



CHRONPESEL.PL



URZĄD OCHRONY DANYCH OSOBOWYCH



Wiedza na temat bezpieczeństwa danych osobowych w Polsce

Raport z badania
maj 2022 r.

Spis treści

• Wstęp	3
• O badaniu	5
• Główne wnioski	5
• Oszuści wyłudzający dane osobowe największym zagrożeniem	6
• Młodzi Polacy przekonani, że trudno ich oszukać	10
• Niebezpieczne zachowania – lista grzechów	15
• Konsekwencje utraty danych osobowych	19
• O bezpieczeństwie danych osobowych najchętniej rozmawiamy ze znajomymi	21
• Autorzy raportu	23



Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo,

druga edycja raportu „Wiedza na temat bezpieczeństwa danych osobowych w Polsce” zbiega się w czasie z kolejną rocznicą stosowania ogólnego rozporządzenia o ochronie danych osobowych (RODO). Unijny akt prawny powstał nie tylko po to, aby we wszystkich państwach członkowskich zapewnić spójną ochronę danych osobowych osób fizycznych, ale przede wszystkim ma on wzmacniać ich prawa.

Mimo że w Polsce ochrona danych osobowych ma już swoją długoletnią tradycję, to rozwój nowoczesnych technologii i postęp społeczny, przynoszą nam nowe wyzwania. Wiemy, że skuteczna ochrona danych osobowych wiąże się z potrzebą systematycznego budowania świadomości obywateli.

Wyniki tegorocznego raportu mogą napawać umiarkowanym optymizmem. Ponad 90% ankietowanych twierdzi, że wie, jak zadbać o bezpieczeństwo swoich danych. Najpewniej czują się przedstawiciele młodego pokolenia w wieku między 18. a 34. r.ż. Jednakże ci sami młodzi ludzie są grupą, która najczęściej popełnia błędy w postaci publikacji zdjęć swoich dokumentów w sieci, udostępnia osobom trzecim loginy i hasła do logowania oraz zostawia dane osobowe w internetowych ankietach – to już niepokoi.

Oprócz wiedzy, potrzeba także rozważań i przewidywania konsekwencji swojego działania, aby zachować bezpieczeństwo swoich danych osobowych.

Co cieszy, ponad połowa ankietowanych deklaruje, że rozmawia o zasadach bezpieczeństwa swoich danych osobowych w sieci z partnerem lub współmałżonkiem, a także ze swoimi dziećmi czy znajomymi.

Nasze zachowania i działania są bardzo ważne. Zatem niech lektura publikacji nie tylko wzbogaci naszą wiedzę, ale także zainspiruje do podejmowania działań służących nam wszystkim. Stańmy się wspólnie ambasadorami dobrych praktyk ochrony danych i prywatności.

Zachęcam do lektury niniejszej publikacji.



Adam Łacki

Prezes Zarządu Krajowego Rejestru Długów
Biura Informacji Gospodarczej SA

Szanowni Państwo,

prezentujemy drugą edycję raportu poświęconego ochronie danych osobowych. Od wielu lat badamy poziom świadomości Polaków w tym zakresie, ich zachowania oraz reakcje na stale zmieniające się uwarunkowania. Świat wokół nas stale ewoluuje – obserwujemy dynamiczny proces cyfryzacji wszystkich usług, przez co coraz więcej czasu spędzamy w przestrzeni wirtualnej. Pojawiają się także nowe przepisy i regulacje, do których należy się dostosować. Nowe okoliczności starają się z kolei wykorzystać oszuści wyłudzający nasze dane osobowe.

Najlepsze, co możemy w tej sytuacji zrobić, to podejmowanie długotrwałych działań edukacyjnych na rzecz stałego podnoszenia świadomości obywateli. Dlatego z przyjemnością prezentuję Państwu drugą edycję raportu, który ponownie przygotowaliśmy wspólnie z ekspertami do spraw bezpieczeństwa danych. Wszystkie wnioski i obserwacje, które w nim umieściliśmy powstały na bazie badania przeprowadzonego w marcu 2022 roku przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych.

Z racji tego, że jest to druga edycja, mamy możliwość porównać aktualną sytuację z tą sprzed roku. Pierwsze wnioski są umiarkowanie pozytywne. W zestawieniu z 2021 rokiem, zwiększyła się grupa osób, które deklarują, że wiedzą, jak rozpoznać próbę oszustwa. Za pozytywne zjawisko należy uznać także bardzo wysoki odsetek ankietowanych, którzy twierdzą, że potrafią zadbać o bezpieczeństwo swoich danych osobowych.

Po drugiej stronie mamy jednak rosnącą grupę osób, z których deklaracji wynika, że nie umiałyby odpowiednio zareagować w przypadku wyłudzenia. Widać zatem, że nasze przekonania nie zawsze przekładają się potem na właściwe zachowania. Z tego jednak względu, poniższy raport powinni przeczytać wszyscy, którzy tematem się interesują.

Opracowanie 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 2022 roku metodą CAWI na reprezentatywnej grupie 1010 respondentów przez IMAS International.

Główne wnioski

40%

Ponad 40 proc. Polaków za największe zagrożenie dla bezpieczeństwa danych osobowych uważa działanie oszustów.



Jak wynika z przeprowadzonego badania, **więcej niż przed rokiem osób ma pewność, że wie, jak rozpoznać taką próbę oszustwa.** Najlepiej wygląda to wśród młodych między 18. a 34. r.ż. Najmniej bezpiecznie czują się z kolei osoby powyżej 65. r.ż.



Pomimo przekonania o swojej wiedzy i wysokim poczuciu własnego bezpieczeństwa, to **młodzi Polacy są grupą, która najczęściej popełnia błędy** w postaci publikacji zdjęć swoich dokumentów w sieci, udostępniania osobom trzecim loginów i haseł do logowania oraz zostawiania danych osobowych w internetowych ankietach.

90%

90 proc. badanych twierdzi, że wie, jak zadbać o bezpieczeństwo swoich danych. Zdecydowaną pewność ma jednak zaledwie 17 proc. społeczeństwa. Najpewniej czują się przedstawiciele młodego pokolenia w wieku między 18. a 34. r.ż.



Równocześnie, w porównaniu z 2021 rokiem, **zwiększyła się grupa osób, która nie wie, co należy zrobić** w przypadku wyłudzenia danych osobowych. Największy wzrost niepewności obserwujemy wśród ankietowanych powyżej 65. r.ż.



O bezpieczeństwie danych **najchętniej rozmawiamy ze swoim znajomymi.** Rzadziej z członkami rodziny.

Oszuści wyłudzający dane osobowe największym zagrożeniem

W 2022 roku nadal tak samo definiujemy zagrożenia dla naszych danych. Co trzeci badany uważa, że najbardziej musimy się obawiać wycieków z baz instytucji lub firm. **Jako najgroźniejszych wskazaliśmy jednak oszustów wyłudzających dane. Na pierwszym miejscu umieściło ich blisko 43 proc. ankietowanych.** Prawie 23 proc. badanych boi się z kolei kradzieży danych ze strony hakerów.

Jedyną grupą, która wyżej od innych zagrożeń stawia wycieki danych, są mężczyźni. Ponad 40 proc. z nich wskazało je jako największe niebezpieczeństwo. Znajdujący się na drugim miejscu oszuści wyłudzający dane, przerażają co trzeciego ankietowanego płci męskiej (37 proc.).



Wykres 1

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



Kradzież danych w wyniku próby wyłudzenia poprzez oszustwo (fałszywe telefony, e-maile, SMS-y itp.)

42,9%

Kradzież danych podczas włamania do komputera lub telefonu

22,7%

Wyciek danych z firm prywatnych

19,3%

Wyciek danych z instytucji państwowych

15,1%

Tylko 55 proc. z nas wie, co należy zrobić w przypadku wyłudzenia danych osobowych, takich jak: imię, nazwisko, adres lub PESEL. Wśród młodych osób w wieku 18–34 lata ten odsetek wynosi około 65 proc. Pozostali nie wiedzą lub mają wątpliwości. Do tych najczęściej przyznają się osoby po 34. r.ż. Blisko 1/3 z nich nie potrafi dokładnie odpowiedzieć na to pytanie.

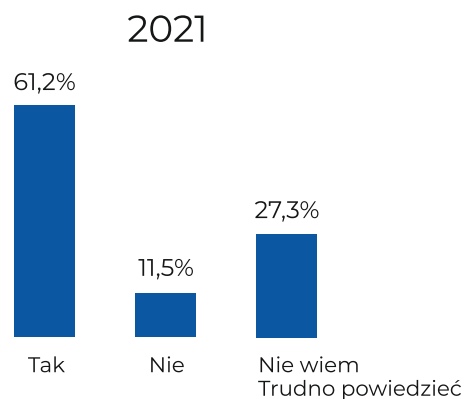
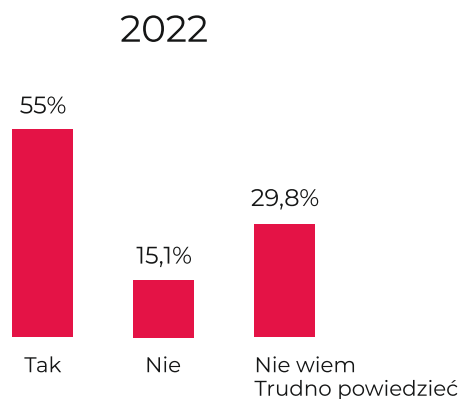
W zeszłym roku odsetek osób, które deklarowały, że wiedzą, co zrobić w takim przypadku był nieznacznie wyższy (61 proc.). Widać zatem, że w porównaniu z 2021 rokiem więcej jest osób, które mają wątpliwości lub wprost deklarują, że nie wiedzą, co zrobić w przypadku wyłudzenia lub kradzieży danych osobowych.

Opisana wcześniej tendencja jest widoczna w każdej, poza najmłodszą, grupie wiekowej. Szczególnie alarmujące powinny być odpowiedzi wśród ankietowanych mających powyżej 65 lat. Tu różnica wśród osób, które wiedzą, jak zareagować wynosi ponad 12 pp.

Wykres 2



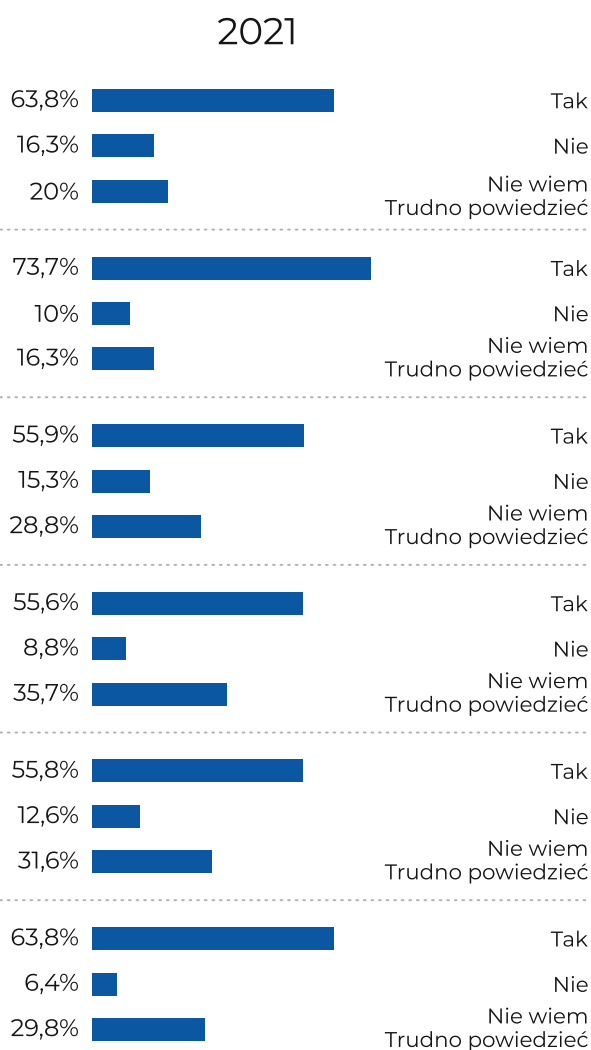
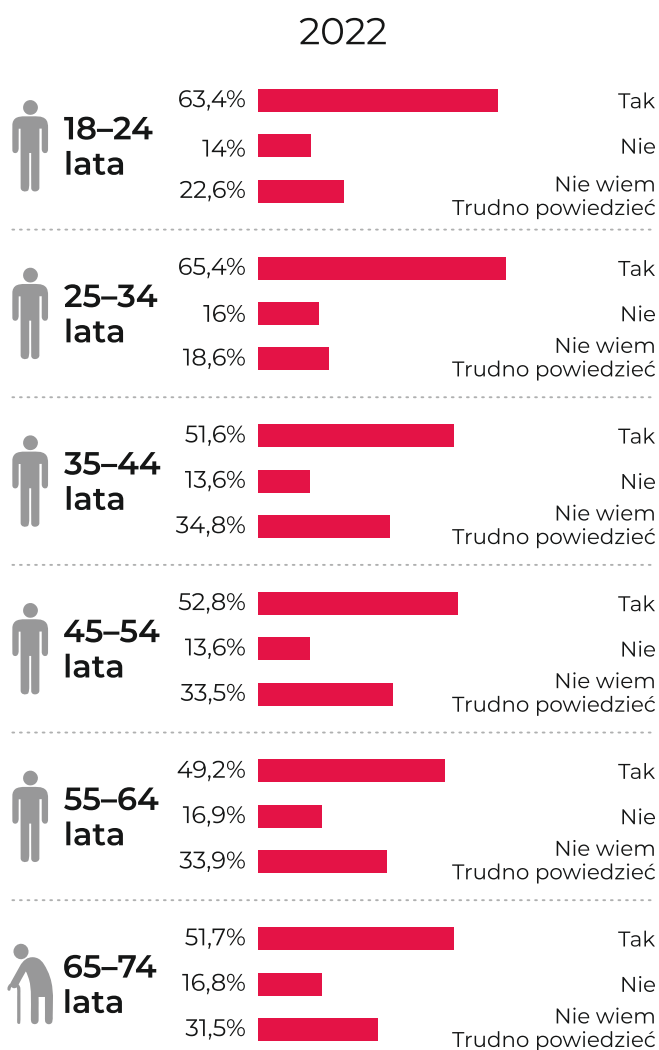
Czy wiesz, jakie działania należy podjąć w przypadku wyludzenia lub kradzieży danych osobowych, takich jak: imię, nazwisko, adres, PESEL?



Wykres 3



Wiem, jak zareagować w przypadku wyludzenia danych osobowych



Ponad 80 proc. z nas sprawę wyłudzenia danych osobowych zgłosiłoby na policję. Blisko 3/4 o zdarzeniu poinformowałaby swój bank, a prawie 40 proc. najbliższą placówkę bankową. 68 proc. badanych zmieniłoby także hasła do logowania w serwisach, z których korzystają. Ponad 45 proc. ankietowanych zgłosiłoby sprawę do UODO, a blisko co czwarty sprawdziłby w biurze informacji gospodarczej, czy ktoś nie próbował już wykorzystać skradzionych danych.



Wykres 4

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





Zdaniem eksperta

Monika Krasińska

dyrektor Departamentu Orzecznictwa i Legislacji, UODO

” To, jak postąpić, gdy nasze dane osobowe zostały wykradzione lub wyludzone, zależy od tego, jakie informacje dostały się w niepowołane ręce. Podstawowymi krokami są:

1. zgłoszenie sprawy na policję,
2. poinformowanie banku,
3. zgłoszenie się do dowolnego urzędu gminy w celu unieważnienia dowodu osobistego (jeśli dodatkowo był w nim wgrany kwalifikowany podpis elektroniczny od prywatnego dostawcy, to w celu jego unieważnienia trzeba skontaktować się bezpośrednio z tym dostawcą),
4. zmiana haseł do logowania i ustawienie dwuskładnikowego uwierzytelnienia,
5. monitorowanie aktywności na kontach,
6. sprawdzenie, czy ktoś nie posłużył się naszymi danymi.

Jednocześnie nieustannie warto też przypominać, że najważniejsza jest zasada ograniczonego zaufania i zachowywanie zdrowego rozsądku. Mimo bowiem deklarowania, że wiemy, jak rozpoznać próby oszustwa mające na celu wyludzenie danych, to w codziennym zachowaniu wciąż popełniamy błędy.

Dotyczy to zwłaszcza młodych, którym radzę, by z większą rozwagą udostępniali w sieci informacje na swój temat. Nie publikowali np. zdjęć różnego rodzaju dokumentów - otrzymanych właśnie dowodów osobistych, kart kredytowych czy praw jazdy.

Nieuleganie emocjom i staranna weryfikacja osób, które nawiązują z nami kontakt za pośrednictwem sieci lub telefonu to kolejna rada. Tylko ostrożność oraz dokładne weryfikowanie informacji i internetowych kontaktów pozwoli ograniczyć ryzyko zdobycia przez cyberprzestępców, którzy stosują coraz bardziej wyrafinowane metody, dostępu do zawartości naszych komputerów czy smartfonów, a za ich pośrednictwem do naszych kont bankowych, kont w portalach społecznościowych czy skrzynek poczty elektronicznej.

Niestety, nawet zachowanie wszystkich zasad bezpieczeństwa może nie wystarczyć, żeby uchronić się przed wykorzystaniem naszych danych osobowych. Nie wiemy na przykład, w jaki sposób zabezpieczone są bazy danych serwisów internetowych, 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.

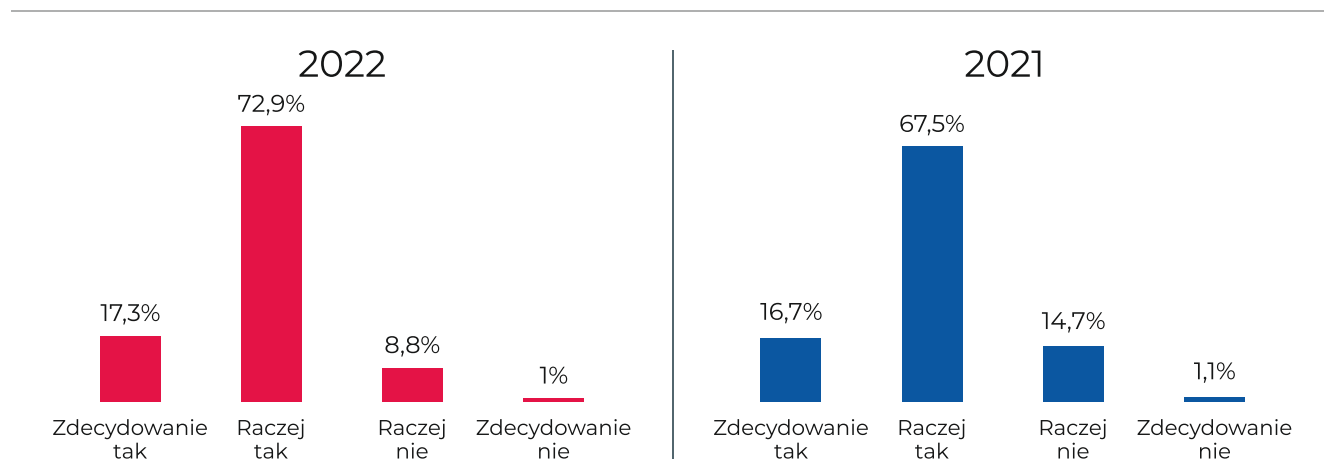
Młodzi Polacy przekonani, że trudno ich oszukać

Zdecydowana większość ankietowanych deklaruje, że wie, jak zadbać o bezpieczeństwo swoich danych osobowych. Tak uważa 90 proc. badanych. Zdecydowaną pewność ma co szósty ankietowany (17 proc.). W porównaniu z przeprowadzonym rok temu badaniem dotyczącym bezpieczeństwa danych w czasie pandemii koronawirusa, obserwujemy nieznaczny wzrost wśród osób, które wiedzą, jak zadbać o swoje bezpieczeństwo lub wydaje im się, że potrafią to zrobić. W 2021 roku ten odsetek wynosił 84 proc.



Wykres 5

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

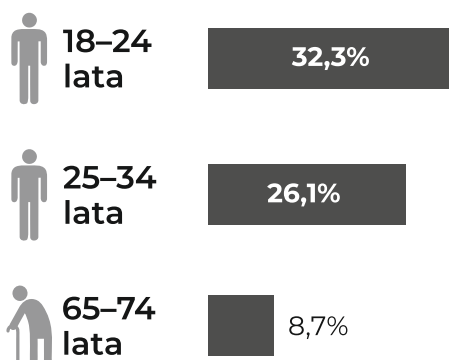


Najpewniej czują się ludzie młodzi. Co trzeci ankietowany w wieku 18–24 lata i co czwarty w wieku 25–34 lata jest absolutnie pewny swojej wiedzy na temat bezpieczeństwa. Najwięcej wątpliwości mają z kolei osoby powyżej 65. r.ż. Tylko niespełna 9 proc. z nich twierdzi, że doskonale wie, jak zadbać o swoje bezpieczeństwo.



Wykres 6

Zdecydowanie wiem, jak zadbać o bezpieczeństwo swoich danych osobowych



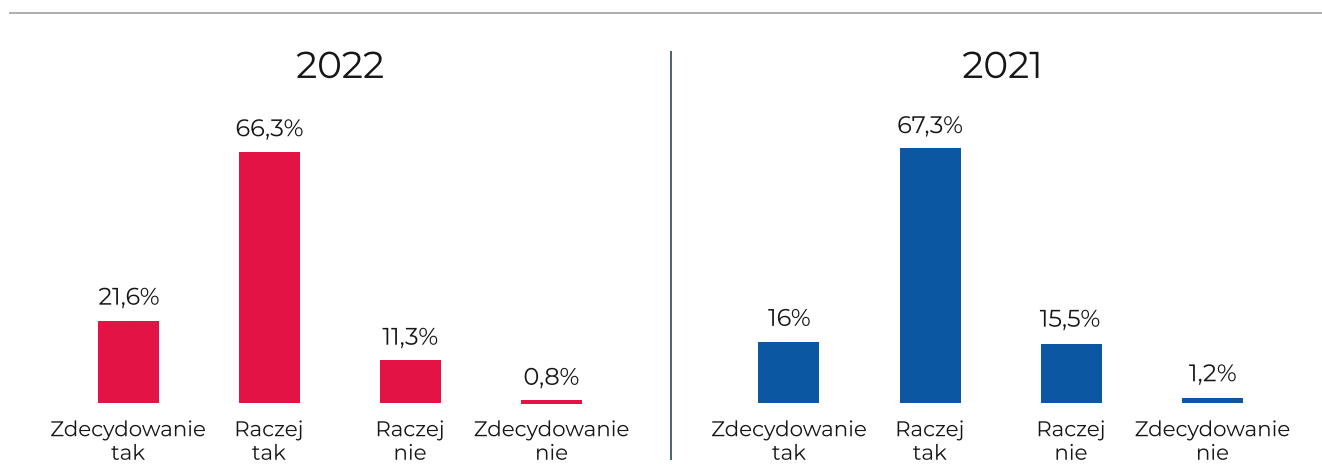
Wysokie jest także przekonanie na temat własnych umiejętności rozpoznania prób oszustwa mającego na celu wyłudzenie danych osobowych. 88 proc. ankietowanych jest przekonanych, że zorientuje się, jeśli będzie miało do czynienia z dzwoniącym oszustem lub fałszywymi wiadomości e-mail i SMS. Zdecydowaną pewność co do tego ma ponad 20 proc. badanych.

W ubiegłym roku odsetek osób, które wiedziały, jak rozpoznać oszusta wynosił 83 proc., zdecydowanie pewnych swoich umiejętności było 16 proc. ankietowanych. Widać zatem niewielki wzrost w tej grupie.

Wykres 7



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



Kobiety częściej niż mężczyźni mają wątpliwości, czy uda im się rozpoznać oszusta. Deklaruje tak ponad 16 proc. z nich (u mężczyzn 7,5 proc.). Warto zwrócić uwagę na zmianę względem zeszłego roku w grupie mężczyzn. Wówczas odsetek mających wątpliwości co do swoich umiejętności u panów był prawie dwukrotnie wyższy.

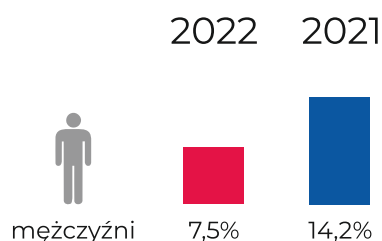
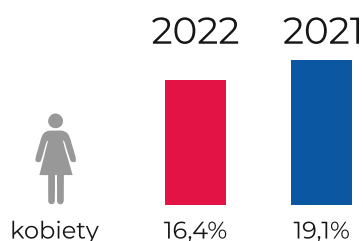
Ponownie największą pewność obserwujemy w grupie najmłodszych respondentów. Co trzeci ankietowany w wieku 18–24 lata i 25–34 lata jest przekonany, że z łatwością rozpozna próbę oszustwa. Mniej pewni są z kolei ankietowani między 45. a 54. r.ż., z których 16 proc. ma poważne wątpliwości, co do własnych umiejętności oraz najstarsza grupa ankietowanych (12,1 proc.).

W porównaniu z ubiegłym rokiem należy zauważyć wzrost liczby osób pewnych zwycięstwa w konfrontacji z oszustami. Zwłaszcza w grupie 18–34 lata oraz, co ciekawe, wśród osób w wieku 55–64 lata.



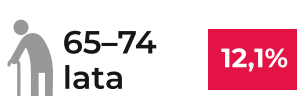
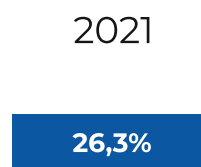
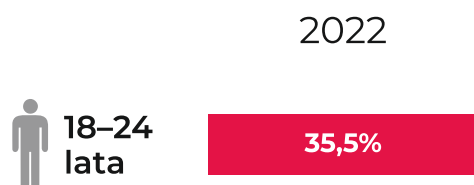
Wykres 8

Nie mam pewności, że rozpoznam fałszywą wiadomość lub nie potrafię tego zrobić



Wykres 9

Mam zdecydowaną pewność, że rozpoznam fałszywą wiadomość

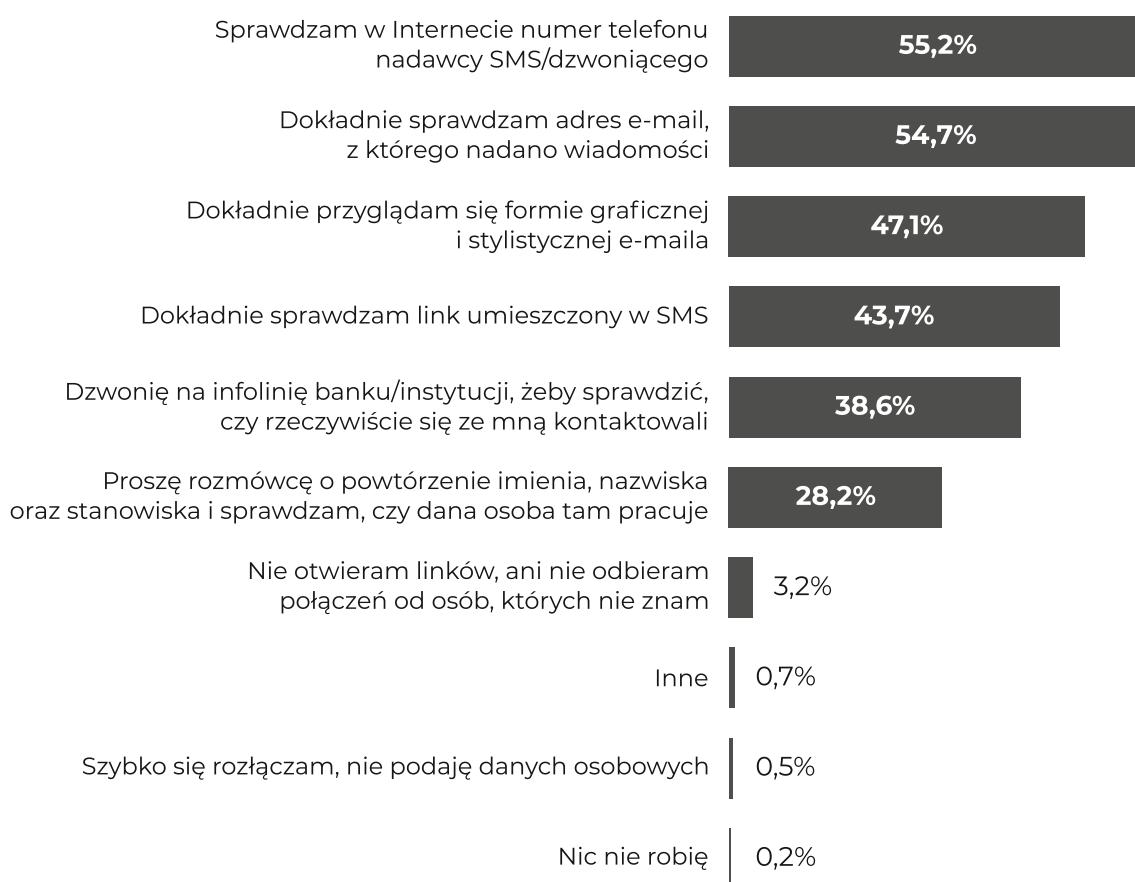


Zapytani o to, jak weryfikują autentyczność otrzymanych wiadomości i połączeń, ankietowani najczęściej wskazują na sprawdzenie rozmówcy w Internecie i przeanalizowanie adresu e-mailowego nadawcy wiadomości. Robi tak 55 proc. badanych. W dalszej kolejności sprawdzamy dokładnie załączony link oraz formę graficzną i treść otrzymanego komunikatu. Najczęściej z internetowej weryfikacji korzystają ludzie młodzi w wieku między 18. a 34. r.ż.



Wykres 10

W jaki sposób weryfikujesz autentyczność otrzymywanych wiadomości lub odbieranych połączeń?



Blisko 40 proc. z nas kontaktuje się także z infolinią instytucji, w imieniu której dzwoni do nas rzekomy konsultant. Tę formę weryfikacji preferują z kolei ankietowani w grupie 45–74 lata.



Zdaniem eksperta

Bartłomiej Drozd

ekspert serwisu ChronPESEL.pl

„ Powinniśmy unikać klikania w jakiegokolwiek linki, kierujące nas do strony z płatnością lub zachęcające do pobrania nowego oprogramowania, które umieszczone są w wiadomościach e-mail lub SMS-ach. Zwłaszcza, jeśli otrzymaliśmy od niezweryfikowanego nadawcy. W takich sytuacjach należy dokładnie sprawdzić adres mailowy oraz strony WWW, do której jesteśmy odsyłani. Oszuści często starają się maksymalnie upodobnić do prawdziwych witryn, więc różnice są na pierwszy rzut oka trudno zauważalne.

To często jedna litera lub pojedynczy symbol.

Dlatego warto poświęcić chwilę czasu na dokładne sprawdzenie. Podszywając się pod pracowników banków, firm energetycznych, dostawców Internetu czy pracowników instytucji publicznych oszuści starają się wykorzystać naszą niewiedzę. Należy pamiętać, że żaden konsultant, ani urzędnik nie będzie przez telefon żądać naszych danych osobowych w celu weryfikacji ani zachęcać do pobrania programów, które to zrobią. Sama taka prośba powinna być dla nas sygnałem ostrzegawczym. W takich sytuacjach warto się rozłączyć i samodzielnie zadzwonić na numer infolinii lub do naszego opiekuna klienta, żeby zweryfikować sprawę. Unikniemy w ten sposób przykrych konsekwencji.



Niebezpieczne zachowania – lista grzechów

Na niewiele zdadzą się różnego rodzaju zabezpieczenia, jeśli sami udostępnimy wrażliwe informacje. Co dziewiąty ankietowany przyznaje, że zdarzyło mu się przekazać osobom trzecim swoje dane do logowania. Największy odsetek takich odpowiedzi udzieliły osoby w wieku 18–24 lata (28 proc.) oraz 25–34 lata (16 proc.). Jednocześnie to dwie grupy, które najczęściej twierdziły, że wiedzą, jak zadbać o bezpieczeństwo swoich danych osobowych. To pokazuje, że wcześniejsze deklaracje nie zawsze są poparte właściwymi zachowaniami.

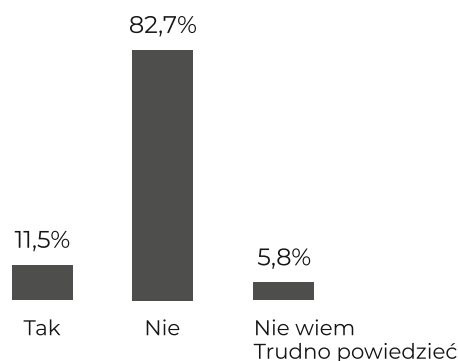
Znacznie bardziej ostrożni w tym aspekcie są ankietowani powyżej 45. r.ż. W porównaniu z 2021 rokiem nie doszło tutaj do znaczących zmian.



Wykres 11

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

LOGIN



Wykres 12

Zdarzyło mi się przekazać osobom trzecim moje dane do logowania

LOGIN

 18–24 lata

28%

 45–54 lata

6,3%

 25–34 lata

16%

 55–64 lata

5,5%

 35–44 lata

13,6%

 65–74 lata

6%

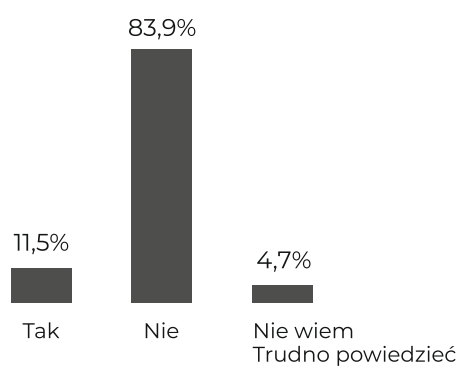
Udostępnianie danych do logowania to jednak nie wszystko. 11,5 proc. ankietowanych przyznaje, że opublikowało kiedyś w sieci zdjęcie swoich dokumentów. W przypadku osób w wieku 18–24 lata, zrobił tak nawet co piąty badany. Niewiele lepiej jest wśród osób między 25. a 44. r.ż.

Sytuacja poprawia się dopiero wśród ankietowanych powyżej 55. r.ż., wśród których ten odsetek spada poniżej 10 proc. Nie musi to jednak oznaczać wyższej świadomości, ale także mniejszą częstotliwość korzystania z sieci.



Wykres 13

**Czy zdarzyło Ci się opublikować
w sieci zdjęcie dokumentów?**



Wykres 14

**Zdarzyło mi się opublikować
w sieci zdjęcia moich dokumentów**



 **18–24
lata**

19,4%

 **45–54
lata**

10,8%

 **25–34
lata**

14,9%

 **55–64
lata**

8,7%

 **35–44
lata**

11,8%

 **65–74
lata**

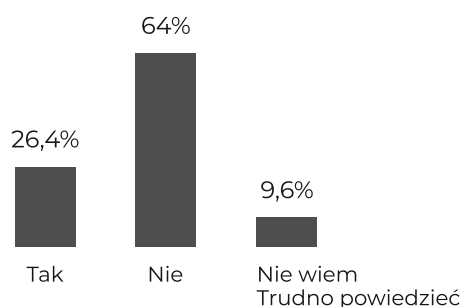
6%

Lista grzechów jest jednak dłuższa. Co czwarty badany przyznaje, że zdarzyło mu się wypełnić w sieci ankietę, która wymagała podania danych, takich jak numer PESEL czy adres zamieszkania. Wśród osób w wieku 18–34 lata dotyczy to nawet co trzeciego badanego.

Wykres 15



Czy zdarzyło Ci się wypełnić ankietę internetową wymagającą podania danych osobowych, np. PESEL, adresu zamieszkania, adresu e-mail?



Wykres 16



Zdarzyło mi się wypełnić ankietę internetową wymagającą podania danych osobowych



18–24
lata

36,6%

45–54
lata

21,6%

25–34
lata

35,6%

55–64
lata

26,2%

35–44
lata

24%

65–74
lata

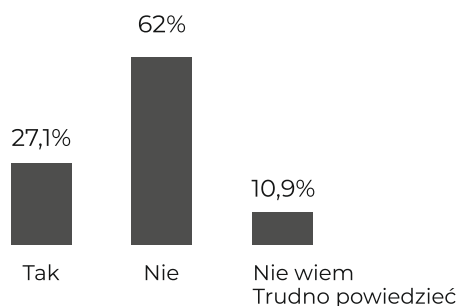
18,1%

Blisko 2/3 ankietowanych deklaruje również, że przez ostatni rok nie zlikwidowało swoich kont w serwisach społecznościowych, z których dawno nie korzystało. Wyjątkiem są osoby w wieku 18–24 lata. Prawie 37 proc. z nich zrobiło porządek w swoich mediach społecznościowych. Względem 2021 roku nie ma tutaj większych zmian.



Wykres 17

Czy przez ostatni rok zlikwidowałeś konta w serwisach internetowych, z których od dawna nie korzystałeś?



Wykres 18

Przez ostatni rok zlikwidowałem swoje konta w mediach społecznościowych, z których dawno nie korzystałem



 **18–24
lata**

36,6%

 **45–54
lata**

22,2%

 **25–34
lata**

27,7%

 **55–64
lata**

26,8%

 **35–44
lata**

26,2%

 **65–74
lata**

28,2%

Konsekwencje utraty danych osobowych

Skutki utraty danych osobowych mogą być bardzo dotkliwe. Oszuści, którzy je przejęli mają wiele możliwości ich wykorzystania. Jak wynika z przeprowadzonego badania, Polacy zdają sobie sprawę z tego, jak przestępcy wykorzystują skradzione dane osobowe.

Zapytani o to, najczęściej wskazują na zaciąganie zobowiązań finansowych w postaci np. umowy kredytowej na zakupy, leasingu lub pożyczki (86 proc.). W dalszej kolejności, jako konsekwencję utraty danych podają możliwe próby oszustwa naszych bliskich z wykorzystaniem skradzionej tożsamości (75 proc.). Blisko 2/3 ankietowanych obawia się także sprzedaży danych oraz wykorzystania ich do założenia firmy, która zaciągnie kolejne zobowiązania finansowe.

Analizując wskazania w poszczególnych grupach, widać jednak, że w zależności od wieku hierarchia możliwych konsekwencji nieznacznie się od siebie różni. Ankietowani między 25. a 34. r.ż., inaczej niż pozostali, najczęściej wskazywali na możliwość wykorzystania skradzionych danych do próby oszustwa naszych bliskich. Z kolei najstarsza grupa badanych, jako drugie możliwe zagrożenie wybrała założenie firmy na przejętą przez przestępców tożsamość.



Wykres 19

W jaki sposób przestępcy mogą wykorzystać Twoje dane osobowe?



Mogą zaciągnąć na moje dane zobowiązania finansowe w postaci np. umów: kredytowej na zakupy albo leasingowej/pożyczkowej

85,8%

Mogą, podszywając się ode mnie, próbować oszukać moich przyjaciół w celu uzyskania korzyści finansowych

75,1%

Mogą sprzedać moje dane osobowe

68%

Mogą założyć firmę na moje dane, na którą zaciągną kolejne zobowiązania finansowe

63,7%

Mogą mnie szantażować w celu uzyskania korzyści finansowych

51,1%

Wykres 20



W jaki sposób przestępcy mogą wykorzystać

Twoje dane osobowe?

Najczęstsze wskazania/Podział na grupy wiekowe



Mogą zaciągnąć na moje dane zobowiązania finansowe w postaci np. umów: kredytowej na zakupy albo leasingowej/pożyczkowej

88,9%

 35–44 lata

Mogą, podszywając się pode mnie, próbować oszukać moich przyjaciół w celu uzyskania korzyści finansowych

82,6%

 25–34 lata

Mogą sprzedać moje dane osobowe

76,3%

 65–74 lata

Mogą założyć firmę na moje dane, na którą zaciągną kolejne zobowiązania finansowe

77,3%

 65–74 lata

Mogą mnie szantażować w celu uzyskania korzyści finansowych

60,3%

 18–24 lata



Zdaniem eksperta

Bartłomiej Drozd

ekspert serwisu ChronPESEL.pl



Konsekwencje związane z wyłudzeniem danych mogą być bardzo poważne.

Dysponując danymi z naszego dowodu osobistego, przestępcy mogą wziąć pożyczkę w Internecie lub zaciągnąć inne zobowiązanie finansowe podszywając się pod nas, np. podczas zakupów w sklepie ze sprzętem elektronicznym lub podpisując umowę z operatorem telekomunikacyjnym. Żeby tego uniknąć powinniśmy rozważnie zarządzać naszymi danymi osobowymi. Przede wszystkim starajmy się nie podawać ich w Internecie w sytuacjach, które tego nie wymagają. Unikajmy wszelkiego rodzaju formularzy wymagających podania numeru PESEL, numeru dowodu osobistego, adresu, nazwiska czy numeru telefonu. Zawsze należy upewnić się, że w przypadku rodzaju usługi, z której chcemy skorzystać, np. zakupów, zasadne jest podawanie wszystkich wymaganych przez serwis danych. Nie ignorujmy także publikowanych w mediach ostrzeżeń, które często bardzo precyzyjnie opisują nowe metody działania oszustów. A jeśli okaże się, że nasze dane wyciekły, jak najszybciej sprawdźmy, czy ktoś nie próbował już ich wykorzystać. W takich przypadkach bardzo ważna jest szybka reakcja.

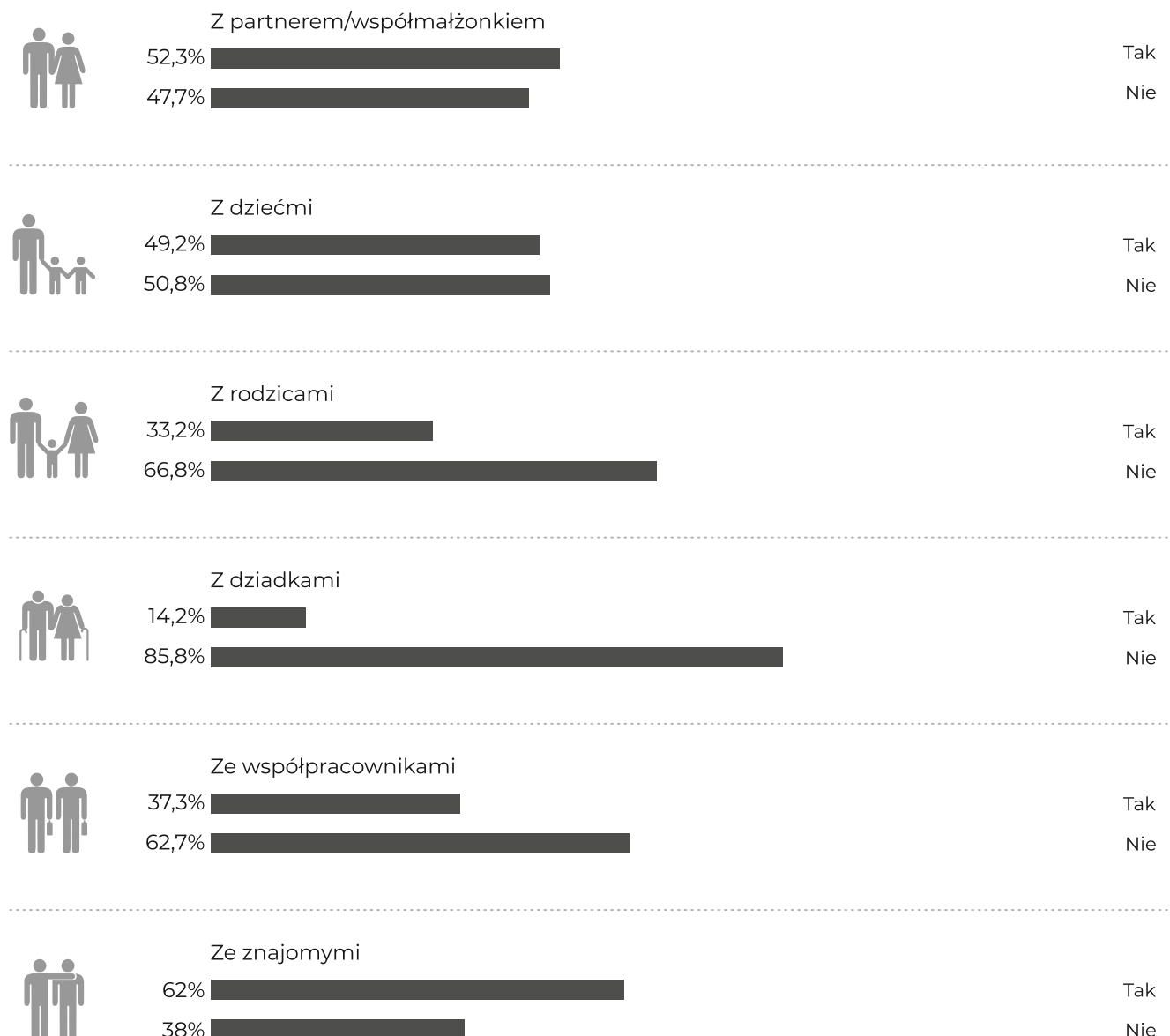
O bezpieczeństwie danych osobowych najchętniej rozmawiamy ze znajomymi

Ponad połowa ankietowanych deklaruje, że rozmawia o zasadach bezpieczeństwa swoich danych osobowych w sieci z partnerem lub współmałżonkiem. Najczęściej dotyczy to osób powyżej 45. r.ż. Połowa ankietowanych rozmawia o tym ze swoimi dziećmi. W przypadku osób w wieku 45–54 lata oraz powyżej 65. r.ż. ten odsetek wynosi ok. 60 proc. Tylko co trzeci ankietowany rozmawia o tych sprawach ze swoimi rodzicami, a niewiele ponad 14 proc. z dziadkami. Najczęściej rozmawiamy o tym ze znajomymi. Tak deklaruje blisko 2/3 ankietowanych.



Wykres 21

Czy zdarza ci się rozmawiać o zasadach bezpieczeństwa w sieci?





Zdaniem eksperta

Urszula Góral

dyrektor Departamentu Współpracy Międzynarodowej i Edukacji, UODO

” Urząd Ochrony Danych Osobowych, w ramach swoich działań edukacyjnych, m.in. prowadząc od 2009 r. ogólnopolski program dla szkół pn. „Twoje dane – Twoja sprawa”, angażuje się w podnoszenie poziomu świadomości w zakresie ochrony danych osobowych i prywatności. Działania te skierowane są przede wszystkim do szkół: uczniów i nauczycieli, ale również obejmują całe otoczenie społeczno-gospodarcze, a także rodziców i opiekunów.

Widzimy potrzebę ciągłego edukowania szczególnie w kwestii promowania bezpiecznych zachowań dzieci w sieci, ponieważ młodzi ludzie są mniej świadomi ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych, co wynika z zapisów ogólnego rozporządzenia o ochronie danych – RODO. Kontynuacja naszych działań edukacyjnych jest niezbędna, ponieważ według danych uzyskanych w badaniu, niestety tylko co drugi rodzic rozmawia z dzieckiem o zasadach bezpieczeństwa w sieci.



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 Kaczmarek Group, do którego należą również takie firmy i marki, jak: firma windykacyjna Kaczmarek 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.



CHRONPESEL.PL



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