Bezpieczeństwo w bankowości internetowej

Mając na uwadze bezpieczeństwo środków zgromadzonych na rachunkach, Bank Polskiej Spółdzielczości S.A. przedstawia poradnik zawierający podstawowe informacje i zasady, o których warto pamiętać korzystając z bankowości internetowej.

Bank BPS
Grupa BPS

Przed zalogowaniem do serwisu i wykonaniem transakcji:

- sprawdź, czy adres strony serwisu transakcyjnego został wpisany prawidłowo: https://e25.pl lub https://www.e25.pl

- sprawdź, czy na pasku adresu strony została wyświetlona zamknięta kłódka, oznaczająca nawiązanie szyfrowanego połączenia z Bankiem (nowoczesne przeglądarki internetowe sygnalizują certyfikaty SSL rozszerzonej walidacji zmianą koloru paska adresu na zielony)

- sprawdź, czy strona serwisu e25 jest zabezpieczona ważnym certyfikatem wystawionym dla witryn e25.pl oraz www.e25.pl, których właścicielem jest Bank Polskiej Spółdzielczości S.A., 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 SMS i na stronie www jest zgodny z Twoją dyspozycją

- w razie wątpliwości sprawdź, czy dane dotyczące certyfikatu są zgodne z poniższymi:

  - ✓ wystawiony dla e25.pl
  - ✓ wystawiony przez Centrum Extended
  - ✓ Validation CA SHA2
  - ✓ ważny od 2015-03-14 do 2016-03-12
  - ✓ właściciel:
    Bank Polskiej Spółdzielczości S.A.
  - ✓ odcisk palca (SHA1) 25 b3 85 00 be 52 1f dd bd b6 c9 b0 63 ec 6c b8 b9 19 e4 77

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 do systemu pocztowego trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych
- nie należy logować się do systemu e25 korzystając z odnośników 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 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

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

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, SMS potwierdzający transakcję) 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

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 e25 powinieneś niezwłocznie skontaktować się z infolinią Banku BPS pod numerem telefonu 801 321 456 lub 86 215 50 00.