Deutsche Bank
db easyNET

Bezpieczne korzystanie z systemu Bankowości Internetowej db easyNET

Spis treści

WZ/2012/10/18, v. 4.1

Wstęp

Deutsche Bank ogromną uwagę poświęca Twojemu bezpieczeństwu.

Dlatego też powierzone nam przez Ciebie środki chronimy z wykorzystaniem najnowocześniejszych i bardzo skutecznych metod zabezpieczeń.

Twoje bezpieczeństwo w internecie zależy również od Ciebie. Dlatego prosimy – zapoznaj się ze wskazówkami, które pomogą w bezpiecznym korzystaniu z naszego serwisu.

Niniejszy podręcznik ma na celu przybliżenie Ci podstawowych zasad bezpieczeństwa oraz wskazanie stanu zabezpieczeń, który pozwoli lepiej chronić Twój komputer, tablet oraz smartfon przed ewentualnymi próbami przechwycenia poufnych danych.

Ogólne Zasady bezpieczeństwa

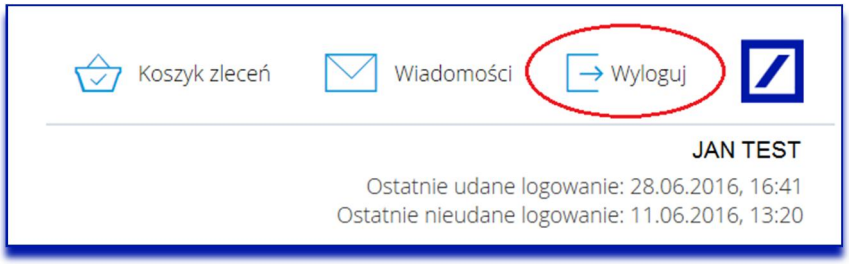
Bezpieczne korzystanie z systemu db easyNET zależy w znacznym stopniu od Ciebie!

Bezpieczny komputer, tablet, smartfon

Dbaj o bezpieczeństwo swojego urządzenia!

Jedną z najważniejszych czynności poprzedzających korzystanie z systemu Bankowości Internetowej db easyNET jest właściwe przygotowanie urządzenia oraz zainstalowanego w nim oprogramowania. Poniżej znajdziesz szczegółowe informacje jak zabezpieczyć swój komputer, tablet oraz smartfon.

1. Do obsługi Bankowości Internetowej korzystaj z legalnego systemu operacyjnego, dla którego producent regularnie dostarcza aktualizacje.
2. Instaluj tylko legalne oprogramowanie, nie instaluj oprogramowania pochodzącego z nieznanych źródeł.
3. Zabezpiecz swój komputer, tablet oraz smartfon programem antywirusowym oraz antyspamowym.
4. Używaj osobistego Firewalla – pozwoli on Tobie lepiej chronić się przed ingerencją z zewnątrz i ograniczy dostęp do informacji o zasobach Twojego urządzenia.
5. Pamiętaj o regularnych aktualizacjach systemu operacyjnego oraz zainstalowanego na nim oprogramowania, w tym w szczególności oprogramowania antywirusowego (wraz z bazą sygnatur wirusów).
6. Pamiętaj o cyklicznym skanowaniu antywirusowym całego systemu zgodnie z zaleceniami producenta oprogramowania antywirusowego. Chroń swój system pocztowy przed przychodzącym spamem. Pamiętaj, że wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą do Ciebie trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych (takich jak NIK czy Kod Dostępu).
7. Nie otwieraj załączników do wiadomości, których nie oczekiwałeś (ani samych wiadomości, których tytuł czy nadawca wzbudzają podejrzenie próby dokonania oszustwa).
8. Pamiętaj, że Bank nie wysyła wiadomości e-mail, w których prosi o zainstalowanie dodatkowego oprogramowania (aktualizację lub podanie poufnych danych).
9. Korzystaj z Bankowości Internetowej tylko na zaufanych urządzeniach. Nie jest zalecane logowanie się do systemu db easyNET z urządzeń ogólnodostępnych (np. w kawiarenkach internetowych) oraz poprzez publiczne sieci WiFi (w tzw. hot-spotach).
10. Twoja przeglądarka internetowa powinna mieć wprowadzone zalecane przez Bank ustawienia (patrz. „Konfiguracja przeglądarki").
11. Nigdy nie pozostawiaj urządzenia bez nadzoru w czasie, kiedy zalogowany jesteś do systemu Bankowości Internetowej.
12. Po zakończeniu pracy z db easyNET pamiętaj o wylogowaniu się z systemu. W celu wylogowania z db easyNET korzystaj z opcji „Wyloguj". Nie zamykaj systemu poprzez zamknięcie karty bądź okna przeglądarki internetowej.



WZ/2012/10/18, v. 4.1

Konfiguracja przeglądarki

Zabezpiecz swoją przeglądarkę!

1. Korzystaj z najnowszych wersji przeglądarek internetowych.

Rekomendujemy aktualizację przeglądarki internetowej do najnowszej wersji dostępnej na rynku.

Przeglądarki internetowe dedykowane dla systemu db easyNET		
Nazwa oraz wersja przeglądarki internetowej	db easyNET (1)	
	urządzenie mobilne	Komputer PC / laptop
Microsoft Internet Explorer 10.x	n/d	-
Microsoft Internet Explorer od wersji 11.x	n/d	+
Microsoft EDGE	n/d	+
Microsoft Internet Explorer Mobile od wersji 11.x	+	n/d
Mozilla Firefox od wersji 46.x	n/d	+
Mozilla Firefox Mobile od wersji 39.x	+	n/d
Google Chrome od wersji 50.x	n/d	+
Google Chrome Mobile od wersji 44.x	+	n/d
Apple Safari od wersji 9.x	n/d	+
Apple Safari Mobile od wersji 9.x	+	n/d

(1) Dostępny pod adresem: https://dbeasynet.deutschebank.pl

Informację o wersji posiadanej przeglądarki oraz protokole szyfrowania znajdziesz wybierając z menu opcję „Pomoc", a następnie w zależności od przeglądarki:

- Microsoft Internet Explorer → Internet Explorer – informacje
- Google Chrome → Ustawienia Google Chrome → Google Chrome – informacje
- Mozilla Firefox → O Mozilli Firefox
- Apple Safari → Safari

2. Przed logowaniem sprawdź, czy Twoja przeglądarka obsługuje pliki cookies.

Cookies to pliki tekstowe, które przechowywane są w urządzeniu końcowym (np. telefon, tablet lub komputer) używanym przez Użytkownika i przeznaczone są do korzystania ze strony internetowej Banku oraz systemu db easyNET za pośrednictwem sieci internet. Cookies nie zawierają żadnych programów oraz same w sobie nie są programami. Nie mogą w związku z tym zawierać wirusów ani nie mogą być wirusami.

Ograniczenia w stosowaniu plików cookies mogą wpłynąć na niektóre funkcjonalności dostępne na stronie internetowej Banku oraz w db easyNET, przy czym zablokowanie automatycznej obsługi plików cookies w ustawieniach przeglądarki internetowej spowoduje brak możliwości korzystania z db easyNET. Treść Polityki Plików Cookies dostępna jest w formacie ogólnodostępnym na stronie internetowej Banku.

3. Nigdy nie wyrażaj zgody na zapisywanie NIKu oraz Kodu Dostępu przez przeglądarkę.

Zalecane jest przez Bank wyłączenie funkcji zapamiętywania haseł oraz formularzy w przeglądarce internetowej. Jeżeli funkcja zapamiętywania haseł i formularzy pozostanie włączona, przy logowaniu do systemu db easyNET NIK oraz Kod Dostępu są automatycznie wpisywane. Wyłączenie tej opcji uniemożliwi zalogowanie się do systemu innym osobom.

- Microsoft Internet Explorer → Menu „Narzędzia" → „Opcje Internetowe" → zakładka „Zawartość" → sekcja „Autouzupełnianie" → „Ustawienia" – odznacz pola „Nazwy użytkowników i hasła w formularzach".
- Google Chrome → Menu „Ustawienia Google Chrome" → „Ustawienia" → „Prywatność" → „Hasła i formularze" – odznacz pole „Proponuj zapisywanie haseł podawanych w Internecie".
- Mozilla Firefox → Menu „Narzędzia" → „Opcje" → „Bezpieczeństwo" → „Hasła" → odznacz pole „Pamiętaj hasła do witryn".

4. Sprawdzaj, czy certyfikat serwera nie został cofnięty, co objawia się wyświetleniem symbolu otwartej kłódki przy adresie strony bądź zmianą tła w pasku adresu na kolor czerwony. Nie zapisuj szyfrowanych stron na dysku, aby uniknąć nieuprawnionego przekierowania na inne strony.

5. Aby zapewnić poprawne funkcjonowanie przeglądarki, usuwaj pliki tymczasowe, które są zapisywane w pamięci podręcznej.

- Microsoft Internet Explorer → Menu „Narzędzia" → „Opcje internetowe" → zakładka „Ogólne", sekcja „Historia przeglądania", przycisk „Usuń" - wybierz opcje „Usuń pliki cookie... „ oraz „Tymczasowe pliki internetowe" Menu „Narzędzia" → „Opcje internetowe" → zakładka „Ogólne", sekcja „Historia przeglądania", przycisk „Ustawienia" → w części „Sprawdź, czy są nowsze wersje przechowywanych stron" zaznacz opcję „Za każdym razem, gdy odwiedzam tę stronę".

WZ/2012/10/18, v. 4.1

- Mozilla Firefox → Menu „Narzędzia” → „Wyczyść historię przeglądania” – zaznacz opcje „Ciasteczka” i „Pamięć podręczna” oraz naciśnij przycisk „Wyczyść teraz”. Możesz też wskazać okres, z którego zostanie usunięta pamięć podręczną.
- Google Chrome → Menu „Ustawienia Google Chrome” → „Narzędzia” → „Wyczyść dane przeglądania…” - wybierz opcję „Opróżnij pamięć podręczną” oraz „Usuń pliki cookie i inne dane witryn” i naciśnij przycisk „Wyczyść dane przeglądarki”. Możesz też wskazać okres, z którego zostanie usunięta pamięć podręczna.

6. Nie ignoruj ostrzeżeń prezentowanych w oknie przeglądarki internetowej.

W nowych wersjach popularnych przeglądarek dostępne są specjalne narzędzia sprawdzające, czy wyświetlona strona internetowa nie ma na celu wyłudzenia poufnych informacji. Są to tak zwane filtry anty-phishingowe. Nie dają one pełnej gwarancji, że dana strona jest na pewno bezpieczna, pozwalają jednak ograniczyć ryzyko kradzieży poufnych danych. Zalecane jest przez Bank włączenie ochrony anty-phishingowej:

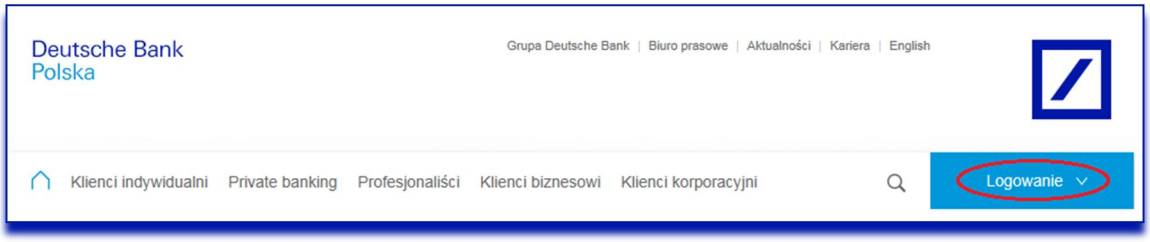
- Microsoft Internet Explorer → „Narzędzia” → w opcji „Filtr witryn wyłudzających informacje” i wybierz „Włącz automatyczne sprawdzanie sieci Web”.
- Mozilla Firefox → „Narzędzia” → „Opcje” → w zakładce „Bezpieczeństwo” zaznacz opcje: „Ostrzegaj, jeśli witryny próbują zainstalować dodatki”; „Blokuj witryny zgłoszone jako stwarzające zagrożenie” oraz „Blokuj witryny zgłoszone jako próby oszustwa internetowego”.

7. Używaj nawigacji z menu systemu db easyNET w celu przechodzenia pomiędzy poszczególnymi funkcjami. Nie używaj opcji „Wstecz”, ani „Dalej” w oknie przeglądarki.
8. Uzupełniając dane transakcji nie korzystaj z funkcji kopiowania.

Bezpieczne Logowanie

Loguj się bezpiecznie!

1. Zawsze loguj się poprzez stronę internetową: https://www.deutschebank.pl lub wpisuj ręcznie w oknie przeglądarki adres: https://dbeasynet.deutschebank.pl/.

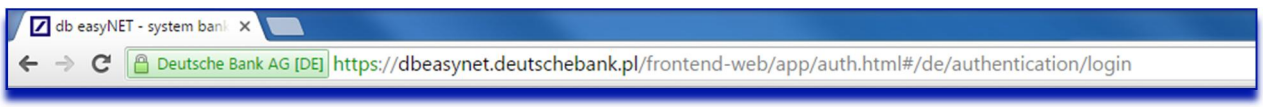


2. Nigdy nie loguj się za pośrednictwem linków otrzymanych w wiadomości e-mail.
3. Nie używaj wyszukiwarek internetowych do znalezienia strony logowania do systemu transakcyjnego Banku.
4. Pamiętaj, że Bank nigdy nie prosi podczas logowania o:
   - Podanie Kodów SMS przesyłanych na urządzenie mobilne Użytkownika.
   - Podanie danych kart debetowych / kredytowych (numeru karty, CVV, daty ważności karty, kodu PIN).
   - Instalację certyfikatów lub dodatkowego oprogramowania na komputerach lub urządzeniach mobilnych.
5. Komunikacja między urządzeniem Użytkownika, a serwerem Banku szyfrowana jest protokołem TLS. Potwierdzeniem bezpiecznego (szyfrowanego) połączenia jest adres URL rozpoczynający się od https (zamiast standardowego http), gdzie „s” oznacza „secure” – bezpieczny. Upewnij się, że adres strony zaczyna się od liter „https”, a nie „http”.

Sprawdzaj, czy na stronie logowania (w pasku adresu lub na dole strony) widoczny jest symbol zamkniętej kłódki.

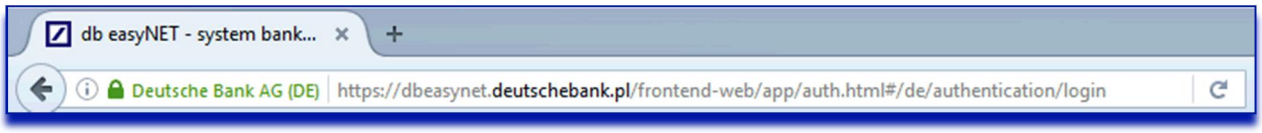
Najnowsze przeglądarki obok paska adresu wyświetlają informacje o instytucji, dla której został wystawiony certyfikat.

Zrzut ekranu wykonany w przeglądarce Microsoft Internet Explorer.



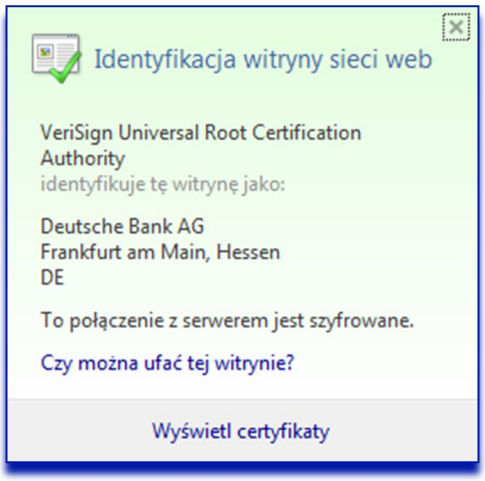
Zrzut ekranu wykonany w przeglądarce Chrome.

WZ/2012/10/18, v. 4.1



Zrzut ekranu wykonany w przeglądarce Mozilla Firefox.

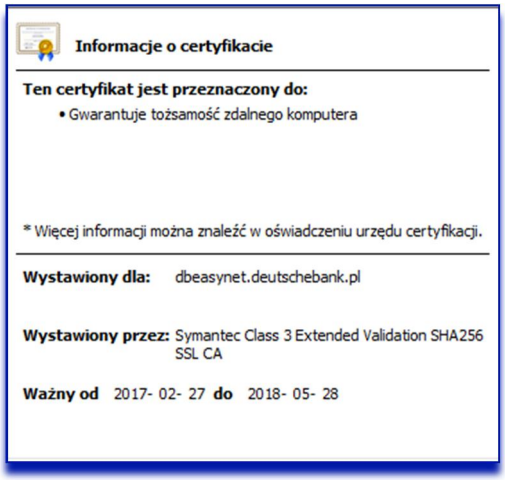
Kliknij dwukrotnie w kłódkę, aby sprawdzić czy wyświetlany certyfikat jest ważny i czy został wydany przez VeriSign dla Deutsche Bank AG.



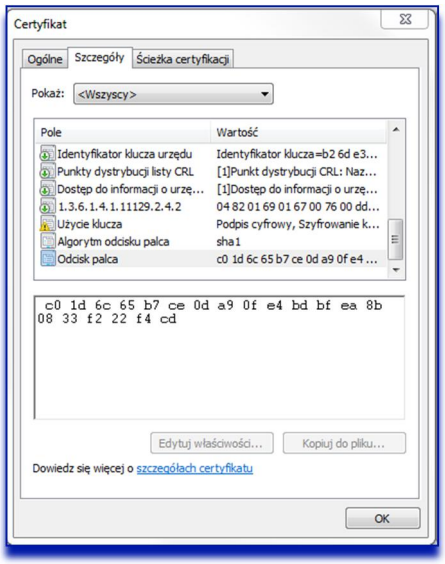
Zrzut ekranu wykonany w przeglądarce Microsoft Internet Explorer.

Sprawdzaj ważność certyfikatu. W tym celu kliknij na wspomniany wyżej symbol zamkniętej kłódki.

Poprawny certyfikat dla db easyNET wygląda następująco:



Zrzut ekranu wykonany w przeglądarce Microsoft Internet Explorer.



Zrzut ekranu wykonany w przeglądarce Microsoft Internet Explorer.

Jeśli zauważysz co najmniej jeden z poniższych objawów:

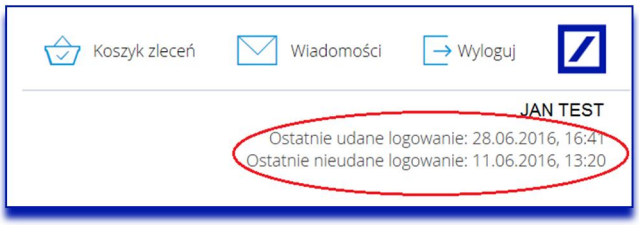
- Kłódka widoczna na pasku adresu strony nie jest zamknięta lub pojawia się przy niej symbol ostrzeżenia.
- Certyfikat jest nieważny lub został wystawiony dla instytucji innej niż Deutsche Bank AG.
- Odcisk certyfikatu – „Odcisk palca" (Thumbprint, Fingerprint) powinien być zgodny ze wskazanym powyżej.
- Strona Bankowości Internetowej przed lub po zalogowaniu wygląda inaczej, lub prezentuje inne komunikaty niż zazwyczaj.
- Proces logowania do db easyNET wygląda inaczej niż zwykle (pojawiają się inne okna, trwa dłużej niż zazwyczaj, pojawiają się prośby o podanie dodatkowych danych).

Przerwij logowanie i niezwłocznie skontaktuj się z pracownikiem Banku!

Opisane wyżej sytuacje oraz wszystkie przypadki niezgodności daty i godziny logowania do systemu zgłoś jak najszybciej pracownikom Banku (dzwoniąc pod numer 801 18 18 18, +48 12 625 80 00* lub odwiedzając najbliższy Oddział Deutsche Bank).

** Opłata za połączenia telefoniczne wg obowiązujących stawek operatora.*

6. Podczas wpisywania Numeru Identyfikacyjnego Klienta oraz Kodu Dostępu zwracaj uwagę, czy nikt nie podgląda wpisywanych danych.
7. Po poprawnym zalogowaniu się do systemu, sprawdź każdorazowo, czy data ostatniego logowania (informacja dostępna w prawym górnym rogu ekranu systemowego db easyNET) jest właściwa.



8. Po zakończeniu pracy w db easyNET zawsze używaj opcji „Wyloguj" zlokalizowanej w prawym górnym rogu ekranu systemowego.

Ochrona Numeru Identyfikacyjnego Klienta (NIK) oraz Kodu Dostępu

1. Nie ujawniaj osobom trzecim danych służących do logowania do systemu (NIKu, Kodu Dostępu).
2. Jeśli podejrzewasz, że ktoś może znać Twój Kod Dostępu – natychmiast dokonaj jego zmiany. Możesz to zrobić bezpośrednio w systemie db easyNET.
3. Okresowo dokonuj zmiany swojego Hasła. Zadbaj, żeby nie składało się ono z informacji, które w jakiś sposób mogą być z Tobą skojarzone (np. data urodzenia, imię itp.). Bank rekomenduje zmianę hasła co 90 dni.
4. Nie przesyłaj nigdy poufnych danych (takich jak NIK, Kod Dostępu) drogą e-mailową.
5. Staraj się nie zapisywać NIKu oraz Kodu Dostepu ani w formie papierowej, ani elektronicznej. Jeśli jednak konieczny jest jednak tego typu zapis – korzystaj z programów do zapamiętywania haseł oferowanych przez znanych dostawców.
6. Nie zapisuj poufnych danych na stałe w pamięci przeglądarek internetowych (patrz. Konfiguracja przeglądarki).

WZ/2012/10/18, v. 4.1

Autoryzacja dyspozycji

Dyspozycje wykonywane w systemie db easyNET są zabezpieczone z użyciem popularnych i sprawdzonych rozwiązań, jakimi są wygodne Hasła SMS, czy karty Kodów TAN. Aby bezpiecznie z nich korzystać, pamiętaj o podstawowych zasadach bezpieczeństwa.

1. Przed potwierdzeniem transakcji dokładnie zweryfikuj poprawność danych zlecanej transakcji (np numer rachunku Odbiorcy).
2. Po otrzymaniu Hasła SMS porównaj, czy dane dotyczące transakcji zawarte w jego treści są zgodne ze złożoną przez Ciebie dyspozycją.
3. Ustal limity operacji przelewów.

Zabezpieczenia zastosowane w systemie db easyNET

Numer Identyfikacyjny Klienta (NIK) i Kod Dostępu

Uwierzytelnienie użytkownika podczas logowania do systemu db easyNET odbywa się po podaniu unikalnego Numeru Identyfikacyjnego Klienta oraz Kodu Dostępu do systemu.

Numer Identyfikacyjny Klienta (NIK) – to 10-cyfrowy numer, który otrzymałeś w Pakiecie Startowym, przekazanym po podpisaniu Umowy o świadczenie Usług Bankowości Elektronicznej.

Kod Dostępu – to 8-cyfrowy kod, znany jedynie Tobie, który wygenerowany został przez Ciebie podczas pierwszego połączenia z Teleserwisem (pod jednym z następujących numerów: 801 18 18 18, +48 12 625 80 00).
Pamiętaj, że możesz wzmocnić zabezpieczenie poprzez zastosowanie kilku prostych zasad. Kod Dostępu nie powinien:

— stanowić składowej NIK,

— zawierać w sobie ciągów takich samych cyfr,

— zawierać bezpośrednio kojarzących się z Twoją osobą dat (daty Twojego urodzenia, dat ważnych dla Twoich bliskich itp.).

Hasła SMS

Jeśli wybrałeś autoryzację transakcji w systemie Bankowości Internetowej Deutsche Bank Polska S.A. w oparciu o bezpieczne i wygodne Hasła SMS – autoryzacja odbywa się po podaniu na formularzu dyspozycji Hasła SMS, które otrzymałeś w związku z tą dyspozycją na przypisany do Ciebie numer telefonu komórkowego.

Pamiętaj! Każdorazowo, gdy zmieniasz numer telefonu, poinformuj o tym Bank, by móc swobodnie kontynuować autoryzację z wykorzystaniem tej wygodnej Metody Autoryzacji.

Uwaga! Podczas korzystania z Metody Autoryzacji opartej o Hasła SMS pamiętaj, by zawsze sprawdzać poprawność strony logowania (patrz: Logowanie) i nie podawać danych związanych zarówno z Twoim telefonem, jak i z samymi Hasłami SMS. Bank nie prosi swoich Klientów o tego typu informacje, a podając je, możesz stać się ofiarą ataku hakerskiego. Bank nie prosi również o zainstalowanie dodatkowego oprogramowania na telefonach. Nigdy nie instaluj również na swoim telefonie oprogramowania, którego pochodzenia nie jesteś pewien. Pamiętaj, że w przypadku zgubienia lub kradzieży telefonu, należy zablokować kartę SIM u operatora.

Jeśli korzystasz z autoryzacji z wykorzystaniem Haseł SMS, zapoznaj się z poniższą informacją dotyczącą groźnego trojana Zeus (ZitMo)

Atak trojana odbywa się w kilku krokach, trojan:

— przechwytuje login i hasło dostępu do systemu bankowości elektronicznej z poziomu komputera,
— zdobywa numer telefonu komórkowego ofiary, instalując złośliwy formularz w przeglądarce ofiary,
— za pośrednictwem wiadomości SMS przekazuje link do „certyfikatu” z prośbą o jego zainstalowanie w telefonie (wersja instalacyjna zawiera w sobie groźnego trojana).

Po wykonaniu instalacji przestępcy mogą przejąć kontrolę nad telefonem komórkowym i inicjować transakcje w bankowości internetowej, potwierdzając je przechwyconymi wiadomościami SMS, które Bank wysyła na wskazany telefon komórkowy.

WZ/2012/10/18, v. 4.1

Karta TAN

Jeśli wybrałeś autoryzację transakcji w systemie Bankowości Internetowej Deutsche Bank Polska S.A. w oparciu o Kody TAN z Karty TAN – autoryzacja odbywa się po podaniu wskazanej przez system pary Kodów z karty.

Pamiętaj, by właściwie zabezpieczać swoją Kartę TAN.
W tym celu:

— Przechowuj ją w bezpiecznym miejscu.

— Nie ujawniaj jej nigdy osobom trzecim.

— W przypadku podejrzenia, że osoba niepowołana mogła wejść w posiadanie karty TAN lub kodów z karty TAN, należy taką kartę natychmiast zablokować.

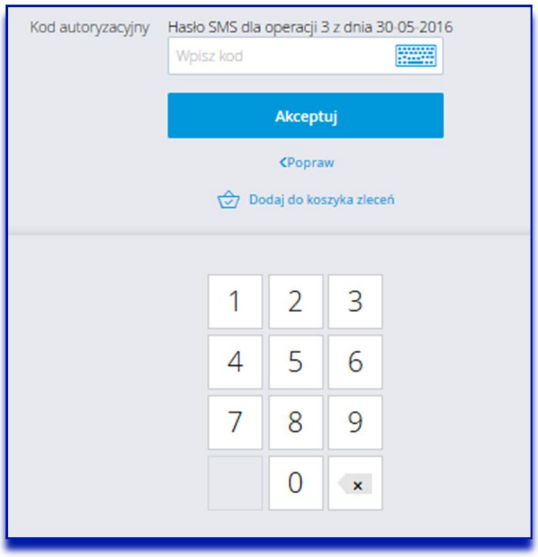
Pamiętaj! Bank nigdy nie wymaga podawania Kodów TAN podczas logowania do bankowości internetowej.

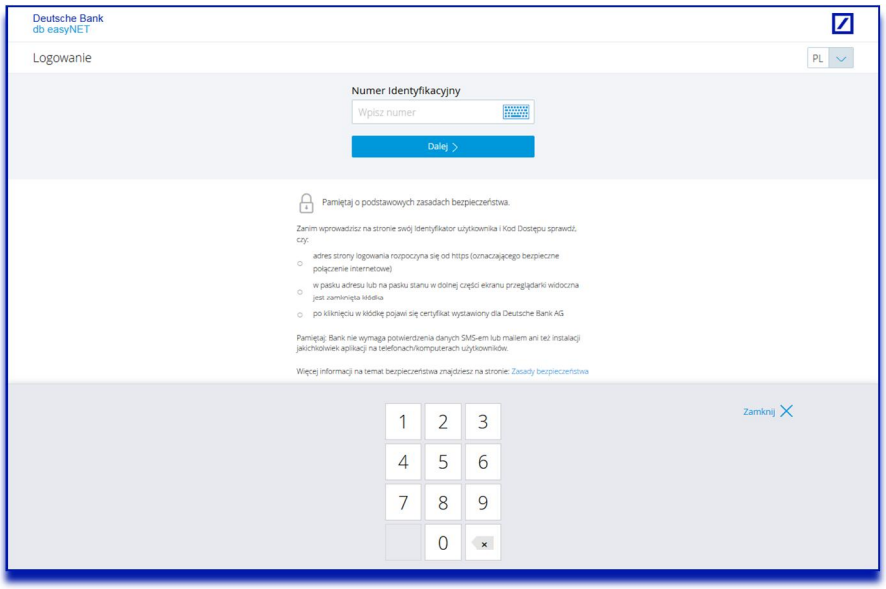
Rewers karty TAN

Wirtualna klawiatura

Klawiatura wirtualna jest dostępna przy logowaniu do db easyNET i zatwierdzaniu dyspozycji.

Wirtualna klawiatura dostępna jest na komputerach oraz urządzeniach mobilnych przy minimalnej rozdzielczości poziomej 1280 pikseli.





W przypadku korzystania z Metody Autoryzacji opartej na Kodach TAN – bezpieczeństwo zwiększają także obrazki dynamicznie, wskazujące pola na Karcie TAN, generowane w momencie autoryzacji transakcji.

Sytuacje alarmowe

Jeśli stwierdzisz zaistnienie jednego z poniższych przypadków:

- nieudana/udana próba zalogowania się na Twoje konto w db easyNET przez osoby do tego nieuprawnione,
- nieudana/udana próba nieautoryzowanych transakcji z poziomu systemu db easyNET,
- podejrzenie przechwycenia przez osobę/osoby nieuprawnioną/nieuprawnione danych do logowania,
- podejrzenie przechwycenia przez osobę/osoby nieuprawnioną/nieuprawnione numeru karty płatniczej,

niezwłocznie skontaktuj się z Bankiem, dzwoniąc pod numer: 801 18 18 18, +48 12 625 80 00* lub odwiedzając najbliższy Oddział Deutsche Bank. Po przedstawieniu naszemu pracownikowi zaistniałego problemu, postępuj zgodnie z jego wskazówkami.

Dodatkowo w sytuacji, gdy sprawa związana jest z podejrzeniem włamania na Twoje konto, jak najszybciej zmień Kod Dostępu do systemu.

** Opłata za połączenia telefoniczne wg obowiązujących stawek operatora.*

WZ/2012/10/18, v. 4.1