

**W NIŻEJ WYMIENIONEJ INFORMACJI OPISUJEMY OBOWIĄZKI SPOCZYWAJĄCE NA KLIENTACH (UŻYTKOWNIKACH USŁUG PŁATNICZYCH), MAJĄCE KLUCZOWE ZNACZENIE DLA BEZPIECZEŃSTWA USŁUG PŁATNICZYCH.**

**OBOWIĄZKI KLIENTA OSTROŻNOŚCIOWE**

Użytkownik, z chwilą otrzymania instrumentu płatniczego ( karty płatniczej, bankowości internetowej , mobilnej ), **powinien podjąć niezbędne środki służące zapobieżeniu naruszenia indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym.**

nr	Obowiązki ostrożnościowe użytkownika
1.	Logowanie oraz wykonywanie dyspozycji za pośrednictwem elektronicznych kanałów dostępu wyłącznie osobiście, z użyciem indywidualnych instrumentów uwierzytelniających.
2.	Zachowanie w tajemnicy informacji zapewniających bezpieczne korzystanie z usług bankowości elektronicznej, w tym informacji przekazanych bankowi dla celów weryfikacji oraz nieudostępnianie i nieujawnianie innym osobom (w tym osobom bliskim lub pracownikom banku) instrumentów uwierzytelniających.
3.	Nieprzekazywanie danych uwierzytelniających osobom trzecim, zwłaszcza podczas przychodzącej rozmowy telefonicznej, nawet jeżeli rozmówca przedstawia się jako pracownik banku.
4.	Nieprzekazywanie danych uwierzytelniających na stronach internetowych lub w aplikacjach, do których dostęp uzyskiwany jest przez linki przesłane przez nieznaną osobę, w tym także na stronach internetowych zawierających znaki graficzne banku.
5.	Nieprzekazywanie danych uwierzytelniających w celu otrzymania płatności przy transakcjach na odległość.
6.	Należyte zabezpieczenie urządzeń i oprogramowania, których klient używa w celu korzystania z usług bankowości elektronicznej, tj. stosowanie legalnego i zaktualizowanego oprogramowania, stosowanie aktualnego oprogramowania antywirusowego, antyspamowego oraz typu <i>firewall</i> , najnowszych wersji przeglądark internetowych oraz niestosowanie aplikacji automatyzujących.
7.	Przechowywanie karty płatniczej oraz kodu PIN z zachowaniem należytej staranności i zasad bezpieczeństwa, np. nieprzechowywanie ich razem, niezapisywanie kodu PIN w telefonie, komputerze lub notatniku.
8.	Przechowywanie indywidualnych danych uwierzytelniających bankowości elektronicznej z zachowaniem należytej staranności, w tym obowiązek nieprzechowywania ich razem.
9.	Nieudostępnianie karty płatniczej lub kodu PIN osobom nieuprawnionym, w tym bliskim lub pracownikom banku.
10.	Nieudostępnianie danych karty w celach innych niż dokonanie transakcji, zgłoszenie reklamacji czy zgłoszenie zablokowania karty.
11.	Pobieranie aplikacji mobilnej banku wyłącznie z autoryzowanego sklepu z aplikacjami.
12.	Nieotwieranie oraz nieodpowiadanie na wiadomości e-mail od nieznanego nadawcy oraz nieotwieranie nieznanego plików z załącznikami.
13.	Zachowywanie fabrycznych zabezpieczeń urządzeń mobilnych.

**OBOWIĄZKI KLIENTA LOJALNOŚCIOWO - INFORMACYJNE**

Sprowadzają się do obowiązku szybkiego reagowania przez użytkownika na zidentyfikowane nieprawidłowości i zagrożenia, tak, aby umożliwić dostawcy usług płatniczych podjęcie

kroków ograniczających negatywne następstwa takich zdarzeń. W tym celu ,użytkownik ma obowiązek **zgłaszać niezwłocznie dostawcy** (lub innemu podmiotowi wskazanemu przez dostawcę)**stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu.** Ponadto użytkownik powinien niezwłocznie powiadomić dostawcę o stwierdzonych nieautoryzowanych, niewykonanych lub nienależycie wykonanych transakcjach płatniczych. **Obowiązek bezpiecznego przechowywania indywidualnych danych uwierzytelniających ma ogromne znaczenie dla ochrony środków pieniężnych użytkownika usług płatniczych i dla ograniczenia ryzyk związanych z oszustwami i nieuprawnionym dostępem do rachunku płatniczego.**

nr	Obowiązki lojalnościowo-informacyjne użytkownika
1.	Niezwłoczne zgłoszenie bankowi utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia lub dostępu do karty w serwisie telefonicznym, w oddziałach banku lub za pośrednictwem serwisu internetowego.
2.	Niezwłoczne zgłoszenie bankowi utraty, kradzieży, przywłaszczenia, nieuprawnionego użycia lub dostępu do instrumentów uwierzytelniających (kod PIN, kod CVC2/CVV2) w serwisie telefonicznym, w oddziałach banku lub za pośrednictwem serwisu internetowego.
3.	Niezwłoczne zgłoszenie bankowi stwierdzenia utraty, kradzieży, przywłaszczenia telefonu, na którym zainstalowana jest aplikacja mobilna i dodana karta zbliżeniowa w postaci wirtualnej lub aplikacja obca, w której zapisane są karty wydane przez bank.
4.	Zgłoszenie bankowi sytuacji poznania przez osobę trzecią danych karty płatniczej lub kodu PIN.

Ponadto Bank nigdy nie wymaga:

nr	dodatkowe ostrzeżenia
1.	ujawnienia przez użytkownika haseł do bankowości elektronicznej (poza miejscami do tego przeznaczonymi w ramach bankowości internetowej).
2.	zainstalowania dodatkowego oprogramowania oprócz aplikacji banku pobranej z autoryzowanego sklepu z aplikacjami mobilnymi.
3.	w przypadku instalacji aplikacji pozwalającej na zdalny dostęp do urządzenia, narażone zostają dane użytkownika i środki na jego rachunku.

Ponadto Bank zaleca:

nr	dodatkowe zalecenia
1.	ochronę haseł używanych do logowania w aplikacjach i na stronach internetowych, jeżeli zostały w nich zapisane dane karty.
2.	zachowanie ostrożności w przypadku płatności kartą w Internecie, wprowadzania PIN-u w terminalu lub bankomacie.
3.	monitorowanie poprawności stanu rachunku.

---

## **Stopień zawinienia użytkownika**

Prawidłowe wykonanie przez użytkownika omówionych wyżej obowiązków ostrożnościowych i lojalnościowo-informacyjnych ma kluczowe znaczenie prawne. Zależy bowiem od niego ciężar finansowy jaki będzie ponosić użytkownik w przypadku wystąpienia transakcji nieautoryzowanej.

Płatnik (klient ) odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z tych obowiązków.

**Należy oczekiwać od użytkowników korzystających z ugruntowanych już w praktyce instrumentów płatniczych, że ich świadomość i ostrożność będą zwiększać się wraz z upływem czasu.**