ZASADY BEZPIECZNEGO KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ

Szanowny Kliencie

aby bezpiecznie korzystać z systemów bankowości internetowej, tj. systemu: eBankNet i eCorpoNet, które umożliwiają nowoczesny, bezpieczny i wygodny dostęp do rachunków i innych produktów Banku Spółdzielczego w Dobczycach zastosuj kilka zasad:

- Do korzystania z systemu konieczny jest komputer podłączony do Internetu, wyposażony w jedną z niżej wymienionych przeglądarek internetowych:
  - Internet Explorer w wersji 11.0 (i wyższych)
  - Mozilla w wersji 1.7 (i wyższych)
  - Mozilla Firefox w wersji 1.0 (i wyższych)
  - Netscape w wersji 6.0 (i wyższych)
  - Opera w wersji 7.0 (i wyższych)
- Przeglądarki muszą mieć **włączone** przyjmowanie plików cookies oraz obsługę javascript.
- W systemach zastosowane zostały najwyższej klasy rozwiązania gwarantujące pełne bezpieczeństwo korzystania z bankowości internetowej, jednak po stronie Użytkownika leży konieczność przestrzegania niżej wymienionych zasad:
- loguj się wyłącznie bezpośrednio ze strony:
  - **usługa eBankNet**: https://e24bsdobczyce.pl,
  - **usługa eCorpoNet**: https://efirma.bsdobczyce.pl
- zanim podasz swoją nazwę **użytkownika i hasło** upewnij się, że w pasku adresu przeglądarki nazwa strony rozpoczyna się od **https**,
- sprawdź, czy na dolnym pasku przeglądarki, na pasku adresu lub obok niego znajduje się ikonka kłódki. Jest to oznaczenie certyfikatu bezpieczeństwa. Po dwukrotnym kliknięciu na kłódkę zostanie wyświetlona informacja, dla kogo certyfikat został wystawiony,
- **https** w adresie oraz **kłódka** są potwierdzeniem, że połączenie z systemem **eBankNet** i **eCorpoNet** jest szyfrowane i zabezpieczone.
- Ze względów bezpieczeństwa po 3 próbach wprowadzenia nieprawidłowego hasła dostęp do systemu zostanie automatycznie zablokowany. W takim przypadku możesz zgłosić dyspozycję odblokowania telefonicznie bądź poprzez zgłoszenie się do placówki banku.

Przypominamy, że bezpieczeństwo bankowości internetowej zależy od Klientów i zalecamy, aby każdy zapoznał się z podstawowymi zasadami bezpiecznego korzystania z usług bankowości internetowej, tzn.:

- **Nie wolno ujawniać nikomu haseł.**
- **Nie wolno odchodzić od komputera podczas zalogowania do systemu.**
- **Po zakończeniu pracy należy wylogować się i zamknąć przeglądarkę.**
- 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.
- Wpisując identyfikator i hasło należy upewnić się, że inne osoby nie mogą ich przechwycić lub podejrzeć.
- Nie należy korzystać z usług bankowości internetowej na ogólnie dostępnych komputerach, np. w kawiarenkach internetowych.
- Nie należy korzystać z usług bankowości internetowej używając nieznanych sieci bezprzewodowych. Nawet szyfrowane sieci bezprzewodowe nie zapewniają poufności przesyłanych informacji.
- Hasło należy regularnie zmieniać.
- Ustalając hasło należy używać kombinacji dopuszczalnych znaków. Należy unikać używania łatwych haseł (jak np. własnego imienia), ale stosować za to hasła trudne do rozszyfrowania (na przykład litery ze słów pochodzących z cytatów z książek lub z wymyślonych zdań).
- Przykład dobrego hasła: iSwz31gtpNR pochodzące ze zdania "Imieniny Sylwestra wypadają zimą 31 grudnia tuż przed Nowym Rokiem".

- Hasło musi mieć długość od 8 do 20 znaków i zawierać co najmniej jedną wielką literę, jedną małą literę, jedną cyfrę.
- W systemie bankowości internetowej jest ustawiony czas automatycznego wylogowania w przypadku braku aktywności, aby zapewnić sobie komfort pracy przy zachowaniu rozsądnego poziomu bezpieczeństwa.
- Jeżeli korzystasz z bankowości internetowej w domu, zadbaj aby Twoje urządzenia służące do połączenia z Internetem były zabezpieczone w odpowiedni sposób (brak dostępu do panelu administracyjnego od strony Internetu, własne, inne nie fabryczne hasło administratora, regularnie uaktualniane oprogramowanie i sterowniki).
- Regularnie instaluj uaktualnienia systemu operacyjnego swojego komputera.
- Używaj oprogramowania antywirusowego ze zaktualizowanymi bazami danych o wirusach i innych zagrożeniach.

Pamiętaj, że:

System eBankNet i eCorpoNet nigdy nie żąda wpisania więcej niż jednego hasła jednorazowego przesłanego za pomocą SMS.

Podczas logowania wpisuje się wyłącznie identyfikator użytkownika i ustalone przez siebie hasło, a w kolejnym kroku uwierzytelnienia podaje się hasło jednorazowe z SMS lub potwierdza logowanie w aplikacji mobilnej.

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. W Internecie krążą maile, w których znajdują się odsyłacze do fałszywych stron bankowości internetowej i prośby o zalogowanie się na takich stronach w celu np. potwierdzenia swoich danych. Bank nigdy nie wysyła tego typu informacji do klientów. Nie próbuj logować się do systemu bankowości internetowej za pomocą odsyłacza przesłanego w takich wiadomościach.

Za pomocą wiadomości SMS wysyłane są tylko hasła jednorazowe służące do potwierdzania operacji zlecanych za pomocą systemu.

Hasło SMS generowane jest automatycznie w momencie zlecania konkretnej operacji i może być użyte tylko do potwierdzenia tej operacji, a nie do innych celów.

Zawsze sprawdzaj, czy informacje otrzymane za pomocą wiadomości SMS lub aplikacji zgadzają się z wykonywaną operacją. W szczególności zwróć uwagę na numery rachunków.

Szanowny Kliencie:

- **Pracownicy banku nigdy nie proszą o podanie hasła do bankowości internetowej.**
- **Pracownicy banku nigdy nie proszą o zestawienie połączenia zdalnego pulpitu ani nie oferują usług pomocy zdalnej.**
- **Chroń swoje hasła!**
- **Nie udostępniaj nikomu haseł jednorazowych.**
- **Nie odpowiadaj na e-maile zachęcające do ujawnienia danych i haseł.**
- **Podawaj hasła wyłącznie, aby autoryzować transakcję.**
- **Nie podawaj haseł na stronie bez certyfikatu.**
- **Zanim podasz hasło - sprawdź certyfikat strony.**
- **Regularnie zmieniaj swoje hasło.**
- **Natychmiast zmień swoje hasło, jeśli zaistnieje podejrzenie, że ktoś mógł je poznać.**
- **Każdorazowo przed podpisaniem oraz wysłaniem przelewu sprawdź poprawność numeru rachunku (tzw. NRB) odbiorcy, unikaj kopiowania numerów NRB.**
- **Unikaj korzystania z bankowości elektronicznej na nieznanych komputerach.**
- **Korzystaj wyłącznie z legalnego i często aktualizowanego oprogramowania antywirusowego, regularnie skanuj swój komputer oraz urządzenia mobilne.**
- **Po zakończeniu pracy w bankowości elektronicznej, nie zostawiaj karty mikroprocesorowej w czytniku podłączonym do komputera.**
- **Kończ pracę w systemie używając opcji Wyloguj - gwarantuje to poprawne zamknięcie sesji przez użytkownika.**