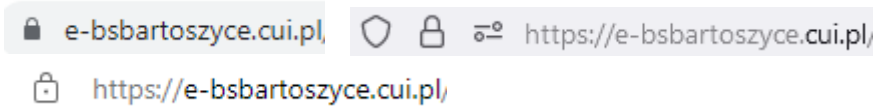
BS w Bartoszycach

Grupa BPS

Zasady bezpiecznego korzystania z bankowości elektronicznej

1. Zawsze sprawdzaj na stronie logowania bankowości elektronicznej aktualne zasady bezpiecznego korzystania z bankowości elektronicznej.
2. Szczegółowe informacje o zagrożeniach dla użytkowników bankowości elektronicznej należy weryfikować na stronie Związku Banków Polskich: http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci (link znajduje się na stronie logowania bankowości elektronicznej).
3. Jeśli otrzymasz komunikat o przerwie konserwacyjnej podczas logowania lub realizacji przelewu, koniecznie zrezygnuj z dalszej pracy w bankowości elektronicznej i skontaktuj się z Bankiem.
4. Zabezpiecz komputer aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall).
5. Regularnie aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej.
6. Uważaj na nietypowe informacje z banku, nie wykonuj podejrzanych poleceń, a w szczególności nie instaluj oprogramowania z niezaufanego źródła, zarówno na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej, jak i w telefonie komórkowym.
7. Po zakończeniu pracy w bankowości elektronicznej wyloguj się używając przeznaczonej do tego opcji w aplikacji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
8. Nie instaluj oprogramowania, jeżeli instrukcja instalacji zawiera zalecenie rezygnacji ze skanowania aplikacji oprogramowaniem antywirusowym.
9. Chroń dane dostępowe do bankowości elektronicznej.
10. Nie loguj się i nie dokonuj płatności w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach.
11. Zweryfikuj czy certyfikat strony wystawiony jest dla ***e-bsbartoszyce.cui.pl*** - Bank Spółdzielczy w Bartoszycach (zweryfikowany przez *Unizeto Technologies S.A.*), poprzez kliknięcie na "zatrzaśniętą kłódkę" w pasku przeglądarki, np.



12. Sprawdź poprawność numeru NRB przed i po podpisie przelewu.
13. Zwróć szczególną uwagę na poprawność numeru NRB po wklejeniu go ze schowka systemu. Najlepiej zrezygnuj z kopiowania NRB.
14. Nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie.
15. Bank nigdy nie sugeruje pomocy zdalnej z wykorzystaniem usług pulpitu zdalnego.

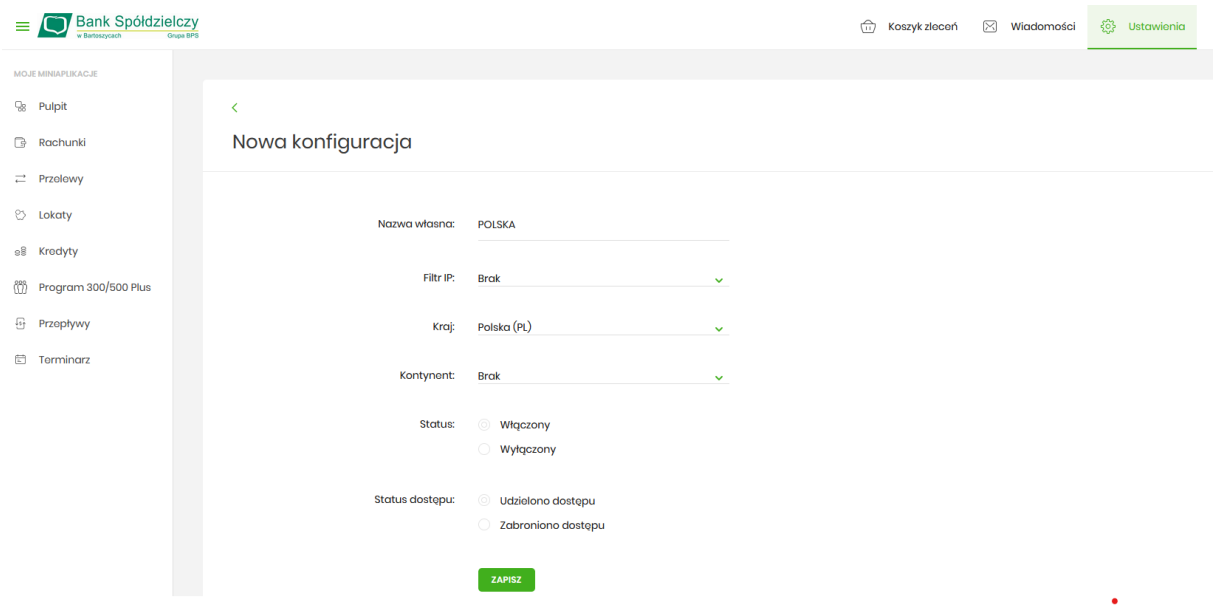
Bankowość korporacyjna - funkcjonalności podnoszące odporność systemu przed zaniedbaniami użytkownika

1. Filtrowanie adresów IP

Funkcjonalność wymaga konfiguracji przez użytkownika.

W bankowości internetowej dostępne jest bardzo skuteczne narzędzie dające możliwość określenia, z jakiego adresu internetowego (IP) dozwolone jest logowanie. Funkcjonalność tą przystosowaliśmy również do tzw. dynamicznych IP poprzez możliwość definiowania klasy adresowej np. dostawcy Internetu, lub na poziomie kraju czy kontynentu.

Filtry IP są definiowane w opcji: Ustawienia -> Filtrowanie adresów IP



Własny adres IP można zweryfikować w opcji: Ustawienia - Historia logowań

W przypadku Klientów posiadających tzw. dynamiczne IP należy na podstawie historii logowań lub po kontakcie z dostawcą Internetu ustalić odpowiednią maskę dla filtru IP.

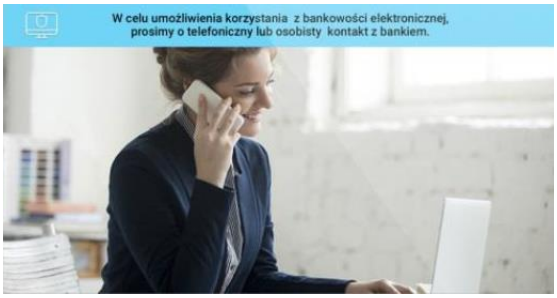
2. IP Intelligence

Dbając o bezpieczeństwo bankowości internetowej Bank Spółdzielczy w Bartoszycach wykorzystuje usługę **IP Intelligence**, weryfikującą reputację zewnętrznego adresu IP, z którego korzysta stacja komputerowa Klienta łącząca się do Internetu.

Swój zewnętrzny adres IP przydzielony przez operatora można sprawdzić pod adresem https://www.moje-ip.eu, a jego reputację w usłudze *IP Intelligence* w ogólnodostępnej bazie adresów IP znajdującej się na stronie https://www.brightcloud.com/tools/url-ip-lookup.php.

W przypadku negatywnej weryfikacji tego adresu usługa logowania do bankowości internetowej jest niemożliwa, wyświetlony zostaje komunikat:

"*W celu umożliwienia korzystania z bankowości elektronicznej, prosimy o telefoniczny lub osobisty kontakt z bankiem*".



W takim wypadku należy skontaktować się z dostawcą usługi dostępu do sieci Internet w celu złożenia wniosku o zmianę reputacji zewnętrznego adresu IP, lub udać się do najbliższego oddziału Banku.

3. Autoryzacja dodawania/edycji szablonów/kontrahentów

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Funkcjonalność zabezpiecza przed nieuprawnioną modyfikacją szablonów przelewów oraz kontrahentów. Ingerencja w listę zdefiniowanych szablonów/kontrahentów możliwa jest jedynie po dodatkowej autoryzacji.

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 są ukierunkowane 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, PIN) 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 zamieszczane na stronie Banku 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-konsumentow

Pamiętaj, że Bank nigdy nie prosi o:

- ✓ Instalację certyfikatów na komputerach i telefonach komórkowych
- ✓ podanie danych kart płatniczych i kredytowych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model)
- ✓ udział w testowaniu nowych funkcjonalności serwisu transakcyjnego
- ✓ wykonanie przelewów testowych ani zwrot środków na rachunki innych klientów

Zachowania użytkownika, a ryzyko wykonywania operacji finansowych przez Internet.

Bankowość elektroniczna jest wygodną i bezpieczną formą korzystania z usług bankowych, w tym składania zleceń finansowych. W ostatnim czasie nasiliły się ataki na Klientów bankowości elektronicznej. Przestępcy nie mogąc złamać zabezpieczeń infrastruktury dostawców bankowości elektronicznej (Banków, dostawców technologii i usług), skupili się na łamaniu zabezpieczeń infrastruktury Klientów i bazowaniu na wzorcach ich zachowań. W czasach globalizacji, szalonego rozwoju usług mobilnych, coraz wyższych wymagań użytkowników co do ergonomii łatwo zapomnieć użytkownikowi o przestrzeganiu podstawowych zasad bezpieczeństwa, co przestępcy, stosując coraz bardziej wyrafinowane metody ataku, mogą wykorzystać.

Szanowny użytkowniku, bezwzględnie stosuj się do zasad bezpieczeństwa jakie publikuje Bank, w przeciwnym razie, Twoja twierdza, jaką jest bankowość elektroniczna, ma zostawione otwarte wrota.

Bank ze swojej strony dokłada starań aby nieustannie rozwijać technologie i usługi, które będą wspierać użytkownika w wygodnym i bezpiecznym korzystaniu z bankowości elektronicznej.