

Wniosek w sprawie korzystania z Systemu Bankowości Elektronicznej (SBE)

☐ o korzystanie z systemu

☐ o nadanie/zmianę uprawnień dla Użytkownika

1. Proszę o udostępnienie możliwości korzystania z SBE:

Dane Posiadacza rachunku:

Imię i nazwisko															
Adres															
PESEL															

2. Proszę o umożliwienie dostępu do systemu Użytkownikowi:

Imię i nazwisko															
Identyfikator															

3. Sposób zatwierdzania transakcji: hasła sms na nr telefonu komórkowego:

+	4	8				-				-			
---	---	---	--	--	--	---	--	--	--	---	--	--	--

4. Limity dla operacji dokonywanych za pośrednictwem SBE:

LIMITY DLA LOGINU		AKTUALNE Zmiana limitów aktualnych możliwa w SBE Użytkownika	MAKSYMALNE Zmiana limitów maksymalnych wymaga złożenia wniosku w placówce Banku
SYSTEM BANKOWOŚCI INTERNETOWEJ	jednorazowy:		
	dzienny:		
	miesięczny:		
MOBILNE PRZELEWY	jednorazowy:		
	dzienny:		
	miesięczny:		
SZYBKIE PRZELEWY	jednorazowy:		
	dzienny:		
	miesięczny:		

5. Rachunki, do których Użytkownik uzyskuje dostęp za pośrednictwem SBE*:

☐	WSZYSTKIE W RAMACH UMOWY _____
--------------------------	--------------------------------

Uprawnienia do wszystkich rachunków:

☐	Odczyt salda	☐	Zrywanie/edycja lokat
☐	Przeglądanie operacji	☐	Zlecenia stałe
☐	Wykonywanie przelewów	☐	Przelewy zagraniczne
☐	Zakładanie lokat	☐	BLIK
☐	Automatyczne dodawanie rachunków T/N	☐	

6. Rachunki, do których Użytkownik uzyskuje dostęp za pośrednictwem SBE:

1			9	3	3	1	0	0	0	4							
---	--	--	---	---	---	---	---	---	---	---	--	--	--	--	--	--	--

Odczyt salda	Zrywanie/edycja lokat
Przeglądanie operacji	Zlecenia stałe
Wykonywanie przelewów	Przelewy zagraniczne
Zakładanie lokat	BLIK

2			9	3	3	1	0	0	0	4							
---	--	--	---	---	---	---	---	---	---	---	--	--	--	--	--	--	--

Odczyt salda	Zrywanie/edycja lokat
Przeglądanie operacji	Zlecenia stałe
Wykonywanie przelewów	Przelewy zagraniczne
Zakładanie lokat	BLIK

3			9	3	3	1	0	0	0	4							
---	--	--	---	---	---	---	---	---	---	---	--	--	--	--	--	--	--

Odczyt salda	Zrywanie/edycja lokat
Przeglądanie operacji	Zlecenia stałe
Wykonywanie przelewów	Przelewy zagraniczne
Zakładanie lokat	BLIK

4			9	3	3	1	0	0	0	4							
---	--	--	---	---	---	---	---	---	---	---	--	--	--	--	--	--	--

Odczyt salda	Zrywanie/edycja lokat
Przeglądanie operacji	Zlecenia stałe
Wykonywanie przelewów	Przelewy zagraniczne
Zakładanie lokat	BLIK

*data, stempel i podpis
pracownika Banku*

*data i podpis Posiadacza Rachunku /
przedstawiciela ustawowego osoby małoletniej*

POTWIERDZENIE ODBIORU LOGINU, HASŁA DO AKTYWACJI SYSTEMU eBankNet

Nr identyfikatora (loginu)	
----------------------------	--

Nr hasła aktywacyjnego (pakietu)	
-------------------------------------	--

data i podpis Użytkownika

Dane Posiadacza rachunku

Miejscowość, data

Modulo

Oświadczenie Użytkownika w zakresie zasad bezpiecznego korzystania z usługi SBE

Niniejszym oświadczam, że:

- 1) zapoznałem/am się z treścią Informacji zamieszczonej poniżej niniejszego Oświadczenia, w wyniku czego uzyskałem/am* informacje na temat zagrożeń związanych z korzystaniem z usługi Systemu Bankowości Elektronicznej oraz zasad bezpiecznego korzystania z usługi Systemu Bankowości Elektronicznej oraz ryzyk związanych z korzystaniem z usługi Systemu Bankowości Elektronicznej,
- 2) Informacja została mi przedstawiona w sposób jasny, przystępny i zrozumiały.

Równocześnie oświadczam, iż na podstawie uzyskanych informacji zobowiązuję się stosować określone poniżej przez Bank zasady bezpiecznego korzystania z usługi Systemu Bankowości Elektronicznej.

Podpis Użytkownika

Podpis pracownika Banku

(podpis czytelny, a w przypadku podpisu nieczytelnego pieczęć imienna)

INFORMACJA DLA POSIADACZA RACHUNKU/UŻYTKOWNIKA DOTYCZĄCA RYZYK ZWIĄZANYCH Z KORZYSTANIEM Z USŁUGI BANKOWOŚCI INTERNETOWEJ

Najczęściej występujące zagrożenia związane z korzystaniem z usługi bankowości elektronicznej:

- **wyłudzenie danych (phishing)** – polega na podszywaniu się przestępcy pod bank w celu wyłudzenia pożądanых informacji lub nakłonienie do określonych działań. Może to polegać na wysyłaniu do klientów banku fałszywych maili z prośbą o podanie danych logowania lub umieszczaniu linka z przekierowaniem do fałszywej strony internetowej banku. Odmianami phishingu jest **smishing**, czyli wyłudzenie danych za pomocą wiadomości SMS oraz **vishing**, czyli wyłudzenie danych w rozmowie telefonicznej.
- **złośliwe oprogramowanie** – zagrożenie polegające na zainstalowaniu na komputerze klienta wirusów czy programów szpiegujących. Przestępcy wykorzystują złośliwe oprogramowanie w celu przechwycenia poufnych danych do logowania oraz innych wrażliwych danych, które zostać wykorzystane do wykonania oszukańczej transakcji lub kradzieży tożsamości.
- **bezpośrednia kradzież** haseł i narzędzi umożliwiających dostęp do bankowości elektronicznej i autoryzacji transakcji. Zabezpieczeniem przed tym zagrożeniem jest bezpieczne przechowywanie środków do autoryzacji oraz niezapisywanie haseł i loginów w formie jawnej.

Mając powyższe na uwadze, należy pamiętać o następujących zasadach bezpiecznego korzystania z usługi bankowości elektronicznej:

- sprawdź czy adres strony logowania do bankowości internetowej Banku Spółdzielczego w Ełku posiada adres rozpoczynający się od <https://>, a na ekranie jest widoczny symbol kłódki oznaczającej nawiązanie połączenia szyfrowanego. Jeżeli jest widoczny symbol kłódki, kliknij w niego dwukrotnie, aby sprawdzić czy jest ważny i czy został wydany dla Banku Spółdzielczego w Ełku przez Unizeto Technologies S.A.,
- zachowaj ostrożność i ograniczone zaufanie w stosunku do wiadomości e-mail pochodzących od nieznanых nadawców (zwłaszcza zawierające załączniki lub odnośniki do stron internetowych),
- do logowania używaj wyłącznie skrótu umieszczonego na stronie internetowej Banku. Naganne jest używanie do logowania adresu lub linku przysłanego w wiadomości e-mail lub SMS,
- w przypadku autoryzacji z wykorzystaniem hasła SMS zawsze sprawdzaj, czy treść wiadomości SMS jest zgodna z wykonywaną przez Ciebie operacją,
- na bieżąco aktualizuj system operacyjny, przeglądarki internetowe i programy antywirusowe,
- nie zapisuj haseł i loginów w formie jawnej,
- bezpiecznie przechowuj środki do autoryzacji transakcji,

- **informuj niezwłocznie Bank o wszelkich podejrzanych sytuacjach,**
- **rozważ ograniczenie możliwości logowania tylko z określonych adresów IP,**
- **po przygotowaniu przenieś przelewy i paczki przelewów do widoku „Podpisy”. Modyfikacja przelewów znajdujących się w widoku „Podpisy” nie jest możliwa bez autoryzacji,**
- **zawsze sprawdzaj numery rachunków swoich kontrahentów przed podpisaniem przelewów, sprawdzenie należy wykonać wówczas, gdy przelewy znajdują się w widoku „Podpisy”,**
- **jeśli nie jest to konieczne, nie umieszczaj na witrynach internetowych danych identyfikujących bank, w którym posiadasz rachunek (nr rachunku, nazwa Banku),**
- Bank nigdy nie kontaktuje się z klientem w celu podania kodów do zatwierdzania operacji, ani w celu podania identyfikatora i hasła do logowania,
- Bank nie rekomenduje pobierania i instalowania jakichkolwiek aplikacji ze źródeł innych niż oficjalne sklepy,
- Bank nie wymaga instalacji żadnego oprogramowania na telefonach wykorzystywanych do autoryzacji hasła SMS.