



Sprawdź przesyłkę z kartą i PIN-em

Gdy dostaniesz kartę lub PIN pocztą, sprawdź, czy koperta nie była otwierana. Jeśli masz wątpliwości – zgłoś się od razu po nową kartę.

Dlaczego? Oszust mógł wcześniej przechwycić Twoją kartę lub PIN i spróbować ich użyć.



Chroń PIN

Najlepiej zapamiętaj PIN, a kopertę zniszcz. Nie trzymaj go razem z kartą i nie zapisuj na karcie. Nie podawaj PIN-u nikomu, nawet pracownikowi banku. Zastanawiaj ręką klawiaturę przy wpisywaniu PIN-u.

Dlaczego? Jeśli ktoś pozna Twój PIN, może wypłacić wszystkie pieniądze z konta.



Chroń kartę fizycznie

Trzymaj kartę w bezpiecznym miejscu. Podczas płatności karta powinna być zawsze w Twoim zasięgu wzroku. Nie pozwól, aby sprzedawca zabrał ją na zaplecze. Nie pożyczaj karty znajomym ani rodzinie.

Dlaczego? Ktoś może skopiować dane z karty albo użyć jej bez Twojej wiedzy.



Wyłącz płatności zbliżeniowe w ryzykownych sytuacjach

Jeśli jesteś w zatłoczonych miejscach, np. autobus czy galeria, możesz wyłączyć tę funkcję w serwisie kartosfera.pl.

Dlaczego? Złodziej może przyłożyć terminal i pobrać pieniądze bez PIN-u.



Chroń dane karty

Imię, nazwisko, data ważności i kod CVC/CVV wystarczą, aby ktoś zapłacił w internecie. Nigdy nie podawaj tych danych obcym.

Dlaczego? Wystarczy zdjęcie karty, aby złodziej zrobił zakupy online Twoim kosztem.



Kupuj w zaufanych sklepach internetowych

Unikaj podejrzanych stron z 'super promocjami'. Zwracaj uwagę, czy sklep ma zabezpieczenia (kłódka w pasku adresu).

Dlaczego? Fałszywe sklepy kradną dane kart – stracisz pieniądze i nie dostaniesz towaru.



Sprawdzaj bankomaty

Obejrzyj bankomat – zwróć uwagę na wystające elementy, dodatkowe kamery czy dziwną klawiaturę.

Dlaczego? Złodzieje montują nakładki, które kopiuje dane karty i PIN.



Ustaw limity transakcji

Ustawienne limity płatności i wypłat – np. zamiast 1000 zł, ustaw 200 zł.

Dlaczego? Jeśli ktoś ukradnie kartę, nie wyczerpie całego konta naraz.



Nie podawaj danych karty przez telefon ani e-mail

Bank nigdy nie prosi o PIN, kod CVV, datę ważności czy kody SMS.

Dlaczego? To jedna z najczęstszych metod wyłudzenia danych.



Zabezpiecz komputer i telefon

Używaj legalnego oprogramowania, antywirusa i zapory sieciowej. Regularnie aktualizuj system.

Dlaczego? Wirusy mogą przejść dane Twojej karty i transakcji.



Nie otwieraj podejrzanych e-maili i załączników

Dlaczego? Mogą zawierać wirusy, które kradną dane z komputera.



Sprawdzaj zabezpieczenia stron płatniczych

Adres powinien zaczynać się od https:// i mieć kłódkę w pasku adresu. Klikając kłódkę sprawdzisz certyfikat.

Dlaczego? Brak szyfrowania oznacza, że ktoś może podejrzeć Twoje dane.



Używaj bezpiecznego dostępu do internetu

Nie rób transakcji kartą przez publiczne Wi-Fi.

Dlaczego? Otwarte sieci są łatwe do przechwytywania danych przez hakerów.



Nie zapisuj danych karty

Nie zapisuj danych karty na komputerze, w telefonie ani w sklepach internetowych.

Dlaczego? Wirusy i włamania mogą ujawnić te dane złodziejom.



Kontroluj wyciągi bankowe

Regularnie sprawdzaj, czy wszystkie transakcje są Twoje. Jeśli coś się nie zgadza – od razu zgłoś to w banku.

Dlaczego? Im szybciej zareagujesz, tym łatwiej odzyskać pieniądze.



Kontaktuj się z bankiem w razie podejrzeń

Jeśli dostaniesz dziwną wiadomość, e-mail lub SMS – zadzwoń do banku i to sprawdź.

Dlaczego? To może być próba ataku na Twoje konto.



Aktualizuj numer telefonu w banku

Na Twój numer przychodzą SMS-y do potwierdzania transakcji. Bank dzwoni też w razie podejrzanych operacji.

Dlaczego? Jeśli numer jest nieaktualny, możesz nie zauważyć, że ktoś próbuje ukraść Twoje pieniądze.



Zastrzeż kartę w razie problemów

Jeśli zgubisz kartę, ktoś ją ukradnie lub podejrzewasz, że dane wyciekły – natychmiast ją zastrzeż:

- tel. +48 86 215 50 50 (całodobowo)
- tel. +48 828 828 828 (ogólnopolski system zastrzegania kart)
- www.kartosfera.pl

Dlaczego? Im szybciej zastrzeżesz kartę, tym mniejsze straty.

Jeśli zignorujesz te zasady, narażasz się na utratę pieniędzy z konta i kradzież danych.

Bezpieczeństwo Twojej karty zależy od Ciebie.

Jeśli masz wątpliwości – zawsze skontaktuj się z Bankiem.