Wymagania systemowe

Do prawidłowego działania systemu eBankNet przez Internet wymagana jest przeglądarka internetowa spełniająca następujące wymogi:

- obsługa protokołu szyfrowania TLS w wersji 1.0
- włączona obsługa JavaScript
- kodowanie polskich znaków ustawione na tryb automatyczny lub Latin2 (ISO-8859-2)

Rekomendowane przeglądarki:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera
- Safari

System operacyjny powinien zawierać wszystkie możliwe aktualizacje bezpieczeństwa.

Rekomendowane systemy operacyjne:

- Windows Vista z dodatkiem Service Pack 2
- Windows 7 z dodatkiem Service Pack 1
- Windows 8.x
- OS X 10.8 (i w wersjach wyższych)
- Linux/Android (z zainstalowaną przeglądarką spełniającą wymagania)

Zalecenie zwiększające bezpieczeństwo wykonywanych transakcji

Loguj się wyłącznie na stronie (tutaj adres www ebankneta). Przed zalogowaniem sprawdź, czy połączenie jest szyfrowane (adres strony musi zaczynać się od "https" oraz posiadać widoczny symbol kłódki) Bank nigdy nie przesyła linków do logowania na skrzynkę e-mail oraz nigdy nie prosi o podanie hasła. Takie wiadomości mają na celu wyłudzenie danych, a następnie za ich pomocą przejęcie środków finansowych klienta.

Jeżeli do autoryzacji operacji w serwisie internetowym używasz kodów SMS, sprawdzaj, czy wiadomość SMS z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją. Szczególną uwagę należy zwrócić na kwotę przelewu oraz numer rachunku konta bankowego.

Nigdy nie należy podawać loginu, hasła, kodów jednorazowych na innych stronach internetowych.

System operacyjny, z którego wykonywane są transakcje bankowe, musi być regularnie aktualizowany. Tyczy się to również systemów mobilnych, przeglądarek internetowych oraz klientów pocztowych.

Ważne jest, aby chronić komputer przed szkodliwym oprogramowaniem. W tym celu należy korzystać z programów antywirusowych (z regularnie aktualizowaną bazą wirusów) oraz zapory internetowej (firewall), która kontroluje przesyłanie informacji do i

z internetu. W przypadku korzystania z bankowości mobilnej należy pamiętać o odpowiednim zabezpieczeniu smartphone'a, tabletu itp (aktualizacje systemu operacyjnego, oprogramowanie antywirusowe).

Nie instaluj programów ze źródeł, do których nie masz zaufania i podchodź ostrożnie do programów pobieranych z Internetu.

Nie otwieraj załączników w wiadomościach e-mail od nieznanych nadawców.

Zwróć uwagę podczas instalowania darmowych programów, wiele z nich posiada wbudowane aplikacje adware, które służą do wyświetlania reklam niezależnie od wykonywanych na komputerze czynności. Niektóre z nich wyposażone są również w moduły szpiegujące "spyware".

Dbaj aby przeglądarka, z której korzystasz była zawsze aktualna, wraz z wtyczkami, które są w niej zainstalowane.

Loguj się wyłącznie osobiście, nikomu nie przekazuj danych autoryzacyjnych.

Regularnie zmieniaj hasło w serwisie internetowym. Bezpieczne hasło powinno składać się z wielkich i małych liter, cyfr i znaków specjalnych (np. , #, @, ?, &) i nie powinno być słowem występującym w słowniku, ani hasłem używanym w innych serwisach internetowych. Bank nigdy nie prosi o podanie pełnego hasła do serwisu internetowego, ani żadnych danych pocztą elektroniczną.

Pamiętaj aby po wykonaniu czynności w serwisie internetowym, poprawnie się wylogować. Aby to uczynić należy w następującej kolejności wykonać operacje: kliknąć wyloguj się, a następnie wyłączyć przeglądarkę.

Najpopularniejsze przeglądarki Mozilla Firefox, Chrome, Opera, Internet Explorer, posiadają szereg zabezpieczeń, 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, loginów, haseł, itp

Aby włączyć ochronę anty-phishingową w przeglądarce:

- Chrome Ustawienia ? Pokaż ustawienia zaawansowane ? W sekcji ?Prywatność? zaznacz opcje: ?Włącz ochronę przed wyłudzeniem danych (phishingiem) i złośliwym oprogramowaniem.
- Internet Explorer Narzędzia ->Filtr witryn wyłudzających informacje i wybierz opcję "Włącz automatyczne sprawdzanie sieci Web".
- Firefox Narzędzia -> Opcje -> Bezpieczeństwo i zaznaczyć opcje: Ostrzegaj, jeśli witryny próbują zainstalować dodatki; Blokuj witryny zgłoszone jako stwarzające zagrożenie oraz Blokuj witryny zgłoszone jako próby oszustwa internetowego.
- Opera Narzędzia -> Preferencje -> Zaawansowane - Bezpieczeństwo, a następnie zaznaczyć opcję: "Włącz ochronę przed oszustwami i złośliwym oprogramowaniem".