AVLAB
CYBERSECURITY FOUNDATION

Jak bezpiecznie funkcjonować w cyfrowym świecie ?

Zgubienie, kradzież dokumentu lub wyciek danych osobowych...

Poradnik Fundacji AVLab dla Cyberbezpieczeństwa

Sierpień 2024

Co możesz zrobić, jeśli Twoja „cyfrowa tożsamość*” została skradziona? **Do kogo** możesz się zgłosić?

- Na policję
- Do banku
- Do urzędu gminy
- Do administratora danych osobowych
- Do Urzędu Ochrony Danych Osobowych (UODO)
- Skorzystaj z Profilu Zaufanego!

Cyfrową tożsamość można tłumaczyć jako przeniesienie danych osobowych do Internetu. Może to być dowód osobisty, prawo jazdy lub inny dokument akceptowany przez polskie urzędy i instytucje. To także dane biometryczne: odciski palców w postaci cyfrowej, zeskanowana tęczówka oka, geometria twarzy - używane do weryfikacji tożsamości, autoryzacji dostępu do systemów informatycznych albo identyfikacji obywatela.

Jeśli Twój nr PESEL lub inne dane osobowe wyciekły...

Oto, co możesz zrobić, jeżeli zostaną poznane Twoje dane z dowodu osobistego na skutek zgubienia dokumentu, kradzieży albo wycieku tych informacji w wyniku cyberataku na organ państwowy bądź prywatną instytucję:

Zgłoś sprawę **na policję**

Przyjęcie sprawy przez dyżurującego policjanta automatycznie unieważni dowód z dniem zgłoszenia.
Utraty dokumentu nie musisz już zgłaszać do urzędu gminy (tak jak w przypadku zgubienia).
Jeżeli ktoś wziął pożyczkę, posługując się Twoimi danymi, należy zawiadomić dodatkowo bank, firmę pożyczkową lub operatora komórkowego, u którego posłużono się danymi w celu podpisania umowy.

Źródło: https://www.gov.pl/web/cyfryzacja/uniewaznienie-dowodu-na-policji-zmiany-w-przepisach

Zgłoś sprawę **w dowolnym banku**

Utratę dokumentu tożsamości (kradzież, zgubienie) możesz zgłosić w DOWOLNYM BANKU (nawet, jeśli nie masz jeszcze konta bankowego w tym oddziale). Wymiana informacji pomiędzy organami państwowymi nie zawsze jest skuteczna, dlatego oprócz policji warto zastrzec dokument przed nieuprawnionym użyciem i potencjalną próbą wykorzystania Twoich danych.

Zastrzeż **dowód osobisty**

Zastrzeż dowód osobisty przez Profil Zaufany. Szybko i bez wychodzenia z domu.

Źródło: https://www.gov.pl/web/gov/zglos-utrate-lub-uszkodzenie-swojego-dowodu-osobistego-uniewaznij-dowod

Zgłoś się **do urzędu**

Zgłoś się do urzędu, aby wyrobić nowy dokument. W przypadku dowodu osobistego jest to dowolny urząd gminy, a w przypadku paszportu – w punkcie paszportowym.

Spraw indywidualnej kradzieży tożsamości lub wskutek zgubienia dowodu nie należy zgłaszać do Prezesa Urzędu Ochrony Danych Osobowych, ale na policję, ponieważ policja jest uprawniona doprowadzenia postępowania i oceny czy doszło do popełnienia przestępstwa.

Zapisuj wszystkie **dowody zgłaszania**

Zapisuj wszystkie dowody zgłaszania sprawy na policję oraz inne dokumenty urzędowe.
Będzie to pomocne w postępowaniu przed sądem, zwłaszcza w sprawach dotyczących szkód majątkowych.

Źródło: https://uodo.gov.pl/pl/138/1300

Wykorzystaj dostępne komunikaty i powiadomienia w razie próby zaciągnięcia zobowiązań na Twoje dane.

Lepiej zapobiegać!

Nie możesz już powstrzymać wycieku danych osobowych. Możesz zabezpieczyć się przed konsekwencjami, **dlatego pamiętaj!** **Powierzając swoje dane komukolwiek nie masz wpływu na sposób ich przetwarzania i zabezpieczenia przed kradzieżą.**

Co możesz zrobić przed faktem wycieku oraz już (niestety) po ujawnieniu danych?
Możesz założyć konto w systemie informacji kredytowej oraz wykupić Alert BIK.
Dzięki alertowi SMS od razu dowiesz się o każdej próbie wyłudzenia kredytu na Twoje dane oraz o opóźnieniach w spłacie kredytów i innych zobowiązaniach.

Inną możliwością jest wykupienie pakietu w usłudze CHROŃ PESEL.
W zamian możesz otrzymać:

CHRONPESEL.PL

- Powiadomienie (24 godziny na dobę), gdy w rejestrze zapytań w systemie KRD BIG S.A. pojawi się informacja dotycząca ujawnienia Twoich danych.
- Powiadomienie o tym, że ktoś próbuje założyć firmę na Twoje dane.
- W niektórych pakietach jest możliwość uzyskania pomocy prawnej (zwrotu jej kosztów), w przypadku gdy do dojdzie do wykorzystania Twoich danych.
- Powiadomienie o wpisaniu do Krajowego Rejestru Długów.
- Sprawdzisz, kto wykorzystał Twój numer PESEL oraz wiarygodność dowolnej firmy.

Powiadomienie przychodzi SMS-em, gdy ktoś próbuje wyłudzić pożyczkę na Twoje dane. 24 godziny na dobę. 7 dni w tygodniu.

Zastrzeż kartę płatniczą!

Należy bezzwłocznie zastrzec kartę płatniczą w przypadku kradzieży, zgubienia albo wycieku informacji poufnych z karty – numeru karty i kodu CVV, które znajdują się na odwrocie.

Możesz to zrobić na trzy sposoby:

1. korzystając z bankowości elektronicznej
2. dzwoniąc na infolinię swojego banku
3. wykorzystać międzybankowy System Zastrzegania Kart pod numerem **828 828 828**

Więcej informacji o Systemie Zastrzegania Kart na: **https://zastrzegam.pl**

mObywatel 2.0

zrób to prościej

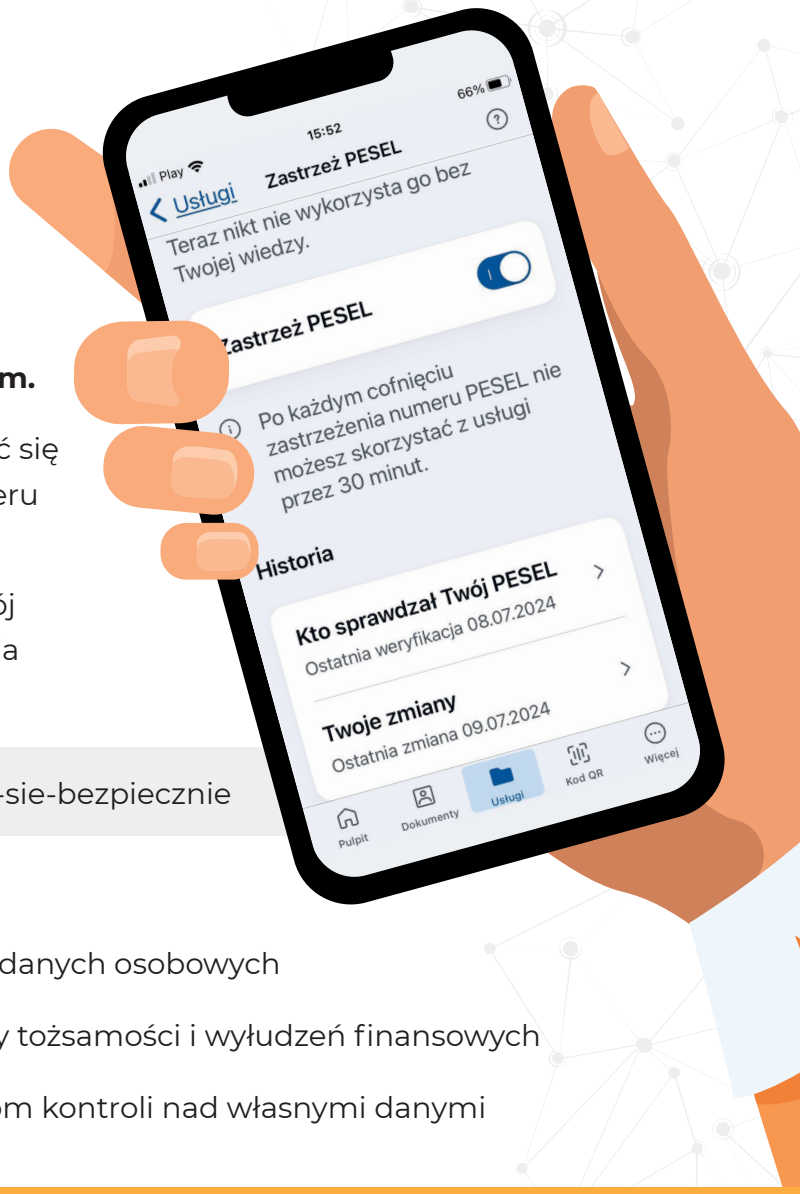
Aplikacja została stworzona przez Ministerstwo Cyfryzacji i umożliwia szybki dostęp do różnych usług administracyjnych, w tym do danych osobowych z dowodu osobistego, prawa jazdy, punktów karnych. **mObywatel 2.0 zainstalujesz na Androidzie oraz iOS.**

Bez wychodzenia z domu zabezpieczysz swój PESEL przed nieautoryzowanym dostępem.

Instytucje finansowe nie będą mogły udzielić pożyczki osobie, która nie może identyfikować się numerem PESEL. Od 1 czerwca 2024 w Polsce wprowadzono obowiązek sprawdzania numeru PESEL klienta przed udzieleniem pożyczki lub podpisaniem umowy kredytowej.

Jeśli zastrzeżesz PESEL uzyskasz też wgląd w historię kto odpytywał system rządowy o Twój numer. Operację zastrzeżenia możesz odwrócić w dowolnym czasie, aby w trakcie udzielania kredytu umożliwić instytucji finansowej sprawdzenie podstawowych danych.

https://www.gov.pl/web/baza-wiedzy/wazne-zmiany-od-1-czerwca-br-zastrzez-pesel-i-czuj-sie-bezpiecznie



W aplikacji mObywatel:

- cofniesz zastrzeżenie PESEL
- sprawdzisz kto weryfikował twój PESEL
- prześledzisz zmiany związane z zastrzeganiem

Dzięki temu:

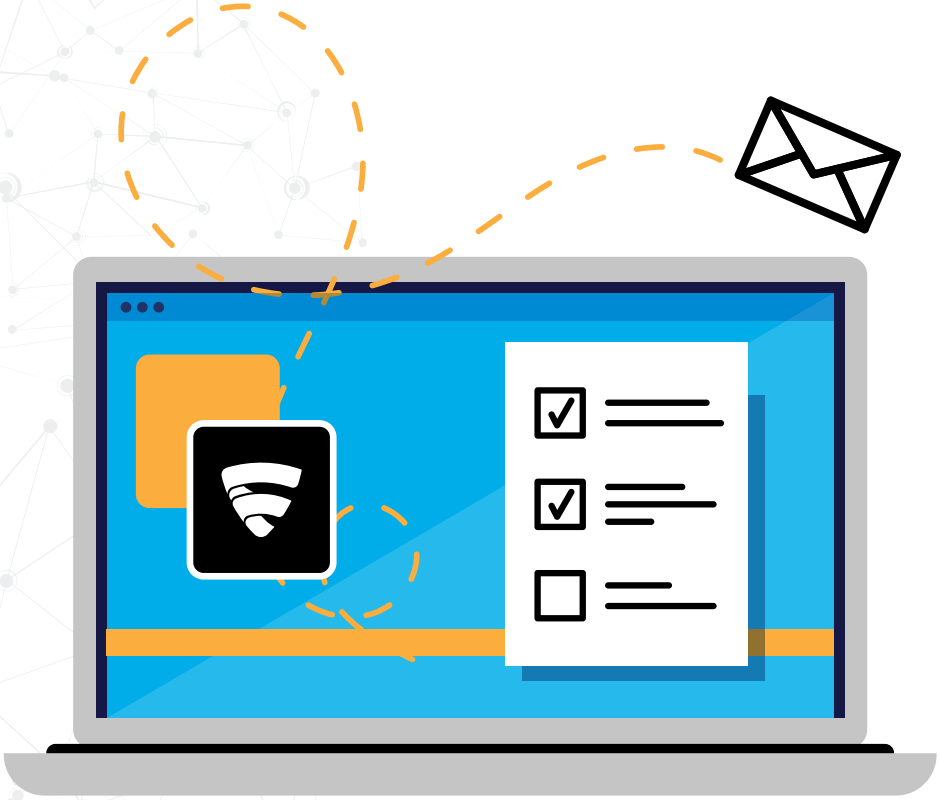
- zwiększasz bezpieczeństwo danych osobowych
- zmniejszasz ryzyko kradzieży tożsamości i wyłudzeń finansowych
- uzyskujesz dodatkowy poziom kontroli nad własnymi danymi

Zachowaj ostrożność

Zastrzeżenie PESEL nie uchroni przed wszystkimi rodzajami oszustw, zwłaszcza jeśli Twoje dane zostały wcześniej upublicznione w wyniku cyberataku na instytucję finansową lub platformę internetową. Blokada PESEL nie zwalnia z zachowania ostrożności podczas korzystania z urządzeń z dostępem do Internetu.

Wyciek hasła lub e-mail do konta

Jeśli z jakiegoś powodu masz obawy, że mogło wyciec Twoje hasło, które było używane do logowania, to na stronie **haveibeenpwned.com** możesz to sprawdzić.



Jak jeszcze sprawdzić wyciek danych lub adresu e-mail?
F-Secure Identity Theft Checker to bezpłatne narzędzie online. Jest dostępne również w pakiecie bezpieczeństwa F-Secure Total oraz występuje jako samodzielny produkt pod nazwą F-Secure ID Protection.

Działanie tej komercyjnej usługi jest bardzo intuicyjne:

Podajesz e-mail, który chcesz sprawdzić (i do którego masz dostęp – na ten adres otrzymasz powiadomienie).
Usługa internetowa weryfikuje dostępność podanego maila w bazach z wycieków.

Jeżeli wynik jest pozytywny, to niestety doszło do ujawnienia wrażliwych danych powiązanych z Twoim adresem e-mail.
W mailu otrzymasz trochę pomocnym informacji, skąd mogło dojść do wycieku.

Ujawnienie danych? Zażądaj informacji od administratora!

Jeśli przekazujesz swoje dane osobowe, pamiętaj, że są one chronione prawem. Niezależnie od tego, jakie dane zostaną wykradzione lub przekazane niezgodnie z prawem, możesz żądać od administratora wyjaśnień z tym związanych.

Mogą to być informacje np. jakie dane wyciekły, do kogo te dane trafiły albo czy wyciek był zgłoszony do Prezesa Urzędu Ochrony Danych Osobowych (PUODO).

Zachowaj korespondencję **z administratorem**

Zachowaj korespondencję z administratorem, jak również wszystkie komunikaty publiczne, które zostały wydane w związku z wyciekiem na potrzeby złożenia skargi do PUODO.

Zachowaj kopię zgłoszenia sprawy na policję bądź dochodzenia roszczeń na drodze cywilnej.

Jeżeli doszło do wycieku Twoich danych możesz skontaktować się z administratorem i zażądać rekompensaty (np. rabatu na usługi), przy czym w tym przypadku decyzja należy do administratora. Podmiot, który dba o renomę, z pewnością rozważy jakąś formę zadośćuczynienia.

Źródło: https://odo24.pl/blog-post.kiedy-administrator-danych-ma-obowiazek-udostepnic-dane-osobowe

Złożenie skargi do Prezesa Urzędu Ochrony Danych Osobowych

Jako osoba fizyczna możesz zgłosić skargę do Prezesa Urzędu Ochrony Danych Osobowych w związku z nieprawidłowym przetwarzaniem Twoich danych osobowych lub innej osoby (musisz mieć pełnomocnictwo).

Zanim wystąpisz ze skargą do Prezesa UODO, zażądaj od administratora prawa dostępu do swoich danych, które Ci przysługuje. Bez względu na to, czy doszło do wycieku, możesz żądać usunięcia swoich danych, ograniczenia przetwarzania i przenoszenia.

Źródło: https://uodo.gov.pl/83

Zgłoszenie sprawy na Policję

Możesz zgłosić podejrzenie popełnienia przestępstwa na Policję w związku z ustawą o ochronie danych osobowych z 10 maja 2018 roku, w której znajdują się przepisy karne, które stanowią, że:

(art. 107 ust. 1)
„Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch."

(art. 107 ust. 2).
Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

art. 46 § 1 kodeksu karnego – orzeczenie o obowiązku naprawienia szkody
W razie skazania sąd może orzec (...) obowiązek naprawienia, w całości albo w części, wyrządzonej przestępstwem szkody lub zadośćuczynienia za doznaną krzywdę.

Źródło art. 107 ust. 1-2: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-danych-osobowych-18722262/art-107

Źródło Kodeks Karny: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-46

Zachowaj dużą ostrożność podczas podawania danych w internecie.

Dokładnie analizuj kierowane do Ciebie komunikaty zawarte np. w wiadomościach SMS, e-mail, by uniknąć np. ataku phishingowego, którego celem może być wyłudzenie danych albo uzyskanie loginów dostępowych do internetowych systemów bankowych bądź innych usług online, z których korzystasz.

Chcesz więcej bezpłatnych materiałów, **które rozwijają wiedzę w obszarze cyberbezpieczeństwa?**

Dostarcza ich **nasz newsletter**

Jedyne co musisz zrobić, to pozostać z nami na liście bezpiecznych użytkowników, którzy będą na bieżąco powiadamiani na adres e-mail.

https://avlab.pl/newsletter

Zobacz rozwiązania, **które polecamy**

Nie musisz już szukać dobrych ofert!
Znaleźliśmy je dla Ciebie!
Możemy je autentycznie zarekomendować,
bez owijania w bawełnę!

https://avlab.pl/polecane-rozwiazania

Przejrzyj nasze **poradniki**

Jak odzyskać konto na Facebooku?
Jaki darmowy antywirus wybrać?
Jaki komunikator polecamy?
Jaki serwer DNS polecamy?

https://avlab.pl/porady

Więcej ciekawych artykułów z zakresu cyberbezpieczeństwa znajdziesz na naszej stronie internetowej

www.avlab.pl

AVLab
CYBERSECURITY FOUNDATION

Fundacja AVLab dla Cyberbezpieczeństwa jako niezależna organizacja stoi na straży ochrony prywatności i bezpieczeństwa w Internecie. Budujemy świadomość użytkowników z zakresu ochrony cyfrowej. Wydajemy opinie, techniczne analizy oraz testy rozwiązań informatycznych w sferze cyberbezpieczeństwa.
Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, dzięki którym jesteśmy rozpoznawalni na całym świecie, jako jedno z najpopularniejszych laboratoriów testujących.

Jesteśmy stowarzyszeni w grupie roboczej non-profit AMTSO (Anti-Malware Testing Standards Organization). W ramach pełnionych funkcji w międzynarodowych środowisku ekspertów pracujemy nad poprawą transparentności, obiektywności oraz jakości przeprowadzanych testów oprogramowania ochronnego.

Aby poznać szczegóły techniczne producenci mogą kierować swoje zapytania na adres: kontakt@avlab.pl

CYBER TRANSPARENCY AUDIT FORUM MEMBER

amtso
The cybersecurity industry's testing standard community
MEMBER