Bezpieczeństwo kart płatniczych oraz płatności mobilnych

Spis treści

Wstęp.....2
I. Podstawowe zasady bezpieczeństwa 2
II. Bezpieczne korzystanie z bankomatu 5
III. Bezpieczne płatności kartą w Internecie.....6

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.

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.

2. Nieudostępnianie karty osobom trzecim

Nie udostępniaj swoich kart płatniczych ani płatności mobilnych osobom nieuprawnionym, np. członkom rodziny lub znajomym - jest to niezgodne z obowiązującymi przepisami prawa, regulaminami kart płatniczych oraz zasadami bezpieczeństwa stosowanymi przez Euro Bank S.A. 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 takich, jak:
- numer karty,
- data ważności,
- trzycyfrowy kod CVV2/ CVC2, znajdujący się na rewersie karty,
- jednorazowe hasła do zatwierdzania operacji internetowych (Hasła OTP)

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 Bank nie zaleca zapisywać wymienionych wyżej danych karty w żadnym miejscu – w tym w komputerach domowych jak i biurowych oraz w telefonach komórkowych, gdyż mogą one paść ofiarą złośliwego oprogramowania 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 upewnij się, iż nie zostały one naruszone przez osoby nieuprawnione. Jeśli znajdują się na nich jakiekolwiek ślady, które mogłyby sugerować, iż zostały one otwarte, bezzwłocznie skontaktuj się z Bankiem poprzez Centrum Obsługi Klienta celem poinformowania o tym fakcie oraz wydania nowej karty Pozostajemy do Twojej dyspozycji przez całą dobę pod numerem telefonu 19 000 (koszt połączenia wg stawki operatora) oraz adresem e-mailowym Info@eurobank.pl

5. 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). Jest to obowiązkiem każdego posiadacza karty.

6. Korzystanie z limitów transakcyjnych

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

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, np. nigdy nie pozwalaj personelowi punktu na zabieranie karty na zaplecze w celu dokonania płatności.

8. Płatności zbliżeniowe

Płatności zbliżeniowe bez potwierdzania PINem możliwe są do zrealizowania maksymalnie do kwoty 50 zł, każda kwota powyżej będzie już wymagała takiej autoryzacji. Płatności zbliżeniowe są w pełni rekomendowane przez organizacje płatnicze VISA oraz MasterCard i uznane jako bezpieczne m.in. z racji tego, że karta nie opuszcza rąk posiadacza. Są one również oparte na technologii mikroprocesorowej spełniającej wymogi najwyższego obowiązującego standardu EMV**.** Jest on technicznym standardem transakcji realizowanych kartami płatniczymi, zapewniającym bezpieczny przekaz danych zapisanych na karcie. Autoryzacja i przesyłanie danych odbywa się za pomocą mikroprocesora (chipa) umieszczonego na karcie.

Transakcje zbliżeniowe, podobnie jak i transakcje standardowe (stykowe), są całodobowo monitorowane przez systemy bezpieczeństwa Banku. Podstawową zasadą bezpieczeństwa przy korzystaniu z kart z usługą zbliżeniowości jest nieudostępnianie jej innym osobom oraz nieprzekazywanie innym osobom PINu, który powinien być znany tylko Tobie. Jeżeli mimo wszystko nie chcesz korzystać z płatności zbliżeniowych, istnieje możliwość całkowitego wyłączenia funkcji zbliżeniowej Twojej karty poprzez kontakt z Centrum Obsługi Klienta, dostępne pod numerem 19 000 (koszt połączenia wg stawki operatora) przez całą dobę.

9. Środki ostrożności przy płatnościach mobilnych VISA

Jeżeli korzystasz z płatności mobilnych VISA pamiętaj, że usługa ta jest przypisana do Twojej aplikacji mobilnej. Dzięki niej możliwe jest wykonywanie operacji bezgotówkowych w punktach sprzedaży przy których do kwoty 50 zł nie jest wymagane potwierdzanie ich PINem. Korzystając z usługi upewnij się, że tylko Ty masz dostęp do telefonu i ustawione są stosowne limity płatności. Pamiętaj też o tym, aby nie przechowywać razem z urządzeniem lub w urządzeniu PINu do płatności mobilnych VISA. Zgodnie z Regulaminem obowiązkiem każdego posiadacza jest jego ochrona.
Dodatkowym środkiem bezpieczeństwa jest wykorzystywanie zabezpieczeń telefonu w celu ochrony usługi płatności mobilnych VISA. Większość modeli telefonów oferuje rozwiązania takie jak zabezpieczanie ekranu wzorem lub pinem, warto też regularnie aktualizować oprogramowanie tak, aby cały czas korzystać z najnowszej jego wersji. Dla zwiększenia bezpieczeństwa zalecane jest korzystanie z oprogramowania antywirusowego w telefonie.

10. Wnikliwa weryfikacja stanu środków na rachunku

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 o tym bezzwłocznie Bank – przez całą dobę nasze Centrum Obsługi Klienta pozostaje do Twojej dyspozycji.

11. Utrata karty

W przypadku zagubienia lub kradzieży karty (lub telefonu z usługą płatności mobilnych VISA), jak najszybciej skontaktuj się z Bankiem w celu jej zastrzeżenia:

• telefonicznie – dzwoniąc pod całodobowy numer 19 000 (koszt wg stawki operatora) lub za pośrednictwem Systemu Zastrzegania Kart pod numerem + 48 828 828 828 (koszt wg stawki operatora)

• osobiście – odwiedzając dowolną placówkę Euro Bank S.A.

• przez Internet – za pośrednictwem serwisu bankowości elektronicznej eurobank online lub w aplikacji mobilnej

• mailowo – wysyłając informację na Info@eurobank.pl

Po zastrzeżeniu karty zostaje ona całkowicie wyłączona i nikt nie może się nią posługiwać. W celu otrzymania nowej karty, w miejsce utraconej, należy złożyć wniosek w dowolnej placówce Euro Bank S.A. lub przez serwis internetowy (oraz, w przypadku korzystania z Bankowości Elektronicznej i karty kredytowej – telefonicznie). Do nowej karty będzie wydany nowy numer PIN.

12. Aktualizacja numeru 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.

13. Monitoring transakcji

Transakcje realizowane przy użyciu kart wydanych przez Euro Bank S.A. są monitorowane przez systemy bezpieczeństwa Banku, które reagują w przypadku zidentyfikowania nietypowej bądź podejrzanej aktywności na karcie. Bank, zgodnie z Regulaminem, ma prawo kontaktować się z posiadaczem karty w celu weryfikacji Transakcji płatniczej.

II. Bezpieczne korzystanie z bankomatu

1. Oględziny bankomatu

Bankomaty mogą być wykorzystane m.in. do dokonania przestępstwa zwanego skimmingiem, polegającego na nielegalnym kopiowaniu zawartości pasków magnetycznych kart płatniczych i przechwytywaniu numerów PIN. Tak pozyskane dane są następnie wykorzystywane do tworzenia fałszywych kart, przy użyciu których realizowane są transakcje bankomatowe poza granicami naszego kraju. Dlatego przed skorzystaniem z bankomatu zwróć szczególna 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;
• górna/boczna ścianka bankomatu – na której w ewentualnym fałszywym panelu (np. z logotypami organizacji płatniczych) może być zainstalowana przez oszustów kamera rejestrująca wprowadzane przez klientów numery PIN;
• klawiatura – pogrubiona i wystająca ponad powierzchnię blatu bankomatu klawiatura może świadczyć o instalacji specjalnej nakładki umożliwiającej przechwycenie i zarejestrowanie wprowadzanych przez klientów numerów 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

Dobrą praktyką podczas wprowadzania numeru PIN jest zasłonięcie klawiatury drugą ręką bądź portfelem tak, by uniemożliwić jego podejrzenie osobom nieuprawnionym lub nagranie przez nielegalne urządzenia rejestrujące. 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 w Internecie

1. Ochrona danych karty

Chroń dane swojej karty. Nie udostępniaj karty ani danych karty (takich jak jej numer, data ważności, trzycyfrowy kod CVV2/CVC2 znajdujący się na odwrocie) osobom nieupoważnionym. Tylko Ty możesz z niej korzystać. Do realizacji transakcji internetowej NIGDY nie jest wymagany kod PIN.

2. Zachowanie szczególnej ostrożności podczas przekazywania poufnych danych karty

Korzystaj wyłącznie z bezpiecznych witryn. Jeśli witryna jest bezpieczna, w oknie przeglądarki pojawi się ikonka zamkniętej kłódki. Jeśli jej nie zobaczysz lub jeśli po kliknięciu na nią wyświetli się komunikat o wygaśnięciu certyfikatu – nie kontynuuj zakupów! Dodatkowo, przed dokonaniem płatności w serwisie dokładnie przestudiuj jego regulamin; są w nim zawierane informacje mówiące o tym w jaki sposób korzystać z serwisu, w jaki sposób będą wykorzystywane dane Twojej karty i jak nawiązać kontakt ze sprzedawcą w razie jakiejkolwiek potrzeby. Jeśli w regulaminie będzie brakowało tych informacji lub też w dalszym ciągu masz dodatkowe pytania, podejmij kontakt ze sprzedawcą celem otrzymania na nie odpowiedzi. Szczególną uwagę zwróć na kwestie dotyczące samych płatności, czy będą one realizowane jednorazowo, czy serwis zapisuje dane Twojej karty, czy też może u sprzedawcy obowiązują płatności subskrypcyjne? Pamiętaj, że korzystając z serwisu wyrażasz zgodę na zapisy znajdujące się w jego Regulaminie.

3. Usługa 3DS oferowana przez Euro Bank S.A.

3D Secure to usługa, która zapobiega nieautoryzowanym transakcjom, np. kiedy ktoś bez Twojej zgody próbuje zapłacić Twoją kartą. Dzięki 3D Secure Twoje transakcje są pod dodatkową kontrolą, bo zanim zapłacisz, otrzymasz SMS-em hasło, którym musisz potwierdzić swój zakup. Rejestracja oraz korzystanie z usługi są bezpłatne. Transakcja internetowa zostanie zrealizowana z jej użyciem tylko wtedy, gdy sklep internetowy również ją oferuje. Pamiętaj również, że numer Twojego telefonu w Banku musi być aktualny.

4. Limity transakcji internetowych

Zarządzaj limitami transakcji internetowych. Możesz je ustawić samodzielnie i dopasować do własnych potrzeb. Jeśli ustawisz limit na wartość „0”, wyłączysz możliwość dokonywania płatności internetowych – zawsze jednak możesz to zmienić! Zmiana jest bezpłatna i możesz jej dokonać poprzez bankowość elektroniczną lub odwiedzając placówkę Euro Bank S.A..

5. 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,
- osobista zaporę (tzw. personal firewall) z aktualnymi polisami i regułami Bezpieczeństwa,
- aktualne oprogramowanie wykrywające złośliwe oprogramowanie typu spyware,
- w ustawieniach przeglądarki internetowej opcja zapamiętywania danych powinna być wyłączona.

Euro Bank S.A. poleca korzystanie z programu IBM Trusteer Rapport, bezpłatny program oferowany przez firmę IBM. Jest on uzupełnieniem ochrony antywirusowej komputera pomagającym w zapobieganiu atakom złośliwego oprogramowania oraz incydentom wyłudzania poufnych danych przekazywanych drogą elektroniczną (phishingu), które są punktem wyjścia do większości oszustw finansowych. Jest rekomendowany przez Euro Bank S.A. jako dodatkowy element ochrony Twojego komputera. Służy jako uzupełnienie innego oprogramowania zabezpieczającego jak oprogramowania antywirusowego czy osobistej zapory firewall. IBM Trusteer Rapport jest w stanie wykrywać, a następnie przerywać proces instalacji złośliwego oprogramowania, w ten sposób eliminując zagrożenie z komputera. Ponadto IBM Trusteer Rapport blokuje podejmowane próby naruszenia zabezpieczeń przeglądarki oraz sesji w Bankowości Internetowej. Więcej informacji o narzędziu IBM Trusteer Rapport można znaleźć na stronie internetowej Banku pod adresem:
https://www.eurobank.pl/produkty,bankowosc-elektroniczna,ibmsecurity-trusteer-rapport,203,229.html

W przypadku pytań, zapraszamy do kontaktu.