

Kraków, 04.07.2016r.

Szanowni Państwo,

W celu wyeliminowania zagrożeń i zwiększenia bezpieczeństwa w zakresie bankowości internetowej przypominam o konieczności zachowania szczególnej ostrożności podczas korzystania z bankowości internetowej naszego Banku:

- Nie należy wchodzić na stronę logowania do systemu korzystając z linków (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;
- Bank nigdy nie prosi użytkownika o podanie hasła jednorazowego podczas logowania do bankowości internetowej, ani bezpośrednio po zalogowaniu do niej, do uwierzytelniania, identyfikacji, potwierdzenia adresu IP dla komputera, danych karty płatniczej, takich jak: numer karty, data ważności i kod CVV, podczas korzystania z serwisu internetowego;
- Przed potwierdzeniem operacji należy przeczytać SMS z kodem, aby upewnić się, że dotyczy on właściwego przelewu oraz czy numer rachunku, na który wysyłane są środki jest zgodny z Państwa zleceniem;
- Należy unikać przeklepania numerów rachunków (tj. używania funkcji: kopiuj/wklej, ctr+c/ctr+v, ctr+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 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 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 jakiegokolwiek oprogramowanie na komputerze należy zachować szczególną ostrożność, a w szczególności nie instalować albo nie uruchamiać oprogramowania pochodzącego z niepewnych źródeł oraz stron internetowych;
- Należy zawsze kończyć pracę korzystając z polecenia „Wyloguj”;
- Jeżeli wygląd strony do logowania wzbudzi Twoje zaniepokojenie, zanim się zalogujesz, skontaktuj się z Bankiem; *(pod numerem tel. +48 12 430 05 34)*
- W przypadku wątpliwości co do prawidłowego działania bankowości internetowej należy niezwłocznie skontaktować się z Bankiem.

W celu zwiększenia Państwa bezpieczeństwa zachęcamy do zmiany sposobu autoryzacji na hasła jednorazowe SMS, gdzie dodatkowo weryfikujecie Państwo operację, która właśnie jest autoryzowana (rodzaj operacji, kwota transakcji, numer rachunku odbiorcy).

Z wyrazami szacunku

*Wioletta Zacharz
Dyrektor Biura Produktów i Procedur Depozytowych
oraz Pozostałych Usług
Bank Spółdzielczy Rzemiosła w Krakowie*