

Wytyczne dla Pacjentów

Wyciekły dane medyczne. Co teraz zrobić?

Krok pierwszy. Zastrzeż numer PESEL

To najważniejsze i zajmuje kilka minut. Zastrzeżenia dokonuje się w aplikacji mObywatel, na stronie gov.pl, w dowolnym urzędzie gminy, w placówce bankowej albo na poczcie.

Zastrzeżenie sprawia, że bank ani inna instytucja nie udzieli kredytu ani pożyczki na Państwa dane, nie zostanie założony nowy rachunek bankowy, notariusz nie sporządzi aktu notarialnego dotyczącego nieruchomości, operator nie wyda duplikatu karty SIM, a bank nie wypłaci w placówce gotówki powyżej trzykrotności minimalnego wynagrodzenia.

Zastrzeżenie nie utrudnia korzystania z opieki zdrowotnej. Nadal można umówić się do lekarza i zrealizować receptę.

UWAGA PRAKTYCZNA Jeżeli planują Państwo wypłatę większej kwoty gotówki w oddziale banku, zastrzeżenie trzeba cofnąć przed złożeniem dyspozycji. Cofnięcie go w trakcie nie pomoże, bo bank i tak wstrzyma wypłatę na dwanaście godzin.

Krok drugi. Sprawdź, czy Twoje dane są w wycieku

Informacje o skradzionych danych mają być udostępniane w serwisie bezpiecznedane.gov.pl. Ponieważ administratorami danych są poszczególne gabinety i placówki, przekazanie informacji do tego serwisu może potrwać kilka dni.

Prosimy nie korzystać z serwisów obiecujących natychmiastowe sprawdzenie wycieku. Same mogą służyć wyłudzeniu danych.

Krok trzeci. Uważaj na telefony i wiadomości

Największe ryzyko pojawia się nie w chwili wycieku, lecz w kolejnych tygodniach i miesiącach. Wiadomości mogą wyglądać wiarygodnie, ponieważ ich autorzy mogą znać Państwa imię, nazwisko, numer PESEL, nazwę leku albo datę wizyty.

- Nie otwierać odnośników w wiadomościach dotyczących recept, wyników badań, dopłat, zwrotów ani weryfikacji danych.
- Nie podawać przez telefon numeru PESEL, hasła, kodu z wiadomości SMS ani danych karty płatniczej. Żadna placówka medyczna, bank ani NFZ o nie nie poprosi.
- Jeżeli rozmówca wywiera presję czasu albo odwołuje się do stanu zdrowia – rozłączyć się i oddzwonić na numer instytucji wyszukany samodzielnie, nigdy podany przez rozmówcę.
- Numer widoczny na wyświetlaczu telefonu może być sfałszowany.
- Nie instalować oprogramowania do zdalnego dostępu na prośbę osoby dzwoniącej.

Krok czwarty. Zabezpiecz konta

- Włączyć uwierzytelnianie dwuskładnikowe w bankowości elektronicznej, poczcie i Internetowym Koncie Pacjenta.
- Zmienić hasła, jeżeli to samo hasło było używane w kilku serwisach.
- Sprawdzać raporty w Biurze Informacji Kredytowej i w biurach informacji gospodarczej pod kątem zapytań kredytowych, których Państwo nie składali.
- Obserwować historię rachunku bankowego przez co najmniej kilka miesięcy.

Krok piąty. Reaguj

- Próbie oszustwa zgłosić do CERT Polska przez formularz incydent.cert.pl albo przesłać podejrzaną wiadomość SMS na numer 8080 – jest to bezpłatne.
- W razie faktycznej szkody zgłosić zawiadomienie na Policji albo w prokuraturze.
- Jeżeli na Państwa dane zaciągnięto zobowiązanie – natychmiast zawiadomić instytucję finansową i zażądać wstrzymania wykonania umowy.

Krok szósty. Znaj swoje prawa

Mają Państwo prawo dowiedzieć się od placówki, jakiego zakresu danych dotyczy naruszenie, prawo dostępu do swoich danych, prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz prawo dochodzenia odszkodowania przed sądem.

Prosimy o zachowanie spokoju. Sam fakt ujawnienia danych nie oznacza, że doszło do szkody. Wykonanie powyższych kroków, a przede wszystkim zastrzeżenie numeru PESEL, istotnie ogranicza ryzyko.