

Wniosek o dostęp do bankowości elektronicznej IB

☐ nadanie uprawnień

☐ zmiana uprawnień

Twoje rachunki dostępne za pośrednictwem systemu bankowości elektronicznej IB (modulo):

1. Twoje dane osobowe (posiadacza i współposiadacza rachunku):
A. Posiadacz rachunku:

Imię i nazwisko/Nazwa :		
Adres zamieszkania/ Adres siedziby:		
PESEL/ REGON:		
Identyfikator:		
Proszę o przesłanie identyfikatora na podany adres e-mail a pierwszego hasła do logowania na podany numer telefonu komórkowego ¹ :	e-mail:	
	Tel:	

Proszę o ustalenie limitów kwotowych dla przelewów:

☐ bez limitów transakcji

☐ z limitami transakcji:

maksymalna kwota jednego przelewu:

maksymalna kwota dzienna wszystkich przelewów:

Proszę też o automatyczne dodawanie do systemu bankowości elektronicznej nowych kont (lokat, rachunków) w ramach w/w modulo:

☐ TAK

☐ NIE

B. Współposiadacz rachunku:

Imię i nazwisko:		
Adres zamieszkania:		
PESEL:		
Identyfikator:		
Proszę o przesłanie identyfikatora na podany adres e-mail a pierwszego hasła do logowania na podany numer telefonu komórkowego:	e-mail:	
	Tel:	

Proszę o ustalenie limitów kwotowych dla przelewów:

☐ bez limitów transakcji

☐ z limitami transakcji:

maksymalna kwota jednego przelewu:

maksymalna kwota dzienna wszystkich przelewów:

Proszę też o automatyczne dodawanie do systemu bankowości elektronicznej nowych kont (lokat, rachunków) w ramach w/w modulo:

☐ TAK

☐ NIE

¹ Warunkiem przyjęcia przez Bank wniosku o udostępnienie kanałów bankowości elektronicznej jest podanie przez Posiadacza/y oraz wszystkich użytkowników adresu e-mail i numeru telefonu komórkowego.

2. Dane użytkowników²:

A. Proszę o nadanie dostępu do systemu bankowości elektronicznej IB dla poniższych osób (pełnomocników), tak **aby mogli zatwierdzać dyspozycje**:

Imię i nazwisko:		
Adres zamieszkania:		
PESEL:		
Identyfikator:		
Proszę o przesłanie identyfikatora na podany adres e-mail a pierwszego hasła do logowania na podany numer telefonu komórkowego:	e-mail:	
	Tel:	
Podpis użytkownika:		

Proszę o ustalenie limitów kwotowych dla przelewów:

☐ bez limitów transakcji

☐ z limitami transakcji:

maksymalna kwota jednego przelewu:

maksymalna kwota dzienna wszystkich przelewów:

B. Proszę o nadanie dostępu do systemu bankowości elektronicznej IB dla poniższych osób, ale **bez prawa do zatwierdzania dyspozycji**:

Imię i nazwisko:		
Adres zamieszkania:		
PESEL:		
Identyfikator:		
Proszę o przesłanie identyfikatora na podany adres e-mail a pierwszego hasła do logowania na podany numer telefonu komórkowego:	e-mail:	
	Tel:	
Podpis użytkownika:		

Twój/Wasz podpis (posiadacza rachunku/przedstawiciela ustawowego)

pieczęć i podpis naszego pracownika

miejsowość, data

² Dla każdego Użytkownika należy wypełnić Tabelę „Użytkownicy” oraz przekazać druk Karta informacyjna klienta oraz Klauzulę informacyjną Banku RODO. W przypadku większej liczby Użytkowników należy dodać kolejną tabelę.

Podstawowe zasady bezpieczeństwa korzystania z bankowości elektronicznej

Twoje pieniądze i dane w banku są cenne. Bank chroni je swoimi systemami, ale Ty też masz bardzo ważną rolę. Jeśli nie będziesz uważać, oszuści mogą przejąć Twoje konto, wykraść pieniądze albo dane osobowe. Dlatego zawsze stosuj się do poniższych zasad:

1. Chroń telefon i dane do logowania Twój telefon to „klucz” do konta – bo masz na nim SMS-y z kodami i aplikację mobilną. Nigdy nie podawaj nikomu loginu, hasła ani kodu BLIK – nawet rodzinie czy znajomym. Oszuści potrafią podszyć się pod Twoich znajomych i prosić o kod. Jeśli ktoś prosi o kod BLIK – zawsze zadzwoń i upewnij się, że jest to znana Tobie osoba. Co się może stać, jeśli nie sprawdzisz? Oszuści w kilka minut wypłacą Twoje pieniądze z bankomatu albo zapłacą nimi w sklepie.

2. Upewnij się, że logujesz się na stronę banku W pasku adresu zawsze musi być kłódka i adres bskamgora24.pl. Kliknij kłódkę i sprawdź certyfikat. Nigdy nie loguj się przez link z SMS-a czy e-maila. Dlaczego? Falszywe strony wyglądają jak prawdziwe, ale kradną Twoje dane.

3. Logowanie i hasła Do logowania podajesz tylko identyfikator, kilka znaków hasła i kod SMS/aplikacji. Zmieniaj hasło regularnie i nie używaj go w innych serwisach. Dlaczego? Jeśli ktoś pozna Twoje hasło z innej strony, może spróbować użyć go w banku.

4. Ostrożnie z wiadomościami i linkami Nie otwieraj podejrzanych e-maili ani SMS-ów. Nie pobieraj załączników od nieznanym osób. Przykład: dostajesz fałszywą fakturę, a po otwarciu wirus przekierowuje Twój przelew do złodzieja.

5. Nigdy nie instaluj programów do „pomocy zdalnej” Oszuści udają pracowników banku i proszą o instalację TeamViewer lub AnyDesk. Dzięki nim mogą przejąć Twój komputer. Pamiętaj: Bank nigdy nie prosi o instalację programów do zdalnej pomocy!

6. Dbaj o bezpieczeństwo urządzeń Zainstaluj i aktualizuj antywirusa. Aktualizuj system, przeglądarkę internetową i aplikacje. Regularnie skanuj komputer i telefon. Dlaczego? Skanowanie pozwala wykryć wirusy i w porę uniknąć problemów! Aktualizacje łatają dziury w systemie, które mogą wykorzystać oszuści!

7. Sprawdzaj przelewy Zawsze porównuj dane w SMS-ie/aplikacji z tym, co wpisałeś. Sprawdzaj numer telefonu przy przelewach BLIK. Najlepiej wpisyj numery kont ręcznie – wirusy potrafią podmienić je w schowku. Przykład: chciałeś wysłać pieniądze znajomemu, a trafiły do złodzieja.

8. Kontroluj konto Regularnie sprawdzaj historię rachunku. Zwracaj uwagę nawet na małe podejrzane przelewy – to może być test przeprowadzany przez oszusta.

9. Unikaj publicznego Wi-Fi Nie loguj się do banku przez darmowe Wi-Fi (np. Na stacji benzynowej). Dlaczego? Oszuści mogą podglądać dane w takich sieciach.

10. Reaguj natychmiast Jeśli coś jest podejrzane – od razu dzwoń do banku: Tel. 75 754 67 14 lub 75 754 67 15 (pn.–pt., 7:00–17:30) E-mail: Rozliczenia-bs.kamiennagora@bankbps.pl

11. Limity operacji Ustaw limity przelewów i wypłat. Nawet jeśli ktoś przejmie konto, nie ukradnie wszystkiego naraz.

12. Bank nigdy nie pyta o... hasła, kody BLIK ani inne poufne dane. Linki do logowania. Instalację dodatkowych programów. Jeśli dostaniesz takie wiadomości – to oszustwo!

13. Nietypowe wiadomości Bank nie wysyła próśb o instalację programów. Jedynymi wyjątkami są aplikacja mobilna i e-podpis.

14. Wylogowanie Po zakończeniu pracy zawsze klikaj „Wyloguj”. Dlaczego? To zamyka sesję połączenia z Bankiem i chroni Twoje konto.

15. Znaj aktualne zasady bezpieczeństwa Sprawdzaj zasady bezpieczeństwa na stronie: zbp.pl/dla-klientow/bezpieczne-bankowanie/bankowosc-internetowa Dlaczego? Oszuści stale zmieniają pomysły na sposoby ataku!

16. Falszywe przelewy Jeśli dostaniesz potwierdzenie przelewu, którego nie robiłeś – natychmiast dzwoń do banku. Dlaczego? Może uda się nam go zatrzymać.

17. Filtrowanie IP Możesz ustawić logowanie tylko z wybranych adresów internetowych (np. z domu). Dlaczego? Dzięki temu nikt obcy się nie zaloguje.

18. Urządzenia zaufane Dodaj urządzenie do zaufanych, wtedy nie trzeba SMS-ów przy logowaniu. Zaufane urządzenie musi być Twoje, z antywirusem i aktualnym systemem. Dlaczego? Urządzenie powinno być dobrze zabezpieczone, jest ono „kluczem” do Twojego konta.

19. Blokada dostępu Możesz sam zablokować lub odblokować konto w opcji „Pomoc w logowaniu”. Działa 24/7 i jest darmowa. Jeśli podejrzewasz, że ktoś obcy próbuje dostać się do Twojego konta, możesz szybko zablokować dostęp i ochronić swoje pieniądze.

Jeśli nie będziesz przestrzegać zasad, ktoś może przejąć Twoje konto, ukraść pieniądze i dane osobowe. Twoje bezpieczeństwo zależy od Ciebie. Jeśli masz wątpliwości – zawsze dzwoń do Banku.