



## ZASADY BEZPIECZEŃSTWA


systemu bankowości internetowej  
BOŚBank24 Twoje e-Konto

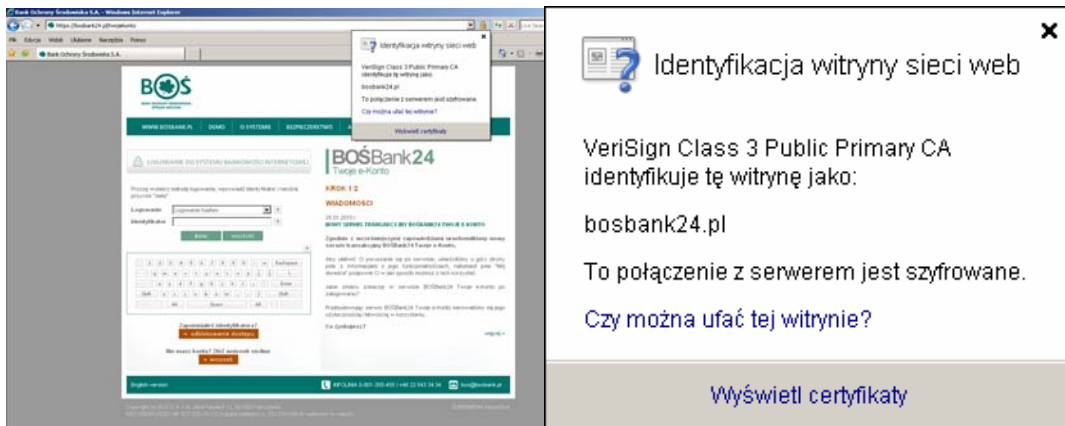
**Spis treści**

<b>1. Podstawowe zasady bezpieczeństwa</b>	<b>3</b>
1) <i>Przed zalogowaniem do BOŚBank24 Twoje e-Konto</i>	3
2) <i>Po zakończeniu pracy w BOŚBank24 Twoje e-Konto</i>	3
<b>2. Przeglądarki internetowe</b>	<b>5</b>
1) <i>Zalecane przeglądarki internetowe</i>	5
2) <i>Internet Explorer</i>	5
3) <i>Mozilla FireFox</i>	5
4) <i>Opera</i>	5
<b>3. Programy i skanery antywirusowe</b>	<b>6</b>
1) <i>Dostępne skanery antywirusowe</i>	6
2) <i>Darmowe programy antywirusowe (freeware)</i>	6
3) <i>Programy antywirusowe udostępniane w wersji testowej (trial)</i>	6
4) <i>Komercyjne pakiety zabezpieczające odpowiedzialne za pełną ochronę komputera</i>	6

## 1. Podstawowe zasady bezpieczeństwa

**BOŚBank24 Twoje e-Konto** – to bardzo bezpieczna usługa dostępu do Twojego konta osobistego przez Internet. Korzystając z systemu internetowego BOŚBank24 Twoje e-Konto zawsze należy pamiętać o zachowaniu podstawowych zasad bezpieczeństwa;

- 1) **Przed zalogowaniem do BOŚBank24 Twoje e-Konto** należy upewnić się, że:
  - ✓ rzeczywiście nastąpiło połączenie ze stroną <https://bosbank24.pl/twojekonto>
  - ✓ połączenie jest szyfrowane **128-bitowym bezpiecznym protokołem SSL**,
  - ✓ certyfikat strony jest prawidłowy, wystawiony dla witryny **bosbank24.pl** przez firmę **VeriSign**. **Certyfikat** można obejrzeć klikając dwukrotnie na **ikonę kłódki** , która symbolizuje szyfrowane połączenie.



**Identyfikacja witryny sieci web**

VeriSign Class 3 Public Primary CA  
identyfikuje tę witrynę jako:  
**bosbank24.pl**

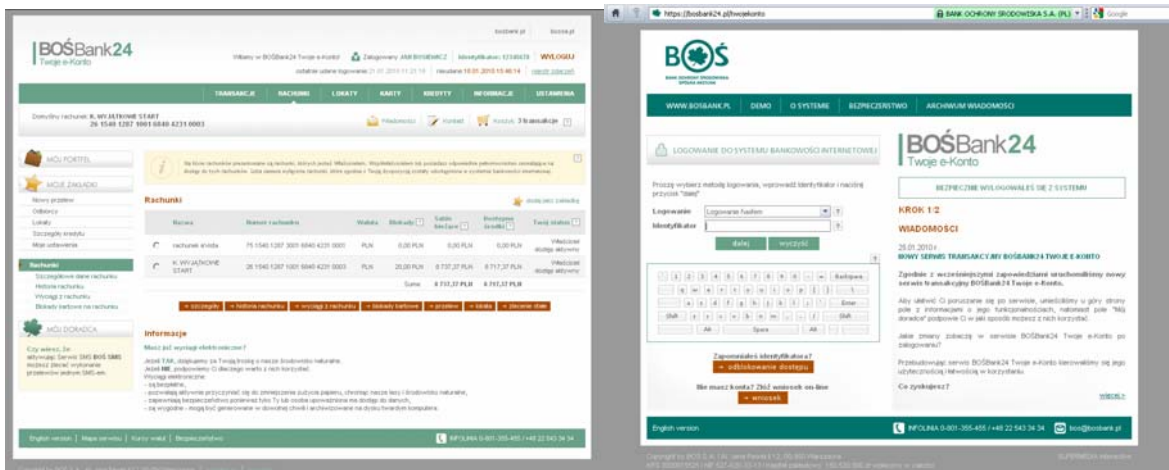
To połączenie z serwerem jest szyfrowane.

Czy można ufać tej witrynie?

[Wyświetl certyfikat](#)

## 2) Po zakończeniu pracy należy:

- ✓ wylogować się używając opcji **Wyloguj**, gwarantuje to poprawne zamknięcie sesji przez użytkownika,
- ✓ zamknąć przeglądarkę internetową.



- 3) **Nie wolno** ujawniać nikomu haseł.
- 4) **Nie wolno** udostępniać nikomu tokena ani karty kryptograficznej.
- 5) Identyfikator można podawać wyłącznie pracownikom BOŚ S.A., jeżeli jest niezbędny do zrealizowania dyspozycji Klienta.
- 6) **Nie wolno** przechowywać haseł, tokena lub karty kryptograficznej razem z identyfikatorem. Hasła - podobnie jak numery PIN do kart płatniczych - najlepiej zapamiętać lub zapisać w sposób uniemożliwiający rozpoznanie przez inne osoby.
- 7) Wpisując identyfikator i hasło należy upewnić się, że nikt ich nie podpatruje. **Nie należy korzystać z usług bankowości internetowej na ogólnie dostępnych komputerach, np. w kawiarenkach internetowych.**
- 8) **Hasła należy regularnie zmieniać.**
- 9) **Każdy internauta musi dbać o bezpieczeństwo swojego komputera. Powinien zawsze mieć zainstalowany program antywirusowy oraz firewall.**
- 10) **Każdy internauta powinien systematycznie sprawdzać oraz instalować dostępne aktualizacje i poprawki dostarczane przez producentów oprogramowania, szczególnie systemu operacyjnego, przeglądarki internetowej, programu antywirusowego.** Użytkownicy korzystający z systemu Microsoft Windows mogą korzystać z automatycznych aktualizacji systemu operacyjnego. Aktualizację wykonujemy, wykorzystując opcję **Windows Update** z menu Start lub ze strony <http://www.update.microsoft.com>
- 11) **Bank nigdy nie wysyła do swoich klientów e-maili z prośbą o podanie poufnych informacji, ani też zawierających linków do stron logowania do systemu transakcyjnego. Nigdy nie odpowiadaj na e-maile, w których jesteś proszony o podanie poufnych danych.** W korespondencji kierowanej do BOŚ S.A. za pomocą poczty elektronicznej nie wolno podawać identyfikatorów ani haseł, numerów kart płatniczych, numerów rachunków bankowych, danych osobowych.
- 12) Bank **nigdy nie pyta** klientów o hasła. Listy, telefony lub formularze, które niespodziewanie pojawiają się w przeglądarce internetowej z pytaniami o hasła, numery kart płatniczych, kody CVV2 lub PIN-y, należy traktować jako próbę wyłudzenia poufnych informacji.
- 13) W przypadku jakichkolwiek pytań czy wątpliwości dotyczących funkcjonowania systemu BOŚBank24 Twoje e-Konto, prosimy o kontakt telefoniczny pod numer: **0-801 355 455** dla krajowych połączeń z telefonów stacjonarnych lub **+48 22 543 34 34** dla połączeń z telefonów komórkowych oraz z zagranicy. Nasi konsultanci są do Państwa dyspozycji w dni powszednie, od poniedziałku do piątku w godzinach 7:45-21:00 oraz w soboty, w godzinach 10:00 - 18:00.

## 2. Przeglądarki internetowe

**BOŚBank24 Twoje e-Konto** – to usługa dostępu do Twojego konta osobistego przez Internet, której prawidłową i bezpieczną pracę zapewnia użycie odpowiedniego oprogramowania skonfigurowanego zgodnie z zaleceniami Banku.

### 1) Zalecane przeglądarki internetowe:

- ✓ Internet Explorer
- ✓ Mozilla Firefox
- ✓ Opera

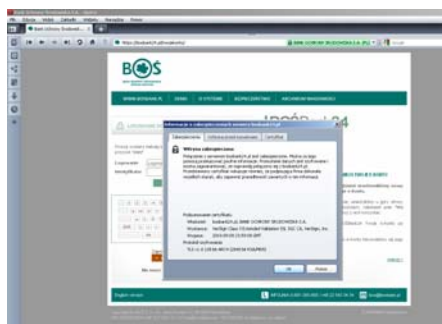
### 2) [Internet Explorer](http://www.microsoft.com/poland/windows/internet-explorer/) <http://www.microsoft.com/poland/windows/internet-explorer/>



### 3) [Mozilla FireFox](http://www.mozilla.com/pl/) <http://www.mozilla.com/pl/>



### 4) [Opera](http://www.opera.com/download/) <http://www.opera.com/download/>



Szczegółowe informacje dotyczące konfiguracji przeglądarek internetowych znajdują się w instrukcji - **Ustawienia przeglądarek internetowych.**

### 3. Programy i skanery antywirusowe

Program antywirusowy chroni komputer przed różnymi odmianami wirusów, makrowirusów, wirusów polimorficznych, robaków, trojanów czy apletów Javy i ActiveX, powinien skanować bieżące operacje, pocztę przychodzącą wraz z załącznikami, oraz posiadać moduł anty spyware.

1) Dostępne skanery antywirusowe online np.:

- **Mks\_Vir**  
<http://www.mks.com.pl/skaner/>
- **Security Check Symantec**  
<http://security.symantec.com/sscv6/default.asp?langid=ie&venid=sym>
- **Active Scan Panda**  
[http://www.pandasoftware.com/activescan/activescan/ascan\\_2.asp](http://www.pandasoftware.com/activescan/activescan/ascan_2.asp)

2) Darmowe programy antywirusowe (freeware), które można zainstalować na swoim komputerze:

- **Avast! Home Edition** - producent ALWIL Software,
- **AVG Anti-Virus Free Edition** – producent Grisoft s.r.o.,
- **Avira AntiVir PersonalEdition Classic** – producent Avira GmbH.

3) Programy antywirusowe udostępniane w wersji testowej (trial):

- **Norton AntiVirus** – producent Symantec Corporation,
- **McAfee VirusScan Home** – producent McAfee, Inc.,
- **mks\_vir** – producent MKS Sp. z o. o.,
- **Kaspersky Anti-Virus** – producent Kaspersky Lab Ltd.,
- **NOD32** - ESET s. r. o.

4) Komercyjne pakiety zabezpieczające w skład których wchodzi szereg aplikacji odpowiedzialnych za pełną ochronę komputera np.: **ArcaVir System Protection, BitDefender Internet Security, CA Internet Security Suite, F-Secure Internet Security, G DATA Internet Security, Kaspersky Internet Security, McAfee Internet Security Suite, Norton Internet Security.**