

Broszura edukacyjna Międzypowiatowego Banku Spółdzielczego w Myszkowie dotycząca bezpiecznego korzystania z bankowości internetowej



BEZPIECZEŃSTWO W BANKOWOŚCI INTERNETOWEJ:

Mając na uwadze bezpieczeństwo środków zgromadzonych na rachunkach, Międzypowiatowy Bank Spółdzielczy w Myszkowie przedstawia poradnik zawierający podstawowe informacje i zasady, o których warto pamiętać korzystając z bankowości internetowej.



Grupa BPS
**MIEDZYPOWIATOWY
BANK SPÓŁDZIELCZY
W MYSZKOWIE**

Twój Bankiem!



Przed zalogowaniem do Systemu eBankNet lub eCorpoNet i wykonaniem transakcji:

- ✓ sprawdź, czy adres strony serwisu transakcyjnego został wpisany prawidłowo tj. <https://ebank.bsmyszkow.pl/> lub <https://ecorpo.bsmyszkow.pl/>,
- ✓ sprawdź, czy na pasku adresu strony została wyświetlona zamknięta kłódka, oznaczająca nawiązanie szyfrowanego połączenia z Bankiem,
- ✓ sprawdź, czy strona Systemu eBankNet lub eCorpoNet jest zabezpieczona ważnym certyfikatem wystawionym dla witryn ebank.bsmyszkow.pl lub ecorpo.bsmyszkow.pl, zweryfikowany przez Unizeto Technologies S.A. (poprawność certyfikatu sprawdzisz klikając w zamkniętą kłódkę widoczną w oknie przeglądarki),
- ✓ sprawdź, czy SMS z kodem dotyczy właściwego przelewu oraz czy numer rachunku odbiorcy i rodzaj operacji wyświetlanej w wiadomości SMS i na stronie www jest zgodny z Twoją dyspozycją,
- ✓ w razie wątpliwości sprawdź, czy dane dotyczące certyfikatu są zgodne z poniższymi:

	System eBankNet	System eCorpoNet
wystawiony dla	bsmyszkow.pl	
wystawiony przez	Unizeto Technologies S.A.	
ważny od - do	29-08-2024 - 29-08-2025	
Odcisk cyfrowy (SHA-256)	51c32f4eee008da39258d496484f6e956ef1bb8a62d385181b7cdb5bec899afa	

[Techniczne wsparcie dla Klientów bankowości internetowej](#)
tel. 34/ 313 78 12 w godzinach pracy Banku (opłata zgodna z taryfą operatora)

Jak zablokować dostęp do bankowości internetowej:

1) w godzinach pracy Banku:

- samodzielnie poprzez kliknięcie w kafelek pn. „Zablokuj dostęp” na stronie przed logowaniem do Systemu eBankNet,
- samodzielnie poprzez 3-krotne wpisanie błędnego hasła,
- telefonicznie, pod numerem telefonu 34/ 313 78 12,
- osobiście w Banku.

2) po godzinach pracy Banku i w dni wolne od pracy Banku:

- telefonicznie, pod numerem telefonu 34/ 313 78 02,
- samodzielnie poprzez kliknięcie w kafelek pn. „Zablokuj dostęp” na stronie przed logowaniem do Systemu eBankNet,
- samodzielnie poprzez 3-krotne wpisanie błędnego hasła.



Zasady bezpiecznego dostępu i wykonywania transakcji:

- połączenie z Internetem musi być bezpieczne (unikaj łączenia się z publicznej sieci WiFi)
- trzeba uważać na fałszywe certyfikaty bezpieczeństwa np. rozsyłane przy pomocy poczty elektronicznej
- należy zawsze korzystać z aktualnych wersji systemu operacyjnego, oprogramowania antywirusowego i przeglądarki internetowej
- system pocztowy powinien być chroniony przed przychodzącym spamem. Wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą trafić wirusy i informacją których celem jest wyłudzenie poufnych danych
- nie należy logować się do systemu eBankNet lub eCorpoNet korzystając z adreśników otrzymanych pocztą elektroniczną lub znajdujących się na stronach nienależących do Banku
- należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach lub u znajomych)
- zalecane jest ręczne wpisywanie danych do zlecenia przelewu np. numerów rachunków, należy unikać wprowadzania numerów rachunków stosowania metody kopiuj/wklej
- nie należy instalować oprogramowania pochodzącego z nieznanego źródła na komputerze, na którym korzysta się z bankowości internetowej
- należy zawsze kończyć pracę z systemem bankowości internetowej korzystając z polecenia - wyloguj
- w przypadku wątpliwości co do prawidłowego działania bankowości internetowej lub stwierdzenia utraty środków należy niezwłocznie skontaktować się z Bankiem 34 313 78 00, 34 313 78 12



PAMIĘTAJ, ŻE BANK NIGDY NIE PROSI O:

- ✓ instalację certyfikatów na komputerze i telefonie komórkowym
- ✓ podanie danych kart płatniczych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model)
- ✓ udział w testowaniu nowych funkcjonalności serwisu transakcyjnego
- ✓ wykonywanie przelewów testowych ani zwrot środków na rachunki innych Klientów



Przypominamy, że bezpieczeństwo transakcji realizowanych w serwisach bankowości internetowej zależy również od Ciebie oraz od zabezpieczeń urządzeń, za pomocą których łączysz się z Bankiem. W przypadku wątpliwości dotyczących bezpieczeństwa transakcji poprzez system eBankNet lub eCorpoNet powinieliście niezwłocznie skontaktować się z informatykiem Międzypowiatowego Banku Spółdzielczego w Myszkowie pod numerem telefonu 34 313 78 12.



Dlaczego zabezpieczenia są tak ważne?

Poziom bezpieczeństwa komunikacji pomiędzy witryną internetową, a jej Klientem zależy od poziomu bezpieczeństwa każdego z elementów uczestniczących w tej komunikacji. Zabezpieczenia po stronie Banku spełniają wysokie standardy i są cyklicznie testowane i audytowane. Dlatego działania cyberprzestępców ukierunkowane są na zabezpieczenia po stronie Klienta.

Bezpieczeństwo korzystania z serwisu bankowości internetowej zależy również od jego użytkowników, w tym także świadomości z obszaru zabezpieczeń własnego komputera. Niezabezpieczony komputer jest narażony na ataki z użyciem złośliwego oprogramowania, a nawet całkowite przejęcie nad nim kontroli. W takiej sytuacji cyberprzestępca, mając do dyspozycji wykradzione dane uwierzytelniające (login, hasło, hasło SMS potwierdzające transakcje) będzie usiłował zrealizować utworzony przez siebie przelew.

W celu zachowania bezpieczeństwa środków zdeponowanych na rachunku bankowym staraj się odpowiednio zabezpieczyć komputer oraz stosuj podstawowe zasady bezpieczeństwa. Śledź na bieżąco informacje zamieszczone na stronie Banku w zakładce „CyberBezpieczeństwo” dotyczące nowych zagrożeń w bankowości internetowej.

Aktualne ostrzeżenia, komunikaty i poradniki dla Klientów banków publikuje również Związek Banków Polskich na stronach internetowych: <http://zbp.pl/dla-klientow>.