Bank Spółdzielczy w Bieczu
Siedziba – Biecz Rynek 15
Sąd Rejonowy dla Krakowa Śródmieścia w Krakowie Wydział XII Gospodarczy KRS
Nr KRS 0000124228, NIP 685-00-07-150

Zmiana sposobu logowania się do bankowości elektronicznej.

Mając na uwadze należytą ochronę środków zgromadzonych na rachunkach oraz promując zasady bezpiecznego korzystania z bankowości internetowej Bank Spółdzielczy w Bieczu wprowadza **zmianę sposobu logowania się do systemu Centrum Usług Internetowych.**

Dotychczasowy sposób logowania się przy wykorzystaniu hasła i tokena zostanie zastąpiony tzw**. hasłem maskowanym**, które polega na wpisaniu w odpowiednie pola tylko kilku losowo wybranych przez system znaków (a nie całego hasła).

Zapraszamy Państwa do naszych placówek w celu bezpłatnej zmiany sposobu logowania się do bankowości elektronicznej.

Ponadto informujemy, że bank umożliwia korzystanie z dodatkowych zabezpieczeń:
1. Usługi SMS powiadamiającej o zalogowaniu się do bankowości elektronicznej lub potwierdzającej realizację przelewu.
2. Usługi SMS blokującej token, polegającej na wysłaniu na nr 535 933 000 wiadomości SMS o treści: blokuj.*numer identyfikatora*. System automatycznie blokuje dostęp do rachunku(ów) powiązanych z numerem identyfikatora podanym w wiadomości SMS oraz w odpowiedzi zwrotnej przesyła klientowi komunikat SMS o treści: „Bank Spółdzielczy w Bieczu: Dostęp został wyłączony dla ID *numer identyfikatora”.* W celu odblokowania dostępu do usługi płatności internetowych klient kontaktuje się z bankiem:
- telefonicznie, podając ustalone wcześniej unikalne hasło do komunikacji w zakresie usługi CUI,
- osobiście w placówce banku.
3. Ograniczenie adresów IP, z których można się logować.

Przypominamy jednocześnie, że:
1. Bank nigdy nie zwraca się o podanie danych poufnych za pomocą poczty elektronicznej – zatem nie należy odpowiadać na żadne e-maile dotyczące weryfikacji Państwa danych (np. identyfikatora czy hasła)

2. Nie należy wchodzić na stronę logowania do systemu korzystając z odnośników otrzymanych pocztą e-mail lub znajdujących się na stronach nie należących do banku.

3. 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.

4. Zawsze należy stosować oprogramowanie antywirusowe oraz zapory (firewall) i na bieżąco je aktualizować.

5. Nie należy przechowywać nazwy użytkownika i haseł w tym samym miejscu oraz nie należy udostępniać ich innym osobom.

6. Należy zawsze przed logowaniem zweryfikować Certyfikat Bezpieczeństwa Banku (m.in. dla kogo został wystawiony oraz czy jest ważny), którego szczegóły są dostępne po kliknięciu na symbol kłódki w oknie przeglądarki.

7. Przed potwierdzeniem 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 ze zleceniem klienta.