BEZPIECZEŃSTWO BANKOWOŚCI ELEKTRONICZNEJ

w Banku Spółdzielczym w Toruniu

ROZDZIAŁ I. BEZPIECZEŃSTWO - IDENTYFIKACJA

W Banku Spółdzielczym w Toruniu dbamy o bezpieczeństwo Twoje i Twoich pieniędzy. W naszym systemie bankowości elektronicznej stosujemy zaawansowane rozwiązania techniczne, aby korzystanie z usługi było nie tylko wygodne, ale także w pełni bezpieczne. Różnorodność zabezpieczeń daje klientowi niezawodny system ochrony konta bankowego.
Wszelkie informacje przekazane przez naszych Klientów są chronione zgodnie z obowiązującymi normami bezpieczeństwa i zachowania poufności.

W Internet Bankingu dostęp do rachunku jest chroniony wielopoziomowym systemem zabezpieczeń.
Do identyfikacji Klienta w usłudze Internet Bankingu używane są:

Numer klienta (identyfikator klienta)

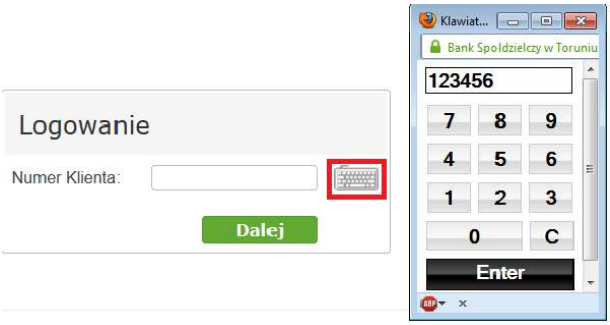
To unikalny numer nadawany każdemu użytkownikowi systemu przez bank w chwili uruchomienia usługi, służący do identyfikacji w Internet Bankingu.

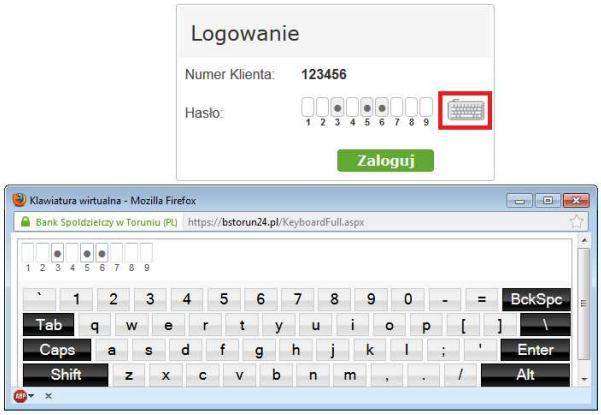
WAŻNE: Aby uniemożliwić dedukcję czy dany identyfikator klienta istnieje w banku ograniczono liczbę prób wpisania Numeru Klienta. **Po trzech nieudanych próbach Twój dostęp zostaje zablokowany**.

Hasło dostępu

1. To indywidualne hasło dostępu klienta do Internet Bankingu, ustalone przez niego przy pierwszym logowaniu. Hasło musi być utworzone wg reguły:
   - ✓ co najmniej 8 znaków,
   - ✓ co najmniej jedna duża litera,
   - ✓ co najmniej jedna mała litera,
   - ✓ co najmniej jedna cyfra,
   - ✓ w haśle do logowania niedozwolone znaki specjalne (np.: <> ?{}[] itp), Serwis sprawuje kontrole nad wpisywanymi znakami i przy próbie wprowadzenia znaku niedozwolonego informuje odpowiednim komunikatem.
2. Przy pierwszym logowaniu będziesz proszony o zmianę hasła dostępu ustalonego przez Bank na hasło własne, znane tylko Tobie, utworzone wg reguły. Aby zmienić hasło wpisujesz we właściwe pola stare hasło, dwukrotnie nowe hasło i zatwierdzasz operację przyciskiem Wykonaj.
3. Hasła nie należy udostępniać osobom trzecim.
4. Hasło może być wielokrotnie zmieniane w serwisie Internet Banking w sekcji Ustawienia.
5. Hasło do logowania w Internet Bankingu jest w wersji maskowalnej. Oznacza to, że w pierwszym oknie podajesz numer klienta, akceptujesz przyciskiem Dalej i przechodzisz do następnego okna, w którym podajesz tylko niektóre znaki swojego hasła dostępu losowo wygenerowane przez system. Zatwierdzasz przyciskiem Zaloguj.
6. Hasło w wersji maskowalnej zabezpiecza przed przechwyceniem go przez programy szpiegujące, w związku z tym nawet jeśli ktoś podejrzy wpisywane przez Ciebie znaki i tak nie uda mu się zalogować na Twoje konto, bo system za każdym razem wymaga innych znaków. Podczas logowania w kolejne aktywne pola należy wpisać odpowiadające im znaki z hasła np. jeśli Twoje hasło to "Torun2013r", a aktywne jest pierwsze, piąte, szóste i dziesiąte pole to należy wpisać litery: "T", "n", "2"oraz "r".

W celu zwiększenia bezpieczeństwa logowania do Internet Bankingu możesz wpisać numer klienta i hasło przy pomocy wirtualnej klawiatury, którą uruchomisz po kliknięciu ikony. W ten sposób unikniesz przechwycenia przez złośliwe oprogramowanie typu „keylogger” znaków wprowadzanych za pomocą standardowej klawiatury.





UWAGA:
W przypadku zapomnienia lub zagubienia hasła skontaktuj się z pracownikiem Oddziału Banku w celu jego anulowania.
Trzykrotna pomyłka w haśle spowoduje zablokowanie usługi. Ponowna aktywacja możliwa jest tylko w Banku.

ROZDZIAŁ II. BEZPIECZEŃSTWO - AUTORYZACJA

Niektóre operacje wykonywane w serwisie Internet Banking m.in. przelewy zewnętrzne na rachunki, które nie zostały wcześniej zdefiniowane w Internet Bankingu, zakładanie lokaty, likwidacja lokaty, tworzenie przelewów zdefiniowanych, wymagają dodatkowej autoryzacji. Dokonywanie transakcji wymaga wprowadzenia przez Użytkownika jednorazowego kodu.

W zależności od wybranej przez siebie opcji:
1. Klient wpisuje kod, otrzymywany w postaci SMS na wskazany przez niego telefon komórkowy lub
2. Klient wpisuje żądany kod z listy haseł jednorazowych, którą otrzymuje z Banku w zabezpieczonej kopercie.

Jednorazowe kody niezbędne do autoryzacji transakcji pozwalają na uniknięcie wykonania zlecenia bez wiedzy właściciela.

Wybraną metodę autoryzacji można w każdej chwili zmienić:
1. w serwisie Internet Banking (opcja w zakładce „Ustawienia” → „Parametry”)
2. w Oddziale Banku

Operacja wymaga potwierdzenia dotychczas wykorzystywaną metodą autoryzacji.
Zmiana sposobu akceptacji z karty kodów jednorazowych na hasła SMS jest możliwa, pod warunkiem, że w siedzibie banku został wskazany numer telefonu komórkowego.

METODY AUTORYZACJI:

Kody SMS

Kod SMS to ciąg sześciu cyfr przesyłany bezpośrednio na wskazany przez użytkownika numer telefonu komórkowego, służący do autoryzacji (zatwierdzenia) niektórych operacji w serwisie Internet Banking m.in.

przelewów zewnętrznych na rachunki, które nie zostały wcześniej zdefiniowane w Internet Bankingu, zakładanie lokaty, likwidacja lokaty, tworzenie przelewów zdefiniowanych.

Kody SMS są:

- **bezpieczne** - ponieważ są przesyłane na wskazany przez użytkownika numer telefonu komórkowego do Internet Bankingu. Każdy kod może być wykorzystany do zatwierdzenia tylko jednej, konkretnej operacji, dla której został wygenerowany (ewentualnie kilku operacji w postaci koszyka płatności). Jej szczegóły otrzymasz wraz z kodem SMS w przesłanej wiadomości tekstowej. Ponieważ każdy kod jest unikalny żadna niepowołana osoba nie będzie go mogła wykorzystać,
- **wygodne** - nie musisz nosić ze sobą aktywnej karty kodów jednorazowych. Kod SMS otrzymasz bezpośrednio na Twoją komórkę, podczas realizacji operacji wymagającej potwierdzenia. Jedyne, czego potrzebujesz to telefon komórkowy, którego numer został wskazany w Banku podczas zawierania umowy o bankowość elektroniczną.
- **nowoczesne** - kody SMS są przesyłane do użytkownika w ciągu kilku sekund.

PRZYKŁADOWY SMS Z HASŁEM:

BS Torun Dane operacji kwota 100,00PLN 2013-03-14 Przelew PRZELEW rach.: 0912...3168696. hasło 162225

Zleconą operacją jest przelew zewnętrzny na kwotę 100,00 na rachunek rozpoczynający się od cyfr 0912, a kończący się na cyfrach 3168696. W tym przykładzie hasło potwierdzające transakcję to 162225.

Pamiętaj!
Zawsze sprawdzaj, czy szczegóły operacji przekazywane w treści wiadomości SMS zgadzają się ze szczegółami zlecenia składanego w Internet Bankingu.

Karta kodów jednorazowych

Karta kodów jednorazowych zawiera 100 jednorazowych, 6-cyfrowych "haseł", przeznaczonych do autoryzacji operacji w Internet Bankingu. Każdy kod służy do potwierdzenia tylko jednej operacji (ewentualnie kilku operacji w postaci koszyka płatności), co uniemożliwia kilkakrotne użycie tego samego kodu. Dodatkowo karta kodów jednorazowych posiada 3-cyfrowy numer identyfikacyjny przydzielany przez system informatyczny Banku.

Pierwszą listę haseł otrzymasz od pracownika Banku w chwili uruchomienia usługi. Każdą następną musisz zamówić i aktywować samodzielnie po odebraniu jej z Banku. Aktywna może być tylko jedna lista. Użytkownik może jednak zamówić więcej list.

Po wybraniu opcji Hasła jednorazowe na ekranie zobaczysz informacje o swoich listach haseł jednorazowych.

Chcąc zamówić nową listę wybierz polecenie Zamów nową listę. W tym momencie do Banku zostanie wysłane zapotrzebowanie na nową listę haseł jednorazowych, a na ekranie pojawi się informacja o zamówieniu nowej listy haseł jednorazowych.

Po odebraniu nowej listy z Banku należy ją uaktywnić poleceniem Aktywuj.

Ostatnie hasło z listy służy do aktywacji kolejnej nieaktywnej listy. Jeżeli nie będziesz miał hasła, nową listę uaktywnić będzie mógł jedynie pracownik Banku.

WAŻNE:
1. Jeżeli zgubiłeś lub skradziono Ci aktywną listę haseł powinieneś niezwłocznie ją zamknąć:
   - korzystając z polecenia Zamknij znajdującego się przy aktywnej liście. Jednak w tym wypadku, aby uaktywnić kolejną listę haseł musisz udać się do Banku,
   - w Oddziale Banku.
2. Pamiętaj o wcześniejszym zamówieniu i odebraniu nowej listy haseł.
3. Ostatnim hasłem z listy nie można podpisać przelewu.
4. Ostatnie hasło z listy służy do aktywacji kolejnej nieaktywnej listy.
5. System pyta tylko raz o hasło jednorazowe. W przypadku pomyłki hasło przepada, a system prosi o następne.

Nawet, gdy karta kodów jednorazowych dostanie się w niepowołane ręce, a jej przypadkowy posiadacz będzie chciał uzyskać dostęp do środków zgromadzonych na rachunku brak znajomości numeru klienta i hasła dostępu uniemożliwi korzystanie z rachunków.

ROZDZIAŁ III. BEZPIECZEŃSTWO – INNE ZABEZPIECZENIA

Obok identyfikacji i autoryzacji w Internet Bankingu stosowany jest szereg innych, dodatkowych zabezpieczeń.

Blokada numeru klienta i hasła dostępu do serwisów Internet Banking oraz SMS Banking

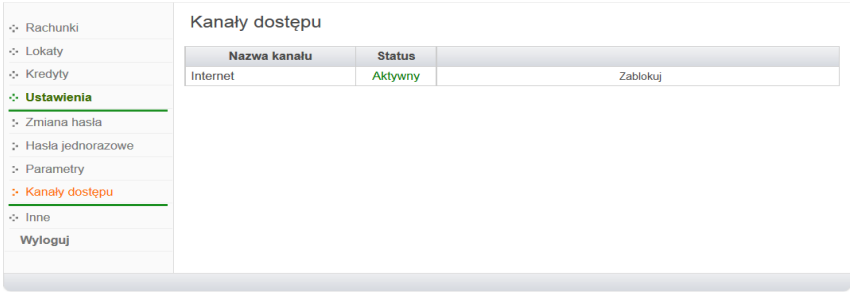
Aby uzyskać dostęp do serwisu Internet Banking oraz SMS Banking, niezbędna jest znajomość własnego Numeru Klienta oraz Hasła dostępu. Dbając o bezpieczeństwo Twoje i Twoich pieniędzy ograniczono liczbę prób wpisania Numeru Klienta oraz hasła dostępu:

1. Aby uniemożliwić sprawdzanie przez niepowołaną osobę, czy dany identyfikator klienta istnieje w Banku ograniczono liczbę prób wpisania Numeru Klienta. Po trzech nieudanych próbach Twój dostęp zostaje zablokowany.
2. Trzykrotna pomyłka w haśle spowoduje zablokowanie usługi. Ponowna aktywacja możliwa jest tylko w Banku.

Proces blokady dostępu do serwisów Internet Banking oraz SMS Banking

Ze względów bezpieczeństwa umożliwiono klientowi zablokowanie dostępu do kanału Internet Banking/SMS Banking:

1. Blokowanie kanału dostępu z poziomu Internet Bankingu.
   a) umożliwia zablokowanie/odblokowanie kanałów dostępu do Internet Bankingu, SMS Bankingu (o ile takie usługi masz włączone w Banku) za pomocą opcji w zakładce Ustawienia → Kanały dostępu (w serwisie klienta).
   b) Zablokować każdy z kanałów dostępu możesz po użyciu polecenia Zablokuj. Program wyświetli pytanie „Czy na pewno zablokować kanał dostępu o nazwie Internet/SMS Banking?”.
   c) Odpowiedź OK zostanie zarejestrowana, program poinformuje, że „Dyspozycja została przyjęta”. Po zablokowaniu status danego kanału zmieni się z „Aktywny” na „Zablokowany”.
   d) Zablokowaną w ten sposób usługę może odblokować operator w Banku.
   e) Również Ty sam możesz odblokować usługę pod warunkiem że nie opuściłeś okna z wymienionym menu.
   Użycie wówczas opcji „Aktywuj” pozwoli Ci wpisać nowe hasło i po akceptacji hasłem jednorazowym odblokujesz dostęp do Internet Bankingu.



2. Blokowanie kanału dostępu poprzez wysłanie na numer telefonu +48 797 339 757 wiadomości SMS o treści:
   a) BI#identyfikator, gdzie identyfikator to login do Internet Bankingu (Numer klienta). Program zweryfikuje, czy podany identyfikator jest powiązany z numerem telefonu (w Internet Bankingu, SMS Bankingu, danych osobowych). W przypadku istniejącego powiązania dostęp jest blokowany i odsyłany odpowiedni komunikat do Klienta.
   b) BI#identyfikator#PESEL - gdzie identyfikator to login do Internet Bankingu (Numer klienta). SMS blokuje dostęp z dowolnego telefonu.

Uwaga: działanie blokowania jest niezależne od posiadania przez klienta usługi SMS Bankingu.

System szyfrowania transmisji przez Internet Banking (SSL)

Wykonywanie operacji finansowych za pośrednictwem Internetu, wymaga zapewnienia maksymalnego poziomu ochrony przed dostępem niepowołanych osób. W tym celu serwis Internet Banking wykorzystuje zaawansowane rozwiązania techniczne, które zapewniają komfort bezpiecznego korzystania z serwisu.

Połączenie z Bankiem chronione jest 128 bitowym protokołem szyfrującym SSL, co praktycznie uniemożliwia przejęcie przez osoby niepowołane kontroli nad aktywną sesją użytkownika.
Protokół SSL to zestaw reguł i standardów zapewniający przeglądarce internetowej bezpieczną wymianę zaszyfrowanych informacji z serwerem WWW z wykorzystaniem tzw. certyfikatów. Zapewnia poufność i integralność informacji wymienianych między Klientem a Bankiem oraz identyfikację serwera, z którym Klient nawiązał połączenie. W trakcie połączenia z Bankiem adres wyświetlany przez przeglądarkę, normalnie zaczynający się od liter http://, powinien zaczynać się od **https://**. Bezpieczne połączenie z witryną internetową za pomocą protokołu SSL jest sygnalizowane poprzez wyświetlenie symbolu zamkniętej kłódki na pasku stanu przeglądarki.
Jednakże, zalecane jest samodzielne sprawdzenie autentyczności certyfikatu, który został zastosowany podczas szyfrowania transmisji. Dane certyfikatu można obejrzeć, klikając na symbol kłódki w pasku stanu przeglądarki.

Rejestracja aktywności

System automatycznie rejestruje wszystkie czynności dokonywane przez Klienta poprzez Internet Banking.
Szczegóły dotyczące logowania i wykonanych operacji dostępne są w "Logu zdarzeń", znajdującym się w sekcji "Inne" w serwisie Internet Banking.

Wygaszanie sesji

To zabezpieczenie stosowane w serwisie Internet Banking, które polega na automatycznym wylogowaniu z serwisu po 15-minutowym braku aktywności.

ROZDZIAŁ IV. BEZPIECZEŃSTWO - ZALECENIA

Bezpieczeństwo operacji wykonywanych poprzez usługę Internet Banking zależy nie tylko od Banku, ale również od użytkownika. Dlatego też, aby bez obaw korzystać z bankowości elektronicznej, stosuj się do zaleceń zawartych na stronie.

Zapoznaj się również z aktualnymi komunikatami Związku Banków Polskich i poradnikiem na temat bezpieczeństwa transakcji bankowych w Internecie

Przestrzegaj zasad bezpiecznego korzystania z usługi Internet Banking

- Nie podawaj kodów jednorazowych, loginu i hasła oraz numeru telefonu na nieznanych stronach.
- Loguj się do Serwisu poprzez stronę:
  - www.bstorun.pl i wybierz opcję logowania, nastąpi wówczas przekierowanie do okna logowania do Internet Bankingu lub
  - https://bstorun24.pl

  Przed zalogowaniem zawsze sprawdź, czy połączenie jest szyfrowane (adres strony zaczyna się wtedy od https) oraz czy w przeglądarce jest widoczny symbol kłódki.
- Nie używaj do logowania adresu ani linku otrzymanego przez e-mail lub komunikator internetowy. Bank nigdy nie wysyła takich wiadomości. Tego typu korespondencję należy traktować jako próbę oszustwa polegającego na wyłudzeniu poufnych danych przez osoby podszywające się pod instytucję finansową.
- Nie zezwalaj przeglądarce na zapisywanie haseł i nazw użytkownika w formularzach.
- Nie przechowuj nazwy użytkownika i hasła dostępu w tym samym miejscu.
- Jeżeli do autoryzacji operacji w serwisie internetowym używasz kodów SMS, zawsze sprawdzaj, czy wiadomość SMS z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją. Zwróć szczególną uwagę na numer rachunku i kwotę operacji.
- Nie korzystaj z komputerów ogólnie dostępnych, np. w kawiarence internetowej, na uczelni.
- Zawsze, kończąc pracę, korzystaj z polecenia Wyloguj.

- Dbaj o aktualizacje posiadanego Systemu operacyjnego.
- Używaj aktualnego oprogramowania ochrony antywirusowej wraz z zaporą.
- Bank nigdy i w żadnej formie nie będzie Cię prosił o podanie hasła (haseł) dostępu do serwisu Internet Banking.
- Bank nie będzie do Ciebie wysyłał żadnych wiadomości poprzez e-mail. Jedyny sposób wysyłania komunikatów do użytkowników to komunikaty widoczne w Serwisie po zalogowaniu lub w opcji [Komunikaty].
- Nie korzystaj z serwisów realizujących płatności, które wymagają ujawnienia numeru klienta, hasła czy kodu do autoryzacji operacji. Udostepnienie ich może pozwolić osobom trzecim na nieuprawniony dostęp do usługi Internet Banking, zmianę Twoich danych lub wykorzystanie ich do celów przestępczych. Pamiętaj również, że ujawnienie danych niezbędnych do logowania lub autoryzacji jest niezgodne z „Regulaminem świadczenia usług w zakresie prowadzenia rachunków bankowych, wydawania kart do rachunków oraz usług bankowości elektronicznej dla klientów indywidualnych, SKO,PKZP i Rad Rodziców w Banku Spółdzielczym w Toruniu", i może skutkować blokadą usługi.

Zapoznaj się z komunikatem Związku Banków Polskich na temat ujawniania informacji wrażliwych serwisom oferującym szybkie płatności.

Regularnie aktualizuj system operacyjny

W przypadku każdego systemu operacyjnego (także mobilnych) podstawową zasadą bezpiecznego korzystania jest stała aktualizacja systemu i posiadanego oprogramowania służącego do korzystania z Internetu, przeglądarki, komunikatorów internetowych, czy programów pocztowych. Aktualizacje usuwają błędy w oprogramowaniu, które mogą być wykorzystane przez osoby trzecie w celu uzyskania naszych poufnych danych.

Zabezpiecz swój komputer i telefon

Ważne jest korzystanie z programów antywirusowych zabezpieczających komputery przed szkodliwym oprogramowaniem oraz z zapory internetowej (tzw. firewall), która kontroluje przesyłanie informacji do i z Internetu zapobiegając tym samym przekazywaniu poufnych danych.

Należy pamiętać również o odpowiedniej ochronie swojego telefonu podczas korzystania z bankowości mobilnej. Część urządzeń (telefony typu smartphone i tablety), to zaawansowane urządzenia wyposażone w system operacyjny, które należy chronić oprogramowaniem antywirusowym.

Korzystaj z legalnego oprogramowania

- Nie instaluj programów ze źródeł, do których nie masz zaufania i podchodź ostrożnie do programów pobieranych z Internetu.
- Nie uruchamiaj programów przesyłanych pocztą elektroniczną. Wiele darmowych programów dostępnych w internecie zawiera aplikację adware, która zawiera programy wyświetlające reklamy (zazwyczaj bannery), niezależnie od czynności wykonywanych przez użytkowników. Ten rodzaj oprogramowania jest często instalowany na komputerach podczas przeglądania stron WWW, bez wiedzy i zgody użytkowników.
- Niektóre programy są również wyposażone w moduły szpiegujące (ang. spyware), które dostarczają autorom aplikacji wielu cennych informacji o użytkowniku - głównie adres IP, używany system operacyjny, przeglądarkę, a niekiedy strony z którymi się łączymy. Aplikacje adware/spyware mogą umożliwić osobom niepowołanym śledzenie danych wpisywanych przez Użytkownika w przeglądarce internetowej, w tym finansowych (numer klienta, PIN, numery kart płatniczych itd.), na co Bank nie ma wpływu ponieważ nie jest stroną uprawnioną do kontrolowania środowiska komputerowego Użytkownika.
- Symptomami zainfekowania komputera są zwykle: spowolnienie działania systemu, zwiększona liczba reklam (szczególnie okienek pop-up), zmiany w działaniu przeglądarki internetowej, problemy z działaniem niektórych programów.

Świadomie dokonuj wyboru przeglądarki internetowej

- Najnowsze wersje popularnych przeglądarek, takich jak Mozilla Firefox, Chrome, Opera czy Internet Explorer zawierają wiele funkcji, np. filtr witryn wyłudzających poufne dane, które w istotny sposób

chronią przed oszustwami w internecie i podnoszą poziom bezpieczeństwa korzystania z bankowości elektronicznej. Oszustwa te, znane są jako "phishing" lub "wyłudzanie informacji". Polegają one zwykle na próbie nakłonienia nas do odwiedzenia fałszywej witryny internetowej, na której możemy być proszeni o podanie poufnych danych osobowych lub numeru karty kredytowej. Ten rodzaj kradzieży tożsamości jest od dłuższego czasu bardzo popularny.

- Pobierz wszelkie uaktualnienia przeglądarek z których korzystasz, wielokrotnie wykrywane w nich były bardzo poważne błędy; krytyczne znaczenie ma instalacja aktualnych poprawek ("łat" - ang. patch) publikowanych na stronach producentów danego oprogramowania. Zabezpieczają one przed wykorzystaniem przeglądarki bez wiedzy użytkownika i w sposób potencjalnie niebezpieczny.
- Jeśli korzystasz z Internet Explorer 6.0 koniecznie zaktualizuj tę przeglądarkę do najnowszej wersji lub zainstaluj inną nowoczesną przeglądarkę internetową.

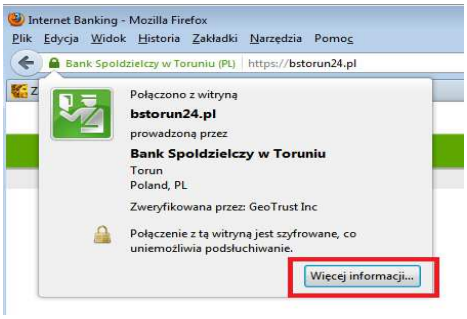
Dokonaj właściwych ustawień przeglądarki

Do poprawnego działania wystarcza dowolna przeglądarka internetowa obsługująca protokół szyfrujący SSL, JavaScript oraz pliki cookies. Zalecane przeglądarki to Internet Explorer, Firefox, Chrome i Safari w wersjach na bieżąco aktualizowanych.

Poprawne działanie systemu jest możliwe po prawidłowym skonfigurowaniu przeglądarki. W Przewodniku dla Klienta korzystającego z Internet Bankingu (Instrukcja użytkownika) konfigurację pokazano na przykładzie przeglądarki Internet Explore.

Sprawdzaj certyfikaty zabezpieczeń

- Po zalogowaniu do serwisu **sprawdź, czy na ekranie widnieje symbol kłódki** oznaczający, nawiązanie połączenia szyfrowanego (**adres zaczyna się wtedy od https a nie od http**).
- Jeżeli znajdziesz symbol kłódki, kliknij na niego, aby sprawdzić, **czy wyświetlony certyfikat jest ważny i czy został wydany dla Banku Spółdzielczego w Toruniu oraz adresu** https://www.bstorun24.pl



Prawidłowy certyfikat powinien zawierać:
- wystawcę: **Geo Trust Inc.**,
- typ certyfikatu: **Geo Trust Extended Validation SSL CA**,
- ważność certyfikatu: **wystawiony dnia 2012-06-12**, natomiast **wygasa dnia 2014-07-15**.

- Jeśli symbol kłódki jest niewidoczny lub jeśli certyfikat został wystawiony dla innego adresu, nie korzystaj z serwisu.
- Sam symbol kłódki nie gwarantuje autentyczności połączenia z Bankiem. Zawsze należy sprawdzić szczegóły certyfikatu.
- **Pamiętaj także, że Bank nigdy nie wysyła żadnych certyfikatów bezpieczeństwa poprzez wiadomość SMS.**

Ustanów hasło do routera

Używając routera lub domowej sieci bezprzewodowej (wi-fi - np. live box) ustanów własne, bezpieczne i trudne do złamania hasło do tych urządzeń. Urządzenia te mają zazwyczaj proste, fabrycznie ustawione hasło, chroniące dostęp do ich panelów administracyjnych. Dzięki znajomości takiego hasła osoba działająca z zewnątrz może zmienić ustawienia routera, co może skutkować przekierowaniem na strony stworzone w celu kradzieży poufnych danych lub dystrybuujących szkodliwe oprogramowanie.

ROZDZIAŁ V. BEZPIECZEŃSTWO – SMS BANKING

SMS Banking to serwis informacyjny umożliwiający dostęp do informacji dotyczących rachunków bankowych za pomocą telefonu komórkowego z dowolnego miejsca na świecie w postaci krótkich wiadomości tekstowych SMS. SMS zawierających informacje o bieżącym saldzie, informację o obrotach na rachunku oraz kwocie dostępnych środków.

Bezpieczny SMS Banking

SMS Banking nie pozwala na wykonywanie przelewów, dlatego nikt nie może wpłynąć na utratę środków przez Klienta. Warto jednak pamiętać, że w momencie utraty telefonu osoba, która pozyska utracony telefon może dowiedzieć się o stanie rachunków i ostatnich operacjach wykonanych przez użytkownika, a co gorsze może na bieżąco dowiadywać się o nowych zdarzeniach na rachunku. Jedynym zabezpieczeniem danych przechowywanych w telefonie są zabezpieczenia telefonu.

Wskazane jest więc, by sukcesywnie kasować w telefonie wiadomości wysłane i odebrane. W przypadku utraty telefonu należy jak najszybciej taki telefon zastrzec u operatora sieci oraz dokonać stosownej zmiany numeru w Banku.