Bank Spółdzielczy w Otwocku
Grupa BPS

# Zasady bezpiecznego korzystania z systemu bankowości elektronicznej w Banku Spółdzielczym w Otwocku

Bezpieczeństwo wszystkich działań w sieci (nie tylko bezpiecznego korzystania z bankowości elektronicznej) zależy w bardzo dużym stopniu od dbałości o zabezpieczenie własnego komputera. Nasz Bank stosuje profesjonalne metody zabezpieczeń sprzętowych i programowych, jednak o ochronę własnego komputera i systemu operacyjnego każdy użytkownik powinien zadbać sam w myśl zasady: *Bank nie ma dostępu do Twojego komputera - tutaj wszystko zależy od Ciebie!*

System bankowości elektronicznej zapewnia wysoki poziom bezpieczeństwa m.in. dzięki wykorzystaniu szyfrowania protokołem SSL oraz stosowaniu haseł jednorazowych przekazywanych między innymi za pomocą wiadomości SMS lub generowanych przez EBO Token Pro.
Hasło SMS lub kod z EBO Token Pro generowane są automatycznie w momencie zlecania konkretnej operacji i może być użyte tylko do potwierdzenia tej operacji, a nie do innych celów.
Hasła SMS jak również kody EBO Token Pro są bezpieczniejsze i wygodniejsze w porównaniu do haseł jednorazowych zapisanych na karcie.

Hasło aktywacyjne wydawane jest wraz z loginem. Hasło może być użyte tylko jeden raz, podczas pierwszego logowania do systemu i nie może być użyte do innych celów.

Przypominamy jednak, że bezpieczeństwo bankowości elektronicznej zależy także od Klientów i zalecamy, aby każdy zapoznał się z niniejszymi zasadami bezpiecznego korzystania z usług bankowości elektronicznej:


## I LOGOWANIE

Podczas logowania system wymaga wyłącznie identyfikatora użytkownika i ustalonego przez siebie hasła (a przy pierwszym logowaniu hasła aktywacyjnego). Jeżeli widzisz stronę logowania, na której trzeba wpisać hasło jednorazowe, albo stronę, na której trzeba podać kilka haseł jednorazowych jednocześnie, potraktuj to jako próbę oszustwa. Wpisując identyfikator i hasło należy upewnić się, że inne osoby nie mogą ich przechwycić. Nie należy korzystać z usług bankowości elektronicznej na ogólnie dostępnych komputerach, np. w kawiarenkach internetowych.


## II INSTALACJA PROGRAMÓW

**Najprostszym sposobem zainstalowania wrogiego programu w Twoim systemie jest nakłonienie Ciebie, byś sam go zainstalował.**

Podchodź bardzo ostrożnie do programów pobieranych z Internetu.

- nie uruchamiaj programów przesyłanych pocztą elektroniczną,

- nie otwieraj plików z rozszerzeniem exe, których pochodzenia nie znasz. Często programy które mają rozszerzenie exe, mogą w „tle" instalować dodatkowe programy wyłudzające informacje z twojego komputera lub dające pełen dostęp do niego poprzez internet,
- pamiętaj, że korzystanie z oprogramowania P2P (np. Bearshare, KaZaA, eMule, DC++ itp.) związane jest z ryzykiem obniżenia bezpieczeństwa Twojego komputera,

## III CERTYFIKAT oraz EMAIL

Połączenie między Twoją przeglądarką a naszym serwerem jest szyfrowane. O szyfrowaniu połączenia świadczy ikona zamkniętej kłódki na pasku stanu Twojej przeglądarki internetowej.

**Pamiętaj, Bank nigdy nie prosi o podanie poufnych danych poprzez Email, więc nigdy nie odpowiadaj na maile, w których jesteś proszony o podanie poufnych danych takich jak:**

- data urodzenia,
- nazwisko panieńskie matki,
- numer rachunku bankowego,
- identyfikator
- hasła,
- data ważności karty oraz numer kodu CVV.

**Nie otwieraj maili z załącznikiem otrzymanych z nieznanego źródła. Załącznik może zawierać wirusa, który automatycznie zainstaluje się na Twoim komputerze.**

## IV AKTUALIZACJA SYSTEMU

**Uaktualniaj regularnie system zainstalowany na Twoim komputerze**

Powinieneś interesować się uaktualnieniami Twojego systemu, które mają wpływ na jego bezpieczeństwo.

Jeśli używasz systemu Microsoft Windows, powinieneś skorzystać z możliwości **automatycznych aktualizacji** systemu Microsoft Windows.

Dostęp do tej opcji można uzyskać na dwa sposoby:

- Wybierając opcję Windows Update w menu Start twojego systemu Windows.
- Wpisując w przeglądarkę adres: http://windowsupdate.microsoft.com.

Możesz również zapoznać się z **informacjami o bezpieczeństwie** na stronach Microsoft Windows: www.microsoft.com/security/protect/default.asp

Jeżeli korzystasz z innego systemu operacyjnego to sprawdź serwis internetowy producenta tego systemu i jeśli to możliwe, zapisz się na listę mailową z informacjami o jego aktualizacjach.

## V H@SŁA I H@SŁA SMS

Posiadacz rachunku i Użytkownicy zobowiązani są do skutecznego chronienia udostępnionych im środków dostępu do Systemu BS 24h (loginu, haseł, certyfikatu, kodów jednorazowych, nośnika danych itp.) oraz nieujawniania ich osobom trzecim.

Identyfikator Użytkownika może być podany pracownikowi Banku w przypadku, kiedy Użytkownik składa w Banku dyspozycję, reklamację lub inne zgłoszenie.

**Dbaj o bezpieczeństwo Twoich haseł**

- Nigdy nikomu nie ujawniaj swoich haseł,
- Nie wolno przechowywać swoich haseł razem z identyfikatorem. Własne hasło do logowania - podobnie jak numery PIN do kart płatniczych - najlepiej zapamiętać lub zapisać w sposób uniemożliwiający rozpoznanie przez inne osoby.
- Kartę z hasłami jednorazowymi należy przechowywać w bezpiecznym miejscu.
- Hasło należy regularnie zmieniać,
- Nigdy nie zapisuj haseł ani nie przesyłaj ich pocztą elektroniczną,
- Jeśli wydaje Ci się że ktoś mógł poznać twoje hasło - zmień je jak najszybciej,
- Stosuj hasła różne od siebie oraz trudne do odgadnięcia.
- Hasło powinno mieć długość min. 8 max. 20 znaków .
- Ustalając hasło należy używać kombinacji cyfr, małych i wielkich liter.

**PAMIETAJ:** Przed wpisaniem H@sła potwierdzającego każdą operację (np. przelew krajowy) porównuj treść wysłanego SMS z treścią operacji, którą autoryzujesz aby upewnić się, że potwierdzasz odpowiednią operację.

## VI PROGRAM ANTYWIRUSOWY

**Używaj programu antywirusowego**

Niestety czasem może się zdarzyć, że w Twoim systemie pojawi się niebezpieczny dla Ciebie program - wirus albo program pozwalający przejąć zdalnie kontrolę nad Twoim systemem.

Dobre programy antywirusowe, na bieżąco aktualizowane, pomogą Ci zwalczać problemy tego typu a nawet im zapobiegać. Jeśli nawet niebezpieczny program zostanie zainstalowany, to program antywirusowy pomoże Ci się ustrzec przed jego uruchomieniem.

**Nigdy nie wyłączaj programu antywirusowego! Wystarczy kilka sekund na zainstalowanie programów szpiegujących, kiedy program antywirusowy jest wyłączony.**

Przykładowy skaner antywirusowy online:

- Skaner internetowy Mks vir

Przykładowe programy antywirusowe:

- BitDefender
- McAfee
- Norton AntiVirus
- Kaspersky Anti-Virus Personal
- Mks_vir
- Avast

Niektóre z wyżej wymienionych aplikacji są darmowe.

**Używaj własnej ściany ogniowej (personal firewall)**

Personal firewall to program, który ostrzeże Cię, jeśli ktoś będzie próbował połączyć się z Twoim komputerem z zewnątrz. Zostaniesz też ostrzeżony, jeśli jakiś program z Twojego komputera spróbuje wysłać informacje do kogoś z zewnątrz.

Używanie personal firewalla wymaga wyższego stopnia znajomości systemu zainstalowanego na Twoim komputerze aby wiedzieć, którym programom pozwolić na dostęp do sieci, a którym nie. Warto

jednak włożyć w tą naukę trochę wysiłku aby utrudnić atak mający na celu uzyskanie dostępu do Twoich poufnych danych.

Przykładowe programy tego typu:

- Sunbelt Personal Firewall
- Comodo Free Firewall
- Outpost Firewall Pro
- Kerio Winroute Firewall
- ZoneAlarm

Niektóre z wyżej wymienionych aplikacji są darmowe.


## VII ADRES STRONY WWW

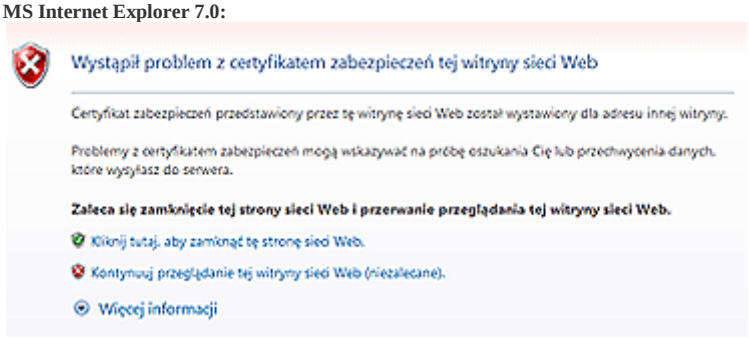
**Obserwuj adres strony, z którą się łączysz.**

Poprawny adres systemu bankowości elektronicznej dla klientów Banku Spółdzielczego w Otwocku rozpoczyna się od: https://ebo.bsotwock.pl

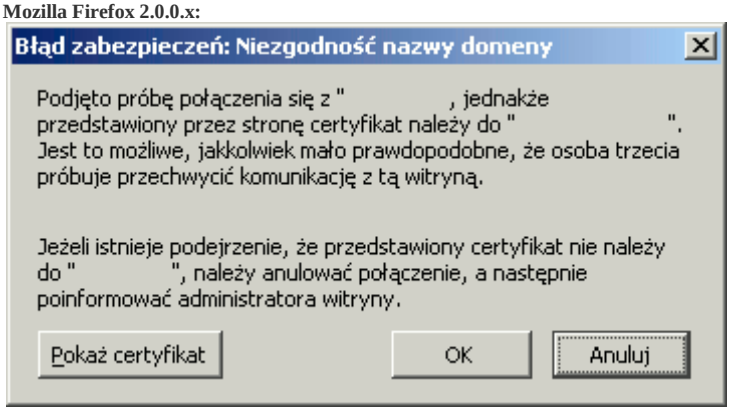
**Jeśli na pasku adresowym przeglądarki widnieje inny adres lub nastąpiło przekierowanie na inny adres to powinieneś nabrać podejrzeń i nie podawać żadnych danych.**

Jeśli ktoś będzie próbował przekierować adres na inny pojawi się następujące ostrzeżenie:

**MS Internet Explorer 7.0:**




**Mozilla Firefox 2.0.0.x:**




Bardzo ważne jest uważne zapoznanie się z informacją i zaakceptowanie certyfikatu tylko z poprawnymi danymi dotyczącymi strony.

Poprzez kliknięcie na przycisk **View Certificate** - **Wyświetl Certyfikat** możesz sprawdzić, dla kogo został on wydany.

## VIII Inne komputery

**Nie należy korzystać z usług bankowości elektronicznej na ogólnie dostępnych komputerach.**

Nie wprowadzaj danych poufnych (identyfikator, hasło) z komputera, do którego dostęp ma wiele osób, w szczególności w kawiarenkach internetowych oraz innych miejscach publicznych. Mogą być na nim zainstalowane programy do przechwytywania danych.


## IX Opcja "Wyloguj"

**Zawsze kończ pracę z systemem poprzez wybranie opcji "Wyloguj"**

Zawsze pamiętaj o tym by kończyć pracę w systemie klikając na przycisk **Wyloguj** z poziomego menu w celu poprawnego zamknięcia sesji. Nie otwieraj kilku okien przeglądarek z aktywnymi sesjami użytkownika w systemie bankowości elektronicznej.

Bank Spółdzielczy w Otwocku nie świadczy usług pomocy zdalnej przy użyciu pulpitu zdalnego lub innego oprogramowania w kontaktach Bank-Klient. Jednocześnie informujemy, że na rynku znane są przypadki zdarzeń których scenariusz jest zbliżony do następującej sytuacji: *Jeśli ktoś, kogo nie znasz, prosi Cię o dostęp do któregokolwiek z Twoich urządzeń i chce, abyś pobrał określone oprogramowanie: Uważaj! Istnieje ryzyko, że możesz stać się ofiarą oszustwa polegającego na uzyskaniu zdalnego dostępu. Zwykle przestępcy dzwonią i zgłaszają wykryty problem z komputerem lub Internetem i oferują pomoc. Prawdopodobnie poinformują, że pracują dla powszechnie znanej firmy, takiej jak Microsoft lub nawet Twój bank. Nigdy nie ufaj rozmówcy, którego telefonu się nie spodziewałeś!*
*Nie ufaj oferowanej "pomocy", o którą nie prosiłeś! Żaden bank ani firma nie poproszą Cię przez telefon o pobranie oprogramowania!*

**Pamiętaj! Jeśli cokolwiek wzbudza Twoje podejrzenia, kiedy korzystasz z usług bankowości elektronicznej, przerwij wykonywanie czynności, o które jesteś proszony i skontaktuj się telefonicznie z najbliższą placówką Banku Spółdzielczego w Otwocku, aktualne dane teleadresowe dostępne na naszej stronie** www.BSotwock.pl.

**#1. Zasada numer jeden**

Nigdy nie dawaj dostępu do swoich urządzeń osobom, których nie znasz.

**#2. Zasada numer dwa**

Nigdy nie udostępniaj nikomu danych logowania do bankowości internetowej ani żadnych haseł.