Bank Spółdzielczy w Wilamowicach
Grupa BPS

ZASADY BEZPIECZNEGO KORZYSTANIA Z BANKOWOŚCI INTERNETOWEJ

Mając na uwadze należytą ochronę środków zgromadzonych na rachunkach zalecane jest zachowanie 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 logowanie **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 wprowadzeniem operacji **należy uważnie przeczytać SMS** z kodem, aby upewnić się, że dotyczy on właściwego przelewu oraz czy numer rachunku na który wysyłane są środki jest zgodny z wprowadzonym zleceniem,
- **Należy unikać** przeklejania numerów rachunków (to jest używania funkcji: kopiuj / wklej, ctr+c / ctrl+v, ctrl+insert / szhift+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** przesyłać mailem żadnych danych osobistych typu hasła, numery kart kredytowych 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 unikać** logowania do Bankowości Internetowej podczas połączenia z niezabezpieczonymi sieciami bezprzewodowymi WiFi lub otwartymi Hotspotami,
- **Należy** na bieżąco aktualizować system operacyjny (Windows) oraz szczególnie narażone na ataki hakerskie oprogramowania, takie jak: przeglądarki internetowe, java, flash player oraz oprogramowanie do obsługi plików pdf,
- **Należy zawsze** stosować oprogramowanie antywirusowe oraz zapory (firewall) i dbać o ich bieżącą aktualizację,
- Instalując jakiekolwiek oprogramowanie na komputerze **należy zachować szczególną ostrożność**, a w szczególności **nie należy instalować albo uruchamiać** oprogramowania pochodzącego z niepewnych źródeł oraz stron internetowych,
- **Należy zawsze** kończyć pracę korzystając z polecenia – Wyloguj,
- W przypadku wątpliwości co do prawidłowego działania Bankowości Internetowej, **należy niezwłocznie skontaktować się z Bankiem**.