Podstawowe zasady bezpiecznej pracy w systemie

Usługi Bankowości Internetowej Bankowość Internetowa Banku Spółdzielczego w Jabłonce jest nie tylko szybka, tania i wygodna, ale także bezpieczna.

System Bankowości Internetowej został stworzony w oparciu o technologię i doświadczenie krakowskiej firmy informatycznej SoftNet Sp. z o.o. - lidera wśród firm zajmującym się oprogramowaniem dla banków spółdzielczych.

Poniżej przedstawiamy elementy bezpieczeństwa gwarantowane przez Bank.

Numer identyfikacyjny – tzw. Login (Identyfikator) - jest to niepowtarzalny ciąg znaków, który otrzymuje każdy użytkownik systemu Bankowości Internetowej. Numer identyfikacyjny razem z hasłem służy do identyfikacji w procesie logowania. Numeru identyfikacyjnego nie należy udostępniać innym osobom, za wyjątkiem uprawnionych pracowników Banku.

Hasło – jest to ciąg znaków zapewniających wyłączność dostępu do Usługi Bankowości Internetowej i służy do identyfikacji w procesie logowania. Otrzymujesz je w specjalnie zabezpieczonej kopercie, tak by nie znał go nikt poza Tobą. Hasła nie należy udostępniać innym osobom. Podczas aktywizacji Usługi Bankowości Internetowej Klient otrzymuje hasło startowe. Służy ono tylko do pierwszego logowania do usługi i przed rozpoczęciem faktycznego z niej korzystania musi być zmienione na nowe.

Uwierzytelnianie – ma na celu sprawdzenie tożsamości użytkownika i jego praw dostępu do systemu. W podstawowej formie polega ono na wprowadzeniu Numeru identyfikacyjnego oraz hasła. Jest to tak zwane uwierzytelnianie proste, które wystarcza do korzystania z usług pasywnych, czyli takich, które nie powodują zmian na rachunku. Forma bardziej zaawansowana, zwana uwierzytelnianiem silnym, polega na posłużeniu się kodem SMS.

Kod SMS – to bezpieczna, tania i łatwa w obsłudze metoda zatwierdzania transakcji internetowych. Do jej stosowania potrzebny jest zwykły telefon komórkowy pracujący w dowolnej sieci telefonii komórkowej w Polsce. Kiedy wykonując przelew w ramach Usługi Bankowości Internetowej, wprowadzisz do formularza wszystkie dane, system wyśle na Twój telefon komórkowy wiadomość SMS z kodem bezpieczeństwa. Kod ten należy wtedy wpisać w odpowiednie pole na ekranie komputera, co będzie oznaczać ostateczne potwierdzenie dyspozycji. Każdy Kod SMS jest unikatowy i aktywny tylko przez okres ważności sesji internetowej, dzięki czemu żadna niepowołana osoba nie jest w stanie go wykorzystać. Z tego właśnie względu Kod SMS daje większą swobodę i bezpieczeństwo w zarządzaniu rachunkiem - stosując go, możesz wykonywać przelewy na dowolne rachunki. Aby korzystać z tego sposobu autoryzacji, wystarczy podać numer telefonu komórkowego na wniosku o udostępnienie/ zmianę Usługi Bankowości Internetowej. Pamiętaj jednak - w przypadku utraty telefonu lub zmiany numeru telefonu należy powiadomić o tym fakcie Bank bądź zastrzec usługę.

Limity transakcji – w trakcie aktywacji Usługi Bankowości Internetowej można określić maksymalną kwotę pojedynczego przelewu, czyli maksymalną sumę pieniędzy, jaką będziesz mógł przelać jednorazowo na rachunek obcy. Każda próba wykonania przelewu powyżej tej kwoty nie powiedzie się.

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 Usłudze Bankowości Internetowej zastosowano jedną z najsilniejszych obecnie metod szyfrowania algorytmem TLS (256 bit) z zastosowaniem certyfikatu uwierzytelnionego przez firmę Unizeto Sp. z o.o. W czasie jego używania adres wyświetlany przez przeglądarkę powinien zaczynać się od liter: **https://**.

Blokowanie dostępu do systemu – trzykrotne błędne uwierzytelnienie Klienta podczas wejścia do Usługi Bankowości Internetowej powoduje zablokowanie dostępu do usług systemu. Aby odblokować dostęp, należy zgłosić się osobiście w dowolnej placówce Banku lub zadzwonić pod jeden z podanych numerów obsługi technicznej systemu: (018) 265-23-01, (018) 264-20-71 i poddać się procedurze telefonicznego uwierzytelniania.

Zastrzeganie numeru telefonu komórkowego – można również zastrzec numer telefonu komórkowego, który został udostępniony Bankowi w celu identyfikacji klienta lub potwierdzania jego dyspozycji. Robi się to w razie utraty lub zniszczenia telefonu oraz w innych uzasadnionych przypadkach. W tym celu należy zgłosić zastrzeżenie osobiście w dowolnej placówce Banku lub telefonicznie dzwoniąc pod jeden z podanych numerów obsługi technicznej systemu: (018) 265-23-01, (018) 264-20-71, poddając się procedurze telefonicznego uwierzytelniania.

Wygasanie sesji internetowej – kiedy system stwierdzi brak aktywności przez ok. 10 minut, następuje wylogowanie z serwisu transakcyjnego i przejście na stronę logowania.

Rejestracja aktywności – system automatycznie rejestruje wszelkie czynności użytkownika w czasie sesji internetowej (np. próby logowania, odczyt historii rachunku, wykonanie przelewu itd.) oraz inne informacje, takie jak certyfikat, adres IP bądź numer telefonu użytkownika.

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

1. Ochrona Numeru identyfikacyjnego (Loginu) i haseł.

- Dbaj o zachowanie poufności swojego hasła dostępu. Haseł nie podawaj nawet pracownikom Banku lub osobom dzwoniącym i podającym się za pracownika Banku.
- W razie podejrzenia, że hasło dostępu zostało ujawnione, natychmiast je zmień lub zablokuj usługę, kontaktując się z najbliższą placówką Banku lub dzwoniąc na jeden z podanych numerów obsługi technicznej systemu: (018) 265-23-01, (018) 264-20-71.
- Dla własnego bezpieczeństwa nigdy nie należy nosić zapisanego loginu z hasłem dostępu Jeżeli uważasz, że musisz zapisać hasło, zrób to tak, żeby osoba niepowołana nie mogła tych informacji poprawnie zidentyfikować.

2. Logowanie do Usługi Bankowości Internetowej

- Loguj się, z portalu internetowego **www.bsjablonka.pl** lub bezpośrednio ze strony serwisu transakcyjnego **ebank.bsjablonka.pl** wpisując właściwy adres w linii adresowej przeglądarki.
- Nigdy nie używaj do logowania adresu lub linku przesłanego w wiadomości e-mail przez inną osobę.
- Przed zalogowaniem upewnij się, że w polu Adres przeglądarki internetowej pierwszą częścią zapisu są litery **https**, a nie http.
- Sprawdź, czy w dolnej części ekranu lub obok adresu strony znajduje się symbol kłódki oznaczający sesję szyfrowaną.
- Jeżeli znajdziesz symbol kłódki, kliknij na niego, by sprawdzić, czy wyświetlony certyfikat jest ważny i czy został wydany dla Banku Spółdzielczego w Jabłonce oraz adresu **ebank.bsjablonka.pl**.
- Jeśli symbol kłódki jest niewidoczny lub jeśli certyfikat został wystawiony dla innego adresu, nie wolno korzystać z serwisu - w takiej sytuacji niezwłocznie skontaktuj się z Bankiem.

3. Korzystanie z Usługi Bankowości Internetowej

- Obsługując serwis transakcyjny, korzystaj tylko z jednego okna przeglądarki.
- Podczas korzystania z serwisu nie używaj klawiszy nawigacyjnych przeglądarki internetowej (tj. Wstecz, Dalej, Odśwież, Zatrzymaj). Serwis transakcyjny ma własne klawisze i hiperłącza, które zapewniają sprawne poruszanie się po jego stronach.
- Jeżeli połączenie z serwisem transakcyjnym zostanie zerwane (np. z winy operatora telekomunikacyjnego), zaloguj się ponownie do usługi i sprawdź, czy system zapamiętał ostatnie zlecenia.
- Po zakończeniu korzystania z serwisu transakcyjnego lub w razie konieczności oddalenia się od komputera bezwzględnie zakończ pracę w serwisie transakcyjnym używając opcji Wylogowanie, a nie poprzez zamknięcie przeglądarki internetowej.

4. Inne zalecenia

- Stosuj się do zaleceń producenta systemu operacyjnego i przeglądarki internetowej oraz instaluj zalecane przez niego uaktualnienia tych programów.
- Systematycznie używaj programów antywirusowych i dbaj o ich aktualizację.
- Używaj osobistego Firewalla. Jest to system ochrony komputera przed ingerencją wewnętrzną lub zewnętrzną przez ograniczenie dostępu do informacji o użytkowniku i zasobach komputera.
- Nie korzystaj z bankowości elektronicznej w miejscach ogólnie dostępnych, takich jak kawiarenki internetowe. Używane tam oprogramowanie może być tak zmodyfikowane lub skonfigurowanie, że dane są gromadzone bez Twojej wiedzy.
- Bank nigdy nie wysyła e-maili wymagających podania danych osobowych Klientów lub też hasła dostępu. 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: (018) 265-23-01, (018) 264-20-71.
- Nie otwieraj i nie uruchamiaj plików oraz programów nieznanego pochodzenia.
- Korzystaj tylko z legalnego oprogramowania.
- Informuj niezwłocznie Bank o wszelkich podejrzanych sytuacjach. Zawsze możesz skorzystać z pomocy obsługi technicznej systemu pod numerami: (018) 265-23-01, (018) 264-20-71. Problem możesz także zgłosić przez e-mail na adres: **centrala@bsjablonka.pl** lub osobiście w dowolnej placówce Banku.