Aby użytkownik traktował bankowość elektroniczną jako bezpieczne narzędzie, powinien przestrzegać następujących zasad:

1. Logując się do systemu eBankNet należy sprawdzić czy użytkownik znajduje się na właściwej stronie. Wszystkie operacje po zalogowaniu się na stronę https://ebank.bsr.com.pl są automatycznie zabezpieczone protokołem SSL wykorzystującym klucz o długości 128 bitów. Uwidocznione jest to poprzez ukazanie się żółtej kłódki w prawym dolnym rogu okna przeglądarki, co sygnalizuje, że strona jest szyfrowana i bezpieczna.
Po dwukrotnym kliknięciu na kłódkę powinna pojawić się informacja, dla kogo został wystawiony certyfikat. Prawidłowa informacja to wystawiono:https://bank.bsr.com.pl.
Należy się także upewnić, czy w pasku adresowym przeglądarki w nazwie strony widnieje oznaczenie HTTPS. Jeśli przy logowaniu się do systemu nie widnieje oznaczenie kłódki oraz oznaczenia https prosimy o ich pilne zgłoszenie do banku na jeden z podanych numerów obsługi technicznej systemu.
2. Nie należy podawać swojego hasła dostępu lub haseł jednorazowych poprzez pocztę elektroniczną. Bank Spółdzielczy nigdy nie wysyła e-maili wymagających podania danych osobowych Klientów lub też hasła dostępu, albo haseł jednorazowych.
Nie wysyłane są również drogą e-mailową linki do stron banku oraz do usług bankowości elektronicznej eBankNet oraz wszelkich stron, gdzie rzekomo ma nastąpić weryfikacja czy aktualizacja danych Klientów.
Bank nie przyjmuje również drogą e-mailową zlecenia wykonania transakcji finansowych.
W przypadku pojawienia się takich przypadków prosimy o ich pilne zgłoszenie do banku na jeden z podanych numerów obsługi technicznej systemu.
3. Nie należy podawać swojego hasła dostępu lub haseł jednorazowych osobom dzwoniącym i podającym się za pracownika banku.
4. Natychmiast wykonać zablokowanie dostępu w przypadku zagubienia listy haseł jednorazowych. W każdej chwili można samemu usunąć za pomocą Internetu listę haseł jednorazowych w przypadku np. jej zaginięcia lub zniszczenia.
Można także zablokować dostęp do swojego loginu poprzez zgłoszenie takiej informacji na jeden z podanych numerów obsługi technicznej systemu.
5. Dla własnego bezpieczeństwa nigdy nie należy nosić zapisanego loginu z hasłem dostępu wraz z listą haseł jednorazowych.
W przypadku nieautoryzowanego uzyskania nazwy loginu i hasła dostępu do systemu eBankNet osoba niepowołana nie jest w stanie wykonać jakichkolwiek transakcji finansowych bez użycia dodatkowego jednorazowego hasła uwierzytelniającego .
Analogicznie w razie nieautoryzowanego uzyskania samej listy haseł jednorazowych osoba niepowołana nie jest w stanie wejść do systemu eBankNet bez znajomości loginu i hasła dostępu.
6. Należy unikać logowania do systemu eBankNet z komputerów, do których nie ma się pełnego zaufania (np. w kawiarenkach internetowych)7. Należy dbać o zabezpieczenie komputera, z którego użytkownik loguje się do systemu tzn. instalować legalne oprogramowanie oraz na bieżąco wszystkie poprawki i uaktualnienia zalecane przez producenta oprogramowania.
8. Wylogowanie się z systemu należy wykonywać poprzez funkcję „Wyloguj”, a nie poprzez zamknięcie przeglądarki internetowej.

Ochrona systemu eBankNet jest zapewniana w kilku warstwach:

W systemie istnieją w chwili obecnej dwa typy blokad:
− blokada autoryzacji,
− blokada transakcji;

Pierwsza z nich występuje po n nieudanych próbach wykonania operacji wymagającej podania hasła dostępu do systemu, czyli:
− zalogowanie do systemu,
− zmiana hasła,
− usunięcie listy haseł,
− usunięcie zamówienia listy haseł;

Blokada transakcji zostaje aktywowana po n nieudanych próbach wykonania operacji wymagającej podania hasła jednorazowego, czyli:
− tworzenie, modyfikacja definicji przelewu,
− wykonanie przelewu;

W przypadku, gdy ilość błędnych autoryzacji nie osiągnie limitu a kolejna jest poprawna, wtedy licznik błędnych autoryzacji ulega wyzerowaniu.
Istnieje również możliwość ręcznego ustawienia dowolnej blokady dowolnemu użytkownikowi. Odblokowanie zarówno ręcznej jak i automatycznej blokady wymaga kontaktu z bankiem.

System bankowości elektronicznej eBankNet został stworzony w oparciu o technologię i doświadczenie znanej firmy informatycznej - lidera wśród firm zajmującym się oprogramowaniem dla banków spółdzielczych.

Szyfrowanie transmisji
Połączenie z kontem internetowym jest transmisją zaszyfrowaną. Dzięki temu wszelkie informacje, które są przesyłane lub otrzymywane są dostępne tylko i wyłącznie dla uprawnionego użytkownika. W systemie eBankNet zastosowano jedno z najsilniejszych obecnie szyfrowań algorytmem SSL o długości klucza 128 bitów. Wszystkie transakcje, które zostaną dokonane na koncie, każdorazowo wymagają dodatkowego uwierzytelnienia poprzez wpisanie hasła jednorazowego.

Wejście do systemu
Aby wejść do systemu eBankNet należy podać:
• numer identyfikacyjny - tzw. Login (10 znakowy), który jest częściowo określany przez bank,
• unikatowe hasło dostępu, które przy pierwszym wejściu do systemu system wymusza do zmiany przez użytkownika (min 8- max 16 znaków)- dzięki niemu użytkownik wchodzi na swoje konto, ale nie może jeszcze realizować transakcji.

Lista haseł jednorazowych
Jest to lista z nadrukowanymi hasłami do autoryzacji/wykonywania transakcji, służącymi do uwierzytelniania operacji dokonywanych przez Internet. Lista haseł jednorazowych jest przypisana do konkretnego loginu (klient może posiadać kilka loginów np. mąż i żona do rachunku

wspólnego). Listę zawiera 50 haseł jednorazowych oznaczonych kolejnymi numerami. System automatycznie sam kontroluje, które hasła z karty są już wykorzystane i prosi o podanie konkretnego numeru z listy.

Blokowanie dostępu do systemu

Trzykrotne błędne uwierzytelnienie Klienta podczas wejścia do systemu eBankNet powoduje zablokowanie dostępu do usług systemu. Aby odblokować dostęp, należy zadzwonić pod jeden z podanych numerów obsługi technicznej systemu.
Natomiast trzykrotne błędne podanie hasła jednorazowego podczas próby realizacji transakcji blokuję możliwość wykonywania transakcji - zalogowanie do systemu jest nadal możliwe.

Przy stosowanych obecnie w Banku Spółdzielczym systemach zabezpieczeń praktycznie jedyną możliwością zdobycia loginu i hasła dostępu oraz jednorazowych haseł jest namówienie samego Klienta do dobrowolnego ich podania.
Z tego też względu należy pamiętać, iż bezpieczeństwo bankowości elektronicznej zależy nie tylko od rozwiązań opracowanych przez firmy informatyczne współpracujące z bankami, ale przede wszystkim od samych klientów.