Zasady bezpiecznego korzystania

z usługi PBSBank24

1. **Korzystaj z najnowszych wersji przeglądarek internetowych.**
   Zalecane przeglądarki w wersji desktopowej to:
   - Firefox: http://www.mozilla.org/pl/firefox/new/
   - Chrome: http://www.google.pl/intl/pl/chrome/
   - Internet Explorer: http://windows.microsoft.com/pl-pl/internet-explorer/download-ie

   Zalecane przeglądarki w wersji mobilnej (dla urządzeń typu smartfon, tablet itp.) to:
   - domyślna przeglądarka systemu Android (oznaczona ikoną Internet) lub Google Chrome - urządzenia z systemem Android,
   - Safari - urządzenia z systemem iOS,
   - Internet Explorer - urządzenia z systemem Windows Phone.

2. **Stosuj dobre praktyki bezpieczeństwa:**
   - zwracaj uwagę na komunikaty przeglądarki,
   - chroń swój identyfikator i hasło przed niepowołanymi osobami,
   - podczas wpisywania loginu i hasła / PINu zwracaj uwagę, czy nikt nie podgląda wpisywanych danych,
   - używaj funkcji *wyloguj* zawsze po zakończeniu pracy,
   - zamykaj wszystkie okna przeglądarki przed odejściem od komputera,
   - logując się do Bankowości Internetowej nie korzystaj z funkcji:
     - autouzupełniania formularzy,
     - zapamiętywania haseł,
     - zapamiętywania sesji przeglądarki

     Powyższe ustawienia są praktyczne, jednak niosą za sobą ryzyko dostępu do Twojego rachunku przez innych użytkowników komputera bez Twojej wiedzy.
   - sprawdzaj poprawność adresu URL - prawidłowy adres to: https://sbe.pbsbank.pl

3. **Używając tokena sprzętowego:**
   - nie udostępniaj go nikomu,
   - w przypadku utraty zgłoś ten fakt niezwłocznie do Banku.

4. **Używając tokena programowego:**
   - nie udostępniaj go nikomu,
   - ustaw PIN do tokena inny niż PIN do telefonu,
   - zawsze sprawdzaj czy informacje o transakcji wyświetlone przez token są zgodne z operacją jaką zamierzasz wykonać,
   - nie odblokowuj systemu operacyjnego swojego urządzenia mobilnego (tzn. rooting, jailbreak)
   - w przypadku utraty zgłoś ten fakt niezwłocznie do Banku.

5. **Używając telekodu / SMS:**
   - nie podawaj nikomu nadanego telekodu / SMS,
   - w przypadku podejrzenia dostania się telekodu w ręce osoby trzeciej natychmiast skontaktuj się z placówką Banku w celu zmiany telekodu.

6. **Regularnie aktualizuj swój system operacyjny i używane oprogramowanie.**
   Każdy system operacyjny, w tym również dla urządzeń mobilnych, wymaga regularnej instalacji aktualizacji, które usuwają błędy w oprogramowaniu. Niezałatane luki mogą zostać wykorzystane przez osoby trzecie do przejęcia danych poufnych. Bezwzględnie unikaj korzystania z systemów, dla których producent nie zapewnia wsparcia w postaci aktualizacji bezpieczeństwa, m. in. Windows XP, Me, 2000, 98, 95, Mac OS X 10.4 i starsze. Informacji o cyklu wsparcia dla swojego systemu operacyjnego szukaj bezpośrednio na stronie producenta.

7. **Korzystaj z programów antywirusowych zarówno na komputerze, jak i urządzeniach mobilnych (smartfon, tablet).**

Dbaj o to, aby to oprogramowanie było zawsze aktualne i włączone. Systematycznie wykonuj skanowania całego komputera.

8. Wykorzystuj jedynie legalne oprogramowanie.

Instaluj jedynie programy, do których masz zaufanie. Unikaj programów pochodzących z nielegalnych lub niepewnych źródeł - mogą one być zainfekowane szkodliwym oprogramowaniem szpiegującym użytkownika.

9. Nie otwieraj załączników poczty email, których nie oczekiwałeś.

Bardzo często szkodliwe oprogramowanie wykorzystuje do infekcji kolejnych komputerów pocztę e-mail. Zawsze ostrożnie podchodź do załączników od nieznanych osób lub takich, których nie oczekiwałeś otrzymać.

10. Używaj osobistej zapory fire wall.

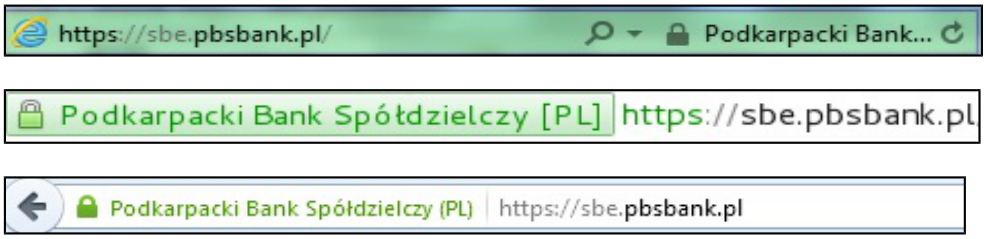
Zapora firewall pełni funkcję strażnika, który kontroluje każdy ruch na styku komputera z Internetem, ograniczając przychodzące i wychodzące połączenia sieciowe. W wielu systemach operacyjnych znajduje się już firewall - wystarczy upewnić się, że jest włączony.

11. Dbaj o bezpieczeństwo połączenia.

Komunikacja między komputerem użytkownika a serwerem banku szyfrowana jest protokołem SSL Potwierdzeniem bezpiecznego (szyfrowanego) połączenia jest:

- adres URL rozpoczynający się od **https** (zamiast standardowego http), gdzie „s" oznacza „secure" –bezpieczny,
- ikona kłódki na dolnym pasku przeglądarki lub pasku adresowym (miejsce zależy od rodzaju i wersji przeglądarki),

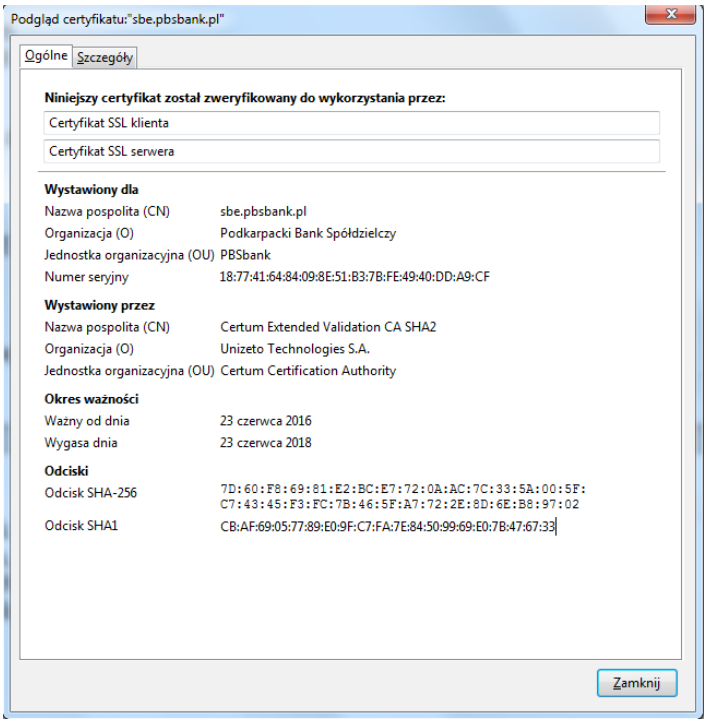
Dodatkowo najnowsze przeglądarki obok paska adresu wyświetlają informacje o instytucji, dla której został wystawiony certyfikat, w tym przypadku: PBSBank.
Poniżej przykład baneru w przeglądarkach Internet Explorer, Chrome i Firefox:



Certyfikat SSL służy do poświadczania autentyczności serwera, z którym komunikuje się dany komputer. Sprawdzenie szczegółów certyfikatu **przed zalogowaniem do serwisu** pozwala się upewnić, że strona z którą nawiązane jest połączenie, to rzeczywiście strona PBSBank.

Prawidłowy certyfikat PBSBank powinien zawierać informacje:

- wystawiony dla: sbe.pbsbank.pl
- wystawiony przez: Certum Extended Validation CA
- ważny od: 23 czerwca 2016
- ważny do: 23 czerwca 2018
- numer seryjny: 18:77:41:64:84:09:8E:51:B3:7B:FE:49:40:DD:A9:CF
- odcisk SHA1: CB:AF:69:05:77:89:E0:9F:C7:FA:7E:84:50:99:69:E0:7B:47:67:33



Uwaga! Jeśli przy wejściu na stronę PBSBank przeglądarka wyświetli jakikolwiek komunikat ostrzegawczy dotyczący certyfikatu, skontaktuj się z infolinią Banku pod numerem 801 372 772 lub +48 13 46 55 750 (koszt połączenia wg taryfy operatora).

12. Uważaj na phishing.

Phishing jest szczególną formą przestępstwa informatycznego polegającego na skłonieniu użytkowników komputerów do ujawnienia swoich danych (nazwa użytkownika, hasło, numer PIN lub inne informacje o dostępach), a następnie wykorzystaniu tych informacji. Phishing jest szczególnie groźny dla użytkowników bankowości internetowej. Wiadomości phishingowe wysyłane do potencjalnych ofiar kierują na strony, które podszywają się pod stronę bankowości internetowej. Typowe sposoby wykradania poufnych informacji to:

- informowanie o rzekomym dezaktywowaniu konta i konieczności ponownej aktywacji - z podaniem wszelkich poufnych informacji; strona przechwytująca informacje jest wówczas łudząco podobna do prawdziwej
- informowaniu o potrzebie podania kolejnych wskazań tokena wymaganych do zalogowania do usługi (np. w celu synchronizacji tokena z Bankowością Internetową),
- tworzenie fałszywych stron serwisów z adresami bardzo przypominającymi oryginalne, a więc łatwymi do przeoczenia dla osób niedoświadczonych w obsłudze przeglądarki internetowej.

Pamiętaj! Wszystkie wiadomości e-mail zawierające prośbę o podanie jakichkolwiek informacji lub zalogowanie się są podejrzane!

PBSBank nigdy nie poprosi Klientów o potwierdzenie loginu lub hasła pocztą elektroniczną, ani nie podaje w wiadomościach e-mail odsyłaczy do strony logowania.
Jedynie na stronie Banku https://www.pbsbank.pl mogą znajdować się odsyłacze do logowania do usługi PBSBank24.
W przypadku jakichkolwiek podejrzeń, co do autentyczności strony, przed zalogowaniem prosimy o kontakt z infolinią Banku pod numerem 801 372 772 lub +48 13 46 55 750 (koszt połączenia wg taryfy operatora).

13. Dokonuj płatności internetowych tylko z wykorzystaniem „pewnych komputerów”.

Nie loguj się do Usługi PBSbank24, nie dokonuj płatności internetowych z komputerów, co do których nie możesz zweryfikować, czy są wyposażone w system antywirusowy i firewall oraz legalne oprogramowanie, w szczególności z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelniach.

14. Wykonuj okresowe skanowanie komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.

Większość programów antywirusowych przy włączonym monitorze antywirusowym ma wykrywalność (detekcję) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, w których wykrywalność monitora antywirusowego jest niższa aniżeli skanera, powoduje to lukę w systemie bezpieczeństwa.

15. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

16. Ustaw w usłudze PBSBank24 limity jednorazowe, dzienne, miesięczne dla transakcji na rachunku.