

BEZPIECZEŃSTWO BANKOWOŚCI INTERNETOWEJ

Mając na uwadze należyłą ochronę środków zgromadzonych na rachunkach przypominamy o konieczności zachowania szczególnej ostrożności podczas korzystania z bankowości internetowej:

- nie należy wchodzić na stronę logowania do systemu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do Banku;
- nie należy odpowiadać na żadne e-maile dotyczące weryfikacji Twoich danych (np. identyfikatora, hasła) lub innych ważnych informacji – Bank nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej;
- zawsze przed logowaniem należy sprawdzić, czy adres strony Banku rozpoczyna się od <https://>;
- należy zawsze przed logowaniem zweryfikować Certyfikat Bezpieczeństwa Banku (m.in. dla kogo został wystawiony oraz czy jest ważny), którego szczegóły są dostępne poprzez kliknięcie na symbol kłódki w oknie przeglądarki;
- przed potwierdzeniem operacji należy uważnie przeczytać SMS z kodem, aby upewnić się, że dotyczy on właściwego przelewu oraz czy numer rachunku, na który wysłane są środki jest zgodny ze zleceniem klienta;
- należy unikać przeklejanania numerów rachunków (to jest używania funkcji: kopiuj / wklej, ctrl+c / ctrl+v, ctrl+insert / shift+insert), zalecane jest ich ręczne wpisywanie do zleceń w systemie bankowości internetowej albo o uważną kontrolę wklejanego numeru rachunku i porównanie tego numeru z oryginalnym, kopiowanym numerem rachunku;
- nie należy przysyłać e-mailem żadnych danych osobistych typu hasła, numery kart kredytowych, numery kart debetowych, itp.;
- nie należy przechowywać nazwy użytkownika i haseł w tym samym miejscu oraz nie należy udostępniać ich innym osobom;
- należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach, u znajomych);
- należy na bieżąco aktualizować system operacyjny (np. Windows) oraz szczególnie narażone na ataki hakerskie oprogramowanie, takie jak: przeglądarki internetowe, java, flashplayer oraz oprogramowanie do obsługi plików pdf;
- należy zawsze stosować oprogramowanie antywirusowe oraz zapory (firewall) i dbać o ich bieżącą aktualizację;
- nie należy instalować albo uruchamiać oprogramowania pochodzącego z niepewnych źródeł oraz stron internetowych, instalując jakiegokolwiek oprogramowanie na komputerze należy zachować szczególną ostrożność;
- należy zawsze kończyć pracę korzystając z polecenia – Wyloguj;
- w przypadku wątpliwości co do prawidłowego działania bankowości internetowej, należy niezwłocznie skontaktować się z Bankiem.

Bank Spółdzielczy w Jaworze
ul. Wrocławska 2, 59-400 Jawor
tel. (76) 870-28-34 fax. (76) 871-18-12
e-mail : sekretariat.bsjawor@bankbps.pl
www.bs-jawor.pl