ZASADY BEZPIECZNEGO KORZYSTANIA Z SYSTEMU EBO

1. Bezpieczeństwo transakcji

W celu zachowania bezpieczeństwa środków zdeponowanych na rachunku bankowym należy odpowiednio zabezpieczyć komputer oraz stosować podstawowe zasady bezpieczeństwa.

Przed zalogowaniem do systemu bankowości internetowej i wykonaniem transakcji należy sprawdzić:

1) czy adres strony serwisu transakcyjnego https://online.bsraciborz.pl został wpisany prawidłowo;
2) czy na pasku adresu strony został wyświetlony symbol przedstawiający zamkniętą kłódkę, oznaczający nawiązanie szyfrowanego połączenia z Bankiem;
3) czy strona jest zabezpieczona ważnym certyfikatem wystawionym dla witryny bankowości internetowej (poprawność certyfikatu można sprawdzić klikając w zamkniętą kłódkę widoczną w oknie przeglądarki);
4) czy SMS z kodem dotyczy właściwego przelewu oraz czy numer rachunku odbiorcy i rodzaj operacji wyświetlanej w SMS i na stronie www jest zgodny ze złożoną dyspozycją;
5) czy dane dotyczące certyfikatu są zgodne z poniższymi:
   a) wystawiony dla: Bank Spółdzielczy w Raciborzu, Śląskie PL https://online.bsraciborz.pl
   b) ważny: aktualna data np. od 10.01.2023 do 10.01.2024

2. Zasady bezpiecznego dostępu i wykonywania transakcji:

1) zabezpiecz komputer, smartfon czy tablet aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall);
2) zadbaj o bezpieczne połączenie z Internetem - unikaj łączenia z publicznej sieci WiFi;
3) uważaj na fałszywe certyfikaty bezpieczeństwa np. rozsyłane przy pomocy poczty elektronicznej;
4) korzystaj z aktualnych wersji systemu operacyjnego, oprogramowania antywirusowego i przeglądarki internetowej;
5) chroń system pocztowy przed spamem. Wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą do systemu pocztowego trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych;
6) nie loguj się do systemu bankowości internetowej korzystając z odnośników otrzymanych pocztą elektroniczną lub znajdujących się na stronach nienależących do Banku;
7) unikaj logowania z komputerów, do których dostęp mają również inne osoby;
8) wpisuj ręcznie dane do zlecenia przelewu np. numery rachunków – unikaj wprowadzenia numerów rachunków stosując metodę kopiuj/wklej;
9) nie instaluj oprogramowania pochodzącego z nieznanych źródeł na komputerze, na którym korzysta się z bankowości internetowej;
10) wyloguj się po zakończonej pracy w systemie bankowości internetowej;
11) śledź na bieżąco informacje zamieszczone na stronie Banku dotyczące zagrożeń w bankowości internetowej, a w razie wątpliwości dotyczących bezpieczeństwa transakcji niezwłocznie skontaktuj się z Bankiem.

PAMIĘTAJ, ŻE BANK NIGDY NIE PROSI O:

1) instalację certyfikatów na komputerach i telefonach komórkowych;
2) podanie danych kart płatniczych i kredytowych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model);
3) udział w testowaniu nowych funkcjonalności serwisu transakcyjnego;
4) wykonanie przelewów testowych ani zwrotu środków na rachunku innych Klientów.

Aktualne ostrzeżenia, komunikaty i poradniki dla Klientów Banku znajdują się na stronie:

1) Związku Banków Polskich,
2) Urzędu Komisji Nadzoru Finansowego.