

Zasady bezpiecznego użytkowania kart

Odbiór karty i numeru PIN.

Po otrzymaniu przesyłek z kartą bądź numerem PIN, sprawdź czy nie ma na nich śladów, które mogłyby sugerować naruszenie przesyłki przez osoby nieuprawnione. W razie jakichkolwiek wątpliwości skontaktuj się z infolinią lub placówką SK banku.

Podpisz kartę zaraz po jej otrzymaniu.

Niezwłocznie po otrzymaniu karty podpisz ją, zgodnie ze wzorem podpisu na umowie lub wniosku, na pasku do podpisu, znajdującym się na rewersie karty.

Nikomui nie udostępniaj kart.

Nie udostępniaj karty osobom nieuprawnionym, dotyczy to również członków rodziny. Za operacje dokonane kartą przez osoby nieupoważnione zawsze odpowiada użytkownik karty. Jeśli chcesz umożliwić pełnomocnikom rachunku korzystanie z karty złóż wniosek o wydanie dodatkowych kart do rachunku.

Zapamiętaj swój osobisty numer identyfikacyjny PIN i nikomu go nie podawaj.

Najlepiej zapamiętać numer PIN i zniszczyć przesyłkę go zawierającą w sposób uniemożliwiający odczytanie przez osoby nieuprawnione. Jeżeli jednak chcesz zapisać numer PIN, pamiętaj, aby przechowywać go w bezpiecznym miejscu, oddzielnie od karty. I nigdy nie zapisuj numeru PIN w telefonie pod nazwą PIN.

Nie udzielaj poufnych informacji.

Numer karty, data ważności, kod CVC2 (trzycyfrowy kody na pasku do podpisu karty) są danymi poufnymi. Nie pozwól na kopiowanie danych z karty przez kogokolwiek. Bank nigdy nie skontaktuje się z Tobą za pośrednictwem poczty elektronicznej czy telefonicznie w celu uzyskania tych informacji. Nie odpowiadaj na maile, które zapraszają do odwiedzenia strony internetowej w celu weryfikacji danych.

Nie trać Karty z pola widzenia podczas transakcji.

Podczas dokonywania transakcji kieruj się zasadą ograniczonego zaufania, w żadnym przypadku nie pozwól aby personel zabrał kartę na zaplecze w celu dokonania płatności.

Dopasuj limity dzienne do swoich potrzeb.

Bank daje Ci możliwość ustalenia dziennych limitów kwotowych na transakcje gotówkowe (wypłaty z bankomatów i terminali POS) oraz bezgotówkowe (płatność w Internecie oraz punktach handlowo-usługowych). Limity te pozwolą w przypadku utraty lub skopiowania karty na ograniczenie strat. Zapoznaj się z treścią komunikatu wywieszonego w placówkach SK banku i umieszczonego na stronie www.skbank.pl informującego o kwotach:

- maksymalnych limitów dziennych;
- limitach transakcji zbliżeniowych oraz off-line.

Pamiętaj, że jesteś odpowiedzialny za transakcje off-line w takim samym stopniu jak za transakcje autoryzowane.

Potwierdzenia transakcji bezgotówkowych.

Nigdy nie podpisuj pokwitowania in blanco. W przypadku operacji w imprinterze (ręcznym powielaczu danych karty) zawsze skreśl pustą część blankietu, aby nie było możliwe dopisanie dodatkowych opłat już po transakcji. Na wydrukach z terminali w miejscu na wpisanie napiwku

wpisz kwotę lub przekreśl wolne miejsce. Po transakcji z wykorzystaniem kalki, zniszcz ją. Niszcz nieprawidłowe pokwitowania.

Przed wyrzuceniem niszcz kopie potwierdzeń transakcji czy innych dokumentów, gdzie znajdują się dane Twoje lub Twojej karty.

Dane zawarte na tych dokumentach mogą ułatwić nieuprawnionej osobie przeprowadzenie transakcji. Jeżeli chcesz zachować potwierdzenia operacji pamiętaj, aby przetrzymywać je w bezpiecznym miejscu. Dobrze jest zachowywać pokwitowania odrzuconych transakcji w celu weryfikacji przyczyny ich niepowodzenia. Takie pokwitowania będą pomocne także jako dowód w przypadku konieczności złożenia reklamacji w banku.

Sprawdzaj wyciągi bankowe.

Na bieżąco kontroluj stan rachunku, do którego wydana jest Twoja karta debetowa oraz wyciągów z rachunku karty kredytowej. W przypadku wykrycia nieprawidłowości w zestawieniu operacji, zweryfikuj niezwłocznie to w placówce lub dzwoniąc na infolinię SK banku. Być może będzie konieczne złożenie pisemnej reklamacji w placówce SK banku.

Ogranicz liczbę posiadanych kart.

Noś ze sobą tylko te karty, których potrzebujesz. Dobrym rozwiązaniem jest noszenie kart poza portfelem, np. w oddzielnym etui albo zamykanej przegródce w torebce. Nieużywane karty zostawiaj w bezpiecznym miejscu w domu.

Okresowo sprawdzaj, czy nie brakuje Ci żadnej karty.

W przypadku stwierdzenia utraty karty, bądź podejrzenia skopiowania karty lub poufnych danych, skontaktuj się z SK bankiem i zablokuj lub zastrzeż kartę.

- W przypadku dodatkowych pytań zapraszamy do placówki SK banku lub prosimy o kontakt z **Infolinią SK banku: tel. 22 763 87 91-92, 801 170 070**, w dni robocze w godz. **08:00-20:00**
- Zastrzeżenia poza godzinami pracy placówek i Infolinii SK banku dokonywane są w **Sekcji Zastrzeżeń First Data Polska S.A.** pod numerem telefonu: **+48 22 515 31 50**, dostępnej **24h/7** dni w tygodniu.

Aktualizacja danych osobowych.

Zadbaj o to by SK bank posiadał Twoje aktualne dane. Pamiętaj o poinformowaniu swojego oddziału SK banku o zmianie adresu do korespondencji, numeru telefonu lub dokumentu tożsamości.

Korzystanie z bankomatu

Bankomaty.

Nie korzystaj z podejrzanie wyglądających bankomatów. Zwróć uwagę czy na otworze czytnika kart nie ma dodatkowych elementów, np. skanera kopiującego dane z paska magnetycznego karty. Klawiatura pogrubiona lub wystająca ponad powierzchnię blatu świadczyć może o istnieniu nakładki pozwalającej na zarejestrowanie wprowadzanego numeru PIN. Sprawdź czy nie ma dodatkowych kamer skierowanych na klawiaturę nagrywających wprowadzany numer PIN. Jeżeli bankomat znajduje się w pomieszczeniu, do którego wejście wymaga użycia czytnika, sprawdź czy nie ma założonego drugiego fałszywego czytnika, który umożliwi skopiowanie danych z Twojej karty.

Jeśli stwierdzisz obecność podejrzanych elementów, w żadnym wypadku nie korzystaj z takiego bankomatu oraz powiadom właściciela bankomatu lub policję.

Wprowadzanie numeru PIN.

Podczas wprowadzania numeru PIN upewnij się, że nikt nie stoi na tyle blisko, by mógł zobaczyć wpisywany kod. Najlepiej zasłonić klawiaturę drugą ręką. Nie korzystaj z pomocy oferowanej przez osoby trzecie, podczas wprowadzania numeru PIN.

Płatności w Internecie.

Sprawdź reputację sprzedawcy.

Korzystaj z wiarygodnych i rekomendowanych przez znajomych sklepów internetowych.

Zachowaj ostrożności podczas podawania poufnych danych.

Zachowaj szczególną ostrożność podczas podawania poufnych danych: numeru karty, daty ważności karty, kodu CVC2. Zwrócić uwagę na obecność kłódki na pasku adresowym przeglądarki, oznaczającej, że połączenie ze stroną jest szyfrowane. Upewnij się, czy strona internetowa, na której podajesz swoje dane oraz dane karty nie ma mechanizmów zapamiętujących te dane i nie wymaga podawania ich przy kolejnych zakupach na tej stronie, co może odbyć się poza Twoją kontrolą.

Miejsca dokonywania płatności internetowych. Nie dokonuj płatności z komputerów w miejscach publicznych. Komputer, z którego dokonujesz płatności powinien posiadać program antywirusowy z aktualną bazą wirusów, zaktualizowaną wersję systemu operacyjnego.

Dodatkowe informacje dotyczące bezpiecznego użytkowania kart znajdziesz na stronach:

Związku Banków Polskich

<http://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe>

MasterCard

<http://www.mastercard.pl/warto-wiedziec/korzystanie-z-karty.html>

<http://www.mastercard.pl/warto-wiedziec/ochrona-przed-oszustwami.html>