CHRONPESEL.PL

KRAJOWY REJESTR DŁUGÓW www.krd.pl

OCHRONA DANYCH OSOBOWYCH W CZASIE PANDEMII

Raport Krajowego Rejestru Długów i serwisu ChronPESEL.pl

Grudzień 2020

O raporcie

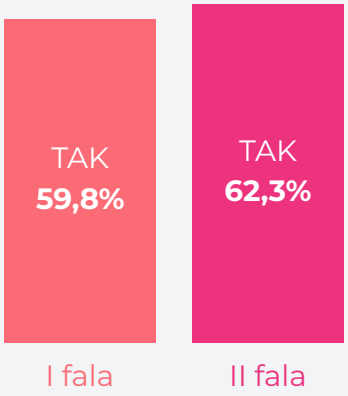
Raport Krajowego Rejestru Długów i serwisu ChronPESEL.pl „Ochrona danych osobowych w czasie pandemii" prezentuje wyniki badań dotyczących świadomości Polaków na temat oszustw i wyłudzeń w trakcie I i II fali epidemii koronawirusa. Porównanie odpowiedzi pozwoliło odpowiedzieć na pytania, jak zmieniło się podejście Polaków do ochrony danych osobowych w tym czasie oraz czy wyciągnęli wnioski po I fali epidemii. Udzielone przez respondentów odpowiedzi umożliwiły również stworzenie portretu oszustów wyłudzających wrażliwe dane. Badania zostały przeprowadzone w kwietniu i listopadzie 2020 r. przez IMAS International na zlecenia Krajowego Rejestru Długów i serwisu ChronPESEL.pl na próbie 515 osób.

Raport Krajowego Rejestru Długów i serwisu ChronPESEL.pl
Grudzień 2020

Szum informacyjny

Pandemia to czas wzmożonej aktywności przestępców próbujących wyłudzić nasze dane osobowe. Ten pogląd podziela prawie 2/3 Polaków. Porównując odpowiedzi z kwietnia i listopada 2020 r. z badania przeprowadzonego przez Krajowy Rejestr Długów i serwis ChronPESEL.pl, widać, że **podczas II fali epidemii te obawy się nasiliły.**

Pytanie:
Czy uważasz, że w czasie pandemii koronawirusa jesteś bardziej narażony/a na wyłudzenie Twoich danych?



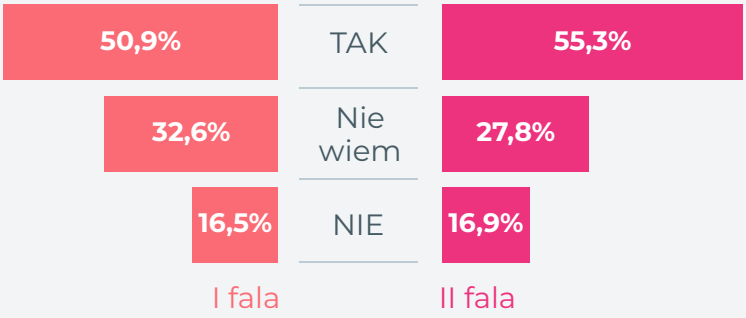
Polacy są niezmiennie zainteresowani informacjami na temat zagrożeń i wyłudzeń w czasie pandemii. Tu odsetek chcących wiedzieć, w jaki sposób przestępcy próbują ich oszukać utrzymuje się na wysokim poziomie – 84,9 proc. badanych, czyli o 1 pp. więcej niż podczas I fali epidemii.

W zestawieniu z tym, nieco zaskakujący może być **zauważalny spadek zaangażowania, jeśli chodzi o samodzielne poszukiwanie informacji i ostrzeżeń dotyczących wyłudzeń i związanych z nimi zagrożeń**. Jeszcze 6 miesięcy temu wiadomości na ten temat starało się zdobyć ponad 60 proc. badanych. Jak wynika z przeprowadzonego w listopadzie badania, podczas drugiej fali ledwie powyżej połowy (51,2 proc.) ankietowanych postępuje w ten sposób. Wpływ na to, że **Polacy rzadziej szukają informacji na temat zagrożeń i wyłudzeń** może mieć fakt, iż mechanizm działania przestępców jest już znany – najczęściej podszywają się pod inne instytucje lub firmy. W zależności od miesiąca i okoliczności zmieniają się tylko urzędy, pod które próbują się podszyć. Dodatkowo wszystkie instytucje na bieżąco informują o próbach oszustwa bazujących na ich nazwie.

Działalność oszustów

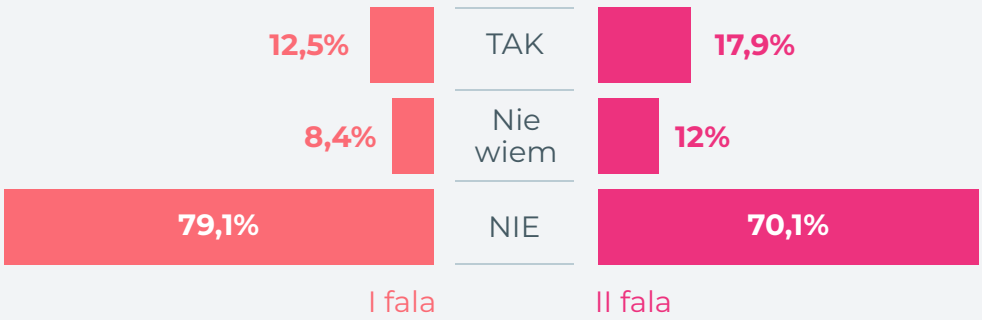
Doświadczenie pokazuje, że **obawy dotyczące większej aktywności oszustów w trakcie epidemii koronawirusa są całkowicie uzasadnione**. Zarówno podczas pierwszej, jak i drugiej fali pandemii ponad połowa Polaków była zdania, że natężyły się próby wyłudzenia danych. Co prawda odsetek osób, które zauważyły większą aktywność nieznacznie spadł, równocześnie jednak co 3. ankietowany nie był w stanie udzielić jednoznacznej odpowiedzi na to pytanie.

Pytanie:
Czy uważasz, że w czasie pandemii koronawirusa nastąpiło natężenie skali wysyłki fałszywych wiadomości mających na celu wyłudzenia danych?



Jednocześnie **wzrosła liczba osób, które doświadczyły próby oszustwa**. Jak wynika z przeprowadzonych badań, 17,9 proc. ankietowanych twierdzi, że w trakcie II fali pandemii otrzymało podejrzaną wiadomość – e-mail, SMS lub telefon. Porównując to z początkiem epidemii widać wzrost o 5,4 pp. Należy zwrócić również uwagę na grupę osób, które na to pytanie odpowiedziały „Nie wiem/trudno powiedzieć". W drugiej edycji badania ten odsetek wyniósł 12 proc., o 4 pp. więcej niż w kwietniu 2020 r.

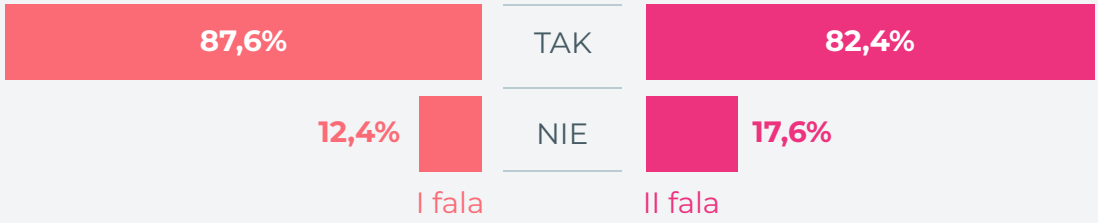
Pytanie:
Czy w czasie II fali pandemii koronawirusa otrzymałeś/aś podejrzany e-mail, sms bądź kontakt telefoniczny skłaniający do podjęcia jakichś działań związanych z koronawirusem?



Świadczy to nie tylko o większej aktywności przestępców próbujących wyłudzić dane, ale również o tym, że stale **powiększa się grupa osób, które mają problem z rozpoznaniem fałszywych wiadomości.**

Potwierdzają to również odpowiedzi na kolejne pytanie dotyczące umiejętności rozpoznania fałszywych wiadomości. Tutaj widać wyraźnie, że obecnie więcej osób ma z tym problem. Podczas I fali pandemii brak pewności deklarowało 12,4 proc. W przeprowadzonym w drugiej połowie listopada badaniu, ten odsetek wzrósł do 17,6 proc.

Pytanie:
Czy wiesz, jak rozpoznać fałszywą wiadomość powołującą się na bank bądź inny powszechnie znany podmiot?

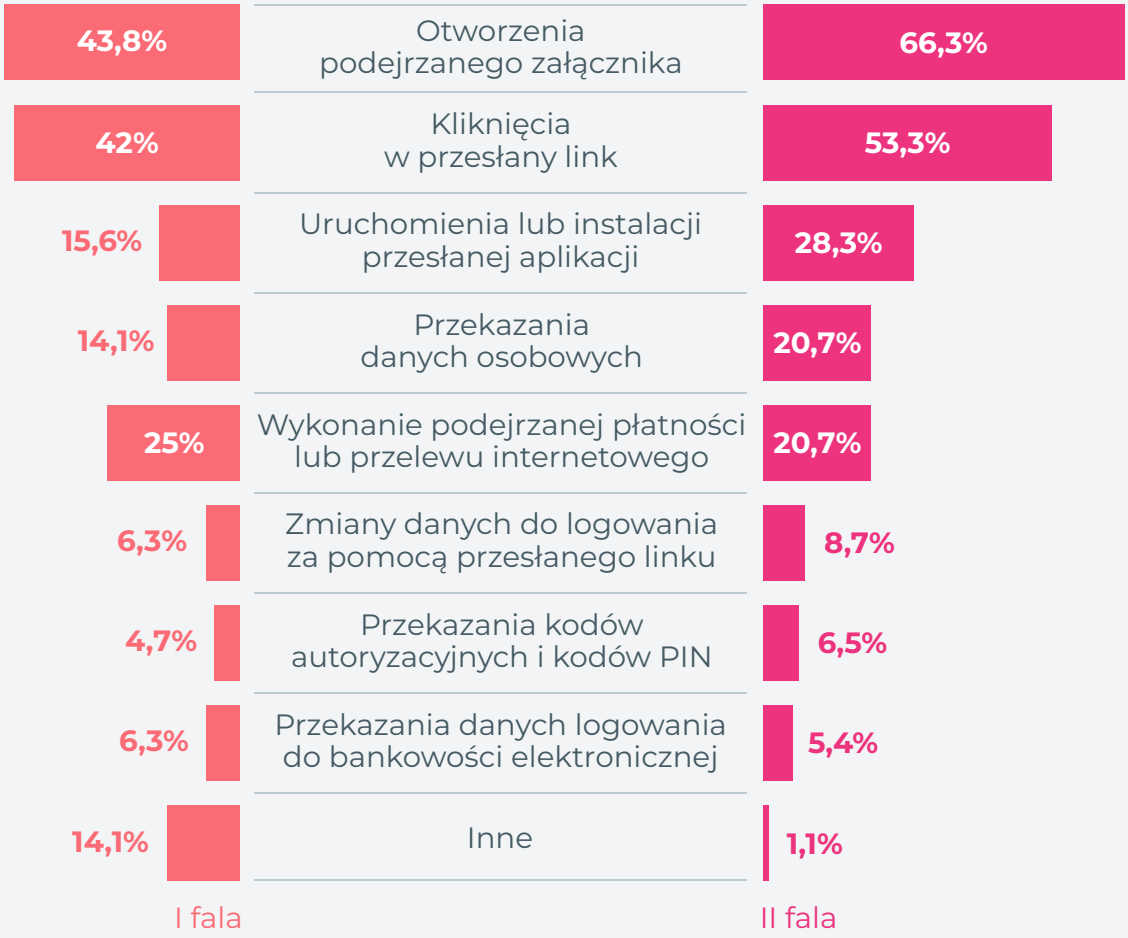


Co 6. Polak otrzymał w czasie pandemii podejrzaną wiadomość powołującą się na bank lub inną instytucję.

Wysyłane przez oszustów wiadomości najczęściej zachęcały do pobrania załącznika, kliknięcia w przesłany link bądź uruchomienia lub instalacji nowej aplikacji. Respondenci zwrócili również uwagę na to, że w przesłanych wiadomościach często byli proszeni o przekazanie danych osobowych lub wykonanie przelewu internetowego. We wszystkich tych przypadkach scenariusz jest łatwy do przewidzenia. W przypadku kliknięcia w umieszczony odnośnik lub pobrania załączonego pliku, na komputerze ofiary zainstalowane zostałoby szkodliwe oprogramowanie, dzięki któremu cyberprzestępcy zyskaliby dostęp do danych i haseł właściciela.

Porównując wyniki badania z początku pandemii z obecnymi, widać wyraźnie, że **próby oszustwa poprzez instalację szkodliwego oprogramowania lub wyłudzenia danych nasiliły się podczas II fali epidemii**.

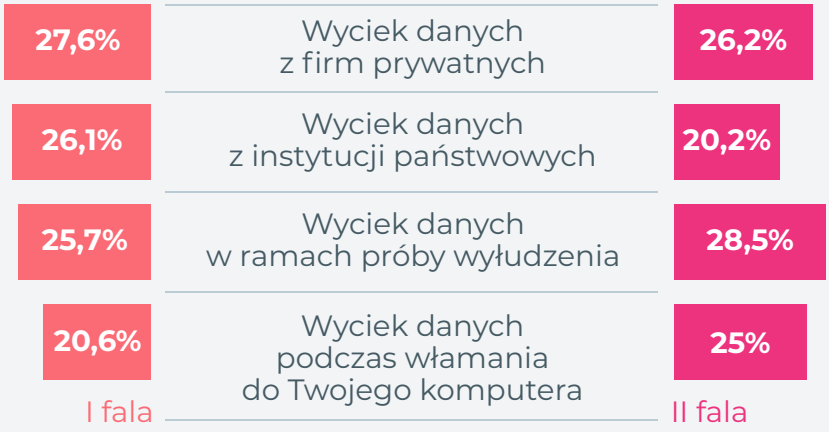
Pytanie:
Do podjęcia jakich działań związanych z koronawirusem skłaniał otrzymany podejrzany e-mail, sms bądź kontakt telefoniczny?



Polacy boją się wycieku ich danych z urzędów i firm

Jak wynika z przeprowadzonego badania, ponad 60% Polaków boi się, że w okresie epidemii koronawirusa ich dane osobowe wpadną w niepowołane ręce. Bardziej niż hakerów, którzy włamią się do ich komputera, obawiają się jednak wycieków danych z urzędów i firm. Co prawda, w trakcie II fali pandemii, odsetek ten w porównaniu z początkiem epidemii jest niższy. Wciąż jednak podobne obawy wyraża blisko połowa (46,4 proc.) Polaków. Równocześnie można zaobserwować wzrost poziomu lęku przed wyłudzeniami, których boi się już prawie 30 proc. badanych oraz atakami hakerów, które budzą strach u co 4. obywatela.

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



Powtarzające się w czasie pandemii wycieki pokazują, że te obawy są uzasadnione.

Skąd wyciekły dane?

Na początku marca 2020 media informowały, że z baz **jednej z firm pożyczkowych** do sieci wyciekły informacje na temat ponad 200 tysięcy klientów.

W kwietniu Polską wstrząsnęła wiadomość o tym, że w Internecie dostępne są imiona, nazwiska, adresy zamieszkania i numery telefonów ponad 50 tysięcy polskich sędziów i prokuratorów, które zostały skradzione z bazy **Krajowej Szkoły Sądownictwa i Prokuratury**. Sprawa wyszła na jaw po tym, jak jeden z oszustów, wykorzystując pozyskane dane, przejął konto w mediach społecznościowych jednej z poszkodowanych osób. W tym samym miesiącu do sieci trafiły poufne informacje na temat kilkuset pacjentów przebywających na kwarantannie w powiecie gnieźnieńskim. Do podobnego incydentu doszło też w **sklepie internetowym Cyfrowe.pl**, który gromadził dane klientów od 2007 r.

Z kolei w sierpniu o wycieku danych z bazy swoich pracowników poinformowała sieć **McDonald's**. Jesień przyniosła informacje o tym, że cyberprzestępcy weszli w posiadanie danych klientów **dwóch aptek internetowych**. Na początku listopada doszło z kolei do wycieku, m.in. numerów PESEL, z bazy **jednego z portali medycznych** gromadzących informacje o zdrowiu ponad 15 tys. pacjentów. W tym samym miesiącu o kradzieży danych, w tym również numerów PESEL, swoich studentów i pracowników poinformował **Uniwersytet Warszawski**.

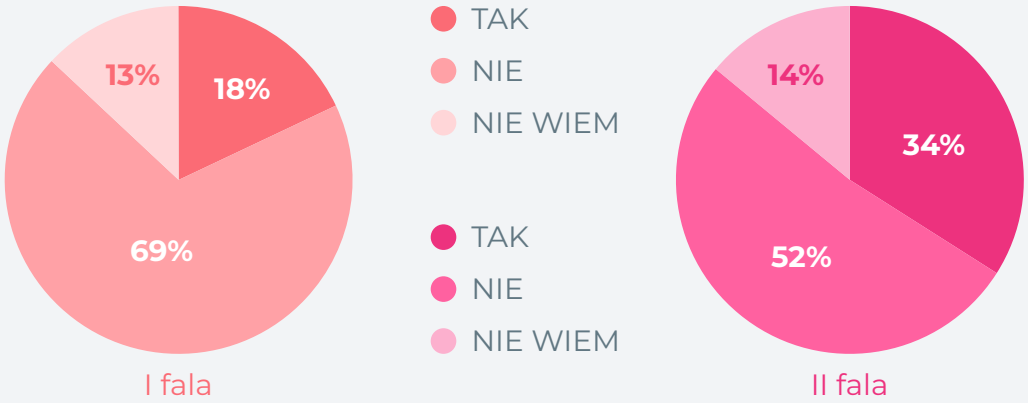
Świadomość zagrożenia a przeciwdziałanie

Ryzyko wycieku to nie jedyne zagrożenie czyhające na użytkowników Internetu. Jest nim także tzw. **phishing**, czyli metoda polegająca na podszywaniu się przez oszustów pod inne osoby lub instytucje w celu wyłudzenia poufnych informacji. Zazwyczaj zaczyna się od maila, który bardzo przypomina wiadomość z naszego banku lub firmy kurierskiej. Internauta jest proszony o kliknięcie w zamieszczony link, żeby sprawdzić swoje dane w serwisie lub zaakceptować nowy regulamin usługi. Wejście na wskazaną stronę kończy się zazwyczaj pobraniem wirusa, dzięki któremu haker zdobywa dostęp do komputera ofiary oraz ujawnieniem danych osobowych.

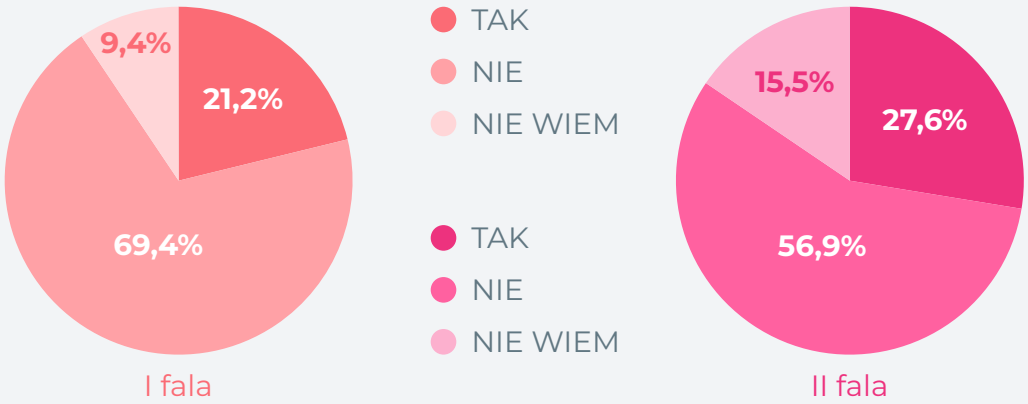
Dodatkowo porównanie wyników badania pokazuje, że pomimo większych obaw oraz zauważalnego natężenia działań oszustów, świadomość zagrożenia jest na stosunkowo wysokim poziomie. Pytanie, w jakim stopniu przekłada się to na realne działania zabezpieczające i przeciwdziałanie próbom wyłudzenia? Patrząc na wyniki obydwu badań, nie wygląda to dobrze.

Jedną z podstawowych zasad zachowania bezpieczeństwa swoich danych w sieci jest regularna zmiana używanych w Internecie haseł. Tymczasem z przeprowadzonego badania wynika, że pomimo wysokiej świadomości zagrożenia, tylko 1/3 Polaków zdecydowało się na taki ruch. Jeszcze mniej, bo zaledwie 16,9 proc. badanych, przyznało, że usunęli swoje konta w serwisach, z których dawno nie korzystali. Uruchomienie dodatkowych programów blokujących spam w urządzeniach, których używają na co dzień zadeklarowało wyłącznie 27,5 proc. badanych.

Pytanie:
Czy w czasie II fali pandemii koronawirusa zmieniłeś/aś hasła do logowania w serwisach internetowych na nowe bądź bardziej skomplikowane?

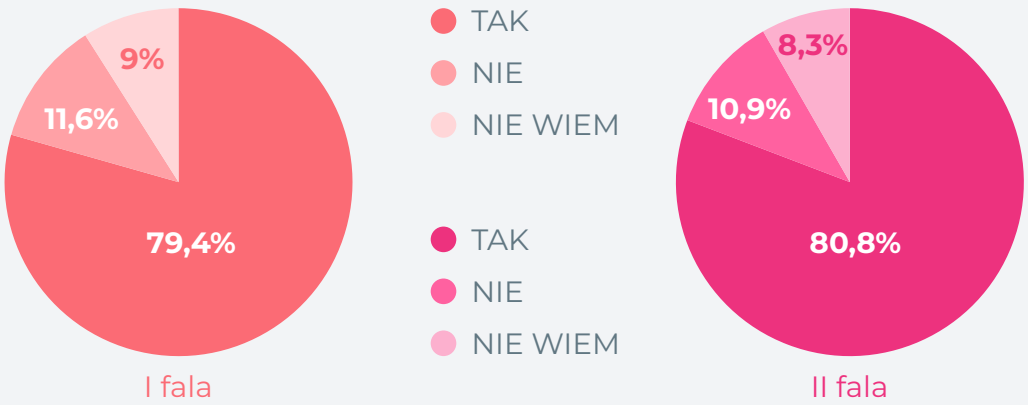


Pytanie:
Czy uruchomiłeś/aś blokady antyspamowe w swoim prywatnym laptopie lub smartfonie celem zwiększenia bezpieczeństwa swoich danych w czasie pandemii koronawirusa?



Warto przy tym zaznaczyć, że porównując odpowiedzi ankietowanych podczas II fali pandemii z wynikami badania z kwietnia 2020 r. widać wyraźnie, że Polacy są lepiej przygotowani i bardziej świadomi zagrożeń. Trudno jednak mówić o sukcesie, jeśli wciąż co 5. Polak (19,2 proc.) deklaruje, że nie ma zainstalowanego żadnego programu antywirusowego.

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



Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl

„Jeżeli nie wiemy, kto i w jakim stopniu ma w Internecie dostęp do informacji na nasz temat, stajemy się łatwym celem dla oszustów, którzy tylko szukają takich okazji. ***Dlatego bardzo ważne jest, by regularnie zmieniać hasła do swoich kont oraz ograniczać miejsca, w których udostępniliśmy nasze dane do minimum****. Z przeprowadzonych badań wynika, że pomimo rosnącej świadomości zagrożenia, wśród użytkowników Internetu wciąż przeważa myślenie na zasadzie – mi na pewno nie przytrafi się coś takiego. To może się zemścić, ponieważ pierwszym krokiem do popełnienia przestępstwa jest uśpienie czujności potencjalnej ofiary. Z doświadczenia wiadomo, że z konsekwencjami wycieku danych możemy mierzyć się nawet kilka lat po tym, jak przestępcy weszli w ich posiadanie. Stąd bardzo ważne, by zachować czujność i odpowiednio się zabezpieczyć."*

Konsekwencje

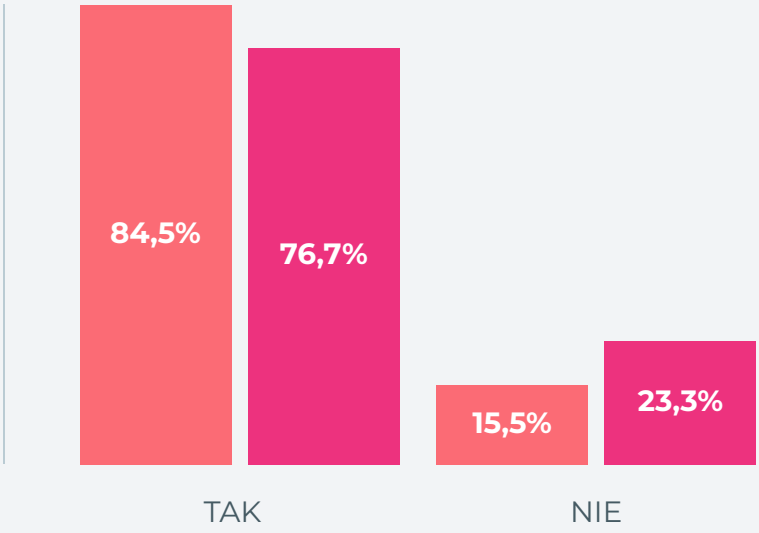
Konsekwencje ataków, które obecnie obserwujemy możemy odczuwać na długo po opanowaniu epidemii. Obecnie niewiele osób się tym przejmuje, ponieważ wydaje się, że mamy poważniejsze zagrożenia, z którymi należy się uporać. Oszuści wykorzystują zdobyte dane do tego, by podszywając się pod ich właściciela wyłudzić kredyt lub zawrzeć umowę leasingową na samochód lub drogi sprzęt elektroniczny. Niestety z konsekwencjami możemy mierzyć się nawet kilka lat po wycieku.

Jak się chronić?

Rozwój epidemii oraz towarzysząca mu wyższa aktywność oszustów wpływa dezorientująco na Polaków. Potwierdzają to wyniki badania, które pokazują, że na przestrzeni ostatnich 6 miesięcy spadła liczba osób, które deklarują, że wiedzą, jak powinny zabezpieczać swoje dane podczas pandemii. Jeszcze w trakcie I fali pewność wykazywało 84,5 proc. badanych. Obecnie już prawie **co 4. Polak nie wie, w jak chronić swoje dane osobowe w czasie pandemii**.

Pytanie:
Czy wiesz, w jaki sposób dbać o bezpieczeństwo danych w czasie pandemii koronawirusa?

I fala / II fala



Bartłomiej Drozd, ekspert serwisu ChronPESEL.pl

W tym trudnym czasie najważniejsza jest świadomość, że ktoś nas może oszukać. Dzięki temu z większą ostrożnością będziemy podchodzić do wszystkich nietypowych komunikatów, które do nas docierają. W drugiej kolejności musimy pamiętać, żeby zawsze weryfikować numer telefonu, adres mailowy oraz procedury wewnętrzne w firmach i instytucjach, które się z nami kontaktują. Zajmie to oczywiście więcej czasu, ale znacznie trudniej będzie nas oszukać. Musimy również zadbać o naszych najbliższych i uczulić ich na to, żeby stosowali zasadę ograniczonego zaufania w sytuacji, gdy ktoś przez telefon prosi o podanie ich danych albo próbuję wprosić się do domu.

Specjaliści zwracają uwagę na to, że nawet zachowanie wszystkich zasad bezpieczeństwa może nie wystarczyć do tego, 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 **Urząd Ochrony Danych Osobowych w swoim komunikacie dotyczącym reagowania w przypadku kradzieży tożsamości rekomenduje m.in. założenie konta w systemie informacji gospodarczej, celem monitorowania swojej aktywności kredytowej**.

Jak to działa w przypadku usługi ChronPESEL.pl?

Jeśli bank, firma pożyczkowa, sklep z zakupami ratalnymi lub operator komórkowy sprawdzi Twoje dane w bazie Krajowego Rejestru Długów BIG S.A., otrzymasz powiadomienie SMS-em oraz e-mailem o tym zdarzeniu. Firmy te przed podpisaniem umowy sprawdzają, czy ich potencjalni klienci nie są wpisani do Krajowego Rejestru Długów BIG S.A. Powiadomienie SMS-owe, jakie dostaniesz, może oznaczać próbę wyłudzenia kredytu, pożyczki, kupna sprzętu elektronicznego lub abonamentu telefonicznego na Twoje konto.

ChronPESEL.pl to jedyne rozwiązanie na rynku, które oferuje kompleksowe zabezpieczenie danych konsumenta. Pomoc nie kończy się na poinformowaniu klienta o potencjalnej próbie wyłudzenia – otrzymuje on również wsparcie w momencie, gdy do tego wyłudzenia dojdzie.

CHRONPESEL.PL

KRAJOWY REJESTR DŁUGÓW www.krd.pl

Redakcja i opracowanie materiału: Departament PR
Kontakt: pr@krd.pl