



## Nie daj się oszukać. Ostrzeżenie dla seniorów i nie tylko

2026-03-06

**Telefony „z banku” lub administracji, SMS-y o zablokowanym koncie, prośby o pilne potwierdzenie danych albo dramatyczne historie o wypadku bliskiej osoby - to dziś najczęstsze metody oszustów, którzy szczególnie często biorą na cel seniorów. Działają szybko, wywierają presję i liczą na strach. Warto wiedzieć, jak się przed tym chronić, zanim dojdzie do utraty oszczędności całego życia lub kradzieży tożsamości.**

Dzisiaj oszustwa rzadko zaczynają się od kradzieży portfela. Coraz częściej zaczynają się od telefonu lub wiadomości, w której ktoś podaje się za pracownika banku, urzędu, policji albo nawet członka rodziny. Oszuści straszą, że konto jest zagrożone, pieniądze mogą zniknąć albo że trzeba natychmiast potwierdzić dane. To pierwszy i najważniejszy sygnał ostrzegawczy. Banki, urzędy, ZUS i policja nigdy nie proszą przez telefon o numer PESEL, numer dowodu, hasła ani kody SMS i nie każą podejmować decyzji w pośpiechu. Gdy pojawia się presja czasu - najczęściej mamy do czynienia z próbą oszustwa. Banki i urzędy nie żądają pilnych informacji przez telefon.

Numer PESEL jest dziś kluczem do wielu spraw finansowych i urzędowych. W rękach przestępców może posłużyć do zaciągnięcia pożyczki, otwarcia konta lub podpisania umowy na cudze nazwisko. Dlatego warto skorzystać z możliwości zastrzeżenia numeru PESEL w państwowym rejestrze. Po zastrzeżeniu instytucje finansowe, operatorzy telefoniczni, notariusze i ubezpieczyciele mają obowiązek odmówić wykonania wielu czynności, które mogłyby narazić właściciela danych na straty. Zastrzeżenie można wykonać w aplikacji mObywatel lub osobiście w urzędzie, a w razie potrzeby - czasowo je cofnąć.

Szczególnie niebezpieczna jest utrata dowodu osobistego. Zgubienie lub kradzież dokumentu trzeba zgłosić natychmiast, ponieważ szybka reakcja powoduje jego unieważnienie i automatyczne zastrzeżenie numeru PESEL. To znacząco ogranicza możliwość wykorzystania danych przez osoby trzecie. Zgłoszenia można dokonać przez internet o każdej porze albo osobiście w urzędzie, a w przypadku kradzieży również na policji. Warto też poinformować swój bank, który korzysta z własnych systemów zabezpieczeń.

Najczęstszym narzędziem oszustów pozostaje telefon i internet. Podejrzane SMS-y z linkami do „dopłaty”, „nagrody” czy „blokady konta”, e-maile podszywające się pod znane instytucje oraz telefony z nieznanymi numerami to współczesna codzienność.

Zasada bezpieczeństwa jest jedna: nigdy nie klikaj w linki z takich wiadomości i nigdy nie loguj się do banku lub urzędu przez link otrzymany w SMS-ie czy e-mailu. Jeśli masz wątpliwości, przerwij rozmowę i samodzielnie skontaktuj się z instytucją, korzystając z oficjalnego numeru telefonu.

Ostrożność warto zachować także w codziennych sytuacjach. Nie należy publikować w internecie zdjęć dokumentów, kart płatniczych ani innych danych osobowych, nawet w zamkniętych grupach czy relacjach. W miejscach publicznych lepiej nie podawać głośno numeru PESEL ani telefonu - w kolejce zawsze może znaleźć się ktoś, kto słucha uważniej, niż się wydaje. Dokumenty papierowe powinny być przechowywane w jednym, bezpiecznym miejscu, a stare rachunki i pisma zawierające dane



osobowe należy niszczyć przed wyrzuceniem.

Najważniejszą ochroną przed oszustami jest jednak rozmowa. Przestępcy liczą na to, że senior podejmie decyzję sam, pod wpływem strachu i bez konsultacji z bliskimi. Dlatego zanim przekażesz jakiegokolwiek dane, wykonasz przelew albo uwierzysz w dramatyczną historię – zatrzymaj się i skontaktuj z kimś zaufanym: dzieckiem, wnukiem, sąsiadem lub przyjacielem. Zadzwoń do bliskich, lepiej zapytać o jeden raz za dużo, niż stracić oszczędności życia.

Nie trzeba odbierać nieznanymi telefonów, nie trzeba się spieszyć i zawsze ma się prawo odmówić oraz zakończyć rozmowę. Ostrożność to nie brak zaufania – to najlepszy sposób, by chronić siebie, swoje dane i swoje pieniądze.

## Chroń swoje dane. Dobre nawyki na co dzień

### Zastrzeż PESEL

Zastrzeżenie numeru PESEL chroni Cię przed kradzieżą tożsamości. Banki, operatorzy i notariusze mają obowiązek sprawdzić, czy PESEL jest zastrzeżony – jeśli tak, muszą odmówić wykonania czynności.

PESEL możesz zastrzec lub cofnąć zastrzeżenie w na stronie [www.gov.pl](http://www.gov.pl), w aplikacji **mObywatel** lub w urzędzie.

### Zgubiłeś dowód? Reaguj od razu

Utrata dowodu osobistego to realne zagrożenie. Zgłoś ją **natychmiast** – dokument zostanie unieważniony, a PESEL automatycznie zastrzeżony.

Zgłoszenia można dokonać w urzędzie lub przez całą dobę przez stronę [www.gov.pl](http://www.gov.pl), w aplikacji **mObywatel** oraz również na policji lub w konsulacie (za granicą). Warto poinformować także bank.

### Nie publikuj dokumentów ani kart płatniczych w internecie

Zdjęcie dowodu lub karty może wystarczyć do oszustwa. Nie udostępniaj ich nawet „na chwilę”.

### Nie podawaj głośno swoich danych w miejscach publicznych

PESEL czy numer telefonu łatwo podsłuchać. Jeśli możesz – pokaż dokumenty lub dane na ekranie zamiast je dyktować.

### Uważaj w mediach społecznościowych

Ogranicz widoczność postów, nie publikuj dokumentów, adresów, numerów telefonów ani informacji w czasie rzeczywistym. Nie klikaj podejrzanych linków **i nigdy nie podawaj kodów**



**Magiczny  
Kraków**

## **SMS.**

### **Nie udostępniaj publicznie numeru telefonu i nie odbieraj nieznanego numeru**

Publiczny numer to częsty cel oszustów. Pamiętaj: banki i urzędy nie żądają podawania informacji przez telefon.

### **Uważaj na fałszywe strony i wiadomości**

Nie loguj się przez linki z SMS-ów i e-maili. Zawsze sprawdzaj adres strony. W razie wątpliwości – przerwij operację lub rozmowę.

### **Włącz dwuskładnikowe logowanie (2FA)**

To prosta i skuteczna ochrona e-maila i kont internetowych. Nie zatwierdzaj logowań, których sam nie inicjujesz.

### **Pamiętaj! Dokumenty papierowe też wymagają ochrony**

Nie zostawiaj ich bez nadzoru i niszczone przed wyrzuceniem. Nie podpisuj żadnych podsuniętych na szybko dokumentów.