

● Twoje dane wyciekły

Plan działania krok po kroku

Nie panikuj i nie działaj pod presją. Zaznaczaj wykonane kroki. Najpierw zabezpiecz pocztę i pieniądze, potem pozostałe konta.

ZACZNIJ OD FAKTÓW

Serwis lub instytucja: _____

Mogły wyciec: ☐ e-mail ☐ telefon ☐ hasło ☐ PESEL ☐ dane finansowe ☐ dane zdrowotne

Pierwsze 30 minut

- 1 Wejdź na oficjalną stronę**
Sprawdź komunikat firmy. Nie korzystaj z linku przesłanego w niespodziewanym SMS-ie lub e-mailu.
- 2 Zabezpiecz skrzynkę e-mail**
Ustaw unikalne hasło, wyloguj obce urządzenia i włącz uwierzytelnianie wieloskładnikowe.
- 3 Usuń powtórzone hasła**
Zmień je wszędzie, gdzie były takie same lub podobne. Zacznij od banku, zakupów i mediów społecznościowych.
- 4 Zastrzeż PESEL, jeśli mógł wyciec**
Zrobisz to bezpłatnie w mObywatelu lub urzędzie. Zastrzeżenie nie blokuje recept, wizyt ani przelewów.

Przez kolejne tygodnie

- 5 Obserwuj rachunki i powiadomienia**
Reaguj na niezbrane transakcje, próby logowania, reset hasła lub zawarcia umowy.
- 6 Spodziewaj się wiarygodnych oszustw**
Przestępca może znać Twoje dane. Sama znajomość PESEL-u, lekarza czy adresu nie potwierdza jego tożsamości.
- 7 Rozłącz się i sprawdź**
Gdy ktoś żąda kodu, pieniędzy lub instalacji aplikacji, zakończ rozmowę i samodzielnie wybierz oficjalny numer.
- 8 Sprawdź e-mail w bazie wycieków**
HavelBeenPwned.com pokaże znane incydenty i umożliwi włączenie powiadomień o kolejnych.

TRZY SYGNAŁY, ŻE TO MOŻE BYĆ OSZUSTWO

1. Presja czasu

„Tylko teraz”, „natychmiast”

2. Prośba o kod lub hasło

Bank nie prosi o pełne dane

3. Instalacja aplikacji

Nie udostępniaj ekranu

Wystarczy jeden z tych sygnałów: rozłącz się i sprawdź kontakt niezależnie.

Jeśli pieniądze już zniknęły

Natychmiast skontaktuj się z bankiem, zastrzeż karty i zgłoś sprawę policji.
Nie usuwaj wiadomości, numerów telefonu ani zrzutów ekranu - to mogą być dowody.