## Jak ochronić się przed kradzieżą danych osobowych?

##### 1. Nie podawaj swoich danych w trakcie rozmów telefonicznych nieznajomym osobom

Czym są dane osobowe? Takie dane to m.in. imię, nazwisko, data urodzenia, adres, numer konta bankowego, informacje o wykształceniu, doświadczeniu zawodowym, numer telefonu, adres e-mail. Obecnie, w niektórych sytuacjach, jako dane osobowe traktowane są również pliki cookies, numer IMEI, nick, login itp.

##### 2. Bardzo dokładnie niszcz stare dokumenty i korespondencję, których chcesz się pozbyć – to fantastyczne źródło wiedzy na Twój temat

I wbrew temu, co możesz myśleć, nie ma pewności, że kiedy trafią do śmieci, nikt ich nie przeczyta. A kiedy trafią w ręce osób niepowołanych, możesz w dość krótkim czasie odczuć to dość boleśnie, poprzez konieczność spłacania kredytu wyłudzonego na Twoje nazwisko.Choć tak naprawdę konsekwencji kradzieży danych może być więcej.

##### 3. Nie zostawiaj swoich dokumentów w rękach osób niepowołanych

Np. nie udostępniaj dowodu osobistego w zastaw, gdy chcesz wypożyczyć kajak lub rower. Nigdy nie wiesz, co stanie się z nim podczas Twojej nieobecności i w czyje ręce trafią Twoje dane, gdy stracisz dowód z zasięgu wzroku. Może trafić w ręce oszustów, złodziei tożsamości.

Żadna instytucja lub placówka nie może żądać od Ciebie zostawienia dowodu osobistego w zamian za wypożyczenie sprzętu. I jest to zakaz usankcjonowany prawnie, za złamanie którego grozi nawet kara pozbawienia wolności.

##### 4. Nigdy nie otwieraj e-maili podejrzanych lub nieznanego pochodzenia

Często spotykaną praktyką, jaką stosują oszuści, jest wysyłanie wiadomości, które zawierają niebezpieczne linki. Prowadzą one do fałszywych stron znanych banków, platform aukcyjnych itp. Znajdziesz na nich ponaglającą informację wzywającą do uzupełnienia w dość krótkim czasie swoich danych osobowych, pod pretekstem zawieszenia konta.

To standardowy przykład próby oszustwa. Pamiętaj, że banki, instytucje finansowe ani żadne inne uczciwe instytucje nie stosują tego typu praktyk! Nigdy więc się do nich nie stosuj i ignoruj tego typu maile!

#### 5. Nie daj się złodziejom

Złodzieje, którzy mają Twoje dane osobowe, mogą nie tylko utworzyć fałszywe konto na portalu społecznościowym, ale również zwrócić się do banku po pożyczkę. Gdy ta zostanie im przyznana, mogą podpisać umowę kredytową. Dlatego też, co jeszcze raz podkreślamy, warto zawsze być czujnym i ostrożnym, a z drugiej strony wzmocnić ochronę, korzystając z Alertów BIK. Dzięki nim zostaniesz zaalarmowany, kiedy ktoś będzie próbował wyłudzić kredyt, poszywając się pod Ciebie.

## 6. Kontroluj czy ktoś nie podszywa się pod Ciebie w internecie

Na bieżąco sprawdzaj czy Twoje dane nie uległy wykradzeniu i czy nikt nie składa wniosków kredytowych na Twoje dane. Możesz to zrobić poprzez:

* założenie konta w BIK, w ramach którego zostanie uruchomiony Alert BIK.  
  Alert BIK wyśle Ci smsa lub e-maila za każdym razem, gdy do banku/firmy pożyczkowej wpłynie wniosek kredytowy złożony na Twoje dane osobowe,
* usługę Sprawdź, kto pobierał Twoje dane w Krajowym Rejestrze Długów. Dzięki niej dowiesz się, kto pytał o Ciebie w KRD i podał Twój PESEL oraz jakie informacje uzyskał i czy nie próbował wyłudzić kredytu na Twoje dane.

## 7. Reaguj gdy dowiesz się o bezprawnym wykorzystaniu Twoich danych

Jeśli dowiesz się, że ktoś złożył wniosek o kredyt/pożyczkę w konkretnym banku/instytucji finansowej na Twoje dane, powiadom natychmiast o tym bank/instytucję pożyczkową. Jeśli Twoje zgłoszenie nie zostało potraktowane odpowiednio poważnie złóż reklamację w firmie w której wykorzystano Twoje dane, a w razie braku porozumienia poproś o pomoc Rzecznika Finansowego lub UOKIK.

Dzięki Alert BIK czy Sprawdź, kto pobierał Twoje dane możesz szybko zareagować gdy jakiś bank/instytucja finansowa zapyta o Twoje dane BIK lub któryś z BIG-ów i zapobiec wyłudzeniu.

Informując bank/ instytucję finansową o kradzieży Twojej tożsamości, ułatwiasz instytucji przekazanie informacji o popełnionym przestępstwie do BIK, który oznaczy Twój profil w odpowiedni sposób, aby dane nie mogły być dalej wykorzystywane przez osoby nieuprawnione.

Każda z wykonanych przez Ciebie czynności będzie chroniła Cię przed przyszłymi możliwymi roszczeniami ze strony instytucji, w których Twoje dane zostały wykorzystane.

Większość instytucji finansowych, w przypadku złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa do organów ścigania (policji/ prokuratury) wstrzymuje czynności windykacyjne, współpracuje z organami ścigania w celu wykrycia sprawcy oraz koryguje wpisy w BIK.

Pamiętaj jednak, że współpraca z instytucjami finansowymi nie rozwiązuje całego problemu. Osoba posiadająca Twoje dane może użyć ich również przy zakupie towarów na raty czy telefonu, podszyć się pod Ciebie na portalach społecznościowych czy założyć fikcyjne rachunki bankowe.

wych. J.Hume