# Bezpieczeństwo w bankowości internetowej

Mając na uwadze bezpieczeństwo środków zgromadzonych na rachunkach Bank Spółdzielczy w Gostyninie przedstawia poradnik zawierający podstawowe informacje i zasady 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 serwisu transakcyjnego został wpisany prawidłowo: https://e24.bsgostynin.pl lub https://www.e24.bsgostynin.pl

- sprawdź, czy na pasku adresu została wyświetlona zamknięta kłódka oznaczająca szyfrowane połączenie z Bankiem (nowoczesne przeglądarki internetowe sygnalizują certyfikaty SSL rozszerzonej walidacji zmianą koloru paska adresu na zielony

- sprawdź czy strona serwisu e24.bsgostynin.pl jest zabezpieczona ważnym certyfikatem wystawionym dla witryny e24.bsgostynin.pl, której właścicielem jest Bank Spółdzielczy w Gostyninie, zweryfikowany poprzez Unizeto Technologies S.A. (poprawność certyfikatu sprawdzamy klikając w zamkniętą kłódkę widoczną w oknie przeglądarki)

- sprawdź czy dane zawarte na stronie podsumowującej przelew takie jak nazwa odbiorcy, numer rachunku bankowego odbiorcy czy rodzaj operacji są zgodne z Twoją dyspozycją

- w razie wątpliwości sprawdź, czy dane dotyczące certyfikatu są zgodnej z poniższymi:
  - ✓ wystawiony dla e24.bsgostynin.pl
  - ✓ wystawiony przez Certum Extended Validation CA SHA2
  - ✓ ważny od 2015-10-22 do 2017-10-21
  - ✓ właściciel Bank Spółdzielczy w Gostyninie
  - ✓ odcisk palca (SHA1) E0:CD:E1:4A:9E:0C:C9:D9:86:C7:D6:D5:AE:2F:E9:7B:FB:99:8B:82

# 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 aktualnej 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 do systemu pocztowego trafić wirusy i oprogramowanie, którego celem jest wyłudzenie poufnych danych
- nie należy logować się do systemu e24.bsgostynin.pl korzystając z odnośników otrzymanych pocztą elektroniczną lub znajdujących się na stronach nienależących do Banku.
- należy unikać logowania z komputerów, do których dostęp również mają inne osoby (np. w kawiarenkach, u znajomych)
- zalecane jest ręczne wpisywanie danych do zlecenia przelewu np. numerów rachunków, należy unikać wprowadzania numerów rachunków metodą kopiuj/wklej
- nie należy instalować oprogramowania pochodzącego z nieznanych źródeł na komputerze, na którym korzysta się z bankowości internetowej
- należy zawsze kończyć pracę z systemem bankowości internetowej na komputerze korzystając z polecenia – wyloguj
- w przypadku wątpliwości co do prawidłowego działania bankowości internetowej lub stwierdzenia utraty środków należy niezwłocznie skontaktować się z Bankiem
- nie przechowywać danych logowania do systemu w pamięci przeglądarki internetowej.

## Pamiętaj, że bank nigdy nie prosi o:

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

# 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 serwisów 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) 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 stornie Banku dotyczące nowych zagrożeń w bankowości internetowej.

Aktualne ostrzeżenia, komunikaty i poradniki dla Klientów banków publikuje również Związek Banków Polskich na stronie internetowej: http://zbp.pl/dla-konsumentow

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

W przypadku wątpliwości dotyczących bezpieczeństwa transakcji poprzez system e24.bsgostynin.pl powinieneś niezwłocznie skontaktować się z Bankiem