Aktualności

Opublikowano: wtorek, 31, maj 2022 08:00
Odsłony: 7759

Szanowni Państwo,

W trosce o wygodę naszych Klientów oraz dążąc do zapewnienia dostępu do stale rozszerzającej się oferty produktów i usług, **Nadobrzański Bank Spółdzielczy w Rakoniewicach wprowadza nowy system informatyczny**. W ślad za tym zmieni się również System Bankowości Internetowej. Jesteśmy przekonani, że nowe rozwiązanie to jeszcze większa wygoda obsługi, oszczędność czasu i pieniędzy. To co niezmienne – to jak zawsze najwyższy poziom bezpieczeństwa.

W związku z powyższym pragniemy poinformować, że główne prace techniczne w tym zakresie będą prowadzone w dniach od 24.06.2022 r. do 27.06.2022 r., co oznacza że wykonywanie operacji w obecnym systemie będzie możliwe do 24.06.2022 r. do godz. 11:00.

System Bankowości Internetowej w nowej odsłonie będzie dostępny od godz. 8.00 w dniu 27.06.2022 r. (poniedziałek). Od tego momentu będzie również dostępna Aplikacja Mobilna na telefony komórkowe, zarówno z systemem Android jak i iOS.

Hasła do pierwszego logowania otrzymają Państwo wiadomością SMS po udzieleniu odpowiedzi na pytania weryfikujące tożsamość przy logowaniu do Bankowości Internetowej.

Szczegółowe informacje dotyczące logowania oraz korzystania z nowego Systemu Bankowości Internetowej zostaną zamieszczone na naszej stronie internetowej www.nbs-rakoniewice.pl

Dotychczasowy system EBO będzie dostępny jeszcze przez 6 miesięcy, jednak tylko w zakresie wglądu do historii operacji na rachunku. Historia rachunku nie będzie widoczna w nowym systemie, będzie również możliwa do uzyskania w placówkach Banku w formie papierowej.

Zachęcamy Państwa do śledzenia aktualności.

Aktualności

Opublikowano: wtorek, 31, maj 2022 08:00
Odsłony: 7759

W przypadku jakichkolwiek pytań i wątpliwości pozostajemy do Państwa dyspozycji.

Przypominamy też o stosowaniu się do zasad bezpieczeństwa. Logowanie powinno nastąpić dopiero po sprawdzeniu informacji o certyfikacie serwisu bankowości internetowej.

Urządzenie dostępowe i oprogramowanie:

- Nie wolno korzystać z komputerów ogólnie dostępnych (np. w kawiarenkach internetowych).
- Nie wolno korzystać z niezaufanych sieci komputerowych.
- Zawsze używać aktualnego oprogramowania ochrony antywirusowej wraz z zaporą oraz aktualizować na bieżąco system operacyjny.Instalowanie i aktualizacja oprogramowania powinna odbywać się zawsze tylko ze sklepów z aplikacjami i z oficjalnych stron producentów. Prosimy nie pobierać oprogramowania z linków i innych nieznanych źródeł

Logowanie:

- Zachowanie poufności danych do logowania. Identyfikator i hasło logowania przeznaczone są tylko dla jednej osoby. Nie wolno udostępniać identyfikatora i hasła logowania innym osobom. Przekazanie tych danych osobom trzecim naraża na ryzyko utraty pieniędzy zgromadzonych na rachunku.
- Nie należy trzymać hasła logowania wraz z obiektem służącym do autoryzacji (np.: token, karta kryptograficzna) w jednym miejscu.
- Kartę kryptograficzną po dokonaniu autoryzacji operacji należy usunąć z komputera.
- Nie wolno zezwalać przeglądarce na zapisywanie identyfikatora i hasła.
- Należy pamiętać o regularnej zmianie hasła, używając kombinacji dużych i małych liter, cyfr oraz znaku specjalnego.
- Nie wolno logować się za pomocą adresu lub linku przesłanego w wiadomości e- mail - adres strony logowania należy wprowadzać samodzielnie lub korzystając z odpowiedniego linku wyłącznie na stronie banku.

Aktualności

Opublikowano: wtorek, 31, maj 2022 08:00
Odsłony: 7759

- Nie wolno podawać na stronie logowania innych danych niż identyfikator i hasło do logowania (logowanie nigdy nie wymaga podawania hasła jednorazowego, PIN-u karty, numeru telefonu, numeru PESEL, daty urodzenia itp.).
- Nie wolno po zalogowaniu do systemu transakcyjnego odchodzić od komputera, a po zakończeniu pracy należy wylogować się i zamknąć przeglądarkę.
- Przed zalogowaniem należy sprawdzić, czy połączenie z bankiem jest szyfrowane – powinna się pojawić kłódka na pasku przeglądarki.
- Należy sprawdzić prawidłowość certyfikatu.

Autoryzacja operacji:

- W trakcie autoryzacji operacji należy koniecznie:

- dokładnie zapoznać się z treścią przesłanej wiadomości SMS i upewnić się, czy treść wiadomości dotyczy właściwej operacji;

- dokładnie sprawdzić, czy w wiadomości SMS cyfry numeru rachunku, na który jest wysyłany przelew, zgadzają się z tymi, które widoczne są na ekranie komputera.

Wiadomości e-mail i MMS:

- Bank nigdy nie wysyła do klientów pytań dotyczących haseł lub innych poufnych danych.
- Bank nigdy nie wysyła wiadomości z prośbą o aktualizację danych.
- Bank nigdy nie podaje w przesyłanych wiadomościach linków do stron transakcyjnych.
- Wiadomości e-mail oraz MMS nieznanego pochodzenia mogą zawierać załączniki ze złośliwym oprogramowaniem, dlatego nie wolno ich otwierać i klikać na linki zawarte w takich wiadomościach. Linki mogą prowadzić do fałszywej strony, która ma wyłudzić dane do logowania.

Nietypowe zachowanie na stronach zawsze powinno budzić czujność! Na przykład: długie oczekiwanie na zalogowanie, pojawiające się niestandardowo wyglądające pola, pojawiają się dodatkowe pola formularza do wprowadzenia dodatkowych danych, prośba o podanie hasła przy operacjach tego niewymagających.

Aktualności

Opublikowano: wtorek, 31, maj 2022 08:00
Odsłony: 7759