

TWOJE PIENIĄDZE TWOJE DECYZJE TWOJE BEZPIECZEŃSTWO

Zadbaj o ochronę finansów z Bankiem Pekao S.A.



Codziennie chronimy pieniądze naszych klientów, wykorzystując nowoczesne technologie i zaawansowane systemy bezpieczeństwa. Ale w świecie cyfrowym najważniejszym elementem ochrony jesteś Ty.

Cyberprzestępcy nie atakują systemów – **atakują ludzi**.
Dlatego warto wiedzieć, jak działać, aby nie dać się oszukać.



Zatrzymaj oszustwo, zanim stracisz pieniądze

- **Telefon z informacją o włamaniu na konto?**
Rozłącz się. To może być próba oszustwa. Zawsze samodzielnie oddzwonić do banku, wybierając numer na klawiaturze numerycznej.
- **Obietnica szybkich i wysokich zysków? Inwestycje?**
To jeden z najczęstszych scenariuszy wyłudzeń.
- **Prośba o pilny przelew lub zaciągnięcie kredytu czy zabezpieczenie środków?**
To częsty mechanizm wyłudzeń – działaj ostrożnie i niczego nie rób pod presją.

Zasada jest prosta: jeśli coś wzbudza emocje – sprawdź to dwa razy.



Jak działają oszuści?

Najczęściej:

- wysyłają fałszywe SMS-y i e-maile z załącznikami/linkami, kody QR,
- przesyłają spreparowane dokumenty,
- podszywają się pod banki, firmę kurierską lub znajomego, instytucje zaufania publicznego, osoby publiczne,
- dzwonią, wywołując presję i strach,
- proszą o szybkie działanie „tu i teraz”.

Zatrzymaj się. Sprawdź. Masz wątpliwości – skontaktuj się z bankiem.



Wizytówka pracownika Banku Pekao S.A. to funkcja bezpieczeństwa dostępna w aplikacji PeoPay oraz serwisie Pekao24, która pozwala potwierdzić, że kontaktuje się z Tobą prawdziwy konsultant banku.



Bank nie potwierdza danych pracownika SMS-em.

Twoje dane to klucz do Twoich pieniędzy

Nigdy nie przekazuj nikomu:



- loginu i hasła do bankowości,
- kodów SMS,
- PIN-u do aplikacji,
- PIN-u do karty płatniczej,
- danych karty płatniczej,
- kodu BLIK.

Pracownik Banku Pekao S.A. nigdy o to nie poprosi

Zapamiętaj – jeśli ktoś:



- każe przekazać kartę „do zniszczenia”,
- każe wypłacić gotówkę i przekazać ją rzekomemu funkcjonariuszowi,
- prosi o przelew na „bezpieczny rachunek”,
- straszy blokadą konta,
- każe instalować aplikacje lub łączyć się zdalnie,
- każe wykonać wpłaty we wpłatomacie, zaciągnąć pożyczkę w celu ochrony środków,

to nie jest bank. To oszust.

Bezpieczne logowanie zaczyna się od Ciebie



Zawsze wpisuj adres banku samodzielnie:
<https://www.pekao24.pl>



**Nigdy nie loguj się przez linki z SMS-ów,
e-maili czy popularnych komunikatorów.**

Zanim klikniesz „zatwierdź” – zatrzymaj się na chwilę

Sprawdź, czy potwierdzasz transakcję czy dodanie karty do cyfrowego portfela.



Zawsze weryfikuj:

- kwotę przelewu,
- numer rachunku odbiorcy.

**Jeśli coś się nie zgadza lub budzi wątpliwości – nie potwierdzaj transakcji.
Skontaktuj się z bankiem. Jedna chwila może uchronić Cię przed stratą pieniędzy.**

Zabezpiecz swoje urządzenia



- Instaluj aplikacje tylko z oficjalnych sklepów.
- Regularnie aktualizuj system i aplikacje.
- Nie instaluj programów „zabezpieczających” na czyjąś prośbę.

Przestępca, który przejmie Twoje urządzenie, może przejąć także Twoje pieniądze.



Zastrzeż numer PESEL w aplikacji mObywatel

**Dzięki temu ograniczysz ryzyko wykorzystania Twoich danych do wyłudzenia kredytu,
pożyczki lub zawarcia umowy bez Twojej zgody.**

Włącz dodatkową ochronę w Banku Pekao S.A.



Logowanie dwuskładnikowe do Pekao24

Dodatkowe potwierdzenie logowania to dodatkowa bariera dla oszustów. Nawet jeśli ktoś pozna Twoje hasło – nie zaloguje się bez drugiego składnika (np. potwierdzenia w aplikacji lub klucza sprzętowego).

Sprawdź, jak włączyć logowanie dwuskładnikowe na www.pekao.com.pl/klient-indywidualny/bankowosc-elektroniczna/logowanie-dwuskladnikowe



Ochrona behawioralna

Zwiększ bezpieczeństwo swoich transakcji – system przeanalizuje sposób korzystania z bankowości i zareaguje, gdy coś odbiega od normy.

Sprawdź, jak włączyć ochronę behawioralną na www.pekao.com.pl/bezpieczenstwo/ochrona-behawioralna



CyberRescue

Wsparcie wtedy, gdy najbardziej go potrzebujesz:

- bezpłatna pomoc w przypadku podejrzenia oszustwa,
- wskazówki, jak zabezpieczyć urządzenia,
- wsparcie po incydencie cyberbezpieczeństwa.

Bo w cyfrowym świecie nie zostajesz sam.

Więcej o usłudze CyberRescue znajdziesz na: www.pekao.com.pl/bezpieczenstwo/cyberrescue

Co zrobić, jeśli podejrzewasz, że możesz być ofiarą oszustwa:



Zastrzeż karty i zablokuj dostęp do bankowości elektronicznej:

w serwisie internetowym **Pekao24** lub aplikacji mobilnej **PeoPay** (wybierz: Ustawienia > Bezpieczeństwo > Blokowanie kanałów dostępu) lub telefonicznie dzwoniąc pod numer **519 222 222**.



Zgłoś oszustwo na infolinii banku

519 222 222

i przekaz wszystkie niezbędne informacje.



Złóż zawiadomienie o podejrzeniu popełnienia przestępstwa na policji lub w prokuraturze i poinformuj o tym nasz bank.

Szybka reakcja zwiększa szansę na ochronę Twoich pieniędzy.

Dowiedz się więcej. Wejdź na www.pekao.com.pl/bezpieczenstwo i sprawdź, jak chronić się przed oszustami.