Bank Pekao

ZASADY BEZPIECZEŃSTWA DLA UŻYTKOWNIKÓW SERWISU

Sprzęt i aplikacje

✓ **Korzystaj jedynie z legalnego oprogramowania i zwracaj uwagę na instalowane oprogramowanie.**

- Korzystaj wyłącznie z legalnego oprogramowania, pochodzącego z pewnego źródła i podchodź ostrożnie do programów pobieranych z Internetu.
- Nie instaluj oprogramowania niewiadomego pochodzenia i nie uruchamiaj programów przesłanych pocztą elektroniczną lub przez komunikatory internetowe.
- Wiele darmowych programów dostępnych w Internecie zawiera funkcje wyświetlające reklamy (adware) niezależnie od czynności wykonywanych przez użytkowników. Ten rodzaj funkcji jest często instalowany wraz z oprogramowaniem na komputerach podczas przeglądania stron WWW, bez wiedzy i zgody użytkowników. Niektóre programy są również wyposażone w moduły szpiegujące (ang. spyware), które dostarczają autorom aplikacji wielu cennych informacji o użytkowniku - głównie adres IP, używany system operacyjny, przeglądarkę, a niekiedy strony, z którymi się łączymy.
- Aplikacje adware/spyware mogą umożliwić osobom niepowołanym śledzenie danych wpisywanych przez użytkownika w przeglądarce internetowej, w tym finansowych (numer klienta, PIN, numery kart płatniczych itd.), na co Bank nie ma wpływu gdyż nie kontroluje środowiska komputerowego użytkownika.
- Symptomami zainfekowania komputera są zwykle: spowolnienie działania systemu, zwiększona liczba reklam (szczególnie okienek pop-up), zmiany w działaniu przeglądarki internetowej, problemy z działaniem niektórych programów.

✓ **Regularnie aktualizuj system operacyjny i przeglądarki internetowe zainstalowane na Twoim komputerze i urządzeniach mobilnych.**

W przypadku każdego systemu operacyjnego (także mobilnych) podstawową zasadą bezpiecznego korzystania jest stała aktualizacja systemu i posiadanego oprogramowania służącego do korzystania z Internetu, przeglądarki, komunikatorów internetowych, czy programów pocztowych. Aktualizacje usuwają błędy w oprogramowaniu, które mogą być wykorzystane przez osoby trzecie w celu uzyskania naszych poufnych danych.

✓ **Zabezpiecz komputer, telefon i tablet programem antywirusowym oraz zaporą sieciową (firewall) i na bieżąco je aktualizuj.**

- Ważne jest korzystanie z programów antywirusowych zabezpieczających komputery przed szkodliwym oprogramowaniem oraz z zapory internetowej (tzw. firewall), która kontroluje przesyłanie informacji do i z Internetu zapobiegając tym samym przekazywaniu poufnych danych.
- Należy pamiętać również o odpowiedniej ochronie swojego telefonu podczas korzystania z bankowości mobilnej. Część urządzeń (telefony typu smartphone i tablety), to zaawansowane urządzenia wyposażone w system operacyjny, które należy chronić oprogramowaniem antywirusowym.

✓ **Aby korzystać z bankowości internetowej nie są potrzebne żadne certyfikaty bezpieczeństwa, Bank ich nie wysyła oraz nie prosi o ich instalacje.** Jeśli więc otrzymasz e-mail z żądaniem zainstalowania certyfikatu bezpieczeństwa w celu korzystania z bankowości internetowej, nie rób tego.

✓ **Świadomie dokonuj wyboru przeglądarki internetowej.**

- Najnowsze wersje popularnych przeglądarek, takich jak Mozilla Firefox, Chrome, Opera czy Internet Explorer zawierają wiele funkcji, np. filtr witryn wyłudzających poufne dane, które w istotny sposób chronią przed oszustwami w Internecie i podnoszą poziom bezpieczeństwa korzystania z bankowości elektronicznej. Oszustwa te, znane są jako "phishing" lub "wyłudzanie informacji". Polegają one zwykle na próbie nakłonienia nas do odwiedzenia fałszywej witryny internetowej, na której możemy być proszeni o podanie poufnych danych osobowych lub numeru karty kredytowej. Ten rodzaj kradzieży tożsamości jest od dłuższego czasu bardzo popularny.
- Pobierz wszelkie uaktualnienia przeglądarek, z których korzystasz, nieaktualne przeglądarki mogą zawierać poważne błędy; krytyczne znaczenie ma instalacja aktualnych poprawek ("łat" - ang. patch) publikowanych na stronach producentów danego oprogramowania. Zabezpieczają one przed wykorzystaniem przeglądarki bez wiedzy użytkownika i w sposób potencjalnie niebezpieczny.
- Jeśli korzystasz z Internet Explorer 7.0 koniecznie zaktualizuj tę przeglądarkę do najnowszej wersji lub zainstaluj inną nowoczesną przeglądarkę internetową.

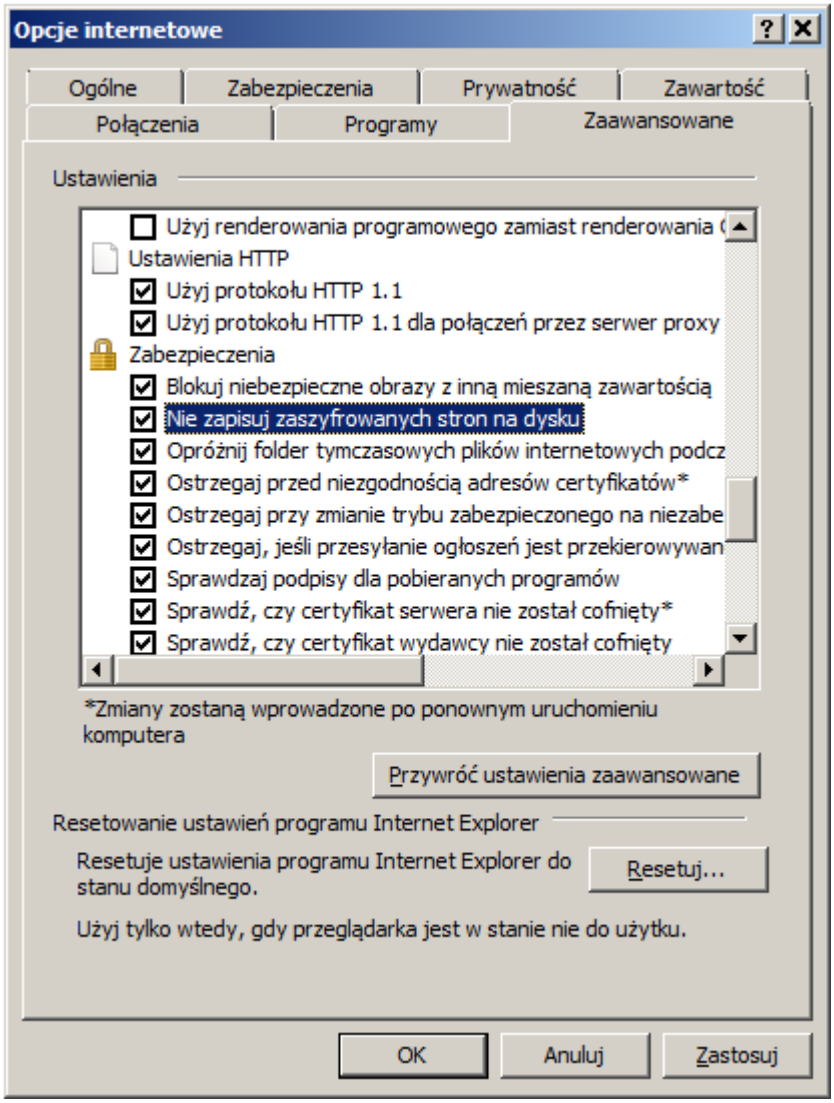
✓ **Dokonaj właściwych ustawień przeglądarki**

- w zależności od wersji przeglądarki sprawdź jak zweryfikować jej wersję i dokonać prawidłowych ustawień. Okienko z informacjami dotyczącymi numeru wersji przeglądarki zostanie wyświetlone, jeśli wybierzesz:
  - **MS Internet Explorer**: Pomoc --> Internet Explorer - Informacje.
  - **Firefox:** Pomoc -->O Mozilli Firefox.
  - **Chrome:** Menu ---> Google Chrome – informacje.
  - **Opera:** Pomoc --> O Operze

- Ustaw pamięć podręczną przeglądarki

  W pamięci podręcznej przeglądarki (cache) przechowywana jest zawartość odwiedzanych stron internetowych. Mogą więc znaleźć się w niej ważne, poufne informacje dotyczące np. stanu rachunków czy operacji wykonywanych przez użytkownika. Ważne jest zatem takie skonfigurowanie przeglądarki, aby informacje dotyczące odwiedzonych stron szyfrowanych - takich jak strona serwisu XelionInternet nie były przez nią przechowywane. W przeglądarkach Mozilla Firefox domyślnie ustawiona jest opcja niezapisywania stron szyfrowanych na dysku.

W zależności od używanej przeglądarki, pamięć podręczną należy ustawić w następujący sposób:
Przeglądarka MS Internet Explorer
W menu NARZĘDZIA wybierz: Opcje internetowe / Zaawansowane / Zabezpieczenia i zaznacz opcję "Nie zapisuj stron szyfrowanych na dysku".



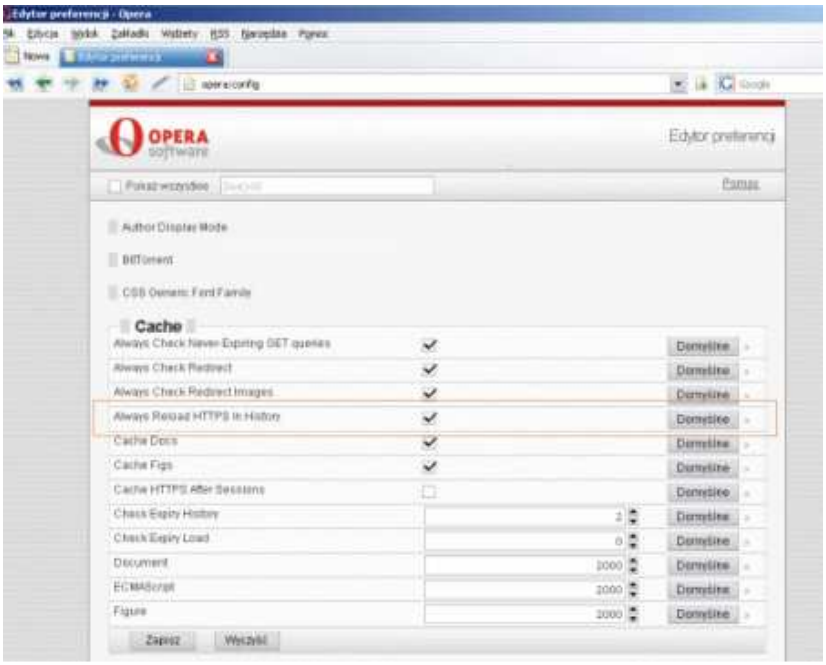
UWAGA!
Zaznaczenie opcji "Nie zapisuj zaszyfrowanych stron na dysku" powoduje brak możliwości pobrania plików PDF z serwisu XelionInternet. Dla tej przeglądarki zalecamy nie zaznaczać tej opcji i po każdym wylogowaniu z serwisu transakcyjnego, ze względów bezpieczeństwa, czyścić dane historii i przeglądania.

W menu NARZĘDZIA wybierz: Opcje internetowe / Ogólne / Historia przeglądania / Usuń, a następnie wybierz klawisz: "Usuń...". Dodatkowo w ustawieniach dotyczących tymczasowych plików internetowych konieczne zaznacz opcję: "Sprawdzaj czy są nowsze wersje przechowywanych stron: przy każdej wizycie na tej stronie".

W menu NARZĘDZIA wybierz: Opcje internetowe / Zabezpieczenia / Poziom zabezpieczeń dla tej strefy / Poziom niestandardowy / Wykonywanie aktywnych skryptów / Włącz.

Przeglądarka Opera

W pasku adresu wybierz opera: config, następnie wybierz "Cache", zaznacz opcję "Always Reload HTTPS In History" i zatwierdź poprzez kliknięcie przycisku "Zapisz".



- Usuń informacje z pamięci podręcznej (cache) / Tymczasowe pliki internetowe.
  W menu NARZĘDZIA wybierz: Preferencje / Zaawansowane / Historia, po czym wybierz opcję "Opróżnij teraz".
  W menu NARZĘDZIA wybierz: Szybka konfiguracja / Włącz obsługę języka JavaScript.

Firefox
W menu NARZĘDZIA wybierz: Opcje / Treść / Włącz obsługę języka JavaScript.

✓ **Ustaw hasło używając routera lub domowej sieci bezprzewodowej (wi-fi - np. live box)**
Używając routera lub domowej sieci bezprzewodowej (wi-fi - np. live box) ustanów własne, bezpieczne i trudne do złamania hasło do tych urządzeń. Urządzenia te mają zazwyczaj proste, fabrycznie ustawione hasło, chroniące dostęp do ich panelów administracyjnych. Dzięki znajomości takiego hasła osoba działająca z zewnątrz może zmienić ustawienia routera, co może skutkować przekierowaniem na strony stworzone w celu kradzieży poufnych danych lub dystrybuujących szkodliwe oprogramowanie.

✓ **Warunkiem korzystania z Serwisu jest posiadanie wyposażenia technicznego i oprogramowania niezbędnego do poprawnego funkcjonowanie usługi, tj. korzystanie z serwisu.**
- **TeleXelion** - wymaga posiadania aparatu telefonicznego (w przypadku serwisu automatycznego - z wybieraniem tonowym),
- **XelionSMS** - wymaga posiadania telefonu komórkowego,
- **XelionInternet** - wymaga posiadania dostępu do Internetu.

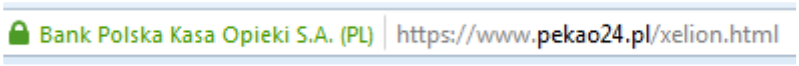
Bank Pekao

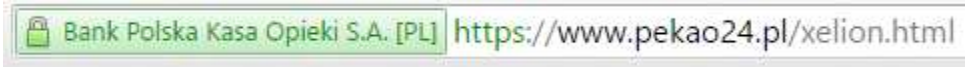
Ochrona poufnych danych

- ✓ **Loguj się wyłącznie osobiście. Chroń dane do logowania i autoryzacji do Serwisu, dbaj o ich poufność, nie wolno ich udostępniać osobom trzecim. Powinny być one przechowywane z zachowaniem należytej staranności. Ujawnienie tych danych innym osobom czy instytucjom stanowi naruszenie Regulaminu Rachunki wkładów oszczędnościowych Xelion Banku Pekao S.A. dla osób fizycznych.**
- ✓ **Chroń swój numer klienta i hasło.**
  - Dbaj o poufność danych do logowania w serwisach Xelion, **loguj się wyłącznie osobiście**. Ujawnienie tych danych innym osobom czy instytucjom stanowi naruszenie Regulaminu Rachunki wkładów oszczędnościowych Xelion Banku Pekao S.A. dla osób fizycznych.
  - **Podczas kontaktów telefonicznych Bank nigdy nie prosi o podanie numeru PIN do serwisu**. Logowanie do usług telefonicznych odbywa się **ZAWSZE** w serwisach automatycznych.
  - **Bank nigdy nie prosi o podanie pełnego hasła do serwisu internetowego.**
  - **Bank nigdy nie prosi o podanie podczas logowania kodów (z karty kodów jednorazowych, kodów SMS)**
  - Jeżeli uważasz, że musisz zapisać numer klienta, PIN, lub hasło zrób to tak żeby osoba niepowołana nie mogła tych informacji poprawnie zidentyfikować.
  - Jeśli więc ktokolwiek poprosi o powyższe dane nie podawaj tych danych.
  - **Regularnie zmieniaj hasło w serwisie internetowym**. Bezpieczne hasło powinno składać się z wielkich i małych liter, cyfr i znaków specjalnych (np. ?, #, @, &) i nie powinno być słowem występującym w słowniku, ani hasłem używanym w innych serwisach internetowych. Zmieniaj PIN oraz hasło co miesiąc.
  - Pamiętaj również, że Bank nigdy nie prosi o przesłanie takich danych pocztą elektroniczną.
  - Jeżeli do autoryzacji operacji w serwisie XelionInternet używasz kodów SMS, zawsze sprawdzaj czy wiadomość SMS z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją. Zwróć szczególną uwagę na:
    - **numer rachunku** - sprawdź czy odpowiada on rachunkowi odbiorcy wykonywanej operacji (Pamiętaj! SMS z kodem autoryzacyjnym zawiera jedynie dwie pierwsze i cztery ostatnie cyfry numeru rachunku),
    - **kwotę operacji** - musi być ona zgodna z tą, która została podana w dyspozycji.
  - Pamiętaj także, że podczas logowania do XelionInternet Bank nigdy nie prosi o podanie kodów z karty kodów jednorazowych.
  - Nie odpowiadaj na wiadomości pochodzące od niezaufanych nadawców, zawierające oferty dotyczące pośredniczenia w przekazywaniu płatności drogą internetową. Mają one zazwyczaj na celu wykorzystanie rachunków bankowych do przekazywania środków pochodzących z kradzieży, co może wiązać się z pociągnięciem do odpowiedzialności karnej.
  - Bądź czujny, a w przypadku jakichkolwiek wątpliwości skontaktuj się z konsultantem TeleXelion (801 350 350) lub Infolinii (801 370 370), którzy poradzą jak w danej sytuacji się zachować.
  - Pamiętaj również, aby bezpiecznie wylogować się z serwisu XelionInternet. W pierwszej kolejności kliknij na przycisk "Wyloguj się", a dopiero później zamknij okno przeglądarki internetowej.
- ✓ **Nie podawaj poufnych informacji na stronach przypominających swoim wyglądem strony Banku.**
  - Nie podawaj kodów jednorazowych, loginu i hasła oraz numeru telefonu na nieznanych stronach.
  - Korzystając z usługi Serwisu, przestrzegaj podstawowych zasad bezpieczeństwa:
    - Loguj się wyłącznie poprzez stronę www.xelion.pl lub www.pekao24.pl/xelion.html. Przed zalogowaniem do XelionInternet zawsze sprawdź, czy połączenie jest szyfrowane (adres strony zaczyna się wtedy od https) oraz czy w przeglądarce jest widoczny symbol kłódki.
    - Nie używaj do logowania adresu ani linku otrzymanego przez e-mail lub komunikator internetowy. Bank nigdy nie wysyła takich wiadomości. Tego typu korespondencję należy traktować jako próbę oszustwa polegającego na wyłudzeniu poufnych danych przez osoby podszywające się pod instytucję finansową.
    - Nie korzystaj z serwisów realizujących płatności, które wymagają ujawnienia numeru klienta, hasła czy kodu do autoryzacji operacji. Udostepnienie ich może pozwolić osobom trzecim na nieuprawniony dostęp do usługi Serwisu, zmianę Twoich danych lub wykorzystanie ich do celów przestępczych. Pamiętaj również, że ujawnienie danych niezbędnych do logowania lub autoryzacji jest niezgodne z Regulaminem Rachunki wkładów oszczędnościowych Xelion Banku Pekao S.A. dla osób fizycznych i może skutkować blokadą usługi.
    - Zapoznaj się z komunikatem Związku Banków Polskich, dostępnym pod adresem http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci, na temat ujawniania informacji wrażliwych serwisom oferującym szybkie płatności.
- ✓ **Nie używaj do logowania adresu lub linku podesłanego w wiadomości e-mail lub SMS, jeśli nie jesteś pewien ich źródła. Zachowaj ostrożność i ograniczone zaufanie w stosunku do wiadomości e-mail pochodzących od nieznanych nadawców. Zalecamy nie odpowiadać na takie wiadomości i nie otwierać przesłanych załączników lub linków.**
- ✓ **Nie ufaj nadawcy wiadomości e-mail.Oszuści mogą spreparować wiadomość tak, by sprawiała wrażenie, że wysłała ją osoba, lub instytucja, której ufasz.**
- ✓ **Sprawdzaj certyfikaty zabezpieczeń**.
  - Po zalogowaniu do serwisu **sprawdź, czy na ekranie widnieje symbol kłódki** oznaczający, nawiązanie połączenia szyfrowanego (**adres zaczyna się wtedy od https a nie od http**).
  - Jeżeli znajdziesz symbol kłódki, kliknij na niego dwa razy, aby sprawdzić, **czy wyświetlony certyfikat jest ważny i czy został wydany dla Banku Polska Kasa Opieki S.A. oraz adresu www.pekao24.pl**
  - Prawidłowy certyfikat powinien zawierać:
    - wystawcę: **Symantec Corporation**,
    - typ certyfikatu: **Symantec Class 3 EV SSL,**

- jednostkę organizacyjną: **Symantec Trust Network**.
  - ważność certyfikatu: **od dnia 2016-07-13 do 2018-07-28** (wg stanu na dzień 21 października 2016 r).
- **Pamiętaj także, że Bank nigdy nie wysyła żadnych certyfikatów bezpieczeństwa poprzez wiadomość SMS.**
- Zaletą rozszerzonego certyfikatu jest jednoznaczna identyfikacja podmiotu, na rzecz którego certyfikat został wystawiony, czyli w tym przypadku naszego Banku. W nowoczesnych przeglądarkach internetowych informacja taka jest prezentowana na zielonym tle w pasku adresu.
- Jeśli symbol kłódki jest niewidoczny lub jeśli certyfikat został wystawiony dla innego adresu, nie korzystaj z serwisu - w takiej sytuacji niezwłocznie skontaktuj się z konsultantem TeleXelion.
- Symbole kłódki prezentowane są w górnej części ekranu, obok adresu strony i w zależności od rodzaju przeglądarki wyglądają tak:

Internet Explorer 

Firefox 

Chrome 

Opera 

✓ **Nie korzystaj z Internetu w miejscach publicznie dostępnych**
- Korzystając z Internetu nie loguj się do serwisu transakcyjnego XelionInternet z miejsc ogólnie dostępnych, takich jak kafejki internetowe, nie otwieraj załączników przesłanych pocztą elektroniczną lub poprzez komunikatory internetowe od nieznanych osób. Często złodzieje i inne osoby niepowołane, rozsyłają za pośrednictwem poczty elektronicznej specjalnie spreparowane programy (konie trojańskie), których ukrytym zadaniem jest szpiegowanie działalności użytkowników. W momencie, gdy ofiara łączy się ze stroną internetową banku, trojan uaktywnia się i rozpoczyna zapisywanie danych wprowadzanych przez użytkownika z klawiatury. Dane te są następnie przesyłane wprost do osób niepowołanych.
- Obsługując serwis transakcyjny XelionInternet, korzystaj tylko z jednego okna przeglądarki, po zakończeniu korzystania z serwisu transakcyjnego lub w razie konieczności oddalenia się od komputera bezwzględnie zakończ pracę w serwisie transakcyjnym używając opcji "Wyloguj" dostępnej w prawym górnym rogu strony.
- Ponadto sprawdzaj datę ostatniego logowania do systemu; jest ona prezentowana po zalogowaniu do serwisu XelionInternet w sekcji "Ustawienia". Dodatkowo dostęp do rejestru zdarzeń jest możliwy z poziomu każdej strony, na której się znajdujesz poprzez wybór linku zamieszczonego na samym dole "Zobacz rejestr zdarzeń".

✓ **Włącz ochronę anty-phishingową w przeglądarce**
- Nie ignoruj ostrzeżeń - 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, które pozwalają ograniczyć ryzyko kradzieży poufnych danych.
- Aby włączyć ochronę anty-phishingową w przeglądarce:

  Internet Explorer

  Wejdź w Narzędzia - Filtr witryn wyłudzających informacje i wybierz opcję "Włącz automatyczne sprawdzanie sieci Web".

  Firefox

  Wejdź w Narzędzia - Opcje - Bezpieczeństwo i zaznaczyć opcje: Ostrzegaj, jeśli witryny próbują zainstalować dodatki; Blokuj witryny zgłoszone jako stwarzające zagrożenie oraz Blokuj witryny zgłoszone jako próby oszustwa internetowego.

  Opera 9.1x

  Wejdź w Narzędzia - Preferencje - Zaawansowane - Bezpieczeństwo, a następnie zaznaczyć opcję: "Włącz ochronę przed oszustwami i złośliwym oprogramowaniem".

✓ **Pamiętaj, Bank nigdy nie będzie:**
- przekazywał poufnych informacji dotyczących korzystania z bankowości elektronicznej i zmian w procedurach bezpieczeństwa w wiadomościach e-mail wysyłanych na prywatne skrzynki e-mail;
- prosił o podanie nazwy producenta, modelu i numeru telefonu do XelionSMS podczas logowania do serwisu internetowego.
- prosił o wykonywanie w ramach testów przelewów lub innych operacji związanych z usługą Serwisu.

Autoryzacja operacji w usłudze Serwisu.

✓ **Niektóre operacje wykonywane w usłudze Serwisu wymagają dodatkowej autoryzacji. Wybierz metodę autoryzacji dostosowaną do swoich potrzeb. Metodę autoryzacji można w każdej chwili zmienić.**
- Niektóre operacje wykonywane w usłudze Serwisu m.in. przelewy zewnętrzne na rachunki, które nie zostały wcześniej zdefiniowane u konsultanta TeleXelion lub w XelionInternet wymagają dodatkowej autoryzacji.
- **W zależności od preferencji mogą być one akceptowane:**
  - kodem SMS,
  - kodem z karty kodów jednorazowych.

  Wybraną metodę autoryzacji można w każdej chwili zmienić:
  - u konsultanta TeleXelion pod numerem 801 350 350,

- w serwisie XelionInternet (w zakładce "Ustawienia").

  Operacja wymaga potwierdzenia dotychczas wykorzystywaną metodą autoryzacji. W przypadku zmiany sposobu akceptacji z karty kodów jednorazowych na kody SMS w serwisie XelionInternet operacja ta jest dodatkowo potwierdzana kodem SMS. Szczegółowy wykaz operacji wymagających akceptacji kodem kodem SMS/ kodem jednorazowym jest dostępny w *Wykazie funkcji serwisów Xelion* dostępnym na stronie www.xelion.pl.

- ✓ **W bankowości elektronicznej XelionInternet możesz zlecać przelewy krajowe i zagraniczne, w tym przelewy walutowe SEPA. Po wypełnieniu odpowiedniego formularza przelewu zawsze sprawdź poprawność wprowadzonych danych. Jeżeli są poprawne to zaakceptuj przelew zgodnie z używaną metodą autoryzacji. Po zaakceptowaniu otrzymasz informację o przyjęciu przelewu do realizacji.** Dokładny opis realizacji przelewu znajdziesz w *Przewodniku po usłudze Serwis* dostępnym na www.xelion.pl
- ✓ **W celu dodatkowej weryfikacji konsultant TeleXelion ma prawo zadać pytania dotyczące danych osobowych, które zostały udostępnione Bankowi, konsultant dzwoni wówczas na numer telefonu wskazany w Umowie jako numer do oddzwonienia. Moment dokonania poprawnej dodatkowej weryfikacji operacji traktowany jest jako moment autoryzacji, określający termin otrzymania przez Bank zlecenia do realizacji.**
- ✓ **W przypadku podania błędnych danych służących do dodatkowej weryfikacji, operację uznaje się za niezłożoną, o czym zostaniesz poinformowany już w trakcie rozmowy.**
- ✓ **Nie ma możliwości odwołania operacji po dokonaniu jej autoryzacji, za wyjątkiem przelewów z datą przyszłą lub cyklicznych, które mogą być odwołane najpóźniej do końca dnia poprzedzającego dzień realizacji wynikający z określonego cyklu lub przyszłej daty realizacji.**

  Szczegółowy opis procesu realizacji przelewów znajdziesz w *Przewodniku po usłudze Serwis* dostępnym na www.xelion.pl
- ✓ **Jeżeli przyczyna odmowy wykonania zlecenia jest zależna od Banku, poinformujemy Cię niezwłocznie o odmowie wykonania zlecenia podając powód oraz procedurę sprostowania błędów stanowiących przyczynę odmowy:**
  - pocztą wewnętrzną serwisu internetowego XelionInternet, lub
  - wiadomością na przekazany Bankowi adres e-mail (jeśli będziesz korzystał z serwisu internetowego XelionInternet), lub
  - wiadomością SMS – na podany numer telefonu do kontaktu (jeśli nie będziesz korzystać z serwisu internetowego XelionInternet i nie podałeś adresu e-mail), lub
  - przesyłką pocztową (o ile powiadomienie nie będzie możliwe w żaden z powyżej wskazanych sposobów).
- ✓ **W przypadku autoryzacji kodami SMS zawsze sprawdzaj czy wiadomość z kodem autoryzacyjnym jest zgodna z wykonywaną przez Ciebie operacją.**

Utrata lub kradzież danych do logowania i autoryzacji w serwisach

W przypadku utraty lub podejrzenia utraty wyłącznej kontroli nad danymi do logowania lub kontroli nad urządzeniami do generowania kodów jednorazowych, ich kradzieży lub nieuprawnionego użycia (podejrzenia nieuprawnionego użycia) powinieneś niezwłocznie:

- zablokować usługę Serwisu w serwisie internetowym lub dokonać zmiany odpowiednio właściwego PIN lub hasła lub metody autoryzacji, lub
- skontaktować się z konsultantem TeleXelion pod numerami 801 350 350; +48 42 683 83 50 lub Infolinii 801 370 370; +48 42 683 83 70 (opłaty wg cennika operatora), w celu zablokowania dostępu do usługi Serwis lub anulowania danych do logowania i autoryzacji zleceń, lub
- zgłosić ten fakt u swojego Doradcy Finansowego.

Bezpieczeństwo kart płatniczych

Wszystkie karty wydawane przez Bank umożliwiają dokonywanie płatności w Internecie
Poniżej prezentujemy elementy bezpieczeństwa transakcji kartą w Internecie:

- ✓ **3D Secure**

  Zabezpieczenie polega na dodatkowym potwierdzeniu realizowanej transakcji internetowej w systemie Banku.

  W celu realizacji płatności kartą za towary lub usługi u akceptantów internetowych należy podać następujące dane: imię i nazwisko Posiadacza/ Użytkownika karty, numer karty i datę jej ważności, a także kod CVV2/CVC2 z rewersu karty jeśli jest wymagany:

  - po zaakceptowaniu płatności jesteś kierowany na stronę internetową Banku - zatytułowaną "Potwierdzenie transakcji kartą",
  - następnie potwierdzasz realizację płatności kodem SMS, który Bank przesyła na podany wcześniej numer telefonu komórkowego.

  Dlaczego warto korzystać z zabezpieczenia 3-D Secure?

  3-D Secure to:

  - dodatkowe bezpieczeństwo - jesteś identyfikowany nie tylko na podstawie numeru karty, daty jej ważności i CVV2/CVC2, ale także w oparciu o kody SMS,
  - standard zabezpieczenia płatności kartami w Internecie, bez którego transakcja może zostać odrzucona,
  - możliwość płacenia w Internecie za zakupy i usługi kartą Maestro.

    Dodatkowe informacje dostępne są pod numerem infolinii 801 324 324 (opłata wg cennika operatora).

- ✓ **Limity dla transakcji dokonywanych bez fizycznego użycia karty**
  - Dzienny albo miesięczny limit takich transakcji możesz ustalić odrębnie dla każdej karty - w kwocie lub/i liczbie transakcji - dzwoniąc pod czynny całodobowo numer infolinii Banku: 801 324 324 (opłaty według cennika operatora) lub odwiedzając dowolną placówkę Banku.
  - Ustalając własne limity masz od razu pewność, że żadna transakcja przekraczająca te limity nie zostanie zrealizowana, niezależnie od tego czy zabezpieczenie 3D Secure zostało wykorzystane czy nie.
  - Przypominamy, że przed ustaleniem limitów transakcje realizowane są do wysokości dostępnego limitu karty kredytowej albo środków dostępnych na rachunku, jeśli transakcja odbywa się z użyciem karty debetowej.
- ✓ **Kod CVV2 / CVC2**
  O jego podanie możesz zostać poproszony podczas dokonywania zakupu na etapie wpisywania danych karty, takich jak numer czy data ważności. Ten trzycyfrowy kod zapisany jest wyłącznie na rewersie karty a jego weryfikacja pozwala sprawdzić, czy osoba podająca dane rzeczywiście jest w posiadaniu karty.
- ✓ **O czym pamiętać dokonując płatności kartą w Internecie**
  - Nigdy nie podawaj numeru karty, daty jej ważności lub kodu CVV2/CVC2 osobom nieuprawnionym oraz nie odpowiadaj na maile z pytaniem o te dane.
  - Dokonując zakupów w Internecie korzystaj z zaufanych serwisów. Zawsze sprawdzaj certyfikaty zabezpieczeń oraz czy strona, na której podajesz dane karty jest szyfrowana (adres rozpoczynający się od https:// oraz występuje symbol kłódki lub zielone pole).
  - Dbaj o bezpieczeństwo karty. W przypadku jej zagubienia, kradzieży, przywłaszczenia lub uzasadnionego podejrzenia, że dane takie jak numer karty czy kod PIN poznały osoby nieuprawnione, a także wtedy, gdy nastąpiło nieuprawnione użycie karty - **niezwłocznie powiadom o tym Bank i zastrzeż kartę**. W tym celu zadzwoń pod czynny całodobowo numer infolinii kartowej Banku +48 (42) 683 83 16 lub 800 120 016 (opłaty wg cennika operatora), lub numer infolinii uruchomionej przez Związek Banków Polskich +48 828 828 828.

Postępowanie w przypadku wystąpienia lub podejrzenia wystąpienia nadużycia

Powiadom niezwłocznie Bank w przypadku stwierdzenia lub podejrzenia dokonania nieautoryzowanych transakcji na rachunku. Informuj o wszystkich podejrzanych zdarzeniach i nietypowych sytuacji zauważonych w trakcie korzystania z usług bankowości internetowych oraz o potencjalnych próbach ataków socjotechnicznych mających na celu np. wyłudzenie Twoich danych.

Jako próbę wyłudzenia poufnych danych należy traktować również wiadomości e-mail nakłaniające do ujawnienia informacji służących do logowania lub autoryzacji, danych umożliwiających bezpieczne korzystanie z usługi Serwisu lub zawierającej linki do strony logowania, a także danych dotyczących kart płatniczych.

Pamiętaj, że w każdej chwili możesz zawiesić lub ograniczyć funkcjonalności płatności internetowych. Wystarczy, że zmniejszysz dzienny lub miesięczny limit transakcji wykonywanych w Serwisie czy też transakcji kartą płatniczą

W przypadku jakichkolwiek pytań lub wątpliwości wyślij wiadomość w poczcie wewnętrznej serwisu internetowego XelionInternet, a w razie potrzeby niezwłocznie skontaktuj się z konsultantem TeleXelion pod numerami 801 350 350; +48 42 683 83 50 lub Infolinii 801 370 370; +48 42 683 83 70 (opłaty wg cennika operatora), który poradzi jak w danej sytuacji się zachować, kontakt jest możliwy przez całą dobę. Każde zgłoszenie będzie poddane szczegółowej analizie, o jej wyniku będziesz poinformowany w wybrany przez Ciebie sposób (np. pisemnie, telefonicznie, pocztą wewnętrzną w serwisie XelionInternet).

Ostrzeżenia o zagrożeniach dla bankowości elektronicznej

Uważnie czytaj komunikaty dotyczące bezpieczeństwa umieszczone na stronie logowania, ekrany prezentowane bezpośrednio po zalogowaniu do serwisu internetowego XelionInternet oraz wiadomości w poczcie wewnętrznej. Będziesz w nich informowany o aktualnych zagrożeniach czy możliwych próbach ataków socjotechnicznych. W sprawach dotyczących np. nieuprawnionego dostępu do XelionInternet czy podejrzenia realizacji transakcji oszukańczych, Bank może również skontaktować się z Tobą telefonicznie.

W przypadku powzięcia przez Bank informacji, iż dane niezbędne do logowania lub autoryzacji transakcji znalazły się w posiadaniu osoby trzeciej dostęp do usługi Serwisu może zostać niezwłocznie zablokowany. Zostaniesz o tym poinformowany w czasie próby zalogowania, telefonicznie na telefon do oddzwonienia lub pisemnie. Informację o przyczynie zablokowania usługi Serwisu będziesz mógł uzyskać również w jednostce Banku.