

Podstawowe zasady korzystania z systemu CUI/CBP

Wprowadzenie

System CUI/CBP to jedno spójne rozwiązanie bankowości internetowej i mobilnej, które automatycznie dostosowuje swój wygląd i funkcjonalności do urządzenia, z którego użytkownik korzysta w danym momencie. Pozwala to na korzystanie z bankowości elektronicznej na dowolnym urządzeniu (komputer stacjonarny, laptop, tablet, telefon komórkowy) wyposażonym w przeglądarkę internetową z dostępem do sieci Internet.

Platformę CUI/CBP wyróżnia innowacyjna koncepcja udostępniania funkcjonalności systemu poprzez komponenty zwane miniaplikacjami. Miniaplikacje wraz z Platformą stanowią środowisko ich działania, tworzą swoisty ekosystem, w którym komunikacja odbywa się za pomocą ujednoczonego protokołu.

Zasady bezpiecznego logowania do systemu CUI/CBP

Nie należy:

- przechowywać danych do logowania i innych środków dostępu łącznie,
- udostępniać środków dostępu innym użytkownikom, osobom,
- zapisywać swojego kodu dostępu,
- logować się i dokonywać płatności w punktach bezpłatnego publicznego dostępu do Internetu w tzw. hot-spotach,
- otwierać strony bankowości elektronicznej poprzez link otrzymany w wiadomości elektronicznej,
- instalować oprogramowania z niezaufanego źródła, przestępcy w ten sposób mogą próbować przejść kontrolę nad urządzeniem użytkownika.

Zaleca się:

- korzystanie wyłącznie ze sprawdzonych i pewnych urządzeń, w żadnym wypadku z ogólnodostępnych stanowisk internetowych (np. w kawiarenkach internetowych, bibliotekach publicznych, szkolnych laboratoriach,
- zabezpieczanie aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall) urządzeń służących do korzystania z bankowości internetowej,
- regularne aktualizacje systemu operacyjnego, przeglądarki internetowej, szczepionek antywirusowych oraz oprogramowania zainstalowanego na urządzeniach wykorzystywanych do korzystania z bankowości internetowej,
- weryfikację, czy numer rachunku (NRB) podpisywanego i przekazywanego do realizacji przelewu jest prawidłowy oraz zwracanie szczególnej uwagi na poprawność numeru NRB po wklejeniu go ze schowka systemu,

- każdorazowe wylogowanie z systemu bankowości internetowej po zakończeniu czynności związanych z obsługą konta.

Przed wprowadzeniem identyfikatora i kodu dostępu użytkownik powinien sprawdzić, czy:

- adres strony logowania rozpoczyna się od https (oznaczającego bezpieczne połączenie internetowe), a w pasku adresu przeglądarki widoczna jest zamknięta kłódka,



- certyfikat jest wystawiony dla Asseco Poland S.A. przez firmę DigiCert Inc, weryfikacji takiej można dokonać poprzez kliknięcie na "zatrzaśniętą kłódkę" w pasku przeglądarki.

