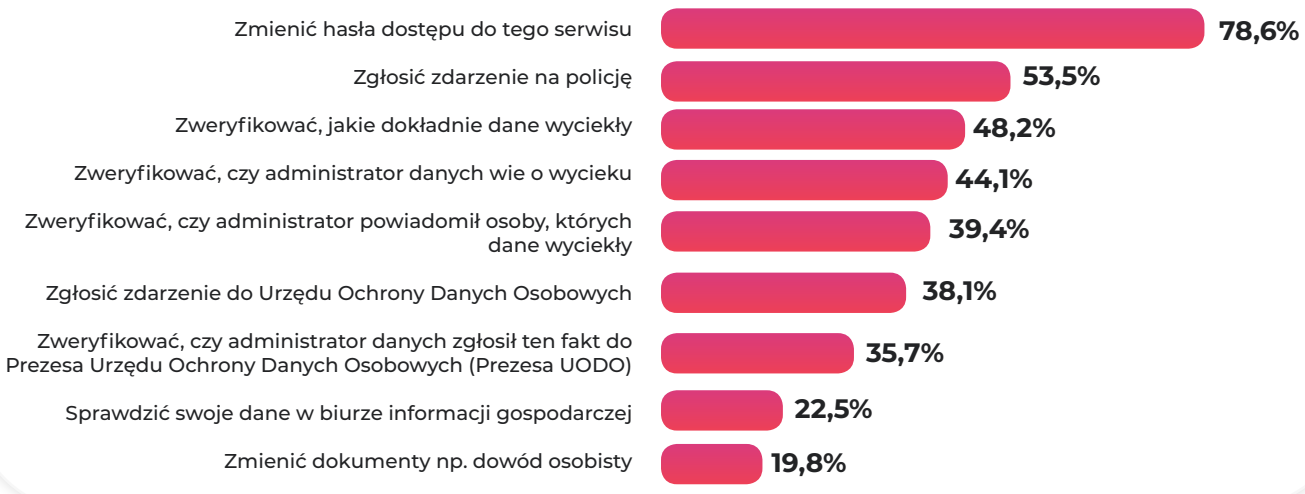
W przypadku wycieku danych osobowych, odsetek tych, którzy wiedzieliby, co należy zrobić jest jeszcze niższy i nie przekracza nawet połowy ankietowanych – 45,1 proc. Co ciekawe, przeciwnie niż w przypadku wyłudzeń, najpewniej czują się najmłodsi respondenci. Około połowa z nich deklaruje, że wiedziałaby, co należy zrobić – 18–24 lata (49,4 proc.), 25–34 lata (50 proc.).

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



Na liście czynności, które w przypadku wycieku danych trzeba wykonać jak najszybciej, ankietowani najczęściej umieszczali zmianę hasła dostępu do serwisu, z którego informacje na nasz temat wyciekły (78,6 proc.), zgłoszenie zdarzenia na policję (53,5 proc.) oraz weryfikację, jakie dokładnie dane mogły wpaść w niepowołane ręce (48,2 proc.).

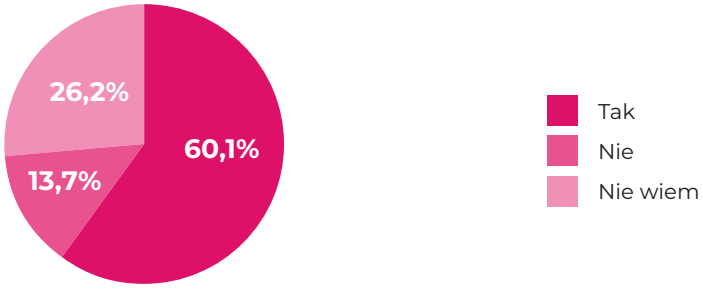
Jakie działania należy podjąć w przypadku wycieku lub kradzieży danych z serwisu/aplikacji, w których miałeś konto?



40 PROC. POLAKÓW NIE WIE, JAKIE MOGĄ BYĆ KONSEKWENCJE WYCIEKU DANYCH OSOBOWYCH

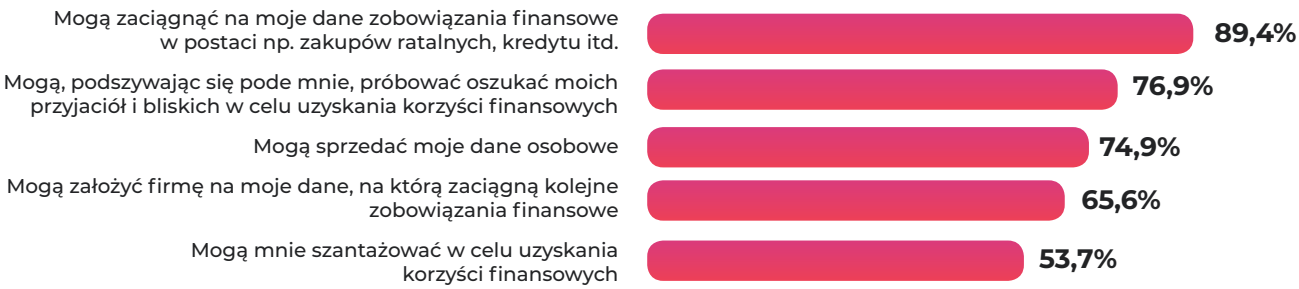
Zdolność do odpowiedniej reakcji na niepożądane wydarzenia to jedno. Inną kwestią jest świadomość możliwych konsekwencji. Z tych, w przypadku wycieku danych osobowych, jak wynika z przeprowadzonego badania, zdaje sobie sprawę niewiele ponad 60 proc. respondentów.

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



Wśród możliwych konsekwencji ankietowani najczęściej wskazywali na możliwość zaciągnięcia zobowiązań finansowych na dane poszkodowanego (89,4 proc.), próbę oszukania rodziny i znajomych ofiary poprzez wykorzystanie jej tożsamości (76,9 proc.) oraz sprzedaż skradzionych danych (74,9 proc.).

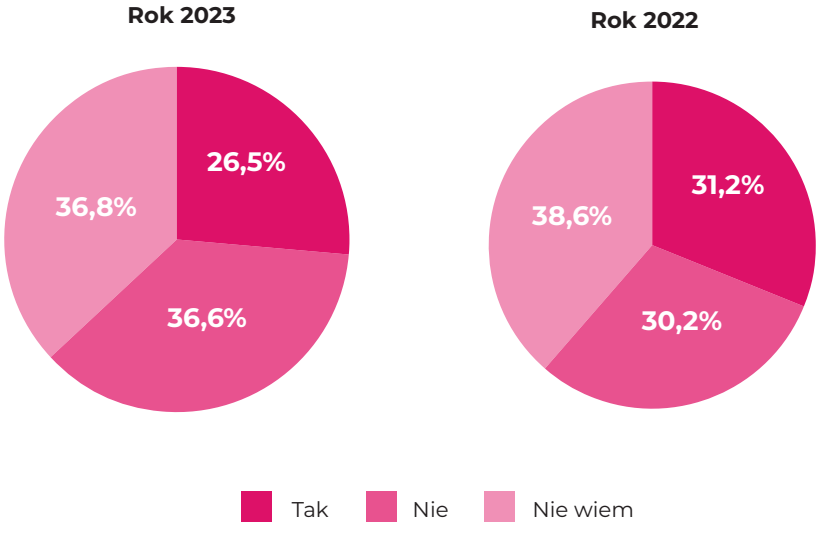
W jaki sposób przestępcy mogą wykorzystać Twoje dane osobowe?



3 NA 4 POLAKÓW NIE WIE, KTO POWINIEN SIĘ ZAJĄĆ NEUTRALIZACJĄ NEGATYWNYCH SKUTKÓW WYCIEKU DANYCH OSOBOWYCH

Zaledwie co czwarty ankietowany (26,5 proc.) deklaruje, że wiedziałby, kto powinien się zająć neutralizacją negatywnych skutków wycieku danych osobowych. To nieznacznie gorszy wynik niż w 2022 roku, kiedy ten odsetek wyniósł ponad 30 proc. badanych (31,2 proc.).

Czy wiesz, kto w przypadku wycieku, powinien zająć się neutralizacją jego negatywnych skutków?



Najczęściej badani wskazują na służby ścigania (65,9 proc.) oraz firmę lub instytucję, która odpowiadała za bezpieczeństwo źle chronionej bazy danych (65,5 proc.). Więcej niż połowa ankietowanych (55,1 proc.) uważa, że neutralizacją negatywnych skutków wycieku powinien się zająć Urząd Ochrony Danych Osobowych.

Uwagę należy zwrócić na blisko 40 proc. badanych (37,8 proc.), zdaniem których ofiara wycieku powinna być aktywna w zapobieganiu jego negatywnych skutków. Przed rokiem ten odsetek był nieco niższy i wyniósł blisko 35 proc.

Kto, w przypadku wycieku danych, powinien zająć się neutralizacją jego negatywnych skutków?

Poszkodowani najczęściej oczekiwaliby od podmiotu odpowiedzialnego za przetwarzanie ich danych osobowych informacji, że w ogóle doszło do wycieku oraz jakie informacje mogły wpaść w niepowołane ręce (63,5 proc.), a także wdrożenia działań, które zmniejszą ryzyko powtórzenia podobnego zdarzenia w przyszłości (60,2 proc.).

Jakiego rodzaju działań oczekujesz od podmiotu odpowiedzialnego za wyciek Twoich danych osobowych?

Małgorzata Dulińska-Majkowska,
kierownik Zespołu Ochrony Danych
i Prywatności w Kaczmarski Group Sp. j.

ZDANIEM EKSPERTA

Zgodnie z przepisami, za zabezpieczenie przetwarzanych danych oraz wdrożenie systemu, który zminimalizuje ryzyko wycieku danych odpowiada administrator. Jeśli już dojdzie do takiego zdarzenia, administrator musi szybko ocenić, czy naruszenie bezpieczeństwa jest na tyle poważne, że doszło do naruszenia ochrony danych osobowych, które należy zgłosić do Urzędu Ochrony Danych Osobowych oraz poinformować o nim wszystkich poszkodowanych. To bardzo ważne, żeby administratorzy, po zasięgnięciu opinii inspektorów ochrony danych, byli przygotowani merytorycznie do podejmowania takich decyzji.

Eksperci zajmujący się ochroną danych osobowych zwracają uwagę na to, że za większość wycieków danych w polskich firmach odpowiadają ich pracownicy. Oczywiście najczęściej wynika to z niewiedzy lub braku ostrożności, dlatego pracodawcy powinni bardzo dużą wagę przykładać także do organizowania regularnych szkoleń oraz innych form edukacji, które będą uwzględniać także stale zmieniające się realia, żeby wszyscy pracownicy byli na bieżąco.

LISTA GRZECHÓW – NIEBEZPIECZNE ZACHOWANIA

Świadomość zagrożeń oraz wiedza na temat potencjalnych konsekwencji to jedno. Bardzo ważne jest także to, żeby przeciwdziałać potencjalnie niebezpiecznym sytuacjom. A jak to wygląda na co dzień?

Większość ankietowanych dba o bezpieczeństwo swoich danych na urządzeniach elektronicznych, z których korzysta każdego dnia. Więcej uwagi poświęcamy jednak naszym komputerom i tabletom.

Niestety nadal stosunkowo wysoki odsetek badanych (25,8 proc.) przyznaje się do tego, że nie zawsze dba o to, by korzystać z unikalnych haseł do logowania. Wśród najmłodszych (18–24 lata) ten wynik jest jeszcze bardziej niepokojący. Ostrożność i korzystanie z niepowtarzalnych haseł deklaruje bowiem zaledwie 54 proc. z nich.

Monika Krasińska,
dyrektor Departamentu Orzecznictwa i Legislacji, UODO,
dyrektor Instytutu Prawa Ochrony Danych Osobowych

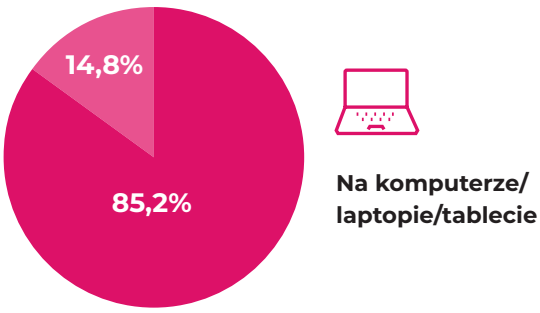
ZDANIEM EKSPERTA

Urząd Ochrony Danych Osobowych nieustannie przypomina o zachowaniu szczególnej ostrożności podczas udostępniania danych osobowych. Zasada ograniczonego zaufania, zachowywanie zdrowego rozsądku, nieuleganie emocjom i staranna weryfikacja osób, które proszą o przekazanie im danych osobowych, pozwolą nam ograniczyć ryzyko zdobycia przez cyberprzestępców informacji, które nas dotyczą.

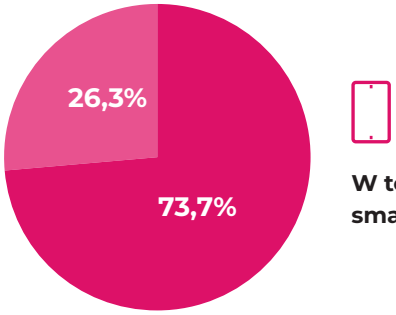
Mimo deklarowania, że wiemy, jak rozpoznać próby oszustwa mające na celu wyłudzenie danych osobowych, to w codziennym zachowaniu niestety wciąż popełniamy błędy. Korzystanie z aktualnego oprogramowania antywirusowego, zmiana haseł do logowania i ustawienie dwuskładnikowego uwierzytelnienia, to pewne podstawowe zachowania, dzięki którym możemy zapewnić bezpieczeństwo danych osobowych. Powinniśmy o tym bezwzględnie pamiętać, zwłaszcza teraz, kiedy przestępcy korzystają z różnych zdobyczy nowych technologii, próbując w coraz bardziej wyszukany sposób zdobyć nasze zaufanie i pozyskać dane osobowe. Jednocześnie Polacy, dopóki nie dotknie ich bezpośrednio kradzież danych osobowych, często – niestety – bagatelizują wagę tak prostych, aczkolwiek skutecznych rozwiązań.

Dodatkowo tylko niespełna 2/3 z nas deklaruje, że weryfikuje regulaminy i polityki prywatności firm i instytucji, z których usług korzystamy. Chlubnym wyjątkiem są tutaj ankietowani w wieku 25–34 lata, wśród których ten odsetek wynosi ponad 75 proc. (76,7 proc.).

Mam zainstalowany program antywirusowy



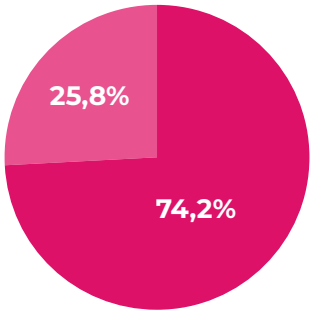
Na komputerze/ laptopie/tablecie



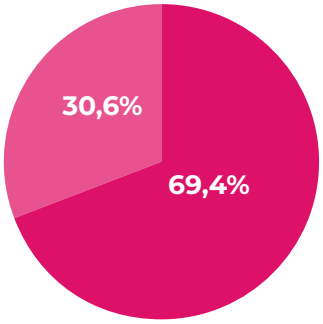
W telefonie/ smartfonie

Tak Nie

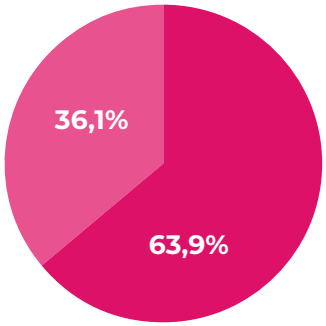
Nie powtarzam haseł do logowania w serwisach, z których korzystam



Zawsze sprawdzam, czy dane osobowe przekazywane przeze mnie firmom/instytucjom mogą zostać przekazane także ich biznesowym partnerom

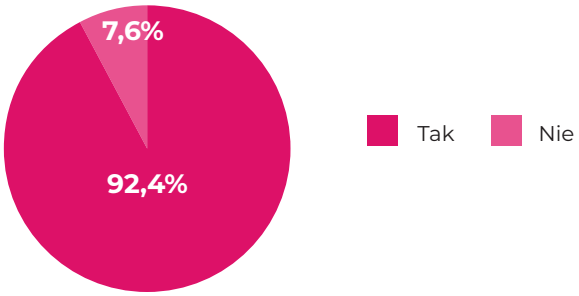


Weryfikuję regulaminy i polityki prywatności na stronach firm/instytucji

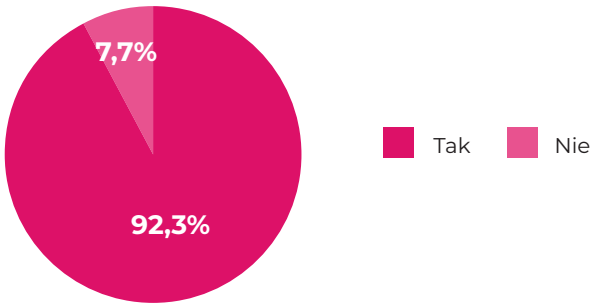


Na pochwałę zasługuje z kolei postawa w sprawie przeciwdziałania potencjalnym oszustwom phishingowym. Zdecydowana większość ankietowanych – ponad 92 proc. – zapewnia, że nie klika w linki otrzymane w e-mailu lub SMS-ie oraz nie otwiera wiadomości nieznanego pochodzenia. Jeszcze wyższy jest odsetek tych, którzy deklarują, że nie podają swojego numeru PESEL w sytuacjach, które tego nie wymagają.

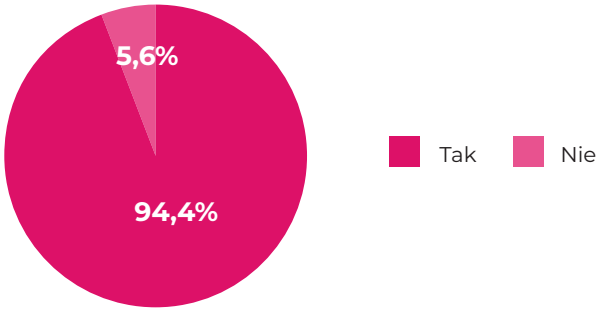
Nie klikam w linki
otrzymane w e-mailu lub SMS-ie



Nie otwieram e-maili
niewiadomego pochodzenia

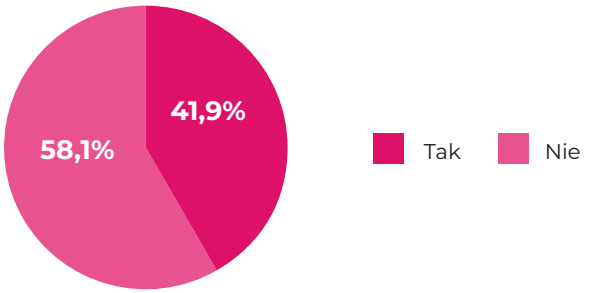


Nie podaję numeru PESEL,
jeśli nie jest to absolutnie konieczne



Niektórych wydarzeń nie da się jednak przewidzieć ani uniknąć. W takich przypadkach ważne jest tylko, żeby odpowiednio szybko zareagować. Jak wynika z przeprowadzonego badania, rękę na pulsie trzyma blisko 42 proc. Polaków, którzy deklarują, że korzystają z programów chroniących przed konsekwencjami utraty danych osobowych (np. ChronPESEL.pl).

Korzystam z programów chroniących przed konsekwencjami utraty danych osobowych



Andrzej Kulik,
dyrektor Departamentu Analiz Rynkowych i Komunikacji w Krajowym Rejestrze Długów

ZDANIEM EKSPERTA

Monitorowanie tego, co dzieje się z naszym numerem PESEL umożliwia natychmiastowe wykrycie i reakcję w sytuacji, gdy ktoś chce na nasze dane wyłudzić kredyt, pożyczkę albo zakup drogiego sprzętu. Instytucje finansowe, jak banki czy firmy pożyczkowe, operatorzy telekomunikacyjni przed zawarciem umowy z nowym klientem sprawdzają w Krajowym Rejestrze Długów, czy nie jest zadłużony. Co ważne, konsument musi się zgodzić na takie sprawdzenie. Jeśli więc nic takiego nie miało miejsca, a w ramach monitoringu zostaniemy powiadomieni, że właśnie ktoś weryfikuje naszą wiarygodność płatniczą, to jest to znak, że ktoś próbuje na nasze konto zaciągnąć jakieś zobowiązanie.

AUTORZY RAPORTU

CHRONPESEL.PL

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.

Instytut Prawa Ochrony Danych Osobowych (IPODO)
Celem działań Instytutu jest zwiększenie świadomości społeczeństwa na temat prawa ochrony danych oraz propagowanie najlepszych praktyk i rozwiązań w zakresie przetwarzania i ochrony danych, poprzez badania, raporty, edukację, doradztwo i współpracę z innymi instytucjami oraz uczestnictwo w procesach tworzenia regulacji prawnych w tej dziedzinie. Instytut tworzy zespół ekspertów, praktyków oraz naukowców mających duży wpływ na powstanie i kształtowanie się systemu ochrony danych w Polsce.