# CitiDirect - dobre praktyki bezpiecznego korzystania z systemu

Bezpieczeństwo systemów transakcyjnych bankowości elektronicznej, a przez to Państwa środków, jest bardzo ważne dla Citi Handlowy. Przypominamy zasady, które pozwolą utrzymać wysoki poziom bezpieczeństwa podczas korzystania z usług bankowości elektronicznej.

Chroń swój komputer! Korzystaj z aktualnych wersji przeglądarki, systemu operacyjnego i programu antywirusowego

citi handlowy
Skorzystaj z możliwości oferowanych przez CitiDirect, aby zwiększyć bezpieczeństwo

Zachowaj czujność i uważaj na ataki hakerów! Strzeż swoich danych wrażliwych, zwracaj uwagę na sytuacje nietypowe

## Chroń swój komputer!

- korzystaj z aktualnej wersji systemu operacyjnego oraz rekomendowanych przeglądarek internetowych
- używaj aktualnego oprogramowania antywirusowego oraz zapory sieciowej (firewall)
- chroń narzędzia oraz dane służące do logowania i autoryzacji transakcji
- chroń swoje dane osobowe – rozważnie korzystaj z dobrodziejstw Internetu
- nie instaluj oprogramowania pochodzącego z niezaufanych źródeł
- nie odpowiadaj na wiadomości e-mail, w których umieszczona jest prośba o podanie danych osobowych lub kodów dostępu – zgłaszaj nam wszystkie takie przypadki
- nie otwieraj załączników i nie uruchamiaj żadnych linków w podejrzanych wiadomościach e-mail oraz SMS
- loguj się do serwisu bankowości elektronicznej z zaufanego komputera i sieci (unikaj tzw. hot-spotów), wprowadzając konkretny adres URL – nie wyszukuj go przy użyciu wyszukiwarek
- sprawdzaj, czy połączenie podczas logowania jest bezpieczne (https, SSL, TLS)
- sprawdzaj autentyczność strony internetowej swojego banku poprzez weryfikację certyfikatu i informacji w nim zawartych
- nie kopiuj numerów rachunków bankowych do przelewów („kopiuj-wklej"), ale wpisuj je samodzielnie i dokładnie weryfikuj
- cyklicznie sprawdzaj, czy numery rachunków w szablonach płatności nie uległy podmianie
- kończąc pracę w serwisie, pamiętaj o wylogowaniu się (wybieraj opcję „Wyloguj")
- zawsze informuj Bank o wszelkich nietypowych sytuacjach i nieprawidłowościach podczas korzystania z usług bankowości elektronicznej

**UWAGA** – zachęcamy do zapoznania się z informacjami na temat bezpieczeństwa opracowanymi przez Związek Banków Polskich. Prezentację na ten temat znajdziesz TUTAJ.

## CitiDirect – skorzystaj z możliwości i podnieś poziom bezpieczeństwa

- korzystaj z wielostopniowej autoryzacji - unikaj sytuacji, w której jedna osoba może samodzielnie zrealizować płatność
- upewnij się, iż transakcje podwyższonego ryzyka, np. transakcje wysokokwotowe, procesowane są przy wykorzystaniu wielostopniowej autoryzacji

**UWAGA – nawet najlepiej zaprojektowane wewnętrzne procesy mogą okazać się niewystarczające, gdy np. jedna osoba ma pełną kontrolę nad transakcjami w systemie.**

- rozważ wykorzystanie wzorców, czyli predefiniowanych formatek płatności
- procesy księgowe twórz tak, aby nie było możliwości zmodyfikowania rachunku beneficjenta przed wprowadzeniem transakcji do systemu (np. w pliku importowanym do CitiDirect)
- zgłoś do Citi Handlowy wniosek o usunięcie dostępu dla pracowników, którzy odeszli z firmy lub są w trakcie długotrwałej nieobecności (np. z tytułu urlopu wychowawczego). W tym celu wykorzystaj wniosek Aktywacja/ Konfiguracja (tabela 3)
- regularnie przeglądaj uprawnienia w systemie bankowości elektronicznej, aby upewnić się, że właściwe osoby posiadają do niej dostęp oraz mają nadane uprawnienia, które są aktualne i niezbędne do realizacji ich zadań zgodnie z tzw. zasadą minimalnych uprawnień
- nikomu nie udostępniaj swojej karty SafeWord ani też nie podawaj żadnych informacji z nią związanych (np. numeru karty czy kodu PIN)
- chroń kod PIN do swojej karty SafeWord i nie ujawniaj go osobom trzecim. Kod PIN to pierwszy i najważniejszy mechanizm obronny, który chroni przed nieautoryzowanym wykorzystaniem karty SafeWord w przypadku jej kradzieży lub zgubienia. Kod PIN nie powinien być nigdzie zapisywany czy też umieszczany w widocznym miejscu i nie powinien być łatwy do odgadnięcia

Zalecamy okresowo zmieniać PIN, w tym celu:

1) włącz kartę SafeWord przyciskiem ON
2) wprowadź aktualny czterocyfrowy kod PIN
3) wybierz przycisk „Pin" na klawiaturze karty SafeWord
4) gdy pojawi się napis NEW PIN, wprowadź nowy czterocyfrowy PIN
5) gdy pojawi się napis AGAIN, raz jeszcze wprowadź czterocyfrowy PIN, ten sam co w kroku powyżej
6) o poprawnej zmianie kodu PIN – karta poinformuje Cię napisem SUCCESS na wyświetlaczu

**UWAGA – zapamiętaj zmieniony kod PIN – jeśli go zapomnisz, jedynym rozwiązaniem będzie wymiana karty SafeWord.**

# Przestrzegamy przed atakami hakerskimi!

W ostatnim czasie w Polsce i na świecie obserwujemy wzmożoną aktywność działań przestępczych w sieci. Coraz częściej zdarzają się incydenty, w których przestępcy usiłują podstępem pozyskać informacje wrażliwe, stanowiące tajemnicę użytkownika systemu.

Przestępcy wykorzystują zaawansowane metody inżynierii społecznej (ang. social engineering) i zazwyczaj kontaktując się z wybraną firmą lub osobą telefonicznie, podszywają się pod pracownika banku (np. z Działu Obsługi Klienta lub Działu Pomocy Technicznej). Pytają o różne szczegóły związane z pracą w systemie bankowości elektronicznej, np.:

- liczbę stopni autoryzacji
- kolejność autoryzacji zleceń
- dane logowania (numer karty SafeWord)

Jeżeli przebieg rozmowy budzi Twoje wątpliwości, zawsze można poprosić rozmówcę o podanie danych osobowych (imię i nazwisko) i skontaktować się w celu ich potwierdzenia z:

» CitiService - 801 24 84 24 lub (22) 690 19 81

» Helpdesk - 801 34 39 78 lub (22) 690 15 21

**UWAGA – Citi Handlowy nigdy nie kontaktuje się z Klientami, aby spytać o hasła do systemów, PIN-y do kart SafeWord czy też jakiekolwiek informacje generowane przez karty SafeWord.**

Jedna z powszechnie stosowanych przez hakerów metod pozyskania poufnych danych polega na wysyłaniu fałszywych wiadomości e-mail. Są one tak sformułowane, aby zainteresować odbiorcę i skłonić go do otwarcia załączonego pliku lub kliknięcia na umieszczony w tekście link. W rezultacie na komputerze instaluje się złośliwe oprogramowanie, które jest wykorzystywane przez przestępcę.

Z rozwagą czytaj otrzymywane wiadomości e-mail. W razie jakichkolwiek wątpliwości skasuj podejrzaną wiadomość.

**UWAGA – skontaktuj się z Bankiem, jeżeli podczas logowania zauważysz jakiekolwiek niepokojące sytuacje, które wzbudzają wątpliwości – np. inny wygląd strony logowania lub niestandardowe komunikaty.**

Znaki Citi oraz Citi Handlowy stanowią zarejestrowane znaki towarowe Citigroup Inc., używane na podstawie licencji. Spółce Citigroup Inc. oraz jej spółkom zależnym przysługują również prawa do niektórych innych znaków towarowych tu użytych. Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923 Warszawa, zarejestrowany przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS 000 000 1538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522 638 400 złotych, kapitał został w pełni opłacony.