e-serwis

Wspierane przeglądarki oraz ustawienia

Infolinia: 0 801 10 20 30

Allianz

Spis treści

1 Wspierane przeglądarki

e-serwis jest portalem informacyjno-transakcyjnym udostępnianym Klientom Allianz poprzez Internet, umożliwiającym składanie dyspozycji oraz uzyskanie informacji o stanie polis/certyfikatów.
e-serwis uruchamiany jest w oknie przeglądarki internetowej, aktualnie pełne wsparcie serwisu dedykowane jest dla przeglądarek:

- Internet Explorer 6.0
- Internet Explorer 7.0
- Internet Explorer 8.0
- FireFox 3.0

2 Ustawienia przeglądarki

Odpowiednie ustawienie parametrów przeglądarki internetowej wpływa na poziom bezpieczeństwa korzystania z systemu bankowości internetowej. Poniżej zamieszczamy wskazówki dotyczące konfiguracji najpopularniejszych przeglądarek internetowych:

- Internet Explorer 6.0
- Internet Explorer 7.0
- Internet Explorer 8.0
- FireFox

Internet Explorer 6.0

Przykładowa bezpieczna konfiguracja przeglądarki internetowej Internet Explorer 6.0:
Należy wybrać **Narzędzia (Tools)** na górnym pasku menu przeglądarki, a następnie pozycję **Opcje internetowe (Internet Options)**, sprawdzić i zmienić ustawienia w następujących zakładkach:

1. Zaawansowane (Advanced)

W grupie **Przeglądanie (Browsing)** opcja Pokaż przyjazne komunikaty o błędach HTTP (Show friendly HTTP error messages) powinna być wyłączona.
W grupie Zabezpieczenia (Security) należy zaznaczyć:

- nie zapisuj zaszyfrowanych stron na dysku (Do not save encrypted pages to disk),
- ostrzegaj przed nieważnymi certyfikatami witryn (Warn about invalid site certificates),
- ostrzegaj, jeżeli przesyłanie formularzy jest przekierowywane (Warn if forms submittal is being redirected),
- użyj SSL 3.0 (Use SSL 3.0),
- użyj TLS 1.0 (Use TLS 1.0).

2. Zabezpieczenia (Security)

Należy nacisnąć przycisk Poziom niestandardowy (Custom Level), a następnie:
w grupie Różne (Miscellaneous) – Wyłącz (Disable):
Nawigowanie ramek podrzędnych w różnych domenach (Navigate subframes across different domains).

3. Ogólne (General)

W sekcji **Tymczasowe Pliki Internetowe (Temporary Internet Files)**, należy kliknąć na Usuń Pliki (Delete Files). Po kliknięciu na Ustawnienia (Settings) należy ustawić opcję Przy każdej wizycie na tej stronie (Every visit to the page), wybrać OK i po powrocie do zakładki **Ogólne (General)** zatwierdzić wprowadzone ustawienia przyciskiem OK. Następnie należy zamknąć i uruchomić ponownie przeglądarkę **Internet Explorer 6.0**.

Internet Explorer 7.0

Przykładowa bezpieczna konfiguracja przeglądarki internetowej Internet Explorer 7.0:
Należy Wybrać **Narzędzia (Tools)** na górnym pasku menu przeglądarki, a następnie pozycję **Opcje internetowe (Internet Options)**, sprawdzić i zmienić ustawienia w następujących zakładkach:

1. Zaawansowane (Advanced)

W grupie **Przeglądanie (Browsing)** opcja Pokaż przyjazne komunikaty o błędach HTTP (Show friendly HTTP error messages) powinna być wyłączona.
W grupie Zabezpieczenia (Security) należy zaznaczyć:

- nie zapisuj zaszyfrowanych stron na dysku (Do not save encrypted pages to disk),
- ostrzegaj przed niezgodnością adresów certyfikatów (Warn about invalid site certificates),
- ostrzegaj przez zmianą trybu zabezpieczonego na niebezpieczny (Warn if changing between secure and non-secure mode),
- sprawdzaj podpisy dla pobieranych programów (Check for signatures on downloaded programs),
- sprawdź, czy certyfikat serwera nie został cofnięty (Check for server certificate revocation),
- sprawdź, czy certyfikat wydawcy nie został cofnięty (Check for publisher's certificate revocation),
- użyj SSL 3.0 (Use SSL 3.0),
- użyj TLS 1.0 (Use TLS 1.0).

2. Zabezpieczenia (Security)

Należy nacisnąć przycisk Poziom niestandardowy (Custom Level), a następnie:

- w grupie Różne (Miscellaneous) – Wyłącz (Disable): Nawigowanie ramek podrzędnych w różnych domenach (Navigate subframes across different domains).
- w grupie Formanty ActiveX i dodatków plug-in – Wyłącz (Disable): Inicjowanie i wykonanie skryptów formantów ActiveX niezaznaczonych jako bezpieczne do wykonania (Initiation and execution of script unchecked off ActiveX as for execution safe), Pobieranie niepodpisanych formantów ActiveX (Collected unsign ActiveX), Zezwalaj na uruchamianie poprzednio nie używanych formantów ActiveX bez monitorowania (Permit start-up without monitoring unused formerly ActiveX).
- w grupie Obsługa skryptów (Scripting) należy włączyć Wykonywanie skryptów apletów języka Java (Java scripts of applets of languages executable).

3. Ogólne (General)

W sekcji **Tymczasowe Pliki Internetowe (Temporary Internet Files)**, należy kliknąć na Usuń pliki (Delete Files). Po kliknięciu na Ustawnienia (Settings) należy ustawić opcję Przy każdej wizycie na tej stronie (Every visit to the page), wybierać OK i po powrocie do zakładki **Ogólne (General)** zatwierdzić wprowadzone ustawienia przyciskiem OK. Następnie należy zamknąć i uruchomić ponownie przeglądarkę **Internet Explorer 7.0**.

Internet Explorer 8.0

Przykładowa bezpieczna konfiguracja przeglądarki internetowej Internet Explorer 8.0:
Należy wybrać **Bezpieczeństwo (Safety)** na górnym pasku menu przeglądarki, a następnie pozycję **Filtr Smart Screen (SmartScreen Filter)** – Włącz filtr Smart Screen (Turn On SmartScreen Filter).
Następnie należy wybrać **Narzędzia (Tools)** na górnym pasku menu przeglądarki, pozycję **Opcje internetowe (Internet Options)**, sprawdzić i zmienić ustawienia w następujących zakładkach:

1. Zaawansowane (Advanced)

W grupie **Przeglądanie (Browsing)** należy odznaczyć: Pokaż przyjazne komunikaty o błędach HTTP (Show friendly HTTP error messages).
W grupie **Zabezpieczenia (Security)** należy zaznaczyć:

- nie zapisuj zaszyfrowanych stron na dysku (Do not save encrypted pages to disk),
- ostrzegaj przed niezgodnością adresów certyfikatów (Warn about invalid site certificates),
- ostrzegaj przez zmianą trybu zabezpieczonego na niezabezpieczony (Warn if changing between secure and non-secure mode),
- ostrzegaj, jeśli przesyłanie ogłoszeń jest przekierowywane do strefy, w której ogłoszenia są niedozwolone (Warn if POST submittal is redirected to a zone that does not permit posts),
- sprawdzaj podpisy dla pobieranych programów (Check for signatures on downloaded programs),
- sprawdź, czy certyfikat serwera nie został cofnięty (Check for server certificate revocation),
- sprawdź, czy certyfikat wydawcy nie został cofnięty (Check for publisher's certificate revocation),
- użyj SSL 3.0 (Use SSL 3.0),
- użyj TLS 1.0 (Use TLS 1.0),
- włącz filtr SmartScreen (Enable SmartScreen Filter).

2. Zabezpieczenia (Security)

Należy nacisnąć przycisk Poziom niestandardowy (Custom Level), a następnie:

- w grupie .NET Framework
  – Monituj (Prompt): Luźny kod XAML (Loose XAML).
- w grupie Formanty ActiveX i dodatki plug-in (ActiveX controls and plug-ins)
  – Wyłącz (Disable): Inicjowanie i wykonanie skryptów formantów ActiveX niezaznaczonych jako bezpieczne do wykonania (Initialize and script ActiveX controls not market as safe for scripting),

– Wyłącz (Disable): Pobieranie niepodpisanych formantów ActiveX (Download unsigned ActiveX controls),
– Włącz (Enable): Zezwalaj na uruchamianie poprzednio nie używanych formantów ActiveX bez monitorowania (Allow previously unused ActiveX controls to run without prompt).

- w grupie Obsługa skryptów (Scripting)
  – Monituj (Prompt): Wykonywanie aktywnych skryptów (Active scripting),
  – Włącz (Enable) Wykonywanie skryptów apletów języka Java (Scripting of Java applets).
- w grupie Różne (Miscellaneous)
  – Wyłącz (Disable): Nawigowanie ramek podrzędnych w różnych domenach (Navigate subframes across different domains),
  – Wyłącz (Disable): Przesyłanie niezaszyfrowanych danych formularza (Submit not-encrypted form data),
  – Wyłącz (Disable): Uruchamianie aplikacji i niebezpiecznych plików (Launching applications and unsafe files),
  – Wyłącz (Disable): Uruchamianie programów i plików w trybie IFRAME (Launching programs and files in an IFRAME).

3. Ogólne (General)

W sekcji **Historia przeglądania (Browsing history)**, należy zaznaczyć Usuń historię przeglądania przy zakończeniu (Delete browsing history on exit), należy przejść do Ustawnienia (Settings) i ustawić opcję Za każdym razem, gdy odwiedzam tę stronę (Every time I visit the webpage). Po powrocie do zakładki **Ogólne (General)** należy zatwierdzić wprowadzone ustawienia przyciskiem OK i następnie uruchomić ponownie przeglądarkę **Internet Explorer 8.0**.

Mozilla FireFox

Przykładowa bezpieczna konfiguracja przeglądarki internetowej FireFox:
Należy wybrać **Narzędzia (Tools)** na górnym pasku menu przeglądarki, a następnie pozycję **Opcje (Options)**, sprawdzić i zmienić ustawienia w następujących zakładkach:

1. Bezpieczeństwo (Security) – należy zaznaczyć opcje:

- ostrzegaj, kiedy witryny próbują instalować dodatki (Warn me when sites try to install add-ons),
- informuj, jeśli oglądana witryna może być próbą oszustwa (Tell me if the site I'm visiting is a suspected forgery) – radiobutton Sprawdź obecność na liście podejrzanych witryn (Check using a downloaded list of suspected sites).

W sekcji **Ostrzeżenia (Warning)** przyciskając przycisk **Ustawienia (Settings)** należy zaznaczyć ostrzeżenia przy:

- otwieraniu strony o niskim stopniu szyfrowania (I' am about to view a page that uses low-grade encryption),
- przechodzeniu ze strony szyfrowanej do nieszyfrowanej (I leave an encrypted page for one that isn't encrypted),
- otwieraniu szyfrowanej strony zawierającej niezaszyfrowane informacje (I'm about to view an encrypted page that contains some unencrypted information).

2. Zaawansowane (Advanced) / zakładka: **Szyfrowanie (Encryption)**

W sekcji **Protokoły (Protocols)** należy zaznaczyć:

- Włącz obsługę SSL 3.0 (Use SSL 3.0) oraz Włącz obsługę TLS 1.0 (Use TLS 1.0),

W sekcji **Certyfikaty (Certificates)**: Kiedy witryna wymaga certyfikatu (When a web site requires a certificate) należy zaznaczyć:

- Wybierz certyfikat automatycznie (Select one automatically).

3. Treść (Content) – należy zaznaczyć opcje:

- Włącz obsługę języka Javascript (Enable JavaScript),
- Włącz obsługę języka Java (Enable Java).

4. Prywatność (Privacy)

W sekcji **Ciasteczka (Cookies)** należy zaznaczyć opcje:

- Akceptuj ciasteczka (Accept cookies from sites), w liście rozwijalnej – Przechowuj należy wybrać do zamknięcia programu Firefox (Keep until: I close Firefox),

W sekcji **Prywatne dane (Private data)** należy zaznaczyć opcje:

- Zawsze czyść prywatne dane przy zamykaniu programu Firefox (Always clear my private data when I close Firefox),

Następnie w tej samej sekcji przyciskając przycisk Wyczyść teraz (Clean now) i zaznaczyć opcje:

- Historię przeglądanych stron (Browsing History),
- Historię pobieranych plików (Download History).

www.allianz.pl

Więcej informacji uzyskasz
pod numerem Infolinii
0 801 10 20 30

e-serwis Wspierane przeglądarki 04/10