

Zasady bezpieczeństwa oraz Twoje obowiązki jako użytkownika bankowości internetowej oraz mobilnej:

1. Aby korzystać z systemu bankowości internetowej lub mobilnej powinieneś mieć aktualny system operacyjny, przeglądarkę oraz działające oprogramowanie antywirusowe i zaporę sieciową („firewall”).
2. Masz obowiązek przechowywać i skutecznie chronić środki dostępu do usługi bankowości elektronicznej lub mobilnej zachowując należytą staranność – w tym także odpowiednio chronić komputery i urządzenia mobilne, przez które z nich korzystasz.
3. Nigdy nie udostępniaj osobom trzecim swojego: loginu, hasła, PIN-u do aplikacji, kodów autoryzacyjnych, kodów BLIK. Nie przekazuj swoich danych przez telefon i w komunikatorach. Nie podawaj danych na stronach innych niż strony banku.
4. Zachowaj szczególną ostrożność, jeśli w jednym miejscu masz podać kilka swoich danych, np. login i hasło do bankowości, PIN i numer PESEL.
5. Zanim wpiszesz login i hasło, upewnij się, że jesteś na właściwej, bezpiecznej stronie logowania do bankowości.
6. Czytaj dokładnie, czego dotyczą SMS-y autoryzacyjne. W przypadku transakcji zawsze sprawdzaj, czy zgadza się numer konta i kwota.
7. Nie przekazuj treści SMS-ów autoryzacyjnych innym przez telefon, mejlem czy komunikatorem. Nie wpisuj kodów nigdzie poza stroną banku. Pamiętaj, że wpisując na stronie banku lub w aplikacji kod z SMS-a autoryzacyjnego zgadzasz się na daną operację.
8. Nigdy nie klikaj w linki w SMS-ach i mejlach. Linki mogą prowadzić do fałszywych stron, na których oszuści przechwycą Twoje dane np. do bankowości czy do karty.
9. Nie otwieraj plików załączonych do podejrzanych mejli. Nie pobieraj aplikacji z nieznanych źródeł. Gdy zainstalujesz je na telefonie, oszuści będą mogli, np. przejąć Twoje SMS-y autoryzacyjne oraz hasła do stron i aplikacji.
10. Nie instaluj dodatkowego oprogramowania by poprawić dostępność usług bankowych, np.: specjalnych aplikacji, certyfikatów. Nikt z banku nie będzie Cię o to prosił.
11. Nie pobieraj aplikacji ani ich aktualizacji za pomocą linków przesłanych w mejlach lub SMS-ach i komunikatorach. Przy instalacji lub aktualizacji czytaj treści zgód i komunikatów o jakie prosi Cię aplikacja. Zwróć szczególną uwagę na uprawnienia do zdjęć, SMS-ów, filmów, kontaktów i geolokalizacji. Nasza aplikacja jest dostępna w autoryzowanych sklepach: Google Play, App Store.
12. Swoją identyfikację Użytkownika możesz podać naszemu pracownikowi w przypadku, kiedy składasz u nas dyspozycję, reklamację lub inne zgłoszenie.

13. W przypadku utraty, kradzieży, wejścia w posiadanie lub podejrzenia wejścia w posiadanie środków dostępu do systemu bankowości elektronicznej lub mobilnej przez osobę nieuprawnioną złóż natychmiast dyspozycję zablokowania dostępu do systemu bankowości elektronicznej lub mobilnej. W imieniu osoby małoletniej/ubezważnionionej złożysz taką dyspozycję, jeśli jesteś jej przedstawicielem ustawowym.
14. Dyspozycję możesz złożyć telefonicznie w czasie godzin pracy Banku pod numerem telefonu +48 40214 22, 33, 37 lub pisemnie w naszej placówce.
15. Mamy prawo zablokować Twój dostęp do kanałów bankowości elektronicznej w przypadku:
- 1) naruszenia przez Ciebie zasad określonych w Regulaminie lub Umowie;
 - 2) celowego wprowadzenia nas w błąd przy zawieraniu Umowy;
 - 3) podejrzenia popełnienia przestępstwa lub wykroczenia przez Ciebie lub osobę trzecią w związku z używaniem kanałów bankowości elektronicznej lub mobilnej.
- Taka blokada będzie trwała, aż przyczyny jej nałożenia zostaną usunięte.
16. Uwierzytelniamy Ciebie, Użytkowników oraz Użytkowników Kart, kiedy rozpoczynacie zlecenie płatnicze oraz:
- 1) chcecie uzyskać dostęp do swojego rachunku w trybie on-line;
 - 2) zlecacie elektroniczną transakcję płatniczą; przeprowadzacie czynności w kanałach zdalnych, które mogą się wiązać z ryzykiem oszustwa związanego z wykonywanymi usługami płatniczymi lub innego naruszenia prawa
17. Jeśli nie zastosujemy silnego uwierzytelnienia Ciebie Użytkownika lub Użytkownika karty, a proces od nas tego wymagał to nie poniesiecie odpowiedzialności za te transakcje. Wyjątkiem są sytuacje, kiedy działaliście umyślnie.
18. Masz obowiązek przechowywać urządzenie mobilne zachowując należyłą staranność w sposób, który zabezpieczy przed jego utratą, dostępem do niego przez osoby nieuprawnione, aby nie mogły z niego skorzystać oraz go ukraść jeśli:
- 1) wykorzystujesz urządzenie mobilne do logowania do usługi bankowości elektronicznej,
 - 2) wykorzystujesz urządzenie mobilne jako urządzenie do silnego uwierzytelnienia.
19. Ty, jako przedstawiciel ustawowy przekazujesz osobie małoletniej lub ubezważnionionej dane identyfikujące, które umożliwiają korzystanie z ograniczonej wersji aplikacji mobilnej, z zachowaniem zasad bezpieczeństwa, o ile taka funkcjonalność jest w naszej ofercie