



Szybki dostęp
Do usług bankowych



CitiDirect

System bankowości internetowej dla firm

Bezpieczeństwo systemu

KONTAKT

Biuro Obsługi Systemów Elektronicznych

tel.: **0801 343 978** lub **+48 (22) 690 15 21**

w dni powszednie w godzinach 8:00 – 17:00

e-mail: helpdesk.ebs@citi.com

Citi Handlowy jest zastrzeżonym znakiem towarowym należącym do podmiotów z grupy Citigroup Inc. Niniejszy materiał reklamowy został wydany jedynie w celach informacyjnych i nie stanowi oferty w rozumieniu art. 66 Kodeksu Cywilnego.

Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS 0000001538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522.638.400 złotych; kapitał został w pełni opłacony.

www.citihandlowy.pl

Bank Handlowy w Warszawie S.A.

citi handlowy

Jednym z najważniejszych celów w rozwoju systemu CitiDirect jest zabezpieczenie Państwa informacji w trakcie połączenia z bankiem. CitiDirect używa najnowszych dostępnych systemów zabezpieczeń, aby zapewnić poufność Państwa w trakcie tworzenia, wysyłania i przeglądania transakcji.

CitiDirect używa cztero – poziomowego systemu zabezpieczeń:

1. Identyfikacja i weryfikacja użytkownika zapobiegająca nieautoryzowanemu dostępowi.
2. Nadawanie praw określonym użytkownikom.
3. Szyfrowanie danych.
4. Kontrolowanie i alarmowanie.

1. Identyfikacja i weryfikacja użytkownika zapobiegająca nieautoryzowanemu dostępowi

Dostęp do systemu CitiDirect jest ograniczony tylko do ściśle określonych użytkowników, za pomocą karty SafeWord (tzw. tokena), która generuje unikalne, dynamiczne hasła pozwalające na zalogowanie się do systemu. Dynamiczne, niepowtarzalne hasła zmniejszają ryzyko wejścia do systemu osób nieautoryzowanych poprzez poznanie hasła – jest ono inne przy każdym logowaniu. Dodatkowo sama karta SafeWord zabezpieczona jest 4-cyfrowym PIN'em, znanym tylko posiadaczowi karty.

2. Nadawanie praw określonym użytkownikom

Prawa użytkowników kontrolowane są za pomocą ich profili dostępowych, które określają konkretny poziom dostępu do opcji w systemie CitiDirect. Profile te są tworzone przez administratorów systemu lub przez Bank Handlowy na podstawie Państwa pisemnej prośby i mają wpływ na: dostęp do określonych rachunków, typów transakcji, wysokość kwoty pojedynczej płatności, schematów i limitów autoryzacji, itd.

3. Szyfrowanie danych

Połączenie pomiędzy użytkownikiem a bankiem jest szyfrowane w celu uniemożliwienia dostępu do danych intruzom. Zastosowany protokół szyfrowania (SSL-3) zapewnia prywatność i niezawodność. 128-bitowe szyfrowanie, wymagane dla instytucji finansowych, umożliwia specjalny cyfrowy certyfikat VeriSign. Dzięki temu w systemie CitiDirect ustanawiane jest bezpieczne połączenie, zapewniające, że tylko uprawnieni użytkownicy będą mogli odczytać zawartość szyfrowanych danych.

W dodatku, SSL chroni spójność danych przesyłanych w bezpiecznym, szyfrowanym połączeniu dzięki Kodowi Weryfikacji Autentyczności (Message Authentication Code – MAC). MAC wykrywa czy w trakcie transmisji dane nie zostały zmienione.

4. Kontrolowanie i alarmowanie

Niewidoczne i nieabsorbujące Państwa, kontrole i alarmy są bardzo ważnym elementem w strukturze bezpieczeństwa systemu CitiDirect. Pozwala to na szybkie wykrycie i zidentyfikowanie nieautoryzowanych prób "wejścia" do systemu CitiDirect. Wszystkie ewentualne zdarzenia zgłaszane są do całodobowego systemu monitoringu, co pozwala na natychmiastowe śledztwo i rozwiązanie problemu.

Niezależnie od zastosowanych zabezpieczeń użytkownik musi zdawać sobie sprawę z zagrożeń występujących w internecie i stosować się do poniższych zasad:

1. Przed rozpoczęciem logowania upewnij się, że jesteś na właściwej bezpiecznej stronie programu. W oknie przeglądarki, na pasku stanu, na dole po prawej stronie musi być widoczna zamknięta kłódka oznaczająca połączenie szyfrowane. Adres strony musi zaczynać się od „https“.
2. Strona internetowa CitiDirect zabezpieczona jest certyfikatem. Nigdy nie ignoruj ostrzeżeń przeglądarki o błędach a w szczególności o błędach certyfikatu. Jeśli stwierdzisz błąd w certyfikacie zgłoś ten fakt niezwłocznie do Banku.
3. Karta SafeWord – generator haseł jednorazowych – czyni CitiDirect odpornym na próby przejęcia hasła. Noś ją zawsze przy sobie a pin do karty zapamiętaj i nigdzie nie utrwalaj. Wszelkie czynności wykonane w CitiDirect są rejestrowane. Każda operacja wykonana za pomocą Twojej karty będzie traktowana jako Twoja. Jeśli udostępnisz pin i kartę osobie trzeciej, czynisz to wyłącznie na Swoją odpowiedzialność. Jeżeli zgubisz kartę, zgłoś się natychmiast do Banku.
4. System posiada zabezpieczenie automatycznie blokujące dostęp po 15 minutach braku aktywności i wymuszające ponowne zalogowanie się. Jednak nigdy nie pozostawiaj otwartego programu dłużej niż to jest potrzebne. Wylogowuj się z systemu od razu po zakończonej pracy lub gdy oddalasz się od komputera nawet na chwilę. Swoim zachowaniem nie stwarzaj możliwości

skorzystania przez osoby niepowołane z otwartej przez siebie sesji programu choćby przez kilka sekund.

5. Dbaj o bezpieczeństwo Twojego komputera. Instaluj na bieżąco uaktualnienia systemu operacyjnego. Używaj programów antywirusowych i oprogramowania chroniącego komputer przed atakami z zewnątrz. Nie instaluj programów niewiadomego pochodzenia.

Dodatkowe informacje na temat bezpieczeństwa znajdują Państwo na witrynie internetowej Związku Banków Polskich pod adresem:

<http://www.zbp.pl/photo/bezpieczenstwo/index.html>

@UWAGA! Za szkody powstałe w wyniku braku stosowania powyższych zasad odpowiada wyłącznie **UŻYTKOWNIK**.

@UWAGA! Ze względów bezpieczeństwa, użytkownik zostanie automatycznie usunięty po 12 miesiącach braku aktywności w systemie. Blokada logowania może nastąpić wcześniej, w przypadku, gdy zdefiniowana data wygaśnięcia profilu użytkownika przypadnie przed upływem tego okresu.