Informacje
na temat bezpieczeństwa płatności internetowych

Bank Handlowy w Warszawie S.A. (Bank) informuje, że:

1. Korzystanie przez Klienta z Citibank Online i Citi Mobile, wymaga użycia odpowiednich urządzeń oraz oprogramowania umożliwiającego uzyskanie przez Klienta dostępu do Citibank Online i Citi Mobile. W tym:
   a) Posiadania dostępu do komputera lub innego urządzenia z systemem operacyjnym obsługującym popularne przeglądarki internetowe np. Internet Explorer, Google Chrome, Mozilla Firefox,
   b) Włączenia obsługi plików typu cookie oraz javascript. (instrukcja konfiguracji urządzenia znajduje się na stronie www.citihandlowy.pl),
   c) Włączenia obsługi protokołu TSL 1.0 oraz 1.1,
   d) Posiadania zainstalowanego programu Adobe Acrobat Reader w wersji 9.0 lub nowszej do obsługi plików PDF;
   e) Posiadania połączenia z internetem z szybkością przepływu danych Transfer do/z sieci zewnętrznej (dla pojedynczej stacji) minimum. 128 kbs, zalecamy 512 kbs
   f) Posiadania otwartych portów http (80) i https (443)
2. W przypadku, gdy Zlecenie Płatnicze lub inna czynność dokonywana przez Klienta w Citibank Online wymaga potwierdzenia Kodem Autoryzacyjnym, Klient powinien zweryfikować dane przesłane w wiadomości tekstowej SMS zawierającej Kod Autoryzacyjny z danymi wprowadzonymi w Citibank Online.
3. Podczas logowania się do Citibank Online, Klient powinien korzystać ze sprzętu zabezpieczonego zaporą sieciową (firewall), która pomaga chronić komputer przed atakami z sieci.
4. Podczas logowania się do Citibank Online oraz Citi Mobile klient powinien korzystać ze sprzętu, na którym zainstalowana jest aktualna wersja:
   a) oprogramowania antywirusowego,
   b) systemu operacyjnego oraz
   c) przeglądarki internetowej.
5. W przypadku wątpliwości, co do autentyczności lub wiarygodności informacji dotyczącej poprawnego i bezpiecznego korzystania z usług płatności internetowych, Klient powinien potwierdzić ich autentyczność i wiarygodność na podstawie informacji zawartych na stronie internetowej Banku (https://www.online.citibank.pl/polish/services/Bezpieczenstwo.htm) lub skontaktować się z CitiPhone.
6. Klient nie powinien otwierać lub odpowiadać na wiadomości e-mail, w których umieszczona jest prośba o podanie danych osobowych lub Kodów Identyfikacyjnych. Takie przypadki powinny zostać zgłoszone do Banku.
7. Klient nie powinien otwierać podejrzanych linków i załączników niewiadomego pochodzenia w otrzymanych wiadomościach e-mail, SMS i MMS.
8. Bank ani jego pracownicy nie proszą o podanie:
   a) hasła do logowania do Citibank Online,
   b) Kodów Identyfikacyjnych,
   c) numeru CVC2 znajdującego się na rewersie Karty Debetowej,
   d) Kodów Autoryzacyjnych.
9. Podczas logowania do Citibank Online lub Citi Mobile, Bank nie pyta o podanie typu numeru telefonu, numeru telefonu oraz nie nakazuje instalacji oprogramowania na telefonie klienta.
10. Bank udostępnia na stronie internetowej (https://www.online.citibank.pl/polish/services/Bezpieczenstwo.htm) informacje w zakresie poprawnego i bezpiecznego korzystania z usług bankowości elektronicznej i płatności internetowych.
11. Bank przekazuje bieżące informacje o zasadach poprawnego i bezpiecznego korzystania z usług bankowości elektronicznej i usług płatności internetowych oraz ostrzeżenia o istotnych zagrożeniach związanych z używaniem bankowości internetowej lub mobilnej poprzez wiadomość w serwisie Citibank Online dostępną po zalogowaniu oraz na stronie internetowej wskazanej w ust. 10. Bank dodatkowo może informować Klienta przekazaniu do Citibank Online istotnych informacji wysyłając wiadomość na Główny Adres E-mail Klienta.

Ponadto Bank informuje, że :

1. Klient nie powinien ujawniać poufnych informacji, w tym numerów kart, nazw użytkownika (tzw. loginów) i kodów (haseł) dostępu oraz nie powinien ich zapisywać. Jeśli występuje konieczność zapisania takich informacji, Klient powinien zrobić to w formie zaszyfrowanej uniemożliwiającej odczytanie ich innym osobom.
2. Klient nie powiniem przechowywać w tym samym miejscu PIN, E-PIN czy CitiPhone PIN i numerów kart.
3. Klient powinien pamiętać, aby hasła i kody dostępu były trudne do odgadnięcia (np. nie używać daty urodzenia, imienia lub nazwiska oraz innych informacji łatwo dostępnych o użytkowniku) i zmieniać je regularnie.
4. W przypadku podejrzenia albo stwierdzenia utraty lub przejęcia danych do logowania Klient powinien skontaktować się niezwłocznie z Bankiem poprzez CitiPhone (+48) 22 692 20 90, w celu zablokowania konta.
5. Klient nie powinien zapisywać haseł oraz przechowywać kodów dostępu w plikach zapisanych na komputerze.
6. Klient powinien chronić kod PIN i dane karty oraz nie ujawniać danych z karty kredytowej osobom trzecim, takich jak data ważności i ostatnie 3 cyfry numeru podanego na odwrocie karty.
7. Przed użyciem numeru PIN, E-PIN lub CitiPhone PIN, Klient powinien upewnić się, że nie zostaną one przekazane osobom trzecim.
8. W przypadku utraty urządzenia, za pomocą, którego Klient korzysta z bankowości internetowej lub przeprowadza transakcje (tj. komputer, laptop, tablet, telefon, itp.), należy niezwłocznie skontaktować się z Bankiem poprzez Citi Phone (+48) 22 692 20 90.

04/2016