

Bezpieczeństwo kart płatniczych (debetowych i kredytowych)

Spis treści

Wstęp.....	2
I. Podstawowe zasady bezpieczeństwa	2
II. Bezpieczne korzystanie z bankomatu	4
III. Bezpieczne płatności kartą kredytową w Internecie.....	4

Wstęp

Celem poradnika jest zapoznanie klientów Euro Bank S.A. z praktycznymi zasadami, tzw. dobrymi praktykami, dotyczącymi bezpiecznego posługiwania się kartami płatniczymi, a zarazem przypomnienie o obowiązkach ciążących na Posiadaczach kart, wynikających z obowiązujących przepisów prawa – Ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych.

I. Podstawowe zasady bezpieczeństwa

1. Ochrona poufnego numeru PIN

PIN do Twojej karty, to numer poufny, znany tylko Tobie! Najlepiej zapamiętaj go i nigdzie nie zapisuj. Ponadto nigdy i nikomu (nawet pracownikowi banku) nie ujawniaj tego numeru. Dobrą praktyką jest zniszczenie przesyłki z numerem PIN w sposób uniemożliwiający jego poznanie przez osoby nieuprawnione.

Jeśli koniecznie chcesz zapisać numer PIN, to zrób to w bezpiecznym miejscu, nie przechowuj go w postaci możliwej do odczytania przez osoby nieuprawnione, nie przechowuj go razem z kartą, a w szczególności nie zapisuj go na karcie!

2. Nieudostępnianie karty osobom trzecim

Nie udostępniaj swoich kart płatniczych osobom nieuprawnionym np. członkom rodziny lub znajomym, ponieważ jest to niezgodne z obowiązującymi przepisami prawa, a także regulaminami kart płatniczych Euro Bank S.A. Ewentualna utrata karty oraz operacje dokonane przy jej użyciu przez osoby nieuprawnione obciążają zawsze Posiadacza karty.

Zamiast tego skorzystaj z możliwości oferowanej przez bank i złóż wniosek o wydanie dla takiej osoby dodatkowej karty kredytowej lub karty debetowej dla Pełnomocnika do rachunku.

3. Ochrona danych karty

Nie ujawniaj osobom nieuprawnionym poufnych danych karty takich, jak:

- numer karty,
- data ważności,
- trzycyfrowy kod CVV2/ CVC2, znajdujący się na rewersie karty.

Euro Bank S.A. nigdy nie prosi o podanie tych danych za pośrednictwem poczty elektronicznej, serwisów internetowych, a także rozmów telefonicznych inicjowanych przez bank. Każdy taki przypadek traktuj jako próbę wyłudzenia poufnych informacji o karcie (tzw. phishing) oraz bezzwłocznie poinformuj o nim bank.

Ponadto zalecamy nie zapisywać wymienionych wyżej danych karty na komputerach domowych i biurowych oraz w telefonach komórkowych, gdyż mogą one paść ofiarą złośliwego oprogramowania takiego, jak np. spyware (program szpiegujący).

4. Wnikliwe oględziny przesyłek pocztowych z kartą oraz numerem PIN

Karta spersonalizowana tzn. taka, która ma na awersie nadrukowane imię i nazwisko Posiadacza oraz numer PIN do karty wysyłane są odrębnymi przesyłkami pocztowymi na adres korespondencyjny klienta. Po otrzymaniu tych przesyłek dokonaj wnikliwych oględzin, w celu upewnienia się, iż nie zostały one naruszone przez osoby nieuprawnione. Jeśli znajdują się na nich jakiegokolwiek ślady, które mogłyby sugerować, iż zostały one otwarte, bezzwłocznie skontaktuj się z bankiem w celu wydania nowej karty.

5. Korzystanie z limitów bezpieczeństwa

Skorzystaj z funkcjonalności oferowanej przez bank i ustaw na karcie indywidualne dzienne limity kwotowe dla transakcji gotówkowych (wypłat z bankomatów) oraz dla płatności bezgotówkowych (płatności dokonywane w punktach handlowo-usługowych i w sieci Internet). Limity te ograniczają ryzyko strat w przypadku ewentualnej utraty karty.

6. Podpisanie karty

Niezwłocznie po otrzymaniu karty podpisz ją na pasku podpisu, znajdującym się na rewersie, zgodnie ze wzorem podpisu złożonym w karcie wzoru podpisu (karty debetowe) lub na umowie o kartę (karty kredytowe).

7. Środki ostrożności podczas płatności bezgotówkowych

Dokonując płatności w punktach handlowo-usługowych (sklepy, restauracje itp.) ani na chwilę nie trać karty z pola widzenia i kieruj się zasadą ograniczonego zaufania. Nigdy nie pozwalaj personelowi punktu na zabieranie karty na zaplecze w celu dokonania płatności.

8. Wnikliwa weryfikacja wyciągów bankowych

Kontroluj na bieżąco stan rachunku karty kredytowej i rachunku osobistego, do którego została wydana karta debetowa, a także sprawdzaj wnikliwie wyciągi bankowe dotyczące tych rachunków. W przypadku pojawienia się jakichkolwiek nieprawidłowości powiadom bezzwłocznie bank.

9. Utrata karty

W przypadku utraty karty wskutek kradzieży, zgubienia lub w sytuacji uzasadnionego podejrzenia, iż poufny numer PIN bądź dane karty zostały poznane przez osoby nieuprawnione, powiadom bezzwłocznie bank oraz zastrzeż kartę.

W celu zastrzeżenia karty płatniczej wydanej przez Euro Bank S.A. skontaktuj się z czynnym 24 godziny na dobę Centrum Obsługi Klienta pod numerem: (+48 71) 795 54 49.

10. Aktualizacja telefonu kontaktowego

Informuj na bieżąco bank o zmianach numeru telefonu kontaktowego. Euro Bank S.A. prowadzi monitoring transakcji kartowych i może podjąć próbę kontaktu telefonicznego z Tobą w celu weryfikacji nietypowych lub podejrzanych transakcji dokonanych z użyciem Twojej karty.

II. Bezpieczne korzystanie z bankomatu

1. Oględziny bankomatu

Bankomaty mogą być wykorzystane do dokonania przestępstwa zwanego skimmingiem, polegającego na nielegalnym kopiowaniu zawartości pasków magnetycznych kart płatniczych i przechwytywaniu numerów PIN, a następnie wykorzystaniu spreparowanych kart do przeprowadzenia transakcji bankomatowych najczęściej poza granicami naszego kraju. Dlatego przed skorzystaniem z bankomatu zwróć szczególną uwagę na te elementy, które są najczęściej wykorzystywane przez oszustów tj.:

- otwór czytnika kart – w otworze tym może być umieszczony miniaturowy skaner kopiujący zawartość paska magnetycznego karty wkładanej do bankomatu;
- klawiatura – pogrubiona i wystająca ponad powierzchnię blatu bankomatu klawiatura może świadczyć o instalacji specjalnej nakładki umożliwiającej przechwycenie i zarejestrowanie wprowadzanych przez klientów numerów PIN;
- górna ścianka bankomatu – w której np. w fałszywym panelu (z logotypami organizacji płatniczych) może być zainstalowana przez oszustów kamera rejestrująca wprowadzane przez klientów numery PIN;

W przypadku stwierdzenia obecności podejrzanych elementów na bankomacie lub jakichkolwiek śladów uszkodzeń, zabrudzeń czy substancji klejących w okolicy wyżej wymienionych „wrażliwych” miejsc bankomatu, bezwzględnie zrezygnuj z jego użycia oraz powiadom o tym niezwłocznie właściciela bankomatu (numer telefonu powinien być umieszczony na bankomacie), Euro Bank S.A. (pod numerem: +48 71 799 11 11), lub Policję (pod numerem 112 lub 997).

2. Ochrona wprowadzanego numeru PIN

Dobłą praktyką podczas wprowadzania numeru PIN jest zasłonięcie klawiatury drugą ręką bądź portfelem tak, by uniemożliwić jego podejrzenie osobom nieuprawnionym.

Nie korzystaj z pomocy oferowanej przez osoby postronne.

3. Korzystanie z tych samych bankomatów

Korzystaj w miarę możliwości z tych samych bankomatów – zdecydowanie łatwiej będziesz mógł wtedy zauważyć różnice w ich wyglądzie.

III. Bezpieczne płatności kartą kredytową w Internecie

1. Weryfikacja sklepów internetowych

Korzystaj z renomowanych, wiarygodnych i rekomendowanych przez znajomych sklepów internetowych. Kieruj się zdrowym rozsądkiem, a także

opiniami internautów zamieszczanymi na forach internetowych oraz grupach dyskusyjnych.

Przed dokonaniem płatności koniecznie przeczytaj regulamin sklepu internetowego oraz informacje dotyczące bezpieczeństwa transakcji.

2. Zachowanie szczególnej ostrożności podczas przekazywania poufnych danych karty

Euro Bank S.A. zaleca, aby nie podawać poufnych danych kart płatniczych tj. numeru, daty ważności, trzycyfrowego kodu CVV2/CVC2 na stronach sklepu internetowego, lecz wyłącznie na zabezpieczonych stronach centrów autoryzacyjnych (np. Polcard, eCard), na które Posiadacz powinien zostać przekierowany w trakcie dokonywania płatności internetowej. Tylko wtedy można mieć gwarancję zapewnienia poufności tych danych.

Przesłanie ww. danych karty oraz Twoich danych jako Posiadacza karty, powinno odbywać się zawsze w sposób bezpieczny, tzn. z wykorzystaniem protokołu https. Adres URL serwisu internetowego powinien rozpoczynać się od przedrostka https (zamiast standardowego http), a ponadto u dołu ekranu przeglądarki lub na pasku adresowym (w zależności od przeglądarki) powinien znajdować się symbol zamkniętej kłódki.

W przypadku jakichkolwiek wątpliwości w trakcie procesu autoryzacji płatności internetowej zrezygnuj z jej przeprowadzenia i poinformuj o nich bank.

3. Bezpieczeństwo miejsca dokonywania płatności internetowych

Nie dokonuj płatności internetowych z komputerów znajdujących się w miejscach publicznych i ogólnie dostępnych takich, jak np. kafejki internetowe czy biblioteki.

Zadbaj o bezpieczeństwo swojego komputera, za pośrednictwem którego dokonujesz płatności internetowe. Powinien on posiadać:

- aktualizowany na bieżąco system operacyjny,
- najnowszą wersję przeglądarki internetowej,
- program antywirusowy z aktualnymi sygnaturami wirusów,
- osobistą zaporę (tzw. personal firewall) z aktualnymi polisami i regułami bezpieczeństwa,
- aktualne oprogramowanie wykrywające złośliwe oprogramowanie typu spyware.

Zachęcamy do odwiedzenia portalu "Bezpieczny bank" (<http://www.zbp.pl/photo/bezpieczenstwo/>), opracowanego przez Związek Banków Polskich i zapoznania się z zamieszczonymi tam rekomendacjami, dzięki którym będziesz mógł zwiększyć bezpieczeństwo Twojego komputera oraz zapoznać się z podstawowymi zagadnieniami bezpieczeństwa w bankowości internetowej.

Polecamy również serwis edukacyjny Związku Banków Polskich „KartyBezTajemnic.pl” (<http://www.kartybeztajemnic.pl>), dzięki któremu będziesz mógł podnieść poziom swojej wiedzy w zakresie funkcjonowania kart płatniczych, praw i obowiązków Posiadacza karty oraz zasad świadomego i bezpiecznego używania kart płatniczych.