BEZPIECZEŃSTWO SERWISU ONEY24.PL

Spis treści

Ogólne zasady bezpieczeństwa korzystania z Internetu

- Zalecamy, by na komputerze były zainstalowane i uruchomione aktualne wersje:
  - **oprogramowania antywirusowego** posiadającego aktualną bazę sygnatur wirusów,
  - **osobistej zapory** (ang. personal firewall) posiadającej uaktualnione polisy i reguły,
  - oprogramowania **wykrywającego** m.in. **spyware**, spam itp.

- Należy **regularnie aktualizować** posiadany **system operacyjny** oraz używane aplikacje (w szczególności przeglądarki internetowe, wtyczki flash, klientów poczty, przeglądarki pdf itp.), tj. instalować okresowo publikowane przez producentów poprawki korygujące luki i błędy zarówno systemu operacyjnego, jak i oprogramowania.

- Zaleca się zachowywać dużą **dozę ostrożności** podczas **pobierania jakichkolwiek plików z Internetu** czy otwierania załączników do wiadomości e-mail bez względu na to, od kogo one pochodzą.
- **Nie zaleca się instalować** nieznanych programów otrzymanych pocztą elektroniczną lub pobranych z niezaufanych witryn www.
- Zaleca się korzystanie z najnowszych wersji przeglądarek internetowych.

Bezpieczeństwo przeglądarek

Wybierz przeglądarkę internetową, której używasz i zapoznaj się z rekomendowanymi przez Oney Polska S.A. ustawieniami bezpieczeństwa.

Oney Polska S.A. rekomenduje używanie najnowszej dostępnej wersji oprogramowania oraz przeprowadzania ich okresowych aktualizacji.

Używanie nieaktualnych wersji jest niebezpieczne

Bezpieczeństwo przeglądarek

Zalecana konfiguracja przeglądarki Mozilla Firefox

Ustawienia wymagane

Menu Firefox > menu Opcje > Opcje:
panel Prywatność > sekcja Historia – z listy rozwijanej wybrać: Program Firefox będzie używał ustawień historii użytkownika – zaznaczyć: Akceptuj ciasteczka
panel Treść > zaznacz: Włącz obsługę języka JavaScript
panel Zaawansowane > Szyfrowanie – zaznacz:

- Włącz obsługę SSL 3.0
- Włącz obsługę TLS 1.0

Więcej o ustawieniach przeglądarki Firefox na stronie producenta.
Istnieją dodatki rozszerzające możliwości przeglądarki Firefox, w tym również wpływające na poprawę bezpieczeństwa korzystania z sieci.

Bezpieczeństwo

Podczas korzystania z serwisu internetowego przeglądarka Opera oraz starsze wersje przeglądarki Firefox (3.x) zapisują w pamięci komputera informacje, które mogą być widoczne nawet po prawidłowym wylogowaniu z serwisu internetowego i zakończeniu sesji. Używając przycisku „Powrót do poprzedniej strony", osoba niepowołana może uzyskać wgląd w odwiedzane przez nas poprzednio ekrany, a co za tym idzie może zobaczyć dane wyświetlone wcześniej w odwiedzonych stronach serwisu internetowego. Należy jednak podkreślić, że w takiej sytuacji osoba niepowołana **nie ma możliwości wykonania żadnej operacji na koncie**. Aby uniknąć opisanego problemu, należy wraz z prawidłowym zakończeniem sesji serwisu internetowego (wylogowanie) dodatkowo **zamknąć zakładkę lub okno, w którym był wyświetlany**. Niemniej, podczas korzystania z serwisu internetowego nie rekomendujemy używania wspomnianych przeglądarek na komputerach dostępnych większemu gronu użytkowników.

Bezpieczeństwo przeglądarek

Zalecana konfiguracja przeglądarki Google Chrome

Ustawienia wymagane

Ustawienia Google Chrome > Opcje:

- zakładka Dla zaawansowanych > sekcja Prywatność > Ustawienia treści > sekcja JavaScript – zaznacz: Zezwalaj na wykonywanie kodu JavaScript w witrynach (zalecane)
- zakładka Dla zaawansowanych > sekcja Prywatność > Ustawienia treści > sekcja Pliki Cookie – zaznacz: Zezwalaj na przechowywanie danych lokalnie (zalecane)
- zakładka Dla zaawansowanych > sekcja HTTPS/SSL – zaznacz: Sprawdź datę ważności certyfikatu serwera

Więcej o zaawansowanych ustawieniach przeglądarki Chrome na stronie producenta.
Istnieją dodatki rozszerzające możliwości przeglądarki Chrome, w tym również wpływające na poprawę bezpieczeństwa korzystania z sieci.

Bezpieczeństwo przeglądarek

Zalecana konfiguracja przeglądarki Internet Explorer

Zalecamy stosowanie przeglądarki Internet Explorer w wersji nie starszej niż 7.0

Ustawienia wymagane

Menu Narzędzia > Opcje internetowe:

- zakładka Ogólne – sekcja Historia przeglądania > Ustawienia – sekcja Tymczasowe pliki internetowe – zaznacz: Za każdym razem gdy odwiedzam tę stronę
- zakładka Zabezpieczenia – strefa Internet – Poziom zabezpieczeń dla tej strefy – wybierz: Poziom niestandardowy > lista Ustawień – sekcja Obsługa skryptów – Wykonywanie aktywnych skryptów – zaznacz: Włącz
- zakładka Prywatność – sekcja Ustawienia – Zaawansowane – zaznacz: Zastąp automatyczną obsługę plików cookie, w sekcji Pliki Cookie tej samej firmy – zaznacz: Zaakceptuj oraz opcję: Zawsze zezwalaj na pliki cookie dotyczące sesji
- zakładka Zaawansowane – lista Ustawień – sekcja Zabezpieczenia – zaznacz:
  - Nie zapisuj zaszyfrowanych stron na dysk (dla IE 7.0, IE 8.0)
  - Ostrzegaj przed niezgodnością certyfikatów
  - Sprawdź, czy certyfikat serwera nie został cofnięty
  - Użyj SSL 3.0 (opcja Użyj SSL 2.0 powinna być odznaczona!)
  - Użyj TLS 1.0
- zakładka Ogólne – sekcja Historia przeglądania – zaznacz: Usuń historię przeglądania przy zakończeniu

Więcej o ustawieniach przeglądarki Internet Explorer na stronie producenta.

Bezpieczeństwo przeglądarek

Zalecana konfiguracja przeglądarki Opera

Ustawienia wymagane

Menu Opera > menu Ustawienia > Preferencje:

- zakładka Zaawansowane > Zawartość – zaznacz: Włącz obsługę JavaScript
- zakładka Zaawansowane > Ciasteczka – zaznacz: Akceptuj ciasteczka tylko z witryny, którą odwiedzam
- zakładka Zaawansowane > Bezpieczeństwo > Protokoły zabezpieczające... > zaznacz:
  - Włącz obsługę SSL 3
  - Włącz obsługę TLS 1

Więcej o zaawansowanych ustawieniach przeglądarki Opera na stronie producenta.
Istnieją dodatki rozszerzające możliwości przeglądarki Opera, w tym również wpływające na poprawę bezpieczeństwa korzystania z sieci.

Bezpieczeństwo przeglądarek internetowych

Podczas korzystania z serwisu internetowego przeglądarka Opera oraz starsze wersje przeglądarki Firefox (3.x) zapisują w pamięci komputera informacje, które mogą być widoczne nawet po prawidłowym wylogowaniu z serwisu internetowego i zakończeniu sesji. Używając przycisku „Powrót do poprzedniej strony" osoba niepowołana może uzyskać wgląd w odwiedzane przez nas poprzednio ekrany, a co za tym idzie może zobaczyć dane wyświetlone wcześniej w odwiedzonych stronach serwisu internetowego. Należy jednak podkreślić, że w takiej sytuacji osoba niepowołana nie ma możliwości wykonania żadnej operacji na koncie. Aby uniknąć opisanego problemu, należy wraz z prawidłowym zakończeniem sesji serwisu internetowego (wylogowanie) dodatkowo zamknąć zakładkę lub okno, w którym był wyświetlany. Niemniej, podczas korzystania z serwisu internetowego nie rekomendujemy używania wspomnianych przeglądarek na komputerach dostępnych większemu gronu użytkowników.

Bezpieczne korzystanie z serwisu internetowego Oney24.pl

Nie wolno nikomu ujawniać swojego identyfikatora do serwisu internetowego Oney24.pl oraz hasła dostępu ani nigdzie zapisywać swoich haseł, w szczególności w plikach na domowym/biurowym komputerze, urządzeniu mobilnym czy w pamięci telefonu. Dane te trzeba zapamiętać.

- Zalecamy okresową zmianę hasła do serwisu internetowego Oney24.pl (np. co 30 dni).
- Dane niezbędne podczas dostępu i korzystania z serwisu internetowego Oney24.pl, tj. identyfikator, hasło wolno podać wyłącznie na stronie logowania do serwisu internetowego Oney24.pl. Logowanie do usług serwisu Oney24.pl z wykorzystaniem jakichkolwiek serwisów pośrednich, agregatorów informacji o transakcjach na rachunku czy też ujawnienie swojego identyfikatora lub hasła w miejscu innym niż strona logowania serwisu internetowego Oney24.pl naraża klienta na niebezpieczeństwo i może stanowić złamanie regulaminu dostępu do systemu.
- Jedynym prawidłowym adresem serwisu internetowego Oney24.pl jest: **https://oney24.pl**
  Przed autoryzacją w serwisie internetowym Oney24.pl należy zawsze upewnić się co do poprawności tego adresu.
- Na stronie logowania do systemu transakcyjnego Oney Polska S.A. nigdy nie prosi Klientów o potwierdzanie tożsamości poprzez podanie jakichkolwiek dodatkowych informacji, takich jak: numer karty płatniczej, kod bezpieczeństwa, data ważności karty, kod PIN, telekom. Ponadto Oney Polska S.A. nie wyświetla na stronie logowania żadnych formularzy lub obcojęzycznych komunikatów w postaci wyskakujących okien, ramek bądź jakichkolwiek niestandardowych elementów graficznych. Każde tego typu zdarzenie należy zignorować, zaniechać logowania oraz powiadomić Oney Polska S.A., dzwoniąc na Infolinię 71 799 70 08.

Bezpieczne korzystanie z serwisu internetowego Oney24.pl

- Oney Polska S.A. nigdy nie prosi Klientów za pomocą serwisu transakcyjnego o podanie jakichkolwiek danych dotyczących telefonu Klienta (numeru, modelu, IMEI) oraz o pobranie bądź instalację jakiejkolwiek aplikacji lub certyfikatu na telefony lub urządzenia mobilne. Po otrzymaniu takiej prośby w dowolnej formie należy ją zignorować oraz powiadomić o zdarzeniu Oney Polska S.A., dzwoniąc na numer Infolinii: 71 799 70 08.
- Wszelkie niestandardowe zachowania systemu transakcyjnego w stosunku do znanych Państwu dotychczas oraz oczekiwanie od Państwa jakichkolwiek dodatkowych informacji, również w postaci wysyłanych e-maili bądź smsów, których rzekomym nadawcą jest Oney Polska S.A. **powinno wzbudzić czujność i wzmożoną ostrożność**, a także skłonić Państwa do nawiązania kontaktu z **Infolinią 71 799 70 08**.
- Połączenie podczas logowania zarówno do internetowego serwisu transakcyjnego, jak i całej sesji użytkownika jest szyfrowane za pomocą 128-bitowego protokołu SSL zapewniającego poufność oraz integralność przesyłanych danych.
- Oznaczeniem nawiązania bezpiecznego połączenia jest ikona kłódki w pasku adresu oraz adres strony, który rozpoczyna się od **https://**. Ponadto elementem paska adresu jest zielona etykieta lub przycisk wskazujący tożsamość witryny – Oney Polska S.A. [PL].
- Potwierdzeniem autentyczności i bezpieczeństwa nawiązanego połączenia jest zgodność parametrów certyfikatu. Sprawdzenie poprawności certyfikatu dla serwisu internetowego Oney24.pl

Sprawdzenie poprawności certyfikatu dla serwisu internetowego Oney24.pl

Powinno się sprawdzać prawidłowość certyfikatu serwera Oney Polska S.A. – certyfikat taki jest używany w celu weryfikacji tożsamości serwera, z którym nawiązano połączenie.

Sprawdzenie polega na:

- upewnieniu się, że certyfikat został wystawiony dla tej samej domeny, z którą nawiązywane jest połączenie (oney24.pl),
- weryfikacji daty ważności certyfikatu – daty jego ważności muszą obejmować datę bieżącą,
- upewnieniu się, że certyfikat został wystawiony przez firmę Certum, która jednoznacznie potwierdziła wiarygodność danych firmy występującej o certyfikat – w tym wypadku Oney Polska S.A.

- **Należy zachować szczególną ostrożność w przypadku korzystania z usług serwisu internetowego w miejscach publicznych, przy użyciu bezprzewodowego dostępu do sieci oraz wykorzystując komputery lub urządzenia mobilne, co do których nie mamy pewności.**
- Nigdy nie należy odpowiadać na wiadomości mailowe, których nadawcy proszą o ujawnienie czy zweryfikowanie danych osobowych Klienta oraz poufnych informacji, takich jak: identyfikator i hasło konta internetowego, numer konta, telekod, numer PIN do karty płatniczej/kredytowej czy też sam numer karty. Zapewniamy, że Oney Polska S.A. nigdy nie wysyła tego typu wiadomości – po otrzymaniu takiego maila należy go zignorować oraz powiadomić Oney Polska S.A., dzwoniąc na Infolinię 71 799 70 08.

Bezpieczne korzystanie z serwisu internetowego Oney24.pl

- Oney Polska S.A. nigdy także nie wysyła maili, w których linki/odnośniki prowadzą bezpośrednio do stron z oknem logowania do serwisu transakcyjnego – po otrzymaniu takiego maila należy go zignorować oraz powiadomić Oney Polska S.A., dzwoniąc na Infolinię 71 799 70 08.
- Zaleca się nie korzystać w trakcie sesji z serwisem internetowym Oney24.pl z innych stron WWW. Adres strony logowania do serwisu internetowego należy każdorazowo wprowadzać w nowo otwartym oknie lub zakładce przeglądarki.
- Należy odpowiednio skonfigurować przeglądarkę internetową, zgodnie z zaleceniami zawartymi w zakładce konfiguracja przeglądarek internetowych

Bezpieczne korzystanie z serwisu Oney24.pl przez telefon

- **Nie wolno nikomu ujawniać swojego telekodu** (hasła autoryzacyjnego) do usług telefonicznych w Oney Polska S.A. ani przechowywać go w postaci zapisanej w jakiejkolwiek formie.
- Zarówno w przypadku rozmów z Infolinią nawiązywanych przez klienta, jak i niezamówionego połączenia telefonicznego nawiązanego przez pracownika Infolinii – klient nigdy nie zostanie poproszony o ujawnienie całości telekodu, a tylko jego wybranych cyfr.
- W razie ujawnienia telekodu lub podejrzenia ujawnienia należy go jak najszybciej zmienić. Zaleca się okresową zmianę telekodu.

Zabezpieczenia serwisu internetowego Oney24.pl

Drogi Kliencie, możesz być spokojny o swoje środki pieniężne. Wielostopniowy system zabezpieczeń i ochrony danych zapewnia pełną dyskrecję i bezpieczeństwo transakcji dokonywanych w serwisie internetowym.

Oto powody, które czynią internetowy system internetowy Oney24.pl bezpiecznym:

- Identyfikacja użytkownika za pomocą dwóch elementów:
  - unikalnego identyfikatora użytkownika,
  - hasła dostępu.
- Szyfrowanie danych za pomocą złożonych technik kryptograficznych.
- Ponowna autoryzacja przy potwierdzaniu operacji finansowych.
- Możliwość ustalenia indywidualnych limitów kwotowych.
- Aktywna kontrola i wykrywanie prób nieudanego logowania.
- Monitoring nieaktywności Klienta.
- Certyfikat wydany przez Certum.

Zabezpieczenia serwisu internetowego Oney24.pl

Certyfikat

Pierwszym krokiem przy nawiązywaniu połączenia przez przeglądarkę klienta z serwerem serwisu internetowego jest pobranie tzw. certyfikatu. Certyfikat to rodzaj dokumentu tożsamości dla serwera WWW, wydanego przez niezależną firmę tzw. Certification Authority (CA).
Certyfikat zawiera m.in.:

- nazwę właściciela certyfikatu,
- nazwę wydawcy certyfikatu,
- publiczny klucz właściciela,
- okres ważności,
- nazwę serwera, dla którego certyfikat jest wystawiany.

Certyfikat dla serwisu internetowego Oney24.pl wystawiła firma certyfikująca Certum. Wydanie certyfikatu zostało poprzedzone sprawdzeniem autentyczności serwisu internetowego oraz weryfikacją praw do domeny internetowej, w której działa serwer Oney Polska S.A.

- Szybki i skuteczny system zmiany hasła i identyfikatora.
- Rygorystyczne wewnętrzne procedury bezpieczeństwa.

Phishing – co powinieneś wiedzieć

Phishing jest rodzajem zagrożenia bezpieczeństwa informacji, stosowanym głównie na szeroką skalę w Internecie. Termin ten tłumaczony jest jako password harvesting fishing, czyli łowienie haseł. Polega na wyłudzaniu poufnych danych od użytkowników Internetu, w tym danych dotyczących systemów bankowości internetowej.

Metoda ta polega najczęściej na podszywaniu się pod instytucję, z której usług korzysta dany użytkownik. W takim przypadku otrzymuje on e-mail z fałszywą prośbą o wysłanie danych w celu weryfikacji swojego konta w systemie lub zalogowanie się na odpowiednio spreparowanej, fałszywej – aczkolwiek wyglądającej jak prawdziwa – stronie internetowej. Prośba ta często poparta jest argumentami mówiącymi o względach bezpieczeństwa, niezbędnej weryfikacji transakcji itp.

Nieświadomy niebezpieczeństwa użytkownik podaje w ten sposób poufne informacje, takie jak: identyfikator, hasło, PIN, numer karty płatniczej, które przechwytuje intruz. W ten sposób uzyskuje dane klienta umożliwiające mu kontrolę nad rachunkiem karty kredytowej i dokonanie kradzieży środków pieniężnych czy też innych oszustw.

Podkreślamy, że Oney Polska S.A. nigdy nie wysyła do swoich klientów e-maili ani wiadomości sms z prośbą o podanie jakichkolwiek poufnych informacji ani też zawierających linków do stron logowania do systemu transakcyjnego lub zachęcających do pobrania aplikacji czy certyfikatów bezpieczeństwa. W przypadku otrzymania takiej wiadomości nigdy nie należy na nią odpowiadać.
Najlepsza reakcja: wiadomość skasować, a o zdarzeniu powiadomić Oney Polska S.A., dzwoniąc na Infolinię 71 799 70 08.
Należy także pamiętać, aby przed logowaniem do serwisów bankowości internetowej zawsze sprawdzać poprawność danych identyfikacyjnych strony logowania, tj. dane certyfikatu (uzyskiwane po kliknięciu symbolu kłódki) oraz poprawność adresu internetowego strony – prawidłowy adres dla serwisu internetowego to **https://oney24.pl**