Bezpieczeństwo systemu eBankNet w Banku Spółdzielczym w Jaworze

System bankowości elektronicznej Banku Spółdzielczego w Jaworze 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. 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,
• unikatowe hasło dostępu, które przy pierwszym wejściu do systemu system wymusza do zmiany przez użytkownika.

Lista TAN (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.

Hasła SMS
Są to hasła jednorazowe wysyłane przez Bank na podany we Wniosku numer telefonu komórkowego, służące do uwierzytelniania operacji dokonywanych przez Internet.

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 numer obsługi technicznej systemu: Tel: (76) 870-28-34 wew. 222 w dni robocze Banku - od poniedziałku do piątku w godzinach 7.30 - 16.30

Natomiast trzykrotne błędne podanie hasła jednorazowego podczas próby realizacji transakcji blokuje możliwość wykonywania transakcji - zalogowanie do systemu jest nadal możliwe.

Przy stosowanych obecnie w Banku Spółdzielczym w Jaworze 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.

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 ebank.bsjawor.pl, są automatycznie zabezpieczone. Uwidocznione jest to poprzez ukazanie się kłódki w oknie przeglądarki (najczęściej na górnym lub dolnym pasku, zależnie od rodzaju 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 ebank.bsjawor.pl

Należy się także upewnić, czy w pasku adresowym przeglądarki w nazwie strony widnieje oznaczenie HTTPS.
Do systemu można się zalogować wyłącznie ze strony głównej Banku tzn. www.bs-jawor.pl wybierając opcję *logowanie do systemu* lub bezpośrednio z adresu ebank.bsjawor.pl
Jeśli przy logowaniu się do systemu nie widnieje oznaczenie kłódki oraz oznaczenia https prosimy o ich pilne zgłoszenie do Banku na numer obsługi technicznej systemu: Tel: (76) 870-28-34 wew. 222 w dni robocze Banku - od poniedziałku do piątku w godzinach 7.30 - 16.30

2. Nie należy podawać swojego hasła dostępu lub haseł jednorazowych poprzez pocztę elektroniczną.

Bank Spółdzielczy w Jaworze nigdy nie wysyła:
• e-maili wymagających podania danych osobowych Klientów lub też hasła dostępu, albo haseł jednorazowych,
• e-maili z linkami do stron Banku oraz do usług bankowości elektronicznej oraz wszelkich stron, gdzie rzekomo ma nastąpić weryfikacja czy aktualizacja danych Klientów,
• żadnych aplikacji na telefony komórkowe, które rzekomo pochodzą z Banku Spółdzielczego w Jaworze i żądają instalacji,
• próśb o podanie modelu telefonu lub pobranie certyfikatu bezpieczeństwa na telefon komórkowy.

Bank nie przyjmuje również drogą e-mailową zleceń wykonania transakcji finansowych.

W przypadku pojawienia się takich przypadków prosimy o ich pilne zgłoszenie do Banku na numer obsługi technicznej systemu: Tel: (76) 870-28-34 wew. 222 w dni robocze Banku - od poniedziałku do piątku w godzinach 7.30 - 16.30

3. Nie należy podawać swojego hasła dostępu lub haseł jednorazowych osobom dzwoniącym i podającym się za pracownika banku.

W przypadku pojawienia się takich przypadków prosimy o ich pilne zgłoszenie do Banku na numer obsługi technicznej systemu: Tel: (76) 870-28-34 wew. 222 w dni robocze Banku - od poniedziałku do piątku w godzinach 7.30 - 16.30

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 numer 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 starannie weryfikować numer konta i kwotę przelewu otrzymaną w wiadomości SMS potwierdzającej daną transakcję.

7. Należy unikać logowania do systemu eBankNet z komputerów, do których nie ma się pełnego zaufania (np. w kawiarenkach internetowych).

8. 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.

9. Wylogowanie się z systemu należy wykonywać poprzez funkcję „Wyloguj”, a nie poprzez zamknięcie przeglądarki internetowej.