



W trosce o bezpieczeństwo transakcji internetowych Bank Spółdzielczy Grodków-Łosiów przygotował dla Państwa poradnik zawierający rady i zalecenia, o których warto pamiętać korzystając z bankowości internetowej.



Grupa BPS

Banki Spółdzielcze i Bank BPS



Przed zalogowaniem do serwisu i wykonaniem transakcji:

- Sprawdź czy adres strony to:
<https://ebank.bsgradkow.pl>
lub <https://mobanknet.bsgradkow.pl>.
- Sprawdź, czy na pasku adresu strony została wyświetlona zamknięta kłódka, oznaczająca nawiązanie szyfrowanego połączenia z Bankiem.
- Sprawdź, czy strony serwisu **ebank.bsgradkow.pl** lub **mobanknet.bsgradkow.pl** są zabezpieczone ważnym certyfikatem wystawionym dla witryn ***.bsgradkow.pl** których właścicielem jest Bank Spółdzielczy Grodków-Łosiów., Zweryfikowany przez **Certum Trusted Network**. (Poprawność certyfikatu sprawdzisz klikając w zamkniętą kłódkę widoczną w oknie przeglądarki).
- W razie wątpliwości sprawdź, czy dane dotyczące certyfikatu są zgodne z poniższymi:

wystawiony dla:

***.bsgradkow.pl** przez **Certum Organization**

Validation: CA SHA2

Ważny od: 2015-09-03 do 2018-09-02

Właściciel: Bank Spółdzielczy Grodków-Łosiów.

Odcisk palca **0c d4 d3 c8 0c 14 96 16a4 e8 98 48 90 70**

81 44 20 54 38 74

- 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 – nigdy ich nie instalować!
- Należy zawsze korzystać z aktualnych wersji systemu operacyjnego, oprogramowania Antywirusowego i przeglądarki internetowej. Nie należy instalować oprogramowania pochodzącego z nieznanego źródła na komputerze, na którym korzysta się z bankowości internetowej.
- System pocztowy powinien być chroniony przed przychodzącym spamem. Wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą do systemu pocztowego trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych.
- Należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach lub u znajomych).
- W przypadku posługiwania się smartfonem lub tabletem należy ustawić blokadę ekranu.



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



Grupa BPS
Banki Spółdzielcze i Bank BPS



Zasady bezpiecznego wykonywania transakcji internetowych:

- Zalecane jest **ręczne wpisywanie danych do zlecenia przelewu** np. numerów rachunków, należy unikać wprowadzania numerów rachunków stosowania metody kopiuj/wklej.
- Należy zawsze kończyć pracę z systemem bankowości internetowej na komputerze korzystając z polecenia – **wyloguj**.
- Bardzo ważnym elementem zabezpieczeń jest informacja o błędnej próbie logowania, oraz o samym zalogowaniu się na konto bankowości internetowej przesyłana poprzez sms na **telefon komórkowy zdefiniowany w Banku**.
- Sprawdź, czy SMS z kodem dotyczy **właściwego przelewu** oraz czy numer rachunku odbiorcy i rodzaj operacji wyświetlanej w SMS i na stronie www jest zgodny z Twoją dyspozycją.

Zasady bezpiecznego posługiwania się kartą płatniczą:

- Zalecane jest uruchomienie usługi SMS bankingu i wybranie opcji powiadomienia o blokadach, będziemy wiedzieć o każdej transakcji kartą niezależnie o typu operacji – może się zdarzyć, że nie będziemy wiedzieć, że karta została skradziona i ktoś inny ją wykorzystuje!
- Numer **CVV/CVC**, który jest na odwrocie karty jest naszym „**pinem**” do transakcji internetowych, należy go przepisać i przechowywać w bezpiecznym miejscu a na **karcie zamazać lub zakleić!**
- W przypadku nie korzystania z płatności internetowych należy limit transakcji wyzerować.
- W przypadku **kart zbliżeniowych** należy przechowywać je w specjalnym futerale odpornym na podsłuch np. **Safe Pocket**.



Przypominamy, że bezpieczeństwo transakcji realizowanych w serwisach bankowości internetowej zależy również od Ciebie oraz od zabezpieczeń urządzeń, za pomocą których łączysz się z Bankiem.



Grupa BPS
Banki Spółdzielcze i Bank BPS



Dlaczego zabezpieczenia są takie 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, SMS potwierdzający transakcję jeśli podamy go fałszywej stronie i nie zweryfikujemy numeru konta**) 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 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>