Komisja
Nadzoru
Finansowego

PRZEWODNIK KLIENTA USŁUG BANKOWOŚCI ELEKTRONICZNEJ

Urząd Komisji Nadzoru Finansowego
Warszawa, 2010

Spis treści

Wprowadzenie

DO KOGO JEST SKIEROWANY TEN PRZEWODNIK?

Jesteś klientem banku? Korzystasz z kart płatniczych, Internetu i telefonu, dokonując transakcji? Z jednej strony to wygoda, z drugiej - zastanawiasz się, czy Twoje pieniądze są bezpieczne.

Przygotowaliśmy dla Ciebie **PRZEWODNIK**, opisujący podstawowe zasady bezpieczeństwa, których jako klient banku korzystający z usług bankowości elektronicznej powinieneś, a nawet musisz przestrzegać.

CZEMU SŁUŻY TEN PRZEWODNIK?

W przypadku bankowości elektronicznej bezpośredni kontakt klienta z pracownikiem banku nie jest konieczny. Jednak osobie, która nie jest prawnikiem ani specjalistą w dziedzinie systemów informatycznych, może brakować informacji, pozwalających na sprawne poruszanie się w tym obszarze. Chcieliśmy wypełnić tę lukę informacyjną na rynku i wzmocnić świadomość oraz pozycję klientów detalicznych banków, korzystających z nowych technik dostępu do swoich pieniędzy na rachunkach bankowych.

CZEGO MOŻESZ DOWIEDZIEĆ SIĘ Z PRZEWODNIKA?

Jest to podany w przystępny sposób zbiór podstawowych zasad bezpieczeństwa, jakimi powinieneś się kierować, korzystając z kart płatniczych, Internetu i telefonu przy dokonywaniu operacji na swoim rachunku.

Więcej informacji na temat usług bankowości elektronicznej znajdziesz w raporcie *Usługi bankowości elektronicznej dla klienta detalicznego – charakterystyka i zagrożenia.*

1. Bankowość terminalowa

Korzystając z kart płatniczych możemy być narażeni na różnego rodzaju niebezpieczeństwa, takie jak np. kradzież naszej karty. Poniżej przedstawione zostały podstawowe zasady bezpieczeństwa dla użytkowników kart płatniczych, które pozwolą zmniejszyć ryzyko związane z tą formą płatności.

ZANIM ZAPŁACISZ KARTĄ

- Przeczytaj dokładnie umowę o kartę płatniczą i regulamin korzystania z niej.
- Jeżeli otrzymałeś z banku nową kartę, to pamiętaj, aby ją podpisać (najlepiej trwałym pisakiem).
- Dobrym zwyczajem jest regularne sprawdzanie wyciągów lub zestawień transakcji dokonanych przy użyciu kart, a także przechowywanie potwierdzeń transakcji (np. wydruków z bankomatu). To szczególnie istotne w przypadku stwierdzenia rozbieżności wyciągu ze stanem faktycznym oraz w odniesieniu do transakcji, które nie doszły do skutku, jako podstawa do złożenia reklamacji u wydawcy karty.
- Sporządź listę numerów kart płatniczych oraz telefonów do ich wydawców i przechowuj ją w bezpiecznym miejscu.
- Noś przy sobie tylko te karty płatnicze, które są często przez Ciebie wykorzystywane.
- Zakazane jest udostępnianie kart osobom nieuprawnionym (czyli wszystkim innym poza posiadaczem lub użytkownikiem). Dotyczy to także najbliższej rodziny.
- Zabronione jest zapisywanie kodu PIN na karcie, bądź przechowywanie go razem z kartą. Niezastosowanie się do tego zalecenia może ograniczyć limit odpowiedzialności posiadaczy karty, o którym mowa w *Ustawie o elektronicznych instrumentach płatniczych*. Ochrona numeru karty i innych poufnych danych jest obowiązkiem posiadacza karty.
- W przypadku utraty karty niezwłocznie powiadom o tym wydawcę karty (bank) - skontaktuj się z centrum autoryzacji kart banku albo zadzwoń do banku. Bank przyjmuje takie zgłoszenia przez całą dobę. Warto wpisać do telefonu numery, pod którymi można zastrzec kartę.

WAŻNE!

Nigdy nie udostępniaj numeru karty płatniczej przez telefon. Pamiętaj, że niezależnie od przedstawianej argumentacji (weryfikacja danych, problemy techniczne, itp.) bank nigdy nie weryfikuje danych zawartych na karcie płatniczej przez telefon.

Bankomat

Bankomaty służą przede wszystkim do wypłaty gotówki za pomocą kart płatniczych. Mogą nas jednak narażać na ryzyko uzyskania przez osoby nieuprawnione dostępu do naszych środków np. poprzez *skimming*, czyli celowe zastąpienie pierwotnego czytnika kart płatniczych takim, który będzie magazynował wszystkie informacje znajdujące się na karcie podczas jej odczytu. Poniżej przedstawiono kilka zasad bezpieczeństwa, których warto przestrzegać, korzystając z bankomatów.

BĄDŹ CZUJNY

- Staraj się korzystać tylko z bankomatów znajdujących się w dobrze oświetlonych, nieodosobnionych miejscach.
- Możesz sprawdzić, czy bankomat, z którego zwykle korzystasz nie ma zainstalowanych nowych urządzeń, np. małej kamery, służącej do podglądania wpisywanych kodów PIN lub też innych, służących do skanowania kart.
- Ustawiając się przy bankomacie zasłoń ciałem jego ekran. Nie zaszkodzi, jeśli zasłonisz drugą ręką wpisywany kod PIN (wówczas, nawet jeśli karta zostanie zeskanowana, istnieje szansa, że przestępcy nie uzyskają Twojego nr PIN).

Punkt handlowo-usługowy

- Płacąc za towary i usługi nie trać karty z pola widzenia.
- Zachowaj potwierdzenia transakcji, zwłaszcza tych, które z różnych powodów nie doszły do skutku (np. odrzucenie transakcji, brak środków).
- W restauracjach, w przypadku otrzymania wydruku z terminala w miejscu na wpisanie napiwku należy - w zależności od uznania - wpisać kwotę napiwku albo przekreślić to miejsce, by udaremnić wypełnienie go przez osobę nieuprawnioną.

WAŻNE!

Kod PIN zawsze wpisuj do terminala osobiście.

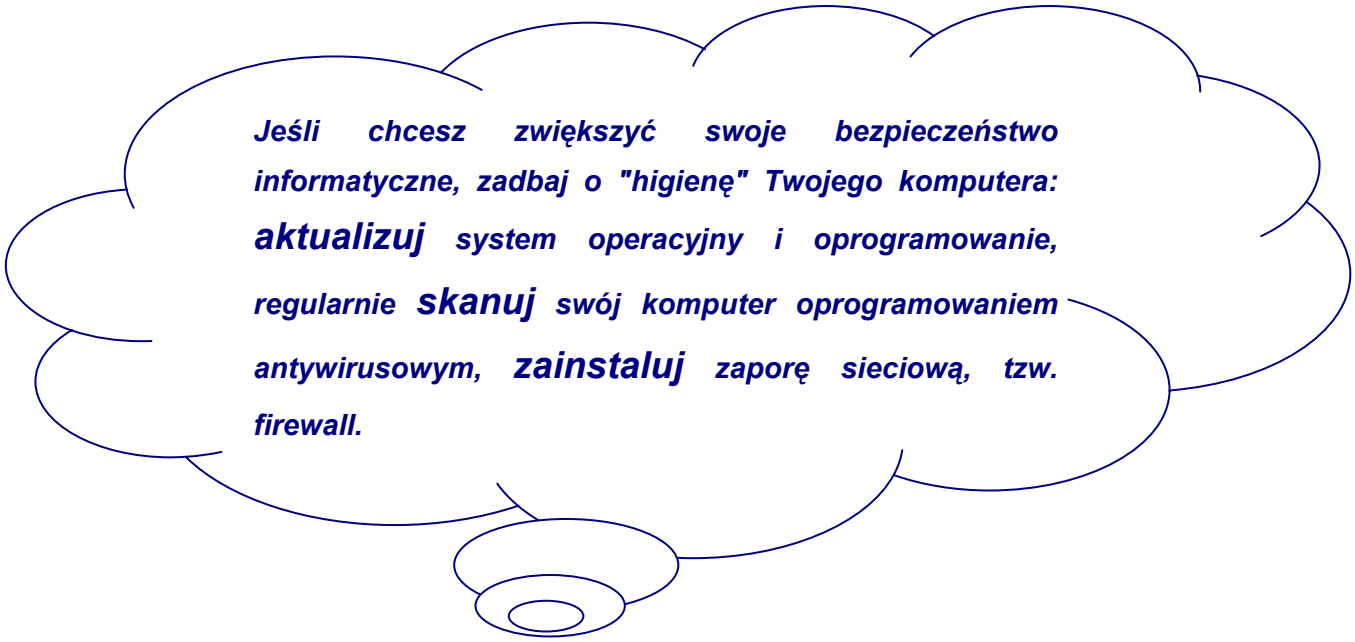
Żaden sprzedawca nie ma prawa żądać od Ciebie podania kodu PIN.

Internet

(ogólne zasady przy płatności kartą)

- Przed dokonaniem transakcji upewnij się, że transmisja danych jest szyfrowana protokołem SSL (Secure Socet Layer). Można to rozpoznać po zamkniętej kłódeczce widocznej w przeglądarce lub po początku adresu internetowego („https://" zamiast „http://"). Transmisja nieszyfrowana wiąże się z ryzykiem „podsłuchania" i wykorzystania w sposób nieuprawniony danych dotyczących Twojej karty.
- Ignoruj pocztę elektroniczną, z której wynika, że należy podać informacje o karcie - nawet w przypadku, gdy korespondencja nosi cechy podobne do korespondencji wydawcy karty. Nie należy także otwierać stron, korzystając z przesłanych w ten sposób odnośników (linków).
- Korzystaj ze sprawdzonych i pewnych komputerów. Nie dokonuj transakcji na ogólnodostępnych stanowiskach (np. w kawiarenkach internetowych), gdyż ryzyko zainstalowania oprogramowania szpiegowskiego na takich komputerach jest większe.

- Zanim skorzystasz z zakupów w mniej znanych sklepach internetowych, sprawdź ich wiarygodność (np. poprzez zapoznanie się z opiniami innych internautów).



2. Bankowość internetowa

Bankowość internetowa, która polega na świadczeniu usług i przeprowadzaniu transakcji bankowych z wykorzystaniem Internetu, może stwarzać pewne zagrożenia dla jej użytkowników. Bardzo często do różnego rodzaju oszustw dochodzi nie tyle z powodu złych zabezpieczeń systemowych, co z winy samego klienta. Poniżej przedstawiono najważniejsze zasady bezpieczeństwa, pomocne w korzystaniu z bankowości internetowej.

PO PIERWSZE BEZPIECZEŃSTWO

- Pamiętaj, że zapewnienie bezpieczeństwa transakcji internetowych nie jest działaniem jednorazowym, lecz procesem ciągłym.

- Przed rozpoczęciem korzystania z serwisu internetowego, dokładnie zapoznaj się z instrukcją obsługi systemu i wymaganiami, dotyczącymi bezpieczeństwa oraz wersją demonstracyjną systemu (zwykle dostępne na stronie internetowej banku). Kilkanaście minut poświęconych na przeczytanie tych informacji znacznie zwiększy poziom bezpieczeństwa Twoich transakcji.

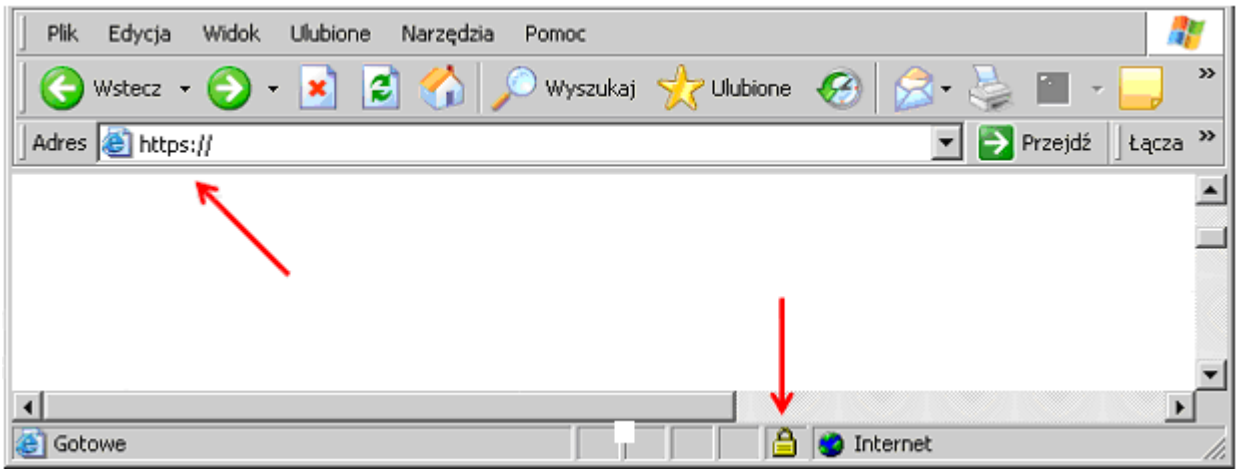
- W szczególności zapoznaj się z procesem autoryzacji dostępu do rachunku oraz sposobem autoryzacji transakcji. W przypadku jakichkolwiek wątpliwości skontaktuj się z pracownikiem banku w celu ich wyjaśnienia, ponieważ jest to najważniejszy element systemu decydujący o bezpieczeństwie Twoich pieniędzy.

- Jeżeli chcesz wykonać transakcję nie korzystaj z komputerów, do których dostęp posiada większa liczba użytkowników (np. kafejki internetowe, biblioteki, hotele, lotniska itp.).

- Podczas logowania do systemu bankowości internetowej zwróć uwagę na prawidłowość wpisanego do przeglądarki internetowej adresu witryny www.

Nigdy nie loguj się do serwisu internetowego banku poprzez linki zawarte w wiadomościach otrzymywanych pocztą elektroniczną. Nie odpowiadaj na listy elektroniczne, w których bank prosi o podanie loginu, hasła dostępu lub kodu jednorazowego oraz nie uruchamiaj linków zawartych w takim e-mailu. W przypadku otrzymania listu z zapytaniem o ww. dane, niezwłocznie powiadom o tym bank telefonicznie, mailem lub osobiście w oddziale.

- W trakcie logowania upewnij się, czy zostałeś „przekierowany" do właściwej witryny, zapewniającej połączenie zabezpieczone kryptograficznie (adres internetowy widoczny w oknie przeglądarki powinien zaczynać się od „https://www. ..." a w oknie przeglądarki powinna pojawić się ikona zamkniętej kłódki).



- Wykorzystuj zabezpieczenia udostępnione bezpłatnie przez bank - w ramach usługi internetowej możesz np. ustawić limit operacji jednorazowej i limit ogólny oraz dzienny limit transakcji wychodzących. Ustaw powiadamianie SMS o operacjach na rachunku (usługa ta w części banków jest dodatkowo płatna).

- Okresowo sprawdzaj saldo na rachunku i wyciąg z wykonanych operacji bankowych.

- W przypadku wysłania błędnego zlecenia wykonania transakcji, niezwłocznie skontaktuj się z bankiem, w celu jej zablokowania [1].

- Chroń poufność identyfikatorów, haseł i narzędzi służących do autoryzacji w systemie bankowości internetowej. To podstawa bezpieczeństwa Twoich środków na rachunku bankowym.

- W przypadku utraty narzędzia służącego do autoryzacji transakcji (lista haseł jednorazowych, karta TAN, token sprzętowy, telefon GSM z tokenem w postaci aplikacji) niezwłocznie dokonaj jego zastrzeżenia, zgodnie z procedurą ustaloną przez bank. Numer telefonu, pod którym można dokonać blokady konta internetowego zapisz w kilku łatwo dostępnych miejscach, nie tylko w pamięci telefonu komórkowego. Czas reakcji w takim przypadku odgrywa kluczową rolę. Bank przejmuje odpowiedzialność za transakcje wykonane po zgłoszeniu zastrzeżenia.

- Jeżeli bank udostępnia taką opcję, wybieraj autoryzację transakcji kodami jednorazowymi, uzyskiwanymi z tokena lub telefonu komórkowego. Historia połączeń i wiadomości SMS może stanowić dowód w przypadku sporu z bankiem. Operatorzy telefoniczni są obowiązani do przechowywania bilingów nawiązywanych połączeń i wiadomości SMS.

- Chroń papierowe listy kodów jednorazowych (karty TAN) przed osobami postronnymi, by nie dać możliwości ich skopiowania, skserowania lub sfotografowania.

- Stosuj silne hasła dostępu. To najważniejszy element systemu zabezpieczeń. Silne hasło musi spełniać warunek poufności, powinno być odpowiednio długie, zawierać małe i duże litery oraz cyfry (minimalną siłę kryptograficzną hasła wymusza zwykle system bankowy).

[1] Na podstawie art. 33 ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych (Dz. U. z dnia 11 października 2002r.) - zlecenia posiadacza dotyczące dokonania operacji przez bank mogą zostać odwołane tylko przed ich wykonaniem. W indywidualnych przypadkach istnieje jednak możliwość odzyskania błędnie przesłanych środków.

- Pamiętaj, że hasło nie może kojarzyć się bezpośrednio z użytkownikiem systemu (imię, nazwisko, marka samochodu, nr telefonu, adres miasto, ulica, itp.).

WAŻNE!

Do przeprowadzania transakcji nie wykorzystuj komputerów, do których dostęp posiada większa liczba użytkowników (np. w kafejki internetowe, biblioteki, hotele, lotniska itp.).

PO DRUGIE OSTROŻNOŚĆ

- Chroń swoją prywatność w Internecie, stosując zasadę ujawniania jedynie minimum niezbędnych informacji. Udostępnianie informacji wrażliwych na własny temat np. w portalach społecznościowych lub ogólnodostępnych komunikatorach sieciowych może ułatwić i zachęcić do podjęcia działań przestępczych.

- Do mailowego kontaktu z bankiem wykorzystuj wyłącznie pocztę elektroniczną, udostępnioną w portalu banku po zalogowaniu się do serwisu.

- W przypadku jakichkolwiek wątpliwości odnośnie witryny, z którą nawiązujesz połączenie, sprawdź jej certyfikat bezpieczeństwa. W tym celu wystarczy „kliknąć" ikonę kłódki i odczytać, dla jakiego podmiotu certyfikat cyfrowy został wydany. Powinien to być bank, z którym się łączysz. W razie wątpliwości należy sprawdzić, czy docelowa domena nie została zarejestrowana jako wyłudzająca informację (dostępna opcja przeglądarki internetowej).

- Nie zapisuj nigdy haseł, loginów ani tym bardziej „statycznych" kodów jednorazowych, służących do autoryzacji transakcji[2] na dysku komputera, dysku sieciowym ani w pamięci telefonu komórkowego lub karty SIM, ani w inny jawny sposób.

[2] Na podstawie art. 32 ww. ustawy, posiadacz jest obowiązany do nieujawniania informacji o działaniu elektronicznego instrumentu płatniczego udostępnionego w ramach umowy o usługi bankowości elektronicznej, których ujawnienie może spowodować brak skuteczności mechanizmów zapewniających bezpieczeństwo zlecanych operacji. Posiadacza obciążają operacje dokonane przez osoby, którym udostępnił informacje.

WAŻNE!

Nie stosuj hasła dostępu do konta w żadnych innych serwisach internetowych (np. Google, Skype, Facebook, Nasza-klasa, Allegro, itp.), ani w serwisach innych banków, z których korzystasz.

- Do wpisywania hasła, jeżeli to możliwe, korzystaj z klawiatury „ekranowej" (obsługiwanej myszką). Uniemożliwia to potencjalne rejestrowanie i przejęcie sekwencji znaków wprowadzonych z „klasycznej" klawiatury.
- Jeżeli system udostępnia taką opcję, włącz powiadamianie SMS o logowaniu do rachunku za pośrednictwem bankowości internetowej oraz o transakcjach wychodzących (opcja zazwyczaj płatna, w zależności od liczby wysłanych komunikatów SMS).
- Systematycznie aktualizuj system operacyjny komputera. W zabezpieczeniach systemów operacyjnych wykrywane są luki, wśród których trafiają się również te o charakterze krytycznym.
- Wyłączaj na swoim komputerze usługi systemowe, z których nie korzystasz (udostępnianie plików, serwery; ftp, telnet, www, zdalny dostęp i inne).
- Zainstaluj program antywirusowy zwłaszcza, jeżeli komputer jest wykorzystywany do gier sieciowych, przeglądania Internetu, ściągania i instalowania oprogramowania. Włącz skanowanie zasobów komputera, zwłaszcza plików zapisanych na dysku, plików otrzymywanych pocztą elektroniczną i pamięci RAM.
- Aktualizuj swoją bazę wirusów, korzystając ze strony producenta oprogramowania antywirusowego. Nieaktualny program antywirusowy może nie spełnić swojego zadania. Z dużą rezerwą stosuj skanery sieciowe oferowane przez nieznane firmy, dające możliwość darmowej kontroli antywirusowej lub przyspieszenie pracy Twojego komputera, ponieważ ich zadaniem może być infekowanie komputera szkodliwym oprogramowaniem.
- Uważnie czytaj komunikaty wyświetlane przez przeglądarkę internetową, program antywirusowy oraz zaporę internetową. Pamiętaj, aby nie zatwierdzać wyświetlanych komunikatów w sposób „mechaniczny".
- Unikaj instalowania oprogramowania z nieznanych źródeł.

- Nie ulegaj rozpowszechnianym stereotypom, według których pewne systemy operacyjne lub aplikacje są odporne na zagrożenia internetowe. Rozwiązanie, które jest bezpieczne dziś, nie musi być bezpieczne również jutro.
- Pamiętaj, że komputer, z którego wykonujesz transakcje internetowe, wymaga Twojego monitorowania.

Dla bardziej dociekliwych klientów

- Sprawdź, czy konfiguracja przeglądarki internetowej odpowiada zaleceniom banku. Zalecenia powinny być opublikowane na bankowych witrynach www. Pamiętaj, że źle skonfigurowana przeglądarka może przechowywać login i hasło dostępu do rachunku po zamknięciu sesji oraz umożliwić wykonywanie szkodliwego kodu podczas przeglądania strony www.
- Zainstaluj zaporę internetową (firewall) i sprawdź reguły filtrowania ruchu sieciowego oraz listę aplikacji, które mogą uzyskiwać połączenie z Internetem. Błędnie skonfigurowana zapora internetowa nie spełni swojej roli.
- Jeżeli system udostępnia taką opcję, przeglądaj informację o logowaniach z użyciem Twojego identyfikatora (adres IP, z jakiego nastąpiło logowanie oraz jego datę i godzinę). Przypadki poprawnego logowania, którego sam nie wykonywałeś, świadczą o przejęciu Twojego loginu i hasła przez osobę trzecią. Nr IP, z którego nastąpiło logowanie powinien być zgodny z numerem zarejestrowanym dla Twojego operatora internetowego. Właściciela zarejestrowanej domeny internetowej możesz ponadto zweryfikować w serwisach internetowych „whois”.
- Korzystaj z dostępnych opcji szyfrowania partycji dyskowej zwłaszcza tej, na której przechowywane są pliki zawierające dane wrażliwe.
- Konto administratora systemu wykorzystuj jedynie do konfiguracji komputera i zabezpieczaj je silnym hasłem. Na co dzień korzystaj z konta użytkownika.
- Wyłączaj zbędne konta użytkowników komputera a te, które są używane, zabezpieczaj hasłem.
- Korzystaj z najnowszych dostępnych wersji oprogramowania, systematycznie aktualizując system operacyjny oraz oprogramowanie przeglądarki internetowej i poczty elektronicznej.

- W procesie aktualizacji oprogramowania korzystaj wyłącznie z oficjalnych witryn producentów i legalnego oprogramowania.

PO TRZECIE WYBÓR OFERTY

- Decydując się na korzystanie z usług bankowości internetowej zacznij od właściwego wyboru dostawcy Internetu i banku świadczącego tego rodzaju usługi. Do korzystania z bankowości internetowej nie jest wymagany dostęp o wysokiej przepływności, natomiast łącze powinno być stabilne i umożliwiać zestawienie połączenia zabezpieczonego kryptograficznie (protokół https).

- Wybierz ofertę banku najbardziej dostosowaną do własnych potrzeb.

- Przeanalizuj, z jakich usług najczęściej korzystasz lub planujesz korzystać, i za które operacje płacisz najwięcej. Wszystkie systemy bankowości internetowej udostępniają podstawowe usługi bankowe (przegląd rachunku, przelewy, lokaty terminowe w zł itp.), często w pakietach, zróżnicowanych pod względem cenowym.

- Sprawdź, czy w ofercie banku są dostępne za pośrednictwem Internetu niestandardowe usługi (np. negocjowane warunki, płatności walutowe itp.), jeżeli chcesz z nich korzystać.

- Zobacz, jakie operacje będziesz mógł wykonać za pośrednictwem konta oraz sprawdź dostępność innych produktów finansowych np. lokat, kredytów, produktów inwestycyjnych.

- Zwróć uwagę, jakie prowizje pobiera bank za operacje wykonane na koncie tj. przelewy, polecenia zapłaty itp.

- Oceń ofertę kart płatniczych, za pomocą których będziesz mógł dokonywać płatności bezgotówkowych.

WAŻNE!

Nie podejmuj nierozważnych decyzji. Dokładnie porównaj dostępne oferty, zanim zdecydujesz się założyć konto.

3. Bankowość telefoniczna

Korzystając z usług bankowości telefonicznej można być narażonym na działania przestępców, którzy podszywając się pod bank, mogą próbować nas okraść. Poniżej przedstawiono kilka podstawowych zasad bezpieczeństwa, o jakich należy pamiętać korzystając z usług bankowości telefonicznej.

- Korzystaj tylko z oficjalnych numerów telefonów dostępnych na stronach internetowych banków, w oficjalnych materiałach reklamowych, na wizytówkach oraz wyciągach bankowych.
- Nie ujawniaj hasła, które ustanowiłeś samodzielnie np. do logowania lub PIN do karty kredytowej – dotyczy to także automatycznego serwisu telefonicznego czy doradcy bankowego. Możesz jedynie podawać hasło, które ustanowiłeś w obecności pracownika banku, przeznaczone bezpośrednio do kontaktu telefonicznego z bankiem (np. telekod).
- Jeżeli masz wątpliwości odnośnie osoby dzwoniącej do Ciebie i przedstawiającej się jako doradca z Twojego banku, poproś ją o podanie nazwiska i ogólnodostępnego numeru telefonu, pod który będziesz mógł zwrotnie zadzwonić, a przede wszystkim zweryfikować prawdziwość numeru np. na stronie internetowej banku.
- Ze względu na poufność przekazywania danych zapewnij sobie odpowiednie warunki do rozmowy telefonicznej z bankiem: staraj się unikać miejsc publicznych, w szczególności takich, gdzie przebywa dużo osób (środki lokomocji, ruchliwa ulica).

Jeżeli odbierzesz telefon z banku w niekomfortowych warunkach (np. w pociągu, kawiarni lub biurze, gdzie przebywają inne osoby), nie podawaj poufnych informacji, lecz poproś o kontakt doradcy w dogodnym dla Ciebie terminie.

4. Bankowość mobilna

W bankowości mobilnej do komunikacji pomiędzy klientem a bankiem wykorzystywane są telefony komórkowe, które niekiedy bywają przedmiotem kradzieży. Poniżej przedstawiono najważniejsze zasady bezpieczeństwa, o których trzeba pamiętać, korzystając z usług bankowości mobilnej.

LOGINY I HASŁA POD OCHRONĄ

- Nie ujawniaj nikomu swoich loginów i haseł, nie podawaj ich na żadnych stronach czy w odpowiedzi na żądania otrzymane e-mailem, nie wysyłaj swoich poświadczeń tożsamości jawnym tekstem SMS i w wiadomościach poczty elektronicznej.
- Nigdy nie zapisuj w pamięci telefonu wrażliwych danych (haseł, numerów kart kredytowych, PIN-ów), jawnym tekstem. Jeśli jednak musisz, użyj oprogramowania szyfrującego, dbając, by główne hasło do jego bazy było odpowiednio silne i bezpiecznie przechowywane.
- Nie pozostawiaj swojego telefonu komórkowego bez nadzoru w miejscach szczególnie narażonych na kradzież, tj. w miejscach publicznych, w szatniach czy w pokojach hotelowych.

Korzystając z WAP loguj się do systemu tylko ze strony internetowej Twojego banku. Po zalogowaniu sprawdź czy w oknie przeglądarki znajduje się symbol kłódki, oznaczający bezpieczne szyfrowanie protokołem SSL. Po zakończeniu pracy wyloguj się. Nie zostawiaj telefonu z otwartą sesją!

TELEFON ZABEZPIECZ JAK KOMUPTER

- Nie korzystaj z telefonów komórkowych nieznanego pochodzenia.
- Zainstaluj na telefonie komórkowym, którego używasz do korzystania z bankowości mobilnej, pakiet oprogramowania zabezpieczającego (skaner antywirusowy i osobista zapora sieciowa).
- Aktualizuj w miarę możliwości oprogramowanie systemowe telefonu (czasem sam producent udostępnia poprawki bezpieczeństwa i zaleca ich zainstalowanie).
- Unikaj oprogramowania z niezaufanych źródeł. Aplikacje instalowane na telefonie komórkowym powinny być podpisane cyfrowo przez dostawcę.
- W miarę możliwości okresowo sprawdzaj swój telefon komórkowy za pomocą wyspecjalizowanego sprzętu np. w celu wykrycia, czy nie zainstalowano na nim oprogramowania *spyphone.*

WAŻNE!

Jeśli musisz zdeponować swój telefon komórkowy, pamiętaj o jego uprzednim wyłączeniu.

URZĄD KOMISJI NADZORU FINANSOWEGO
Plac Powstańców Warszawy 1
00-950 Warszawa

tel. (+48 22) 262-50-00
fax (+48 22) 262-51-11 (95)
e-mail: knf@knf.gov.pl

Departament Relacji Zewnętrznych
tel. (+48 22) 262 56 66

www.knf.gov.pl