VOLKSWAGEN BANK

Podstawowe zasady bezpieczeństwa

Volkswagen Bank przywiązuje dużą wagę do kwestii bezpieczeństwa swoich Klientów korzystających z usług i systemów Banku. Jednak bezpieczeństwo w bankowości elektronicznej zależy nie tylko od Banku, ale i od Klienta. Dlatego przypominamy podstawowe zasady bezpieczeństwa:

1. Korzystaj wyłącznie ze sprawdzonych i pewnych urządzeń dostępowych (komputer, tablet, telefon etc.). w przypadku ogólnodostępnych stanowisk internetowych (np. w kawiarenkach internetowych, bibliotekach publicznych) prawdopodobieństwo, że program szpiegujący działa w tle, jest bardzo duże. Stosuj zasadę ograniczonego zaufania.
2. Nie otwieraj podejrzanych maili i załączników. Uważaj na umieszczone w wiadomościach linki. Mogą one zainfekować Twoje urządzenia wirusem.
3. Uważnie czytaj komunikaty i powiadomienia pojawiające się w trakcie logowania i wykonywania transakcji. Pamiętaj, że przestępcy potrafią podrabiać strony www, w tym strony banków. Jeśli strona Banku wygląda inaczej lub miałeś do czynienia z nietypowym jej działaniem, skontaktuj się z nami.
4. Bank nigdy nie prosi o podanie pełnego hasła logowania do systemu bankowości internetowej. Prośby takie kierowane do Klienta (e-mailem, SMS-em lub telefonicznie) są próbą wyłudzenia danych.
5. Uważnie czytaj treści SMS-ów, w tym potwierdzenia transakcji. Podane w wiadomości czynności, numer operacji, numer rachunku i kwota muszą zgadzać się ze zlecanymi przez Ciebie w serwisie e-direct. Zwracaj uwagę na treść SMS-a od Banku, nawet jeśli wykonujesz transakcje bardzo często.
6. Nigdy nie używaj do logowania adresu lub linku wysłanego w wiadomości e-mail lub SMS, jeśli nie jesteś pewien jej źródła.
7. Przed zalogowaniem sprawdź, czy połączenie z Bankiem jest bezpieczne. Adres witryny internetowej Banku powinien rozpoczynać się od skrótu: "https://", a nie "http://". Brak litery "s" w skrócie "http" oznacza brak szyfrowania. Twoje dane są w takiej sytuacji transmitowane przez internet tekstem jawnym, co naraża Cię na niebezpieczeństwo przechwycenia danych przez osoby nieuprawnione.
8. Bank nigdy nie wysyła certyfikatów bezpieczeństwa poprzez wiadomość SMS lub e-mail.
9. Nie instaluj na żądanie dodatkowego oprogramowania na komputer, tablet lub telefon – pamiętaj, że Bank nigdy o to nie prosi.
10. Regularnie aktualizuj system operacyjny i przeglądarki internetowe. Pamiętaj, że Windows XP nie jest już wspierany przez producenta. Aktualizacje legalnego oprogramowania często niwelują „dziury", które starają się wykorzystać oszuści.
11. Zabezpiecz komputer aktualnym oprogramowaniem antywirusowym.
12. Aplikacje na urządzenia mobilne pobieraj wyłącznie z oficjalnych sklepów: AppStore, Google Play lub Windows Store. Znajdujące się tam programy przechodzą proces weryfikacji, a więc gwarantują Ci bezpieczeństwo.
13. Uważnie czytaj ostrzeżenia Banku przed nowymi zagrożeniami. Zamieszczane są one w Aktualnościach na stronie Banku oraz wysyłane pocztą wewnętrzną w systemie transakcyjnym.
14. Nigdy nie udostępniaj osobom trzecim numeru Klienta ani hasła. Numer Klienta jest poufnym numerem nadawanym przez Bank, nie możesz go zmienić.
15. Nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie.

16. Sprawdzaj datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.
17. Niezwłocznie skontaktuj się z Bankiem w razie wątpliwości dotyczących bezpieczeństwa dostępu do bankowości internetowej.

Bezpieczeństwo bankowości internetowej

Bezpieczne logowanie

Obsługa internetowa e-direct pozwala na zarządzanie Twoimi rachunkami. Oto jak chronimy Twoje dane:

- potwierdzamy tożsamość właściciela/pełnomocnika rachunku,
- przyznajemy numer Klienta, a Klient indywidualnie ustala swoje hasło.

Autoryzacja transakcji odbywa się w następujący sposób: Klient za każdym razem potwierdza je posługując się aplikacją VWFS Token Mobilny.

Pamiętaj, aby nie odpowiadać na wiadomości mailowe, w których jesteś proszony o podanie albo zweryfikowanie Twoich danych. Bank nie wysyła tego rodzaju zapytań drogą mailową.

Zadbaj też o bezpieczeństwo komputera, z którego korzystasz. Posługuj się tylko legalnym oprogramowaniem, aktualizuj na bieżąco system operacyjny oraz programy antywirusowe i przeglądarki internetowe. Unikaj komputerów, które są dostępne publicznie, gdyż nie są one należycie zabezpieczone, przez co Twoje połączenie z Bankiem może być śledzone.

Pamiętaj, że Bank nigdy nie poprosi Cię o podanie:

- kodu jednorazowego podczas logowania do serwisu transakcyjnego ani bezpośrednio po zalogowaniu do niego,
- kilku kodów jednorazowych jednocześnie (wyjątkiem jest tylko konieczność użycia dwóch kodów podczas aktywacji lub zmiany nowego narzędzia autoryzacji),
- kodu jednorazowego w trakcie rozmowy telefonicznej nawiązanej przez pracownika Banku, chyba że kontakt telefoniczny następuje z Twojej inicjatywy,
- kodu jednorazowego do uwierzytelnienia, identyfikacji, potwierdzenia adresu IP dla Twojego komputera,
- danych karty płatniczej, takich jak: numer karty, data ważności i kod CVV, podczas korzystania z serwisu internetowego.

Pamiętaj, że w trakcie rozmowy telefonicznej nawiązywanej przez pracownika Banku, Klient nie jest proszony o podawanie kodów z narzędzi autoryzacyjnych, chyba że kontakt następuje z Twojej inicjatywy.

W razie jakichkolwiek wątpliwości prosimy o rozłączenie się i skontaktowanie się z konsultantem, by potwierdzić, czy połączenie było wykonane przez pracownika Banku.

Hasła i sposoby autoryzacji

Wszystkie spersonalizowane dane do logowania (identyfikator, hasło) oraz inne informacje potwierdzające tożsamość powinieneś chronić w sposób zapewniający ich poufność.

W pierwszej kolejności potrzebne jest potwierdzenie Twojej tożsamości jako właściciela (pełnomocnika) rachunku. Na podstawie Twojego numeru Klienta, hasła oraz akceptacji operacji kodem PIN w aplikacji VWFS Token dokonywana jest identyfikacja, dzięki której możesz zalogować się do Serwisu e-*direct*.

Dostęp do systemu transakcyjnego zostaje automatycznie zablokowany w momencie trzykrotnego podania błędnych danych identyfikacyjnych. Aby odblokować dostęp należy zadzwonić na Infolinię Banku pod numerem 800 103 301 (z telefonów stacjonarnych i z zagranicy) lub (22) 528 96 28.

Zalecamy regularną zmianę hasła (np. raz w miesiącu).

Nowi Klienci

Po podaniu identyfikatora Klienta zostaniesz poproszony o podanie hasła tymczasowego, które otrzymasz w wiadomości SMS. Następnie konieczna będzie zmiana hasła.

Hasło:

- musi mieć min. 8 znaków,
- maks. długość to 15 znaki,
- hasło musi posiadać przynajmniej jedną cyfrę, jedną dużą i małą literę
- hasło musi posiadać przynajmniej jeden znak specjalny

Bezpieczeństwo urządzeń dostępowych

Celem zapewnienia właściwego poziomu ochrony komputer Klienta powinien posiadać:

- **regularnie aktualizowany, legalny system operacyjny (np. Windows)**
- **aktywne i aktualne oprogramowanie chroniące przed złośliwym oprogramowaniem i zwalczające je**
  Oprogramowanie do zwalczania złośliwego oprogramowania pozwala na wykrycie, usunięcie i zabezpieczenie przed wieloma zagrożeniami występującymi w internecie. Za złośliwe oprogramowanie uznaje się program, który instaluje się na komputerach lub innych terminalach bez zgody użytkownika i narusza jego prawa. Do złośliwego oprogramowania zaliczamy m.in.: wirusy komputerowe, trojany, programy szpiegujące, keyloggery (oprogramowanie przechwytujące wpisywane przez użytkownika znaki) czy oprogramowanie typu backdoor, adware, robaki i inne.
- **oprogramowanie antyspamowe**
  Rodzaj oprogramowania służącego do analizy otrzymywanej korespondencji elektronicznej (e-mail) i wyfiltrowaniu niechcianej poczty (tzw. spamu).
- **aktywną zaporę sieciową (tzw. firewall)**
  Zapora sieciowa (tzw. firewall) jest jednym ze sposobów zabezpieczania i monitoringu

komputerów, sieci i serwerów przed dostępem osób niepowołanych. Chroni ona komputer poprzez ograniczenie dostępu do jego zasobów tylko dla dozwolonego ruchu sieciowego.

- **Do obsługi systemu transakcyjnego zalecane są dwie ostatnie najnowsze wersje następujących przeglądarek internetowych:**
  FireFox
  Chrome
  Microsoft Edge
  Opera
  Safari

Użytkownik powinien także korzystać z legalnego i pochodzącego z pewnych źródeł oprogramowania.

Bezpieczna komunikacja z Bankiem

Przypominamy, że w ramach bankowości internetowej Volkswagen Bank GmbH Sp. z o.o. Oddział w Polsce nigdy nie prosi swoich Klientów o poufne dane, takie jak:

- pełne dane do logowania do systemu transakcyjnego,
- kodu PIN do aplikacji VWFS Token Mobilny,
- telekodu, danych kart płatniczych i kredytowych,
- kodu PIN do karty, aplikacji etc.

Tych informacji nie należy nikomu udostępniać.

Dlatego w przypadku otrzymania e-maila lub telefonu z prośbą o ujawnienie powyższych danych, prosimy o nieudzielanie żadnych informacji i pilny kontakt pod numerem telefonu +48 22 528 96 28 lub przesłanie wiadomości na adres bezpieczenstwo@vwbank.pl.

Bank również:

- nie wysyła na telefon komórkowy żadnych certyfikatów bezpieczeństwa lub innych aplikacji do zainstalowania,
- nigdy nie przesyła na skrzynkę e-mail linków do logowania do bankowości internetowej.

Bank prowadzi własne działania ochronne celem zapewnienia bezpieczeństwa bankowości internetowej Klientów. W sytuacjach podejrzanych będzie kontaktował się telefonicznie z Klientem, celem wyjaśnienia nietypowych aktywności.

Bezpieczeństwo transakcji

Po zalogowaniu system:

- analizuje, ile czasu upłynęło od ostatniej operacji po zalogowaniu,
- po przekroczeniu dopuszczalnego okresu bezczynności (5 minut) automatycznie Cię wyloguje.

VOLKSWAGEN BANK

Nasz system zapewnia bezpieczeństwo także, kiedy podajesz poufne dane podczas pracy z Serwisem e-direct:

- począwszy od strony logowania połączenie Twojej przeglądarki internetowej z Bankiem jest szyfrowane,
- ma to na celu zabezpieczenie transmisji przed przechwyceniem danych przez nieupoważnione osoby,
- do szyfrowania wykorzystywany jest jeden z najbardziej zaawansowanych bezpiecznych protokołów transmisji – TLS – o sile co najmniej 128 bitów (w zależności od używanej przeglądarki).

W momencie zauważenia komunikatu o prowadzonych pracach technicznych w Serwisie e-direct lub automatycznego wylogowania z aktywnej sesji, prosimy o wzmożoną czujność. Przestępcy są w stanie generować fałszywe informacje wyświetlane na zainfekowanym komputerze.

Jak jeszcze zapewniamy Ci bezpieczeństwo?

- identyfikatorem bezpiecznego połączenia jest symbol zamkniętej kłódki pojawiającej się na pasku stanu Twojej przeglądarki internetowej,
- szyfrowanie połączenia wymaga uzyskania przez Bank certyfikatu potwierdzającego autentyczność jego stron,
- aby sprawdzić ważność certyfikatu potwierdzającego, że jesteś na prawdziwej stronie internetowej Volkswagen Bank, kliknij dwukrotnie ikonę kłódki.

Ze względu na nasilające się w ostatnich czasach zjawisko phishingu – polegające na tym, że oszuści zbierają poufne dane poprzez sfałszowane strony banków – zawsze w przypadku wątpliwości co do autentyczności stron Volkswagen Bank sprawdź certyfikat bezpieczeństwa.

Zwracaj uwagę czy numer konta i bank odbiorcy przelewu podpisywany kodem PIN w aplikacji VWFS Token Mobilny zgadza się z wpisanym przez Ciebie numerem podczas wykonywania przelewu.

Prosimy także zwrócić uwagę na zasady bezpiecznego korzystania z kart płatniczych, szczególnie w miejscach o wzmożonym ruchu turystycznym.

TELEdirect

Jeśli korzystasz z systemu telefonicznej obsługi rachunków TELEdirect:

- identyfikacja wymaga podania trzech z sześciu cyfr Twojego osobistego telekodu, co uniemożliwia podejrzenie lub podsłuchanie pełnego telekodu w trakcie rozmowy telefonicznej,
- dodatkowym zabezpieczeniem jest „losowanie" kolejności wybierania ww. trzech cyfr – system pyta o cyfry telekodu w dowolnej kolejności np. 2-3-6,
- dzięki temu dostęp do Volkswagen Bank przez telefon jest jednym z najbezpieczniejszych spośród wszystkich oferowanych obecnie na rynku.

Zmiana limitów operacji

VOLKSWAGEN BANK

Limity operacji określają dopuszczalną wartość transakcji na Twoim rachunku. Dotyczą transakcji wykonywanych przez internet oraz IVR. Każdy kanał dostępu ograniczony jest dwoma limitami: limit jednorazowy wskazuje maksymalną kwotę jednej operacji, natomiast limit dzienny to suma wszystkich operacji zlecanych w jednym dniu. Ze względów bezpieczeństwa, w momencie uruchomienia Twojego rachunku Bank ustawia limity na poziomie 2 000 zł dla jednej operacji i 5 000 zł dla sumy operacji dziennych.

Limity operacji można sprawdzić oraz zmodyfikować logując się do serwisu transakcyjnego, wybierając zakładkę „Konta” oraz menu „Informacje o koncie”. Następnie należy przejść do sekcji „Limity operacji” i wybrać opcję „Zmień limity”. Każda zmiana wartości limitów wymaga autoryzacji hasłem SMS.