Banki

Dokumentacja użytkownika

Konfiguracja przeglądarek internetowych pod kątem pracy w systemie def3000/CEB oraz def2500/REB

Wersja systemu: def3000/CEB: 2.35.002C, def2500/REB: 3.41.004C
Data wydania dokumentu: 2015-05-18
Przeznaczenie dokumentu: poufny, zewnętrzny
Identyfikator dokumentu: DOC.UZT_def3000_CEB_def2500_REB_Konfiguracja_Przegladarek_Internetowych

Solutions for Demanding Business

Spis treści

Rozdział 1. Informacje o dokumencie

Niniejszy dokument jest dokumentacją użytkownika systemów def3000/CEB: 2.35.002C, def2500/REB: 3.41.004C.

Historia zmian:

Data	Autor	Wersja systemu	Opis zmiany
2012-10-30	Marzena Biniecka	2.30.000C	Aktualizacja dokumentacji
2013-05-02	Marzena Biniecka	2.31.003C	Aktualizacja dokumentacji
2014-09-16	Marzena Biniecka	2.33A.001C	Aktualizacja dokumentacji
2015-01-08	Marzena Biniecka	2.33A.001C, 3.38.006C	Uzupełnienie dokumentacji
2015-05-15	Marzena Biniecka	2.35.003C, 3.41.004C	Aktualizacja dokumentacji

Rozdział 2. Konwencje typograficzne

W dokumentacji stosowane są następujące konwencje typograficzne:

Konwencja typograficzna lub znak wizualny	Opis
Standardowy Czcionka Verdana 8, Kolor czcionki RGB: (70, 72, 71), Justowanie tekstu, Interlinia 1 wiersz	Podstawowy tekst dokumentacji
Tabela Czcionka Verdana 8, 7 lub 6, Kolor czcionki RGB: (70, 72, 71) lub (255, 255, 255)	Tekst w tabeli
Pogrubienie	Nowe pojęcia. Wyróżnienie ważnych fragmentów tekstu.
Pogrubienie Kolor czcionki RGB: (0, 69, 123)	Nazwy parametrów systemowych. Tekst - może zawierać małe i wielkie litery, cyfry oraz znaki specjalne.
Pogrubienie Kolor czcionki RGB: (31, 178, 89)	Nazwy uprawnień. Tekst - może zawierać małe i wielkie litery, cyfry oraz znaki specjalne.
Kursywa	Pozycje na listach wartości. Komunikaty systemowe. Parametry lub zmienne, których rzeczywiste nazwy lub wartości mają być dostarczane przez użytkownika. Nazwy opcji systemu. Ścieżki, np. *Dane archiwalne -> Przeglądanie*.
Uwaga Kolor czcionki RGB: (0, 69, 123)	Tekst uwagi, komentarza, zastrzeżenia - informacje, na które należy zwrócić uwagę podczas czytania dokumentacji lub pracy z systemem np. **Uwaga**: Podany powyżej adres internetowy jest przykładowy. Informację o adresie strony usług internetowych udostępnia Bank.
Ostrzeżenie Kolor czcionki RGB: (255, 0, 0)	Tekst ostrzeżenia - ostrzeżenia zawierają bardzo ważne informacje, na które należy zwrócić szczególną uwagę podczas czytania dokumentacji lub pracy z systemem, np. **Uwaga!** Zmiany przeksięgowań nie są kontrolowane przez system i wykonywane są wyłącznie na własną odpowiedzialność operatora!
Link Kolor czcionki RGB: (0, 0, 255)	Odwołania do innych rozdziałów lub fragmentów tekstu. Adresy URL
`Kod źródłowy` Courier New 8, 7 lub 6, Kolor czcionki RGB: (70, 72, 71), Interlinia 1 wiersz	Fragmenty kodu źródłowego. Przykłady wydruków
CAPS LOCK	Wyróżnienie nagłówków akapitów. Nazwy klawiszy na klawiaturze - kombinacje klawiszy, które należy nacisnąć jednocześnie zawierają znak "+" pomiędzy, np. CTRL+F.
[ ]	Nazwy przycisków, np. [Czynności]

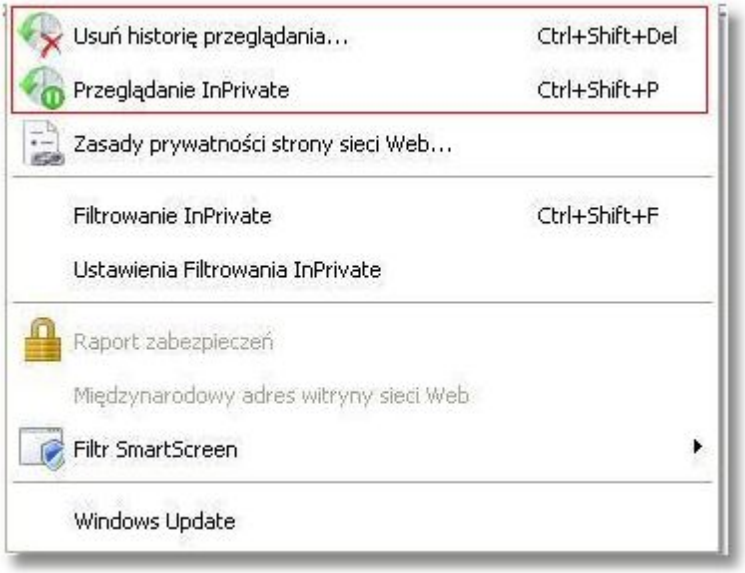
Rozdział 3. Wstęp

Niniejszy dokument zawiera opis konfiguracji poszczególnych przeglądarek internetowych pod kątem pracy w Centrum Usług Internetowych.

Rozdział 4. Konfiguracja przeglądarki Internet Explorer 8.0

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki. W przypadku, gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Internet Explorer 8.0 zawiera dodatkowe udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecane jest użycie jednej z dwóch funkcjonalności dostępnych na pasku zakładek w menu **Bezpieczeństwo**:

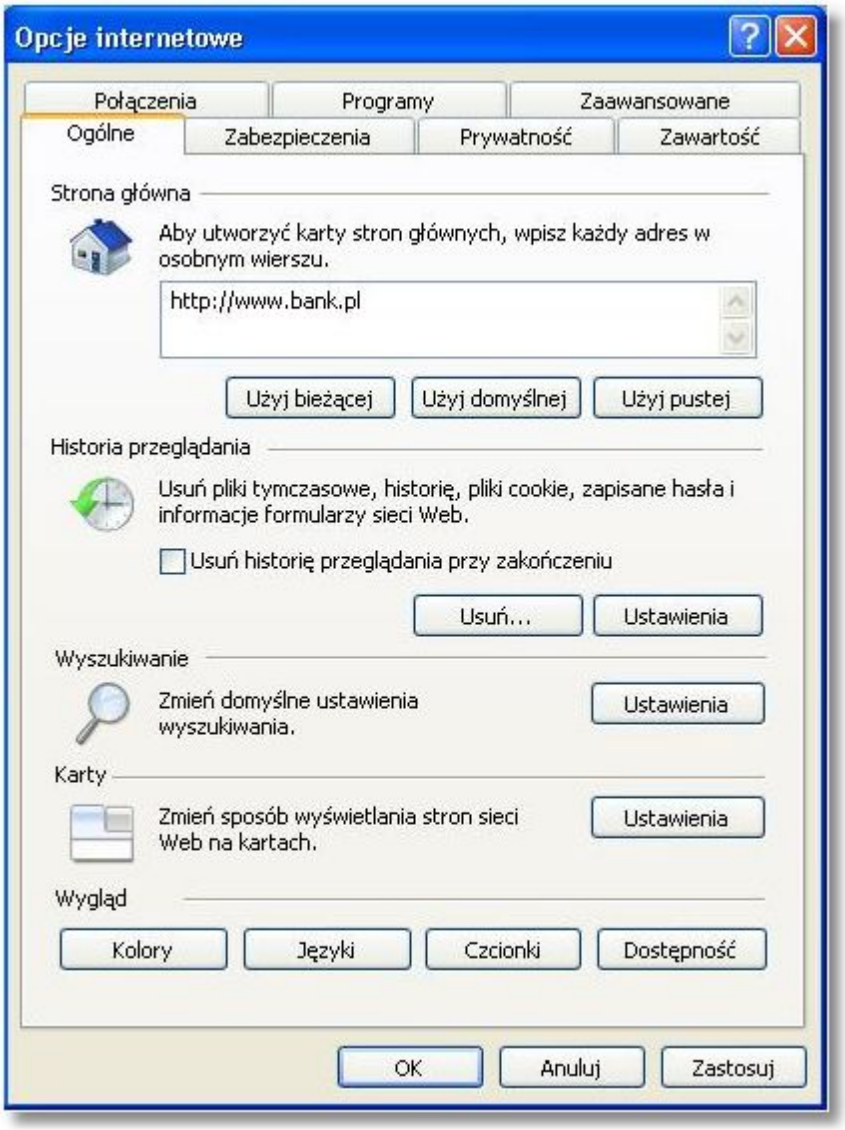
- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej włączenie trybu **Przeglądanie InPrivate**, zaś po jej zakończeniu zamknięcie okna przeglądarki
- Jeśli nie używano trybu **Przeglądanie InPrivate**, po zakończeniu pracy zalecamy użycie funkcji **Usuń historię przeglądania** (<CTRL>+<SHIFT>+<DEL>) .



Oba te narzędzia pomagają chronić dane użytkownika przed choćby przypadkowym ujawnieniem.

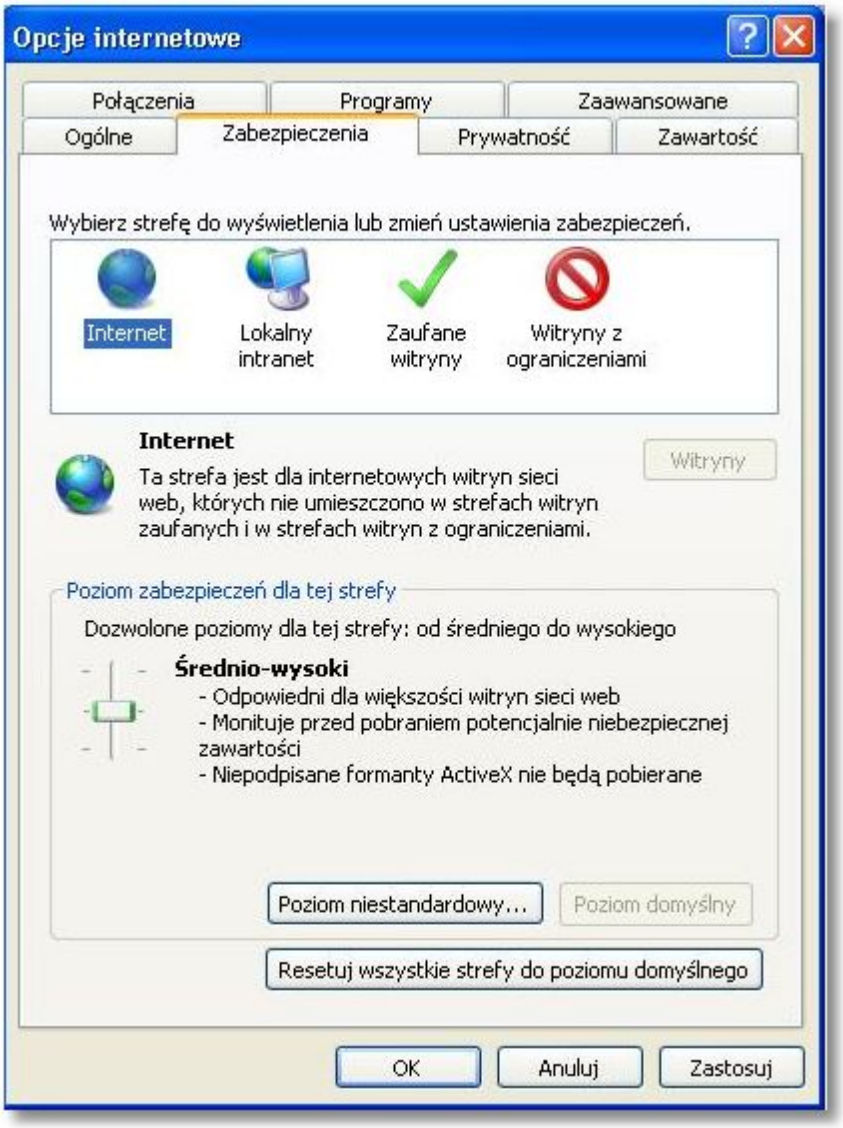
Aby poprawnie skonfigurować przeglądarkę, z menu *Narzędzia* należy wybrać *Opcje internetowe*.

W zakładce *Ogólne*:
- w sekcji **Historia przeglądania** zalecane jest usunięcie plików tymczasowych, plików cookie, historii, danych formularzy i haseł; w tym celu należy wybrać przycisk [Usuń...], a następnie na formatce **Usuwanie historii przeglądania** nacisnąć przycisk [Usuń wszystko...] (lub po kolei wybierać *Usuń pliki..., Usuń pliki cookie..., Usuń historię... , Usuń formularze..., Usuń hasła...*) i zatwierdzić odpowiedź *Tak*,
- w sekcji **Historia przeglądania** po naciśnięciu klawisza [Ustawienia[zalecane jest zaznaczenie w części **Tymczasowe pliki internetowe** opcji **Sprawdź, czy są nowsze wersje przechowywanych stron**: *Za każdym razem, gdy odwiedzam tę stronę*,
- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] proponuje się ustawienie w części **Historia liczby dni trzymania stron w historii** na 0,
- w celu poprawnego wyglądu aplikacji po wciśnięciu w części **Wygląd** przycisku [Dostępność...] powinny być odznaczone opcje *Ignoruj kolory określone na stronach sieci Web, Ignoruj style określone na stronach sieci Web, Ignoruj rozmiary czcionek określone na stronach sieci Web, Formatuj dokumenty używając mojego arkusza stylów*.



W zakładce *Zabezpieczenia*:

- dla Internetu zaleca się ustawienie poziomu zabezpieczeń na Średnio-wysoki.



Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku powinny być wybrane następujące ustawienia:

- w części Formant ActiveX i dodatki plung-in powinna być odznaczone opcje Inicjowanie i wykonywanie skryptów formantów ActiveX niezaznaczonych jako bezpieczne do wykonania, Pobieranie niepodpisanych formantów ActiveX oraz Zezwalaj na uruchamianie poprzednio nie używanych formantów ActiveX bez monitorowania
- w części Obsługa skryptów powinny być zaznaczone opcje Wykonywanie skryptów apletów języka Java, Włącz filtr XSS
- w części Pobieranie powinna być zaznaczona opcja Automatyczne monitorowanie dla pobrań plików
- w części Różne powinna być odznaczona opcja Nawigowanie ramek podrzędnych w różnych domenach

W zakładce *Prywatność*:

- w części **Ustawienia** zaleca się wybrać ustawienie prywatności dla strefy internetowej na Średni.

Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Zaawansowane] powinny być wybrane następujące ustawienia:

- w części **Blokowanie wyskakujących okienek** należy zaznaczyć opcję *Włącz blokowanie wyskakujących okienek*.

Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji.
W tym celu należy w zakładce **Prywatność** w części **Blokowanie wyskakujących okienek** w opcji *Ustawienia* wpisać adres strony banku internetowego oraz nacisnąć przycisk [Dodaj].
W zakładce *Zawartość*:

- zaleca się w sekcji **Autouzupełnianie** po wciśnięciu przycisku [Ustawienia] odznaczyć opcję *Nazwy użytkowników i hasła w formularzach*.

W zakładce *Zaawansowane*:

- w części **Multimedia** dla poprawnego wyświetlania grafiki na stronach aplikacji powinna być zaznaczona opcja *Pokaż obrazy*,
- w części **Przeglądanie** powinna być zaznaczona opcja *Pokaż przyjazne komunikaty o błędach HTTP*,
- w części **Zabezpieczenia** należy zaznaczyć: *Nie zapisuj zaszyfrowanych stron na dysku, Ostrzegaj przed niezgodnością adresów certyfikatów, Ostrzegaj przed zmianą trybu zabezpieczonego na niebezpieczny, Sprawdzaj podpisy dla pobieranych programów, Sprawdź czy certyfikat serwera nie został cofnięty, Sprawdź czy certyfikat wydawcy nie został cofnięty, użyj TLS 1.0, Włącz filtr SmartScreen, Włącz obsługę macierzystego protokołu XMLHTTP, Włącz przechowywanie DOM, Włącz zintegrowane uwierzytelnianie systemu Windows,*
- w części **Zabezpieczenia** należy odznaczyć: *Użyj SSL3.0.*

Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

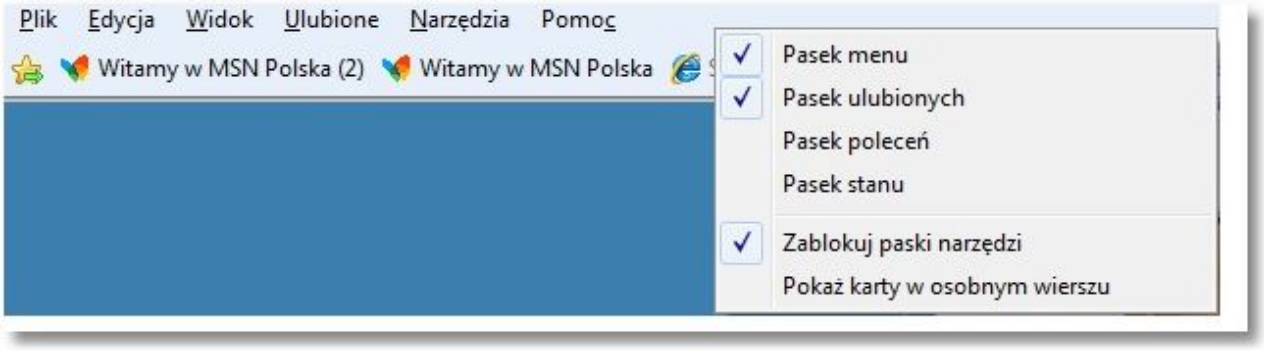
Rozdział 5. Konfiguracja przeglądarki Internet Explorer 9.0

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki. W przypadku, gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana. Przeglądarka Internet Explorer w wersji 9.0 wspiera następujące systemy operacyjne: Windows Vistax32,Windows Vistax64,Windows 7x32,Windows 7x64.
Przeglądarka Internet Explorer 9.0 zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecane jest użycie jednej z dwóch funkcjonalności dostępnych na pasku zakładek w menu **Bezpieczeństwo**:

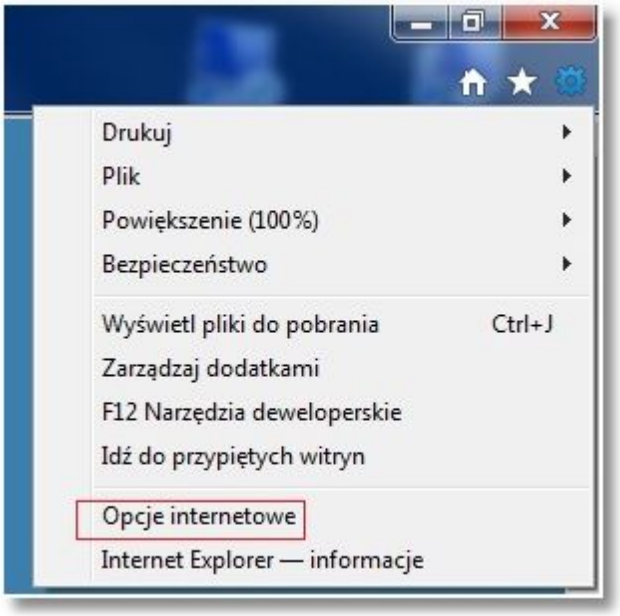
- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej włączenie trybu **Przeglądanie InPrivate**, zaś po jej zakończeniu zamknięcie okna przeglądarki
- Jeśli nie używano trybu **Przeglądanie InPrivate**, po zakończeniu pracy zalecamy użycie funkcji **Usuń historię przeglądania** (<CTRL>+<SHIFT>+<DEL>).

Oba te narzędzia pomagają chronić dane użytkownika przed choćby przypadkowym ujawnieniem. Przeglądanie **InPrivate** zapobiega przechowywaniu danych dotyczących sesji przeglądania. Dotyczy to między innymi plików cookie, tymczasowych plików internetowych i historii. Paski narzędzi i rozszerzenia są domyślnie wyłączone.

Domyślnie przeglądarka Internet Explorer w wersji 9.0 nie pokazuje paska menu. W celu wyświetlenia paska menu należy nacisnąć lewy klawisz <ALT> na klawiaturze, następnie ustawić kursor myszy na pasku menu, kliknąć prawy przycisk myszy oraz zaznaczyć opcję *Pasek menu*. Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.

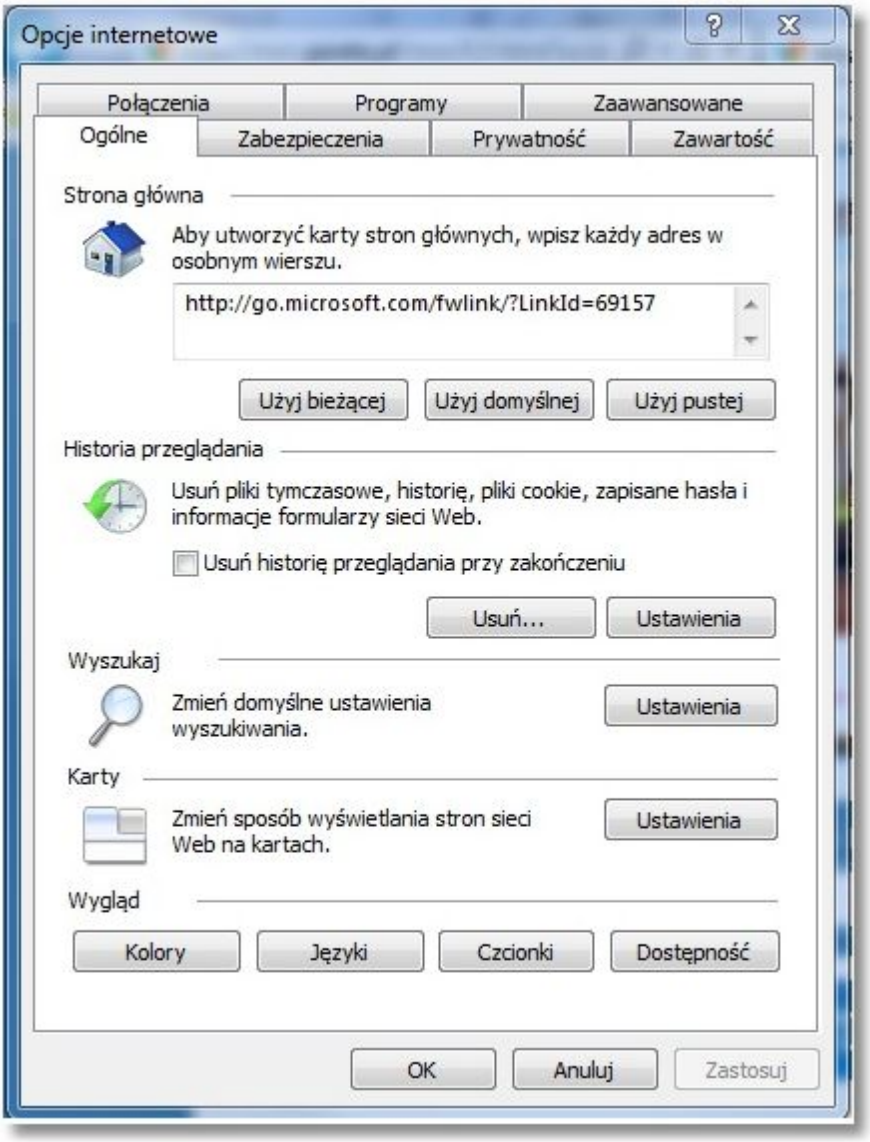


Aby poprawnie skonfigurować przeglądarkę, z menu **Narzędzia** należy wybrać *Opcje internetowe*.



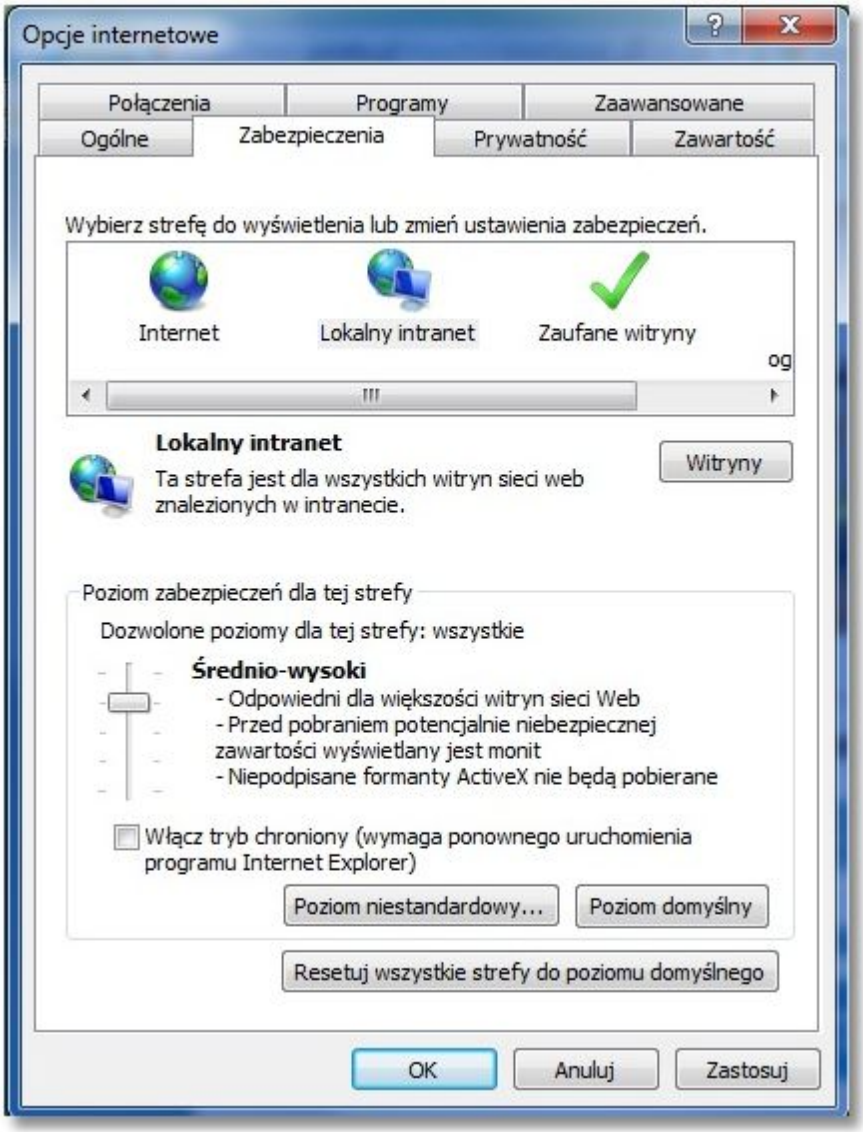
W zakładce *Ogólne*:

- w sekcji **Historia przeglądania** zalecane jest usunięcie plików tymczasowych, plików cookie, historii, danych formularzy i haseł; w tym celu należy wybrać przycisk [Usuń...], a następnie na formatce *Usuwanie historii przeglądania* nacisnąć przycisk [Usuń] (lub po kolei wybierać *Usuń pliki..., Usuń pliki cookie..., Usuń historię... , Usuń formularze..., Usuń hasła...*) i zatwierdzić odpowiedź *Tak*,
- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] zalecane jest zaznaczenie w części **Tymczasowe pliki internetowe** opcji *Sprawdź, czy są nowsze wersje przechowywanych stron*: *Za każdym razem, gdy odwiedzam tę stronę*,
- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] proponuje się ustawienie w części **Historia liczby dni trzymania stron w historii** na 0,
- w celu poprawnego wyglądu aplikacji po wciśnięciu w części **Wygląd** przycisku [Dostępność...] powinny być odznaczone opcje *Ignoruj kolory określone na stronach sieci Web, Ignoruj style określone na stronach sieci Web, Ignoruj rozmiary czcionek określone na stronach sieci Web, Formatuj dokumenty używając mojego arkusza stylów*.



W zakładce *Zabezpieczenia*:

- dla Internetu zaleca się ustawienie poziomu zabezpieczeń na Średnio-wysoki.



Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Poziom niestandardowy] powinny być wybrane następujące ustawienia:

- w części **Formanty ActiveX i dodatki plung-in** powinny być włączone opcje *Inicjowanie i wykonywanie skryptów formantów ActiveX niezaznaczonych jako bezpieczne do wykonania, Pobieranie niepodpisanych formantów ActiveX oraz Zezwalaj na uruchamianie poprzednio nie używanych formantów ActiveX bez monitorowania*
- w części **Obsługa skryptów** powinny być włączone opcje *Wykonywanie skryptów apletów języka Java, Włącz filtr XSS*
- w części **Różne** powinna być włączona opcja *Nawigowanie ramek podrzędnych w różnych domenach*

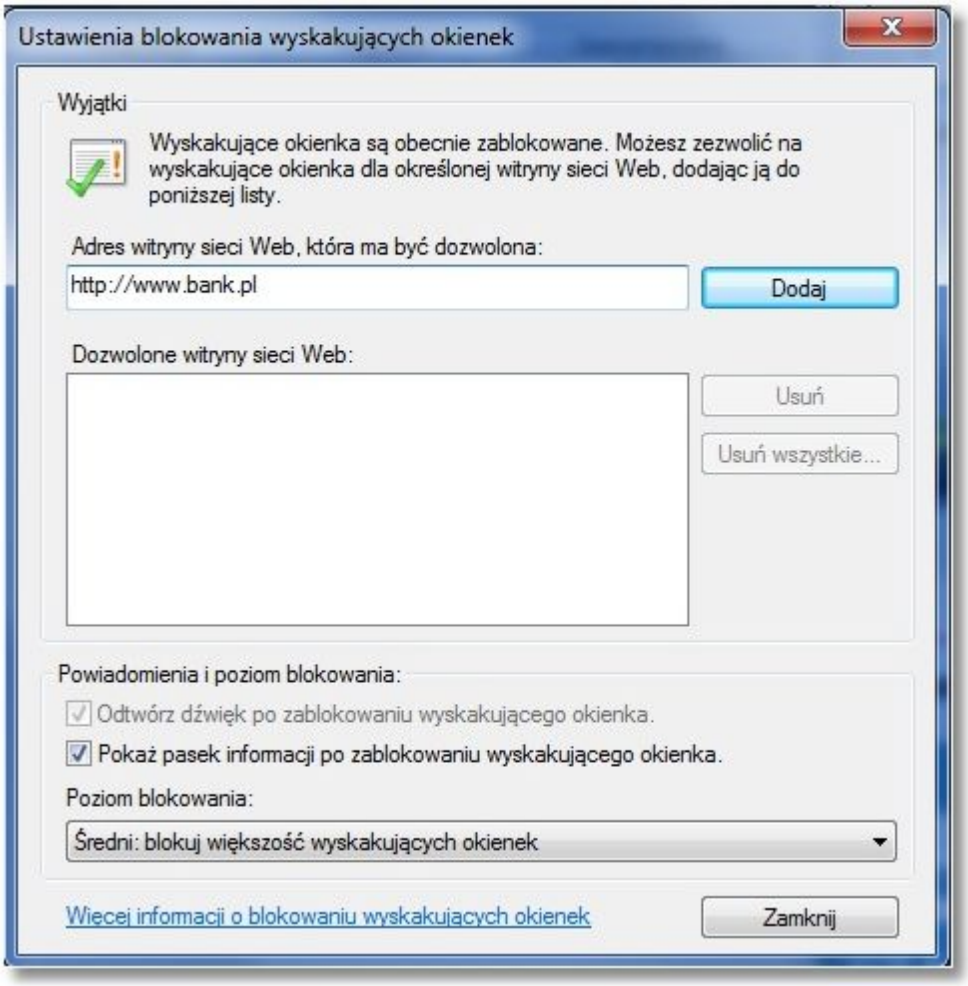
W zakładce *Prywatność*:

- w części **Ustawienia** zaleca się wybrać ustawienie prywatności dla strefy internetowej na Średni.

Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Zaawansowane] powinny być wybrane następujące ustawienia:

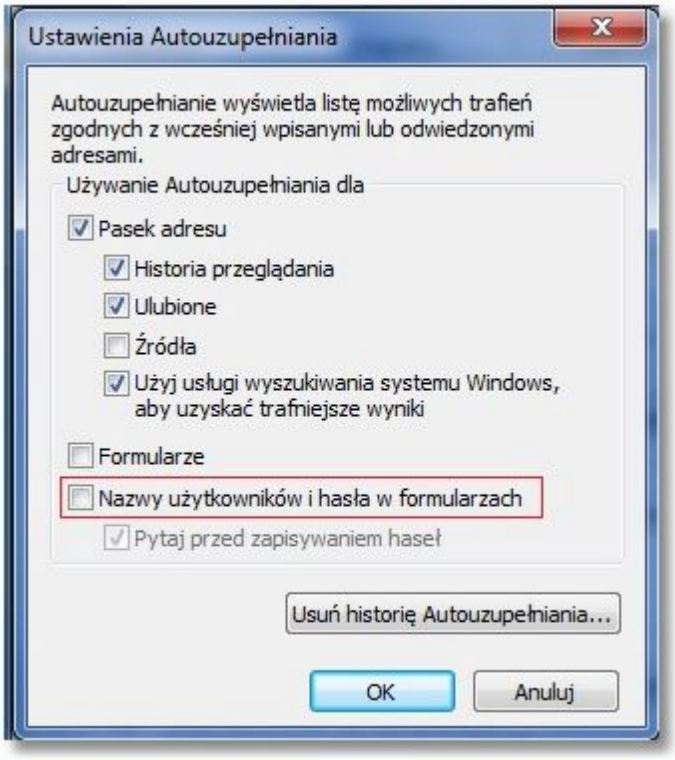
- w części **Blokowanie wyskakujących okienek** należy zaznaczyć opcję *Włącz blokowanie wyskakujących okienek*.

Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji.
W tym celu należy w zakładce *Prywatność* w części **Blokowanie wyskakujących okienek** w opcji *Ustawienia* wpisać adres strony banku internetowego oraz nacisnąć przycisk [Dodaj].



W zakładce *Zawartość*:

- zaleca się w sekcji **Autouzupełnianie** po wciśnięciu przycisku [Ustawienia] odznaczyć opcję *Nazwy użytkowników i hasła w formularzach*.



W zakładce *Zaawansowane*:

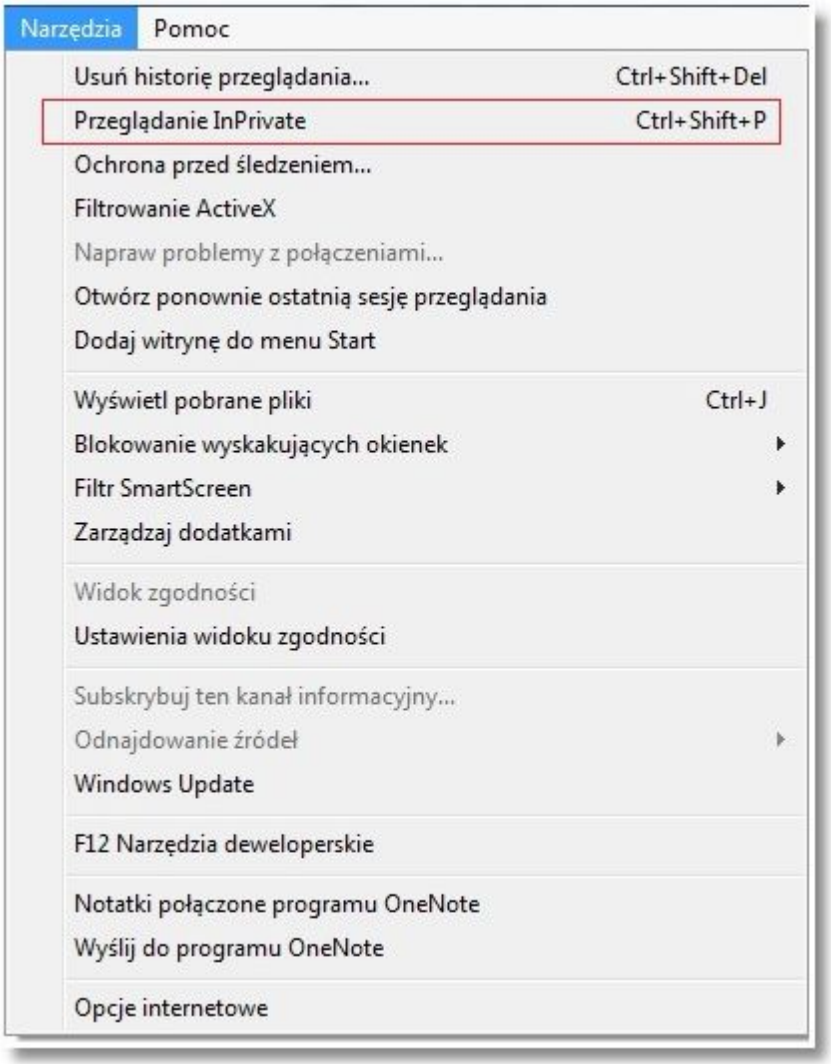
- w części **Multimedia** dla poprawnego wyświetlania grafiki na stronach aplikacji powinna być zaznaczona opcja *Pokaż obrazy*,
- w części **Przeglądanie** powinna być zaznaczona opcja Pokaż przyjazne komunikaty o błędach HTTP,
- w części **Zabezpieczenia** należy zaznaczyć: *Nie zapisuj zaszyfrowanych stron na dysku, Ostrzegaj przed niezgodnością adresów certyfikatów, Ostrzegaj przed zmianą trybu zabezpieczonego na niebezpieczny, Sprawdzaj podpisy dla pobieranych programów, Sprawdź czy certyfikat serwera nie został cofnięty, Sprawdź czy certyfikat wydawcy nie został cofnięty, użyj TLS 1.0, Włącz filtr SmartScreen, Włącz obsługę macierzystego protokołu XMLHTTP, Włącz przechowywanie DOM, Włącz zintegrowane uwierzytelnianie systemu Windows,*
- w części **Zabezpieczenia** należy odznaczyć: *Użyj SSL3.0.*

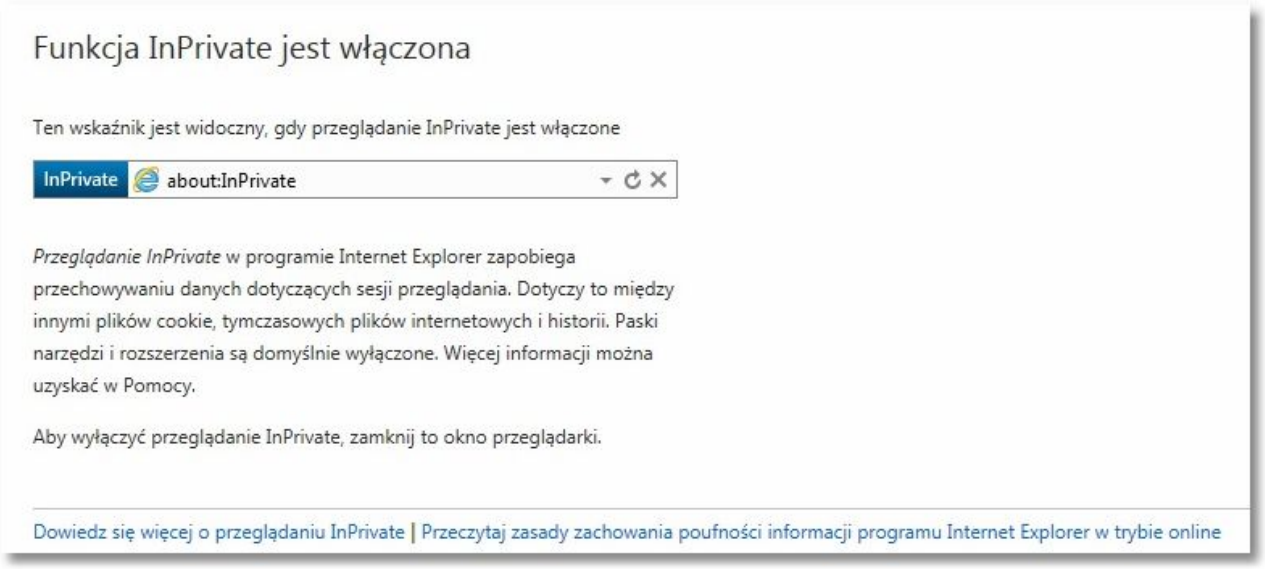
Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

Rozdział 6. Konfiguracja przeglądarki Internet Explorer 10.0

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Internet Explorer w wersji 10.0 wspiera następujące systemy operacyjne: Windows Vistax32, Windows Vistax64, Windows 7x32, Windows 7x64.
Przeglądarka Internet Explorer10.0 zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecane jest użycie jednej z dwóch funkcjonalności dostępnych na pasku zakładek w menu **Bezpieczeństwo**:

- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej włączenie trybu **Przeglądanie InPrivate**, zaś po jej zakończeniu zamknięcie okna przeglądarki.
- Jeśli nie używano trybu **Przeglądanie InPrivate**, po zakończeniu pracy zalecamy użycie funkcji **Usuń historię przeglądania** (Ctrl+Shift+Del).



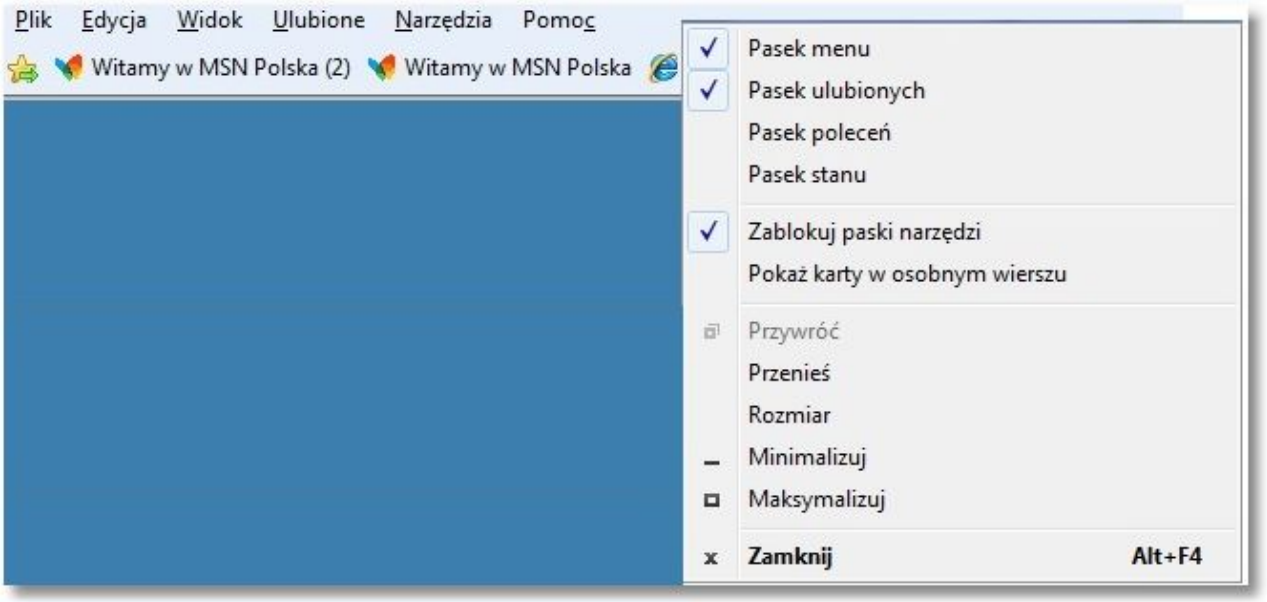


Funkcja **Przeglądanie InPrivate** umożliwia zachowanie poufności historii przeglądania na współużytkowanych komputerach. Dane historii zbierane w czasie przeglądania sieci Web przez okno programu Internet Explorer w trybie InPrivate, np. tymczasowe pliki internetowe, historia adresów internetowych lub pliki cookie, zostaną usunięte po zamknięciu okna. Nie ma to wpływu na historię w innych oknach programu Internet Explorer (w których nie jest używane przeglądanie InPrivate).
Przeglądanie InPrivate zapobiega lokalnemu przechowywaniu na komputerze następujących elementów:

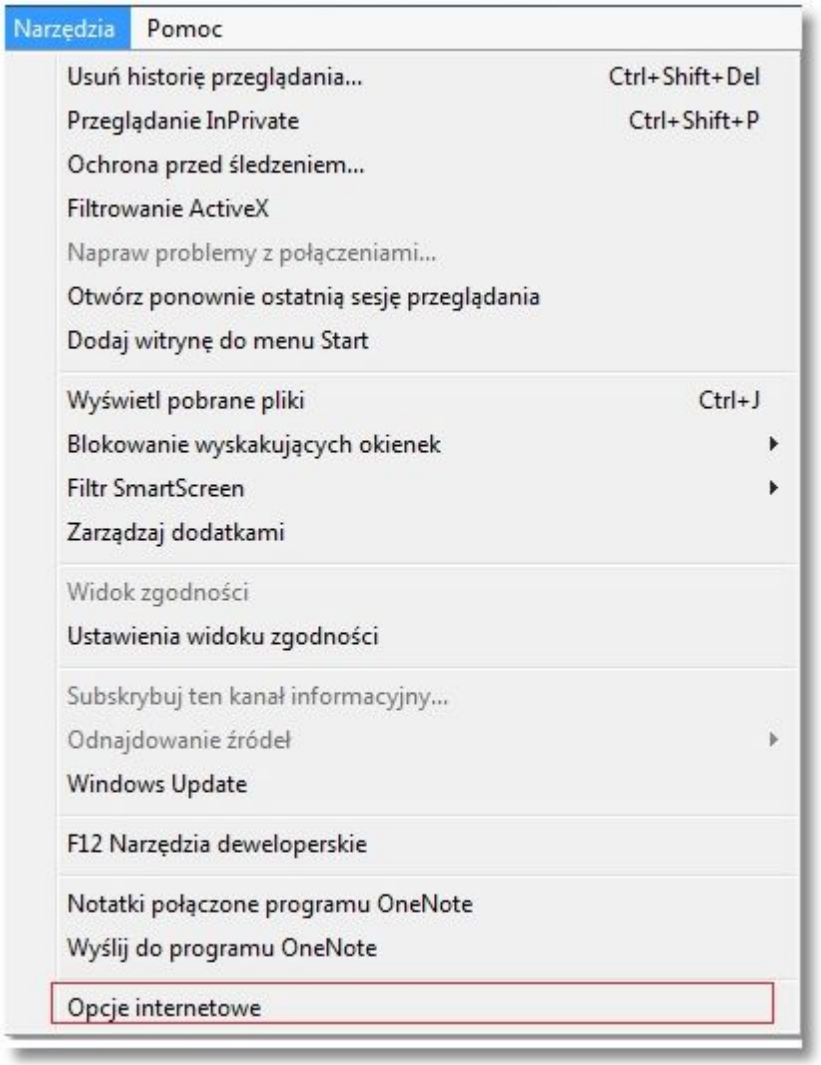
- Nowe pliki cookie nie są przechowywane.
- Nowe wpisy historii nie są rejestrowane.
- Nowe tymczasowe pliki internetowe zostaną usunięte po zamknięciu okna Przeglądania InPrivate.
- Dane formularzy nie są przechowywane.
- Wprowadzone hasła nie są przechowywane.
- Adresy wpisane na pasku adresu nie są przechowywane.
- Zapytania wpisane w polu wyszukiwania nie są przechowywane.

Oprócz tego program Internet Explorer wysyła do witryn sieci Web żądanie *Nie śledź w czasie sesji Przeglądania InPrivate*. Przeglądanie **InPrivate** nie jest przeznaczone do ukrywania tożsamości przez użytkownika przed usługodawcą internetowym ani serwerami sieci Web w Internecie. Funkcja ta nie zapobiega wysyłaniu danych, takich jak adres IP użytkownika, do odwiedzanych witryn sieci Web.

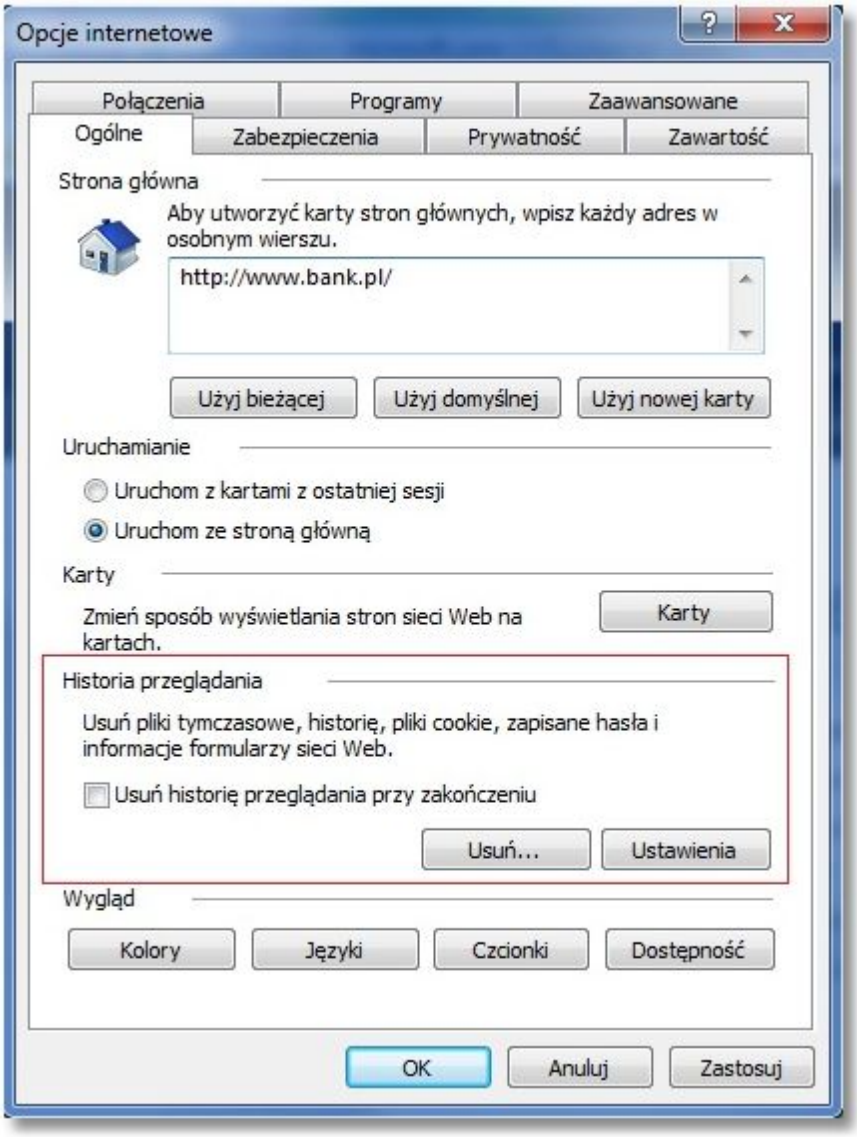
Domyślnie przeglądarka Internet Explorer w wersji 10.0 nie pokazuje paska menu. W celu wyświetlenia paska menu należy nacisnąć lewy klawisz Alt na klawiaturze, następnie ustawić kursor myszy na pasku menu, kliknąć prawy przycisk myszy oraz zaznaczyć opcję *Pasek menu*. Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.



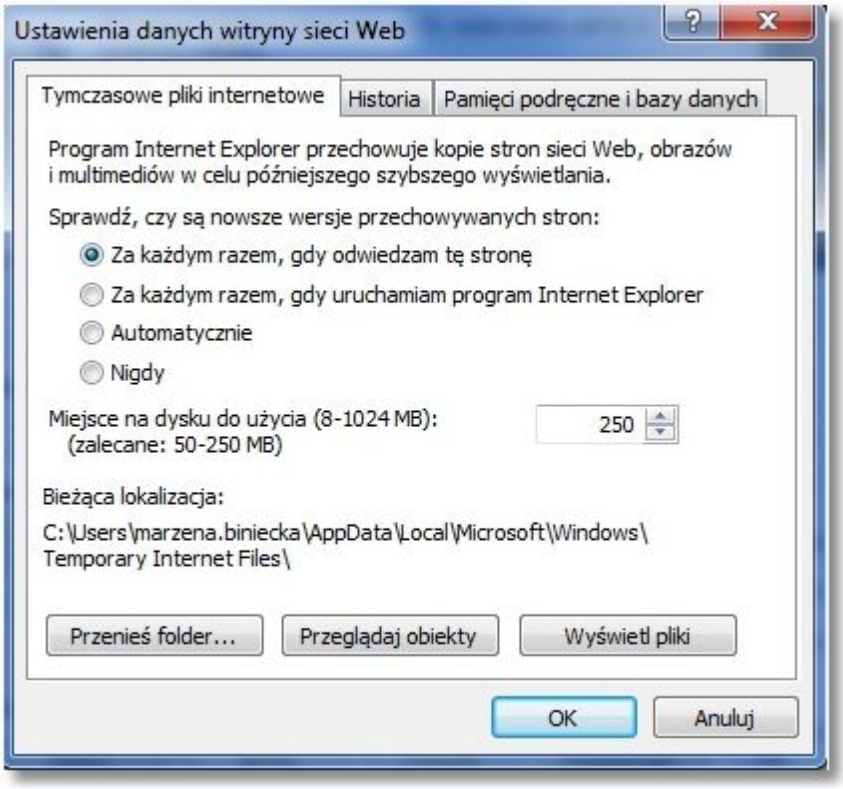
Aby poprawnie skonfigurować przeglądarkę z menu *Narzędzia* należy wybrać *Opcje internetowe*.



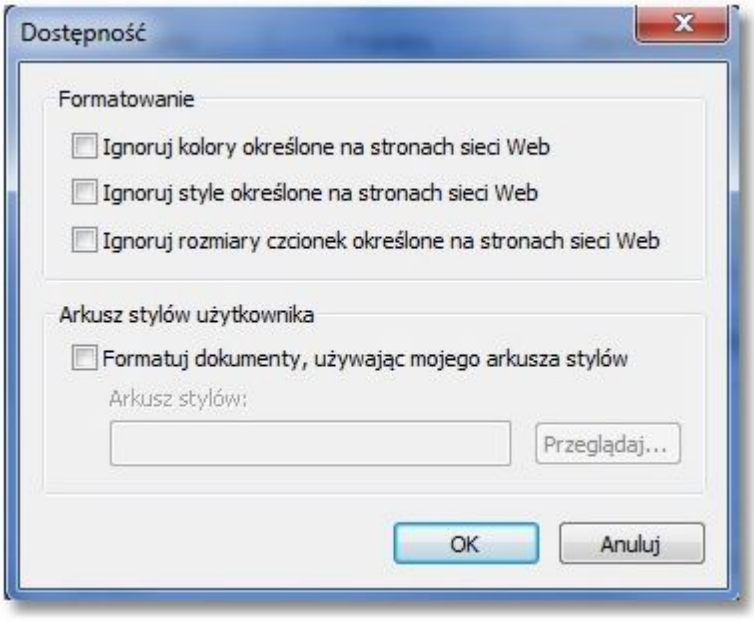
W zakładce *Ogólne*:



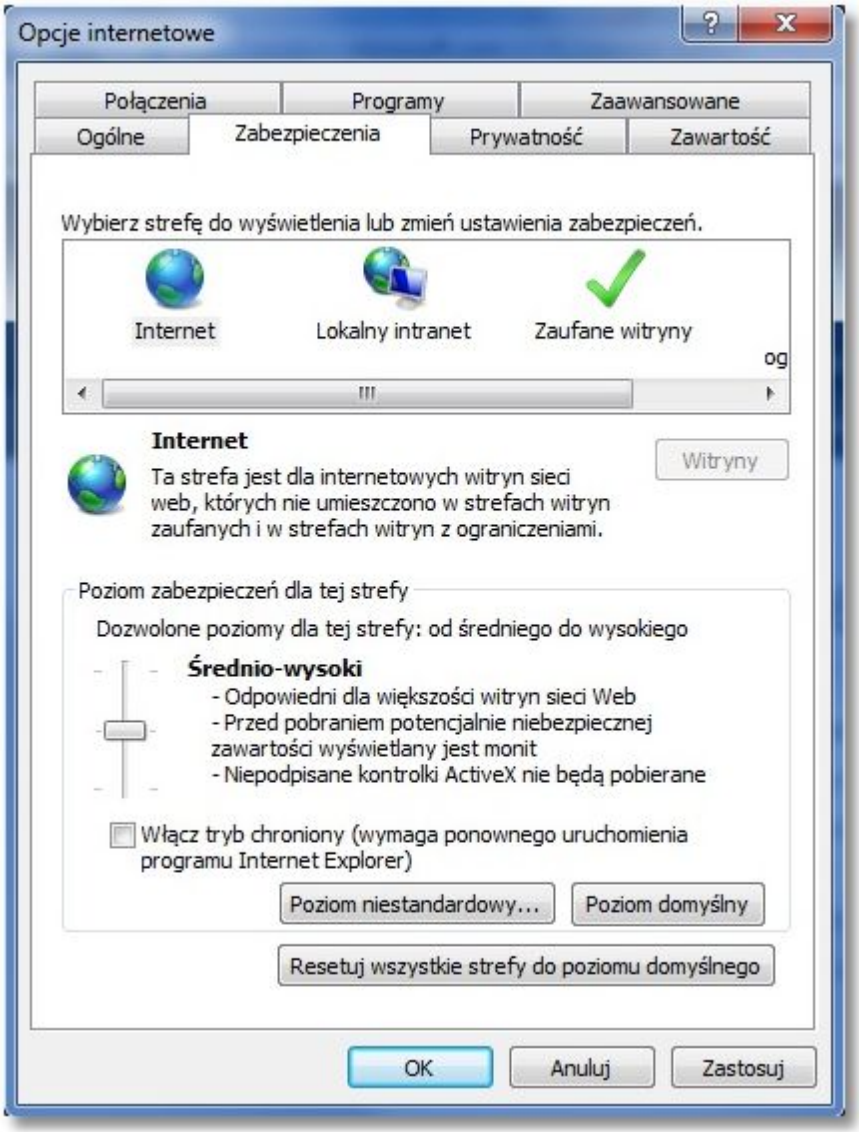
- w sekcji **Historia przeglądania** zalecane jest usunięcie plików tymczasowych, plików cookie, historii, danych formularzy i haseł; w tym celu należy wybrać przycisk [Usuń], a następnie na formatce **Usuwanie historii przeglądania** nacisnąć przycisk [Usuń] (lub po kolei wstawić znaczniki przy pozycjach: Pliki cookie i dane witryn sieci WEB, Historia, Historia pobierania, Dane formularzy, Hasła) i zatwierdzić przyciskiem Usuń], a następnie [OK],
- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] zalecane jest zaznaczenie w części **Tymczasowe pliki internetowe** opcji: *Za każdym razem, gdy odwiedzam tę stronę*,



- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] proponuje się ustawienie w części **Historia liczby dni trzymania stron w historii** na 0,
- w celu poprawnego wyglądu aplikacji po wciśnięciu w części **Wygląd** przycisku [Dostępność...] powinny być odznaczone opcje *Ignoruj kolory określone na stronach sieci Web*, *Ignoruj style określone na stronach sieci Web*, *Ignoruj rozmiary czcionek określone na stronach sieci Web*, *Formatuj dokumenty, używając mojego arkusza stylów*.



W zakładce *Zabezpieczenia*:
- dla Internetu zaleca się ustawienie poziomu zabezpieczeń na Średnio-wysoki.



Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Poziom niestandardowy] powinny być wybrane następujące ustawienia:

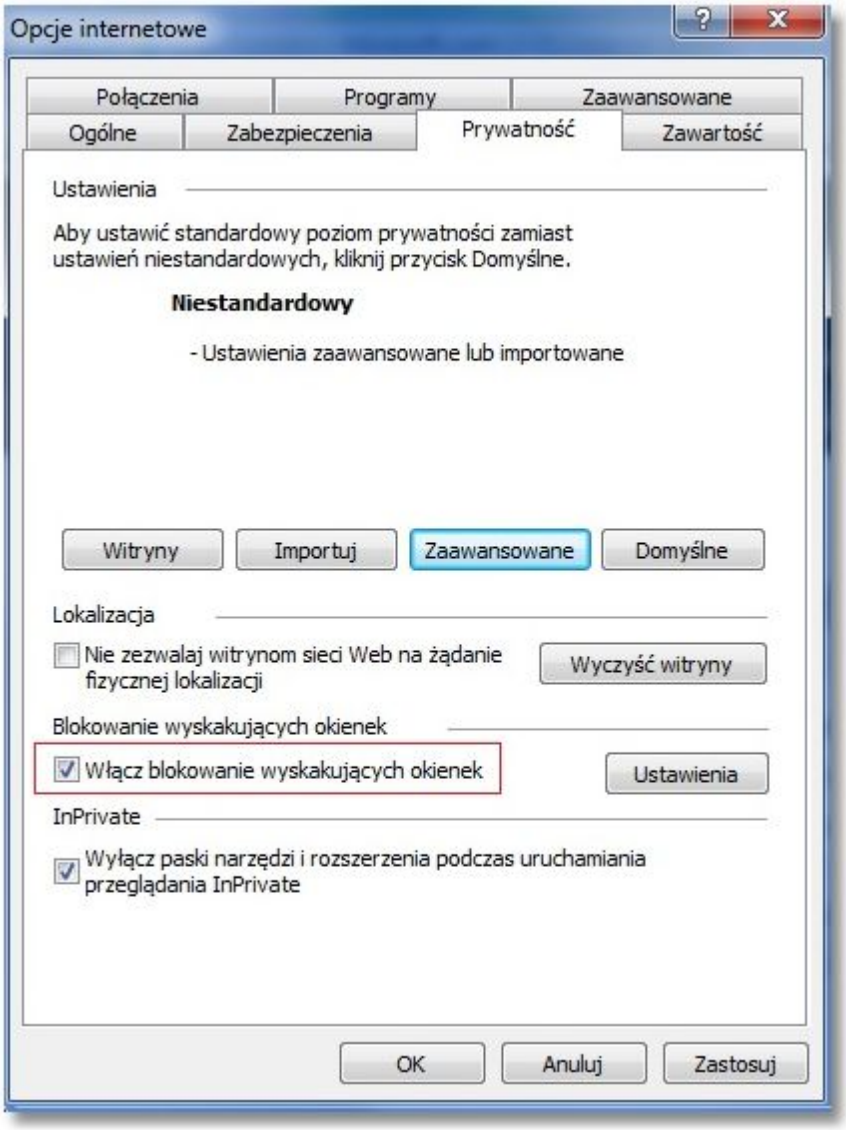
- w części **Kontrolki ActiveX i wtyczki** powinny być wyłączone opcje *Inicjowanie i wykonywanie skryptów kontrolek ActiveX niezaznaczonych jako bezpieczne do wykonania*, *Pobieranie niepodpisanych kontrolek ActiveX* oraz *Zezwalaj na uruchamianie poprzednio nie używanych kontrolek ActiveX bez monitorowania*
- w części **Obsługa skryptów** powinny być włączone opcje *Włącz filtr XSS, Wykonywanie skryptów apletów języka Java*
- w części **Różne** powinna być wyłączona opcja *Nawigowanie ramek podrzędnych w różnych domenach*

W zakładce *Prywatność*:

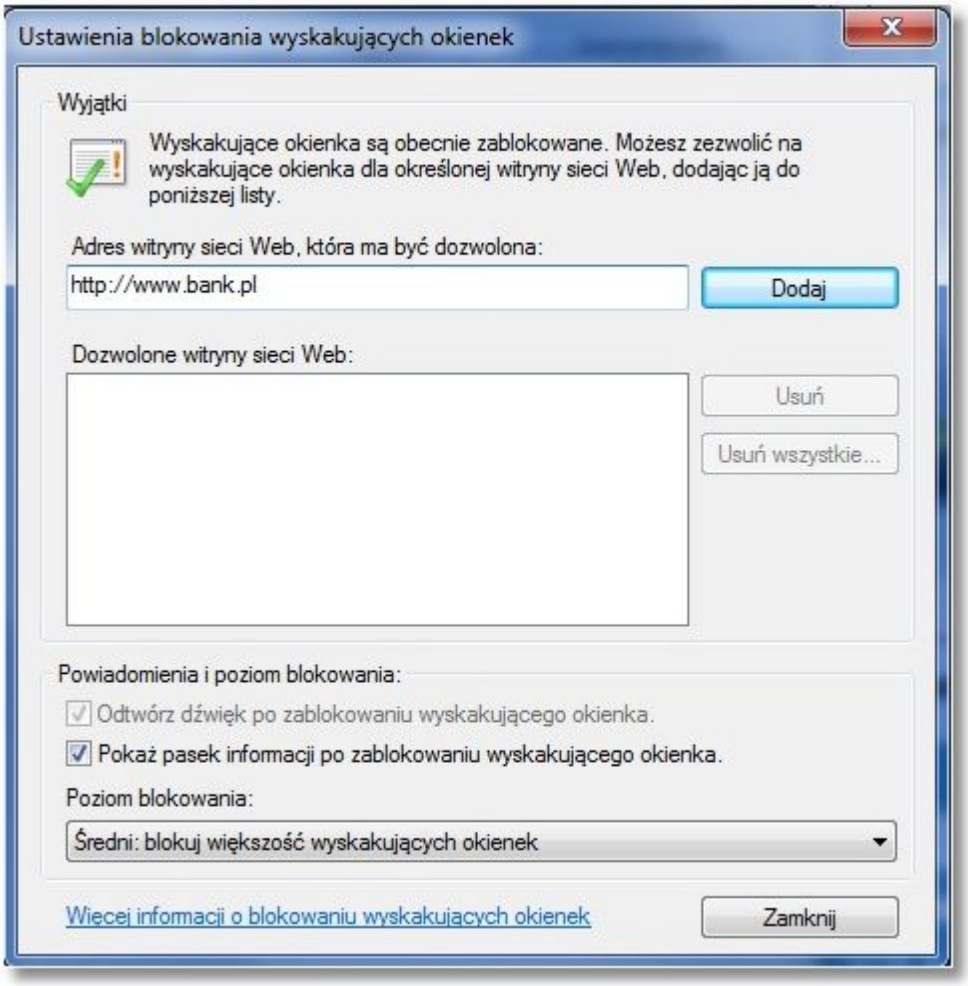
- w części **Ustawienia** zaleca się wybrać ustawienie prywatności dla strefy internetowej na Średni.

Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Zaawansowane] powinny być wybrane następujące ustawienia:

- w części **Blokowanie wyskakujących okienek** należy zaznaczyć opcję *Włącz blokowanie wyskakujących okienek*.

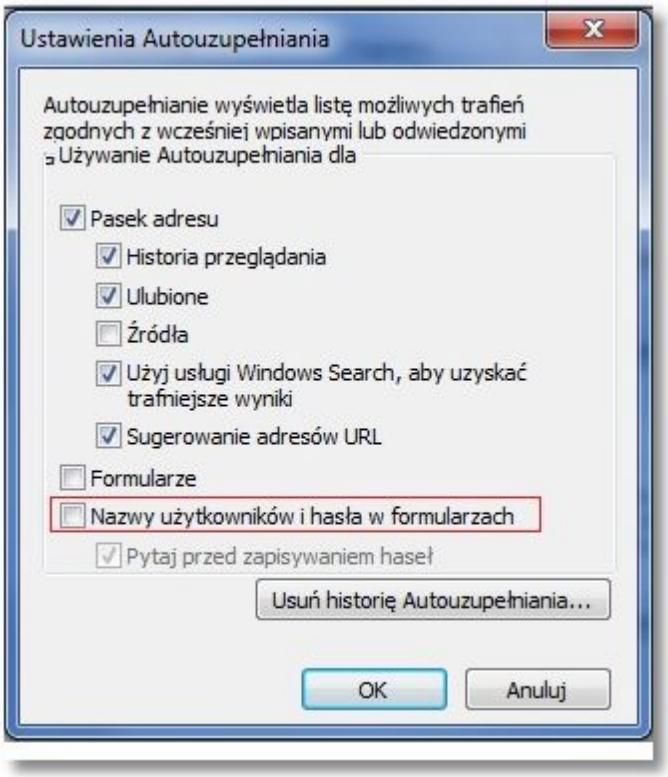


Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji.
W tym celu należy w zakładce *Prywatność* w części **Blokowanie wyskakujących okienek** w opcji *Ustawienia* wpisać adres strony banku internetowego oraz nacisnąć przycisk [Dodaj].



W zakładce *Zawartość*:

- zaleca się w sekcji **Autouzupełnianie** po wciśnięciu przycisku [Ustawienia] odznaczyć opcję *Nazwy użytkowników i hasła w formularzach*.



W zakładce *Zaawansowane*:

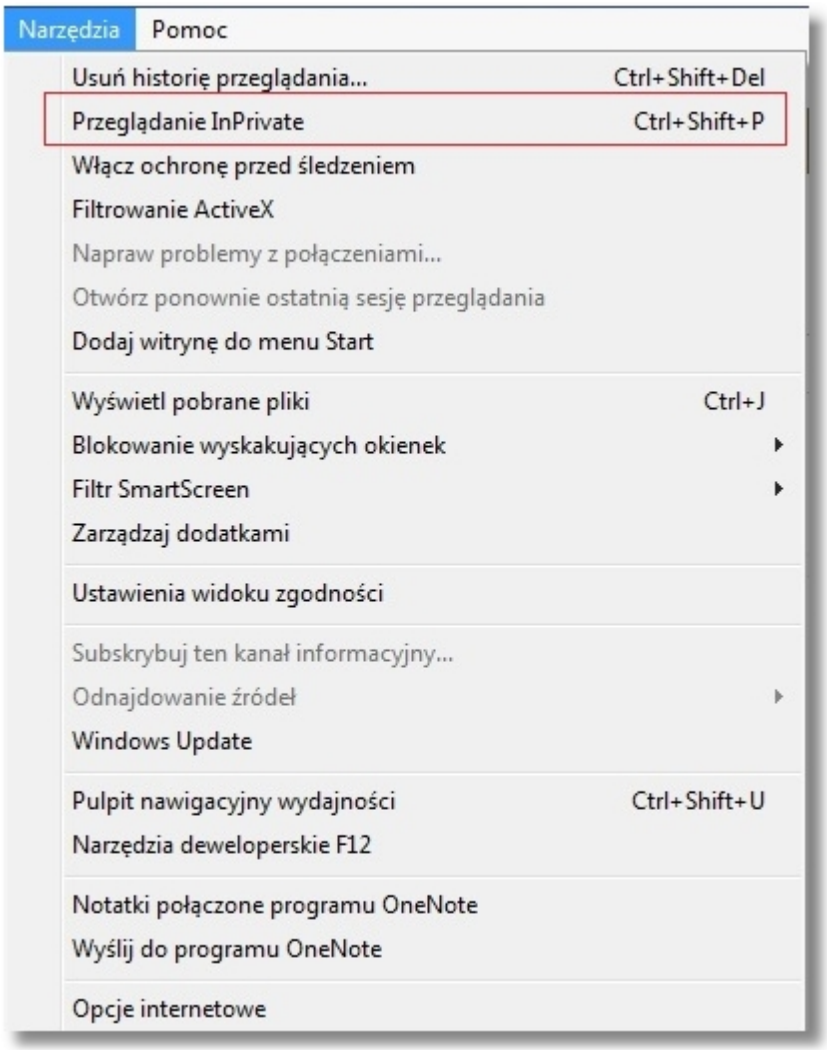
- w części **Multimedia** dla poprawnego wyświetlania grafiki na stronach aplikacji powinna być zaznaczona opcja *Pokaż obrazy*,
- w części **Przeglądanie** powinna być zaznaczona opcja Pokaż przyjazne komunikaty o błędach HTTP
- w części **Zabezpieczenia** należy zaznaczyć: Nie zapisuj zaszyfrowanych stron na dysku, Ostrzegaj przed niezgodnością adresów certyfikatów, Ostrzegaj przed zmianą trybu zabezpieczonego na niebezpieczny, Sprawdzaj podpisy dla pobieranych programów, Sprawdź czy certyfikat serwera nie został cofnięty, Sprawdź czy certyfikat wydawcy nie został cofnięty, użyj SSL 3.0, użyj TLS 1.0, Włącz filtr SmartScreen, Włącz obsługę macierzystego protokołu XMLHTTP, Włącz przechowywanie DOM, Włącz zintegrowane uwierzytelnianie systemu Windows

Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

Rozdział 7. Konfiguracja przeglądarki Internet Explorer 11.0

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Internet Explorer w wersji 11.0 wspiera następujące systemy operacyjne: Windows Vistax32, Windows Vistax64, Windows 7x32, Windows 7x64.
Przeglądarka Internet Explorer 11.0 zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecane jest użycie jednej z dwóch funkcjonalności dostępnych na pasku zakładek w menu *Bezpieczeństwo*:

- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej włączenie trybu **Przeglądanie InPrivate**, zaś po jej zakończeniu zamknięcie okna przeglądarki.
- Jeśli nie używano trybu **Przeglądanie InPrivate**, po zakończeniu pracy zalecamy użycie funkcji **Usuń historię przeglądania** (Ctrl+Shift+Del).

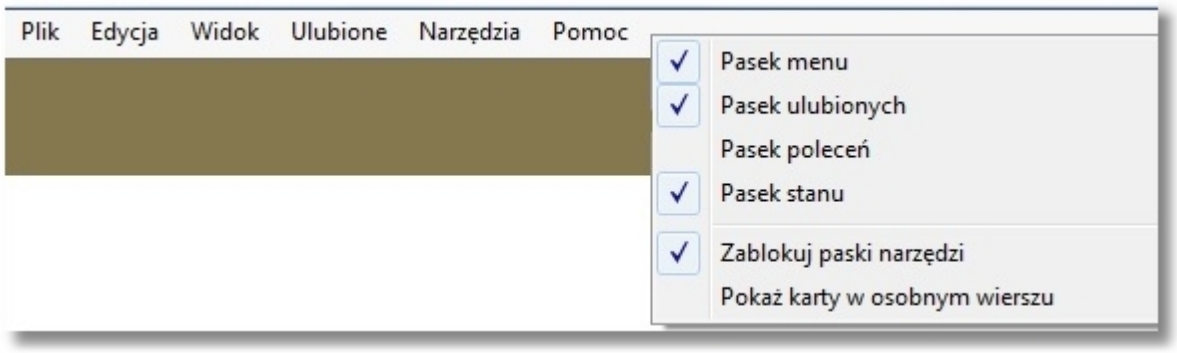


Funkcja **Przeglądanie InPrivate** umożliwia zachowanie poufności historii przeglądania na współużytkowanych komputerach. Dane historii zbierane w czasie przeglądania sieci Web przez okno programu Internet Explorer w trybie InPrivate, np. tymczasowe pliki internetowe, historia adresów internetowych lub pliki cookie, zostaną usunięte po zamknięciu okna. Nie ma to wpływu na historię w innych oknach programu Internet Explorer (w których nie jest używane przeglądanie InPrivate).
Przeglądanie InPrivate zapobiega lokalnemu przechowywaniu na komputerze następujących elementów:

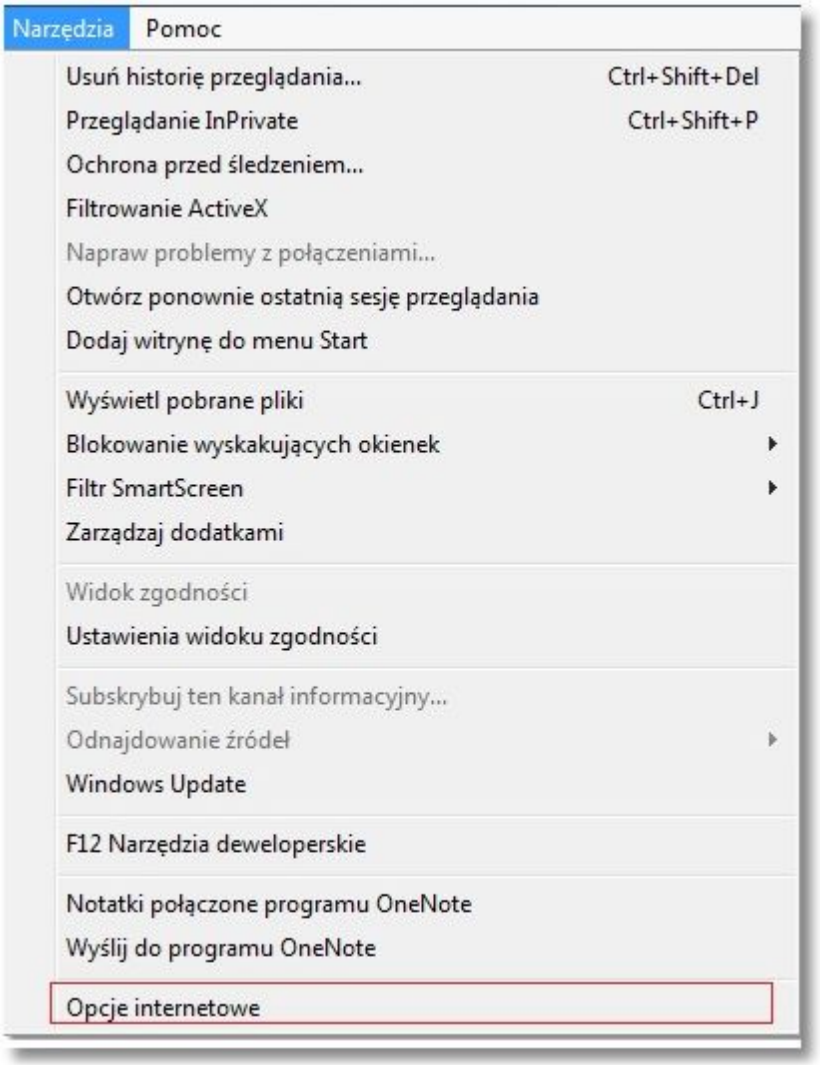
- Nowe pliki cookie nie są przechowywane.
- Nowe wpisy historii nie są rejestrowane.
- Nowe tymczasowe pliki internetowe zostaną usunięte po zamknięciu okna *Przeglądania InPrivate*.
- Dane formularzy nie są przechowywane.
- Wprowadzone hasła nie są przechowywane.
- Adresy wpisane na pasku adresu nie są przechowywane.
- Zapytania wpisane w polu wyszukiwania nie są przechowywane.

Oprócz tego program Internet Explorer wysyła do witryn sieci Web żądanie *Nie śledź w czasie sesji Przeglądania InPrivate*. Przeglądanie **InPrivate** nie jest przeznaczone do ukrywania tożsamości przez użytkownika przed usługodawcą internetowym ani serwerami sieci Web w Internecie. Funkcja ta nie zapobiega wysyłaniu danych, takich jak adres IP użytkownika, do odwiedzanych witryn sieci Web.

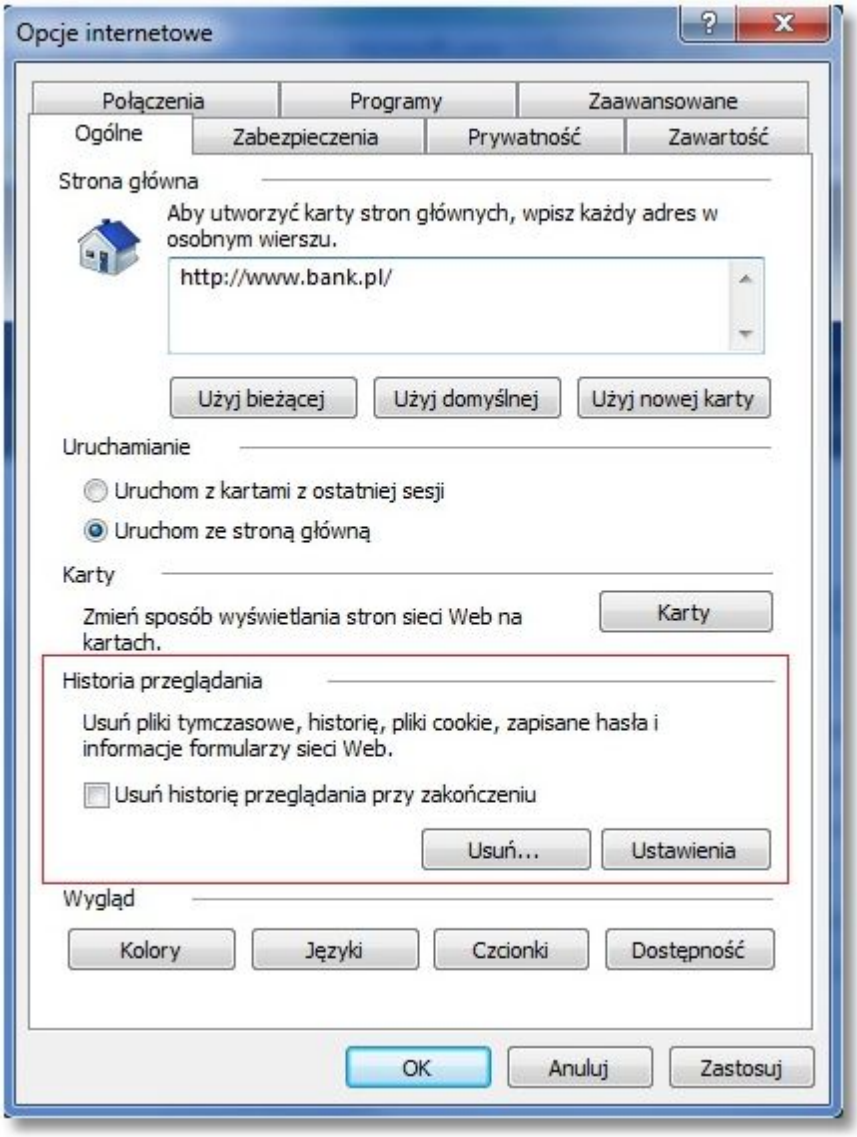
Domyślnie przeglądarka Internet Explorer w wersji 11.0 nie pokazuje paska menu. W celu wyświetlenia paska menu należy nacisnąć lewy klawisz Alt na klawiaturze, następnie ustawić kursor myszy na pasku menu, kliknąć prawy przycisk myszy oraz zaznaczyć opcję *Pasek menu*. Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.



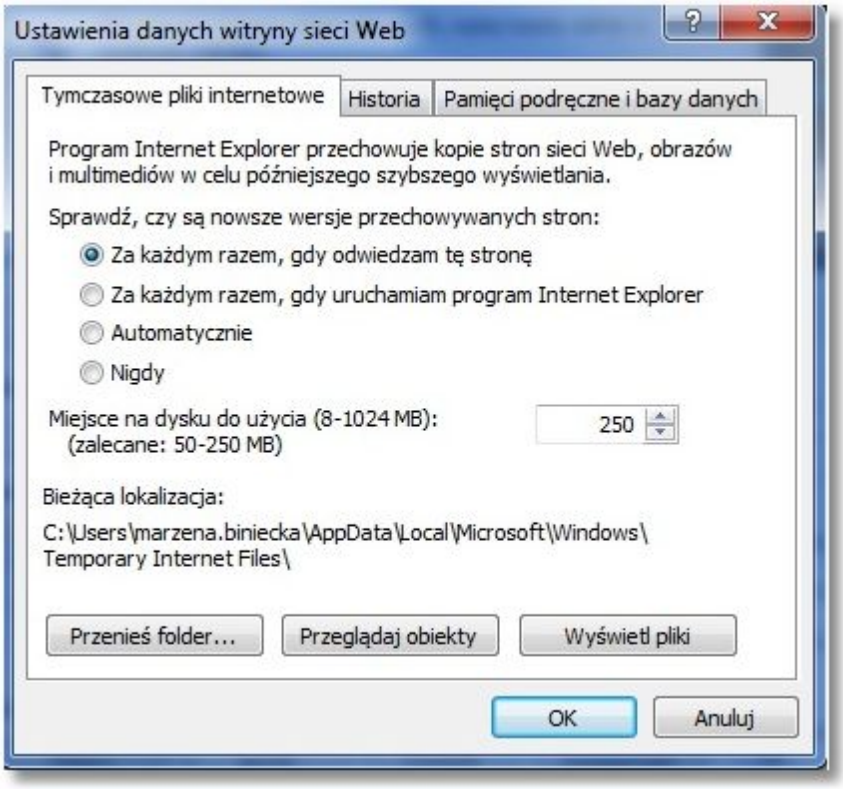
Aby poprawnie skonfigurować przeglądarkę, z menu *Narzędzia* należy wybrać *Opcje internetowe*.



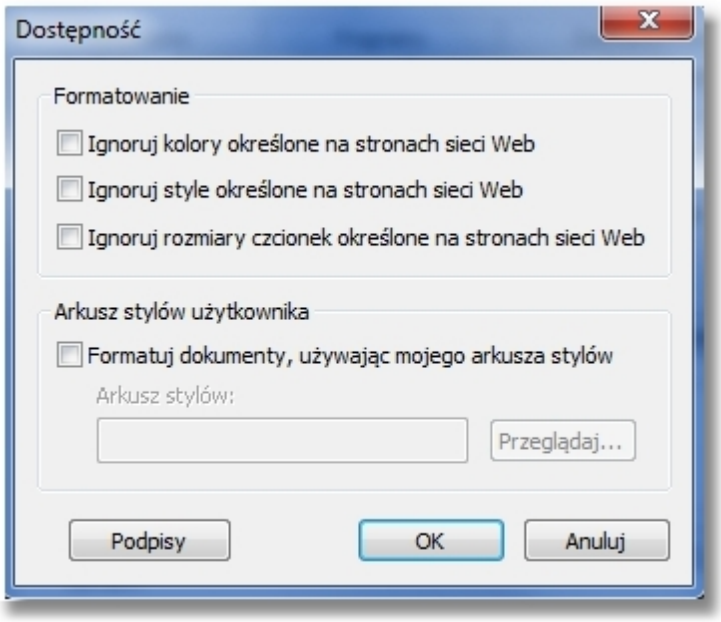
W zakładce *Ogólne*:



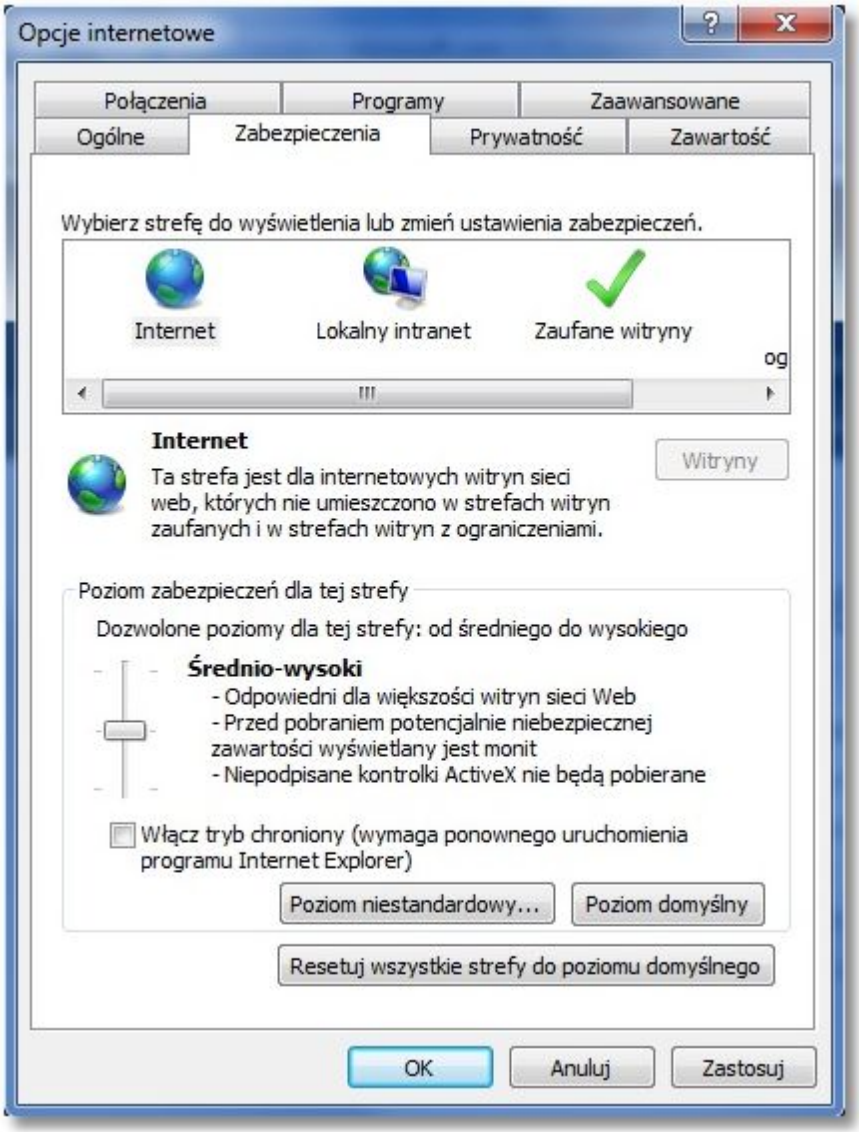
- w sekcji **Historia przeglądania** zalecane jest usunięcie plików tymczasowych, plików cookie, historii, danych formularzy i haseł; w tym celu należy wybrać przycisk [Usuń], a następnie na formatce *Usuwanie historii przeglądania* nacisnąć przycisk [Usuń] (lub po kolei wstawić znaczniki przy pozycjach: Pliki cookie i dane witryn sieci WEB, Historia, Historia pobierania, Dane formularzy, Hasła) i zatwierdzić przyciskiem Usuń] a następnie [OK],
- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] zalecane jest zaznaczenie w części **Tymczasowe pliki internetowe** opcji: *Za każdym razem, gdy odwiedzam tę stronę*,



- w sekcji **Historia przeglądania** po naciśnięciu przycisku [Ustawienia] proponuje się ustawienie w części **Historia liczby dni trzymania stron w historii** na 0,
- w celu poprawnego wyglądu aplikacji po wciśnięciu w części **Wygląd** przycisku [Dostępność...] powinny być odznaczone opcje *Ignoruj kolory określone na stronach sieci Web*, *Ignoruj style określone na stronach sieci Web*, *Ignoruj rozmiary czcionek określone na stronach sieci Web*, *Formatuj dokumenty, używając mojego arkusza stylów*.



W zakładce *Zabezpieczenia*:
- dla Internetu zaleca się ustawienie poziomu zabezpieczeń na *Średnio-wysoki*.



Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Poziom niestandardowy] powinny być wybrane następujące ustawienia:

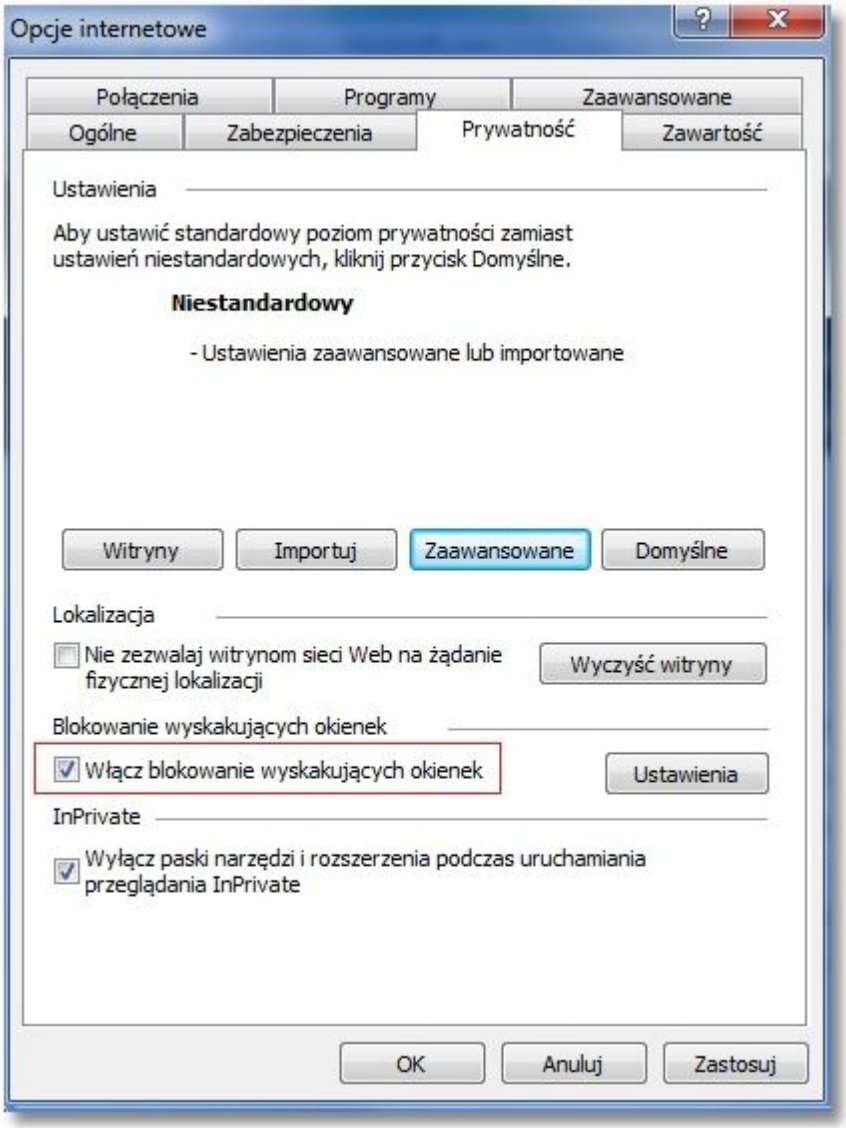
- w części **Kontrolki ActiveX i wtyczki** powinny być wyłączone opcje *Inicjowanie i wykonywanie skryptów kontrolek ActiveX niezaznaczonych jako bezpieczne do wykonania*, *Pobieranie niepodpisanych kontrolek ActiveX* oraz *Zezwalaj na uruchamianie poprzednio nie używanych kontrolek ActiveX bez monitorowania*
- w części **Obsługa skryptów** powinny być włączone opcje *Włącz filtr XSS, Wykonywanie skryptów apletów języka Java*
- w części **Różne** powinna być wyłączona opcja *Nawigowanie ramek podrzędnych w różnych domenach*

W zakładce *Prywatność*:

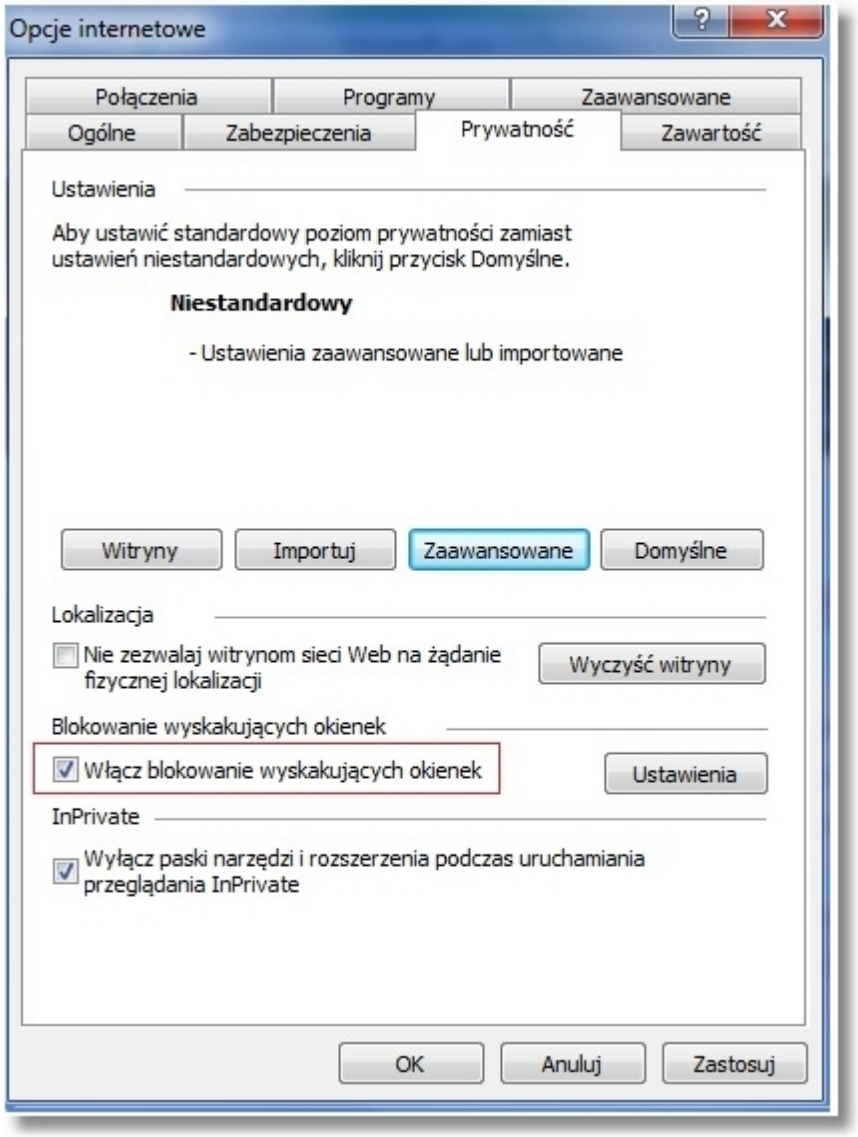
- w części **Ustawienia** zaleca się wybrać ustawienie prywatności dla strefy internetowej na Średni.

Jeżeli użytkownik stosuje niestandardowy poziom zabezpieczeń, to dodatkowo po naciśnięciu przycisku [Zaawansowane] powinny być wybrane następujące ustawienia:

- w części **Blokowanie wyskakujących okienek** należy zaznaczyć opcję *Włącz blokowanie wyskakujących okienek*.

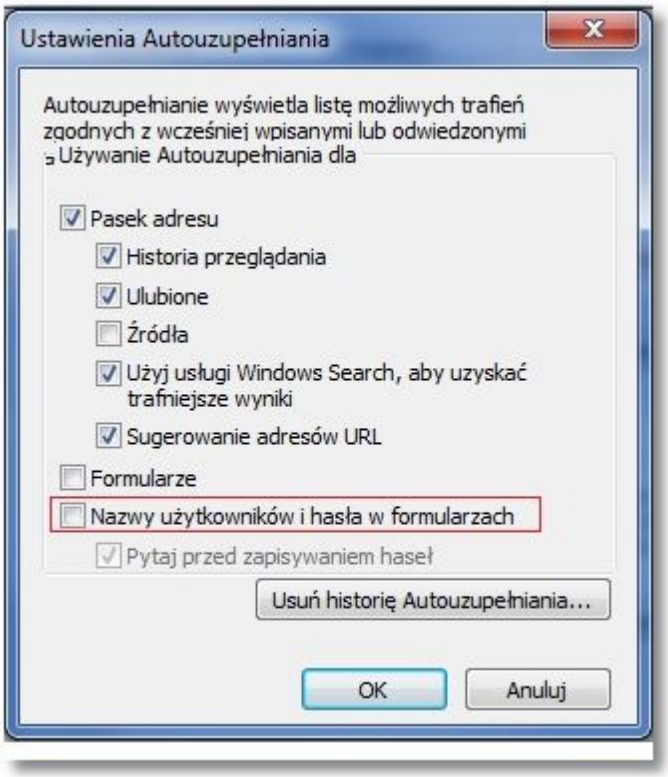


Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji.
W tym celu należy w zakładce *Prywatność* w części **Blokowanie wyskakujących okienek** w opcji *Ustawienia* wpisać adres strony banku internetowego oraz nacisnąć przycisk [Dodaj].



W zakładce *Zawartość*:

- zaleca się w sekcji **Autouzupełnianie** po wciśnięciu przycisku [Ustawienia] odznaczyć opcję *Nazwy użytkowników i hasła w formularzach*.



W zakładce *Zaawansowane*:

- w części **Multimedia** dla poprawnego wyświetlania grafiki na stronach aplikacji powinna być zaznaczona opcja *Pokaż obrazy*,
- w części **Przeglądanie** powinna być zaznaczona opcja *Pokaż przyjazne komunikaty o błędach HTTP*
- w części **Zabezpieczenia** należy zaznaczyć: Nie zapisuj zaszyfrowanych stron na dysku, Ostrzegaj przed niezgodnością adresów certyfikatów, Ostrzegaj przed zmianą trybu zabezpieczonego na niebezpieczny, Sprawdzaj podpisy dla pobieranych programów, Sprawdź czy certyfikat serwera nie został cofnięty, Sprawdź czy certyfikat wydawcy nie został cofnięty, użyj TLS 1.0, Włącz filtr SmartScreen, Włącz obsługę macierzystego protokołu XMLHTTP, Włącz przechowywanie DOM, Włącz zintegrowane uwierzytelnianie systemu Windows,
- w części **Zabezpieczenia** należy odznaczyć: *Użyj SSL3.0.*

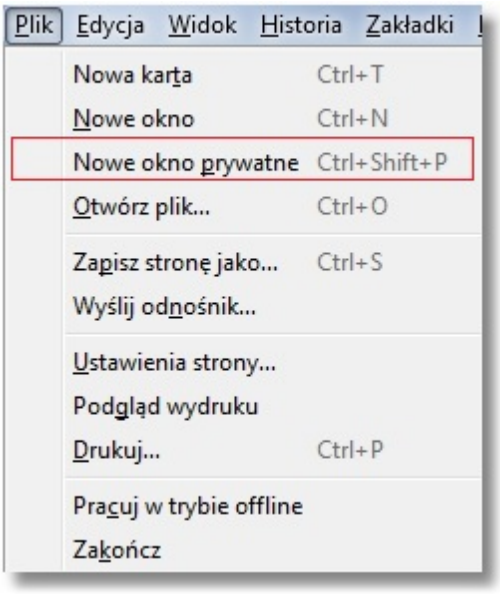
Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

Rozdział 8. Konfiguracja przeglądarki Firefox 32.0

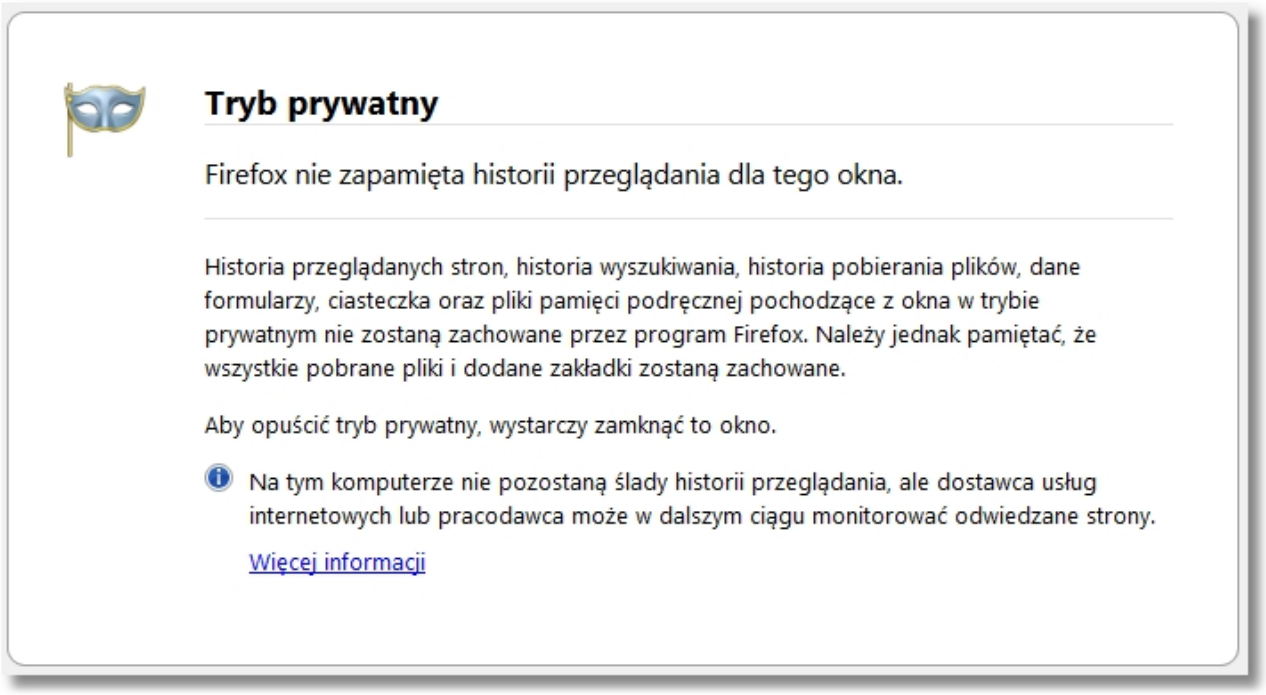
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Firefox w wersji 32.0 wspiera następujące systemy operacyjne: Windows 2000 / XP / Vista / Windows7 / XP64 / Vista64 / Windows7 64 / Windows8 / Windows8 64.
Znacznie poprawiony został tryb prywatności, między innymi możliwe jest kasowanie wszystkich prywatnych danych przy zamknięciu przeglądarki. W trybie prywatnym Firefox nie zachowa historii przeglądanych stron, historii wyszukiwania, historii pobierania plików, danych formularzy, ciasteczek oraz plików pamięci podręcznej.
Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład jest to komputer, z którego w firmie korzystają inni pracownicy lub publiczny komputer w kafejce internetowej, bibliotece itp.) zalecane jest:

- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej przejście w prywatny tryb przeglądania sieci, zaś po zakończonej sesji - jego wyłączenie lub zamknięcie przeglądarki.
- Jeśli nie użyto trybu prywatnego, zalecane jest po zakończonej pracy wejście w historię przeglądania i usunięcie wpisu dotyczącego Systemu Bankowości Internetowej przez wybranie opcji *usuń całą witrynę*.
- Alternatywnie można usunąć całość historii przeglądania z ostatnich kilku godzin lub całego dnia.

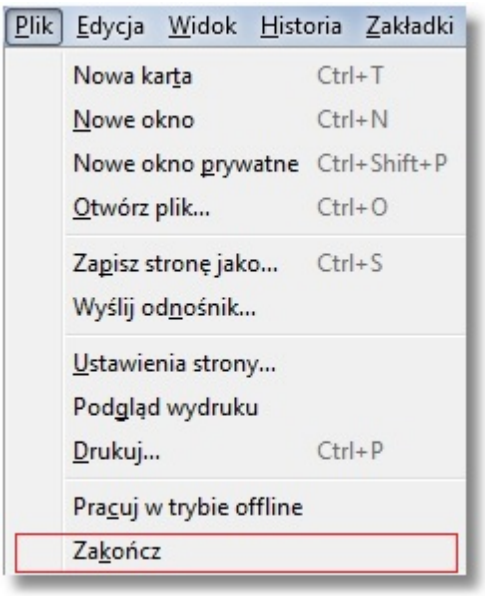
Prywatny tryb przeglądania sieci upraszcza ochronę informacji prywatnych. By go włączyć należy wybrać z menu *Plik*, następnie wybrać *Nowe okno prywatne* lub nacisnąć [Crtl]+[Shift]+[P]. W chwili przejścia do tego trybu przeglądarka zapamiętuje aktualnie otwarte karty, po czym zamyka je i otwiera tylko jedną, czystą kartę.



Od tej pory wszystkie czynności użytkownika podlegają specjalnej ochronie. Firefox nie zachowa historii przeglądanych stron, historii wyszukiwania, historii pobierania plików, danych formularzy, ciasteczek (cookies) oraz plików pamięci podręcznej. W ten sposób wrażliwe dane użytkownika po zakończeniu korzystania z sieci Internet nie zostaną narażone na nawet przypadkowe ujawnienie.

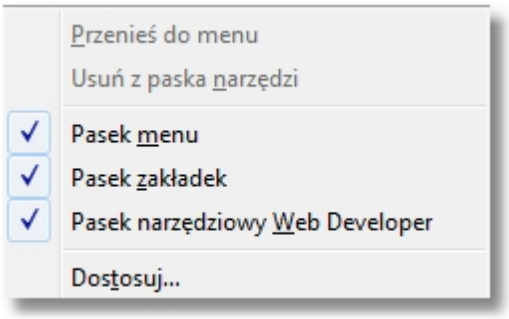


Po zakończeniu pracy w trybie prywatnym (w menu *Plik*) należy wybrać opcję *Zakończ*. Informacje związane z przeglądanymi stronami zostaną bezpiecznie usunięte, a zapamiętane wcześniej karty zostaną ponownie otwarte.

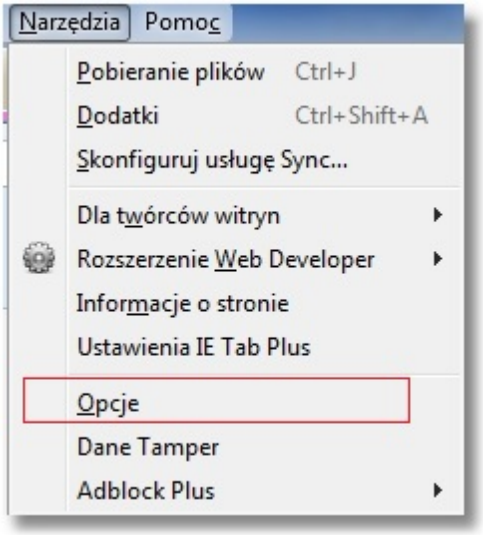


Usuwanie całej witryny z historii przeglądania jest przydatne, jeśli chcemy by przeglądarka "zapominała", że dana witryna była odwiedzana. W celu usunięcia całej witryny z historii przeglądania należy otworzyć historię przeglądania (wybrać z menu *Historia*), następnie opcję *Wyświetl całą historię* albo nacisnąć [Crtl]+[H] i kliknąć prawym przyciskiem myszy w stronę, której chcemy się pozbyć. Następnie należy wybrać z menu kontekstowego *Usuń całą witrynę*.
Zachęcamy do korzystania z trybu prywatnego – pomaga on poprawić bezpieczeństwo i chroni wrażliwe dane użytkownika przed przypadkowym ujawnieniem.

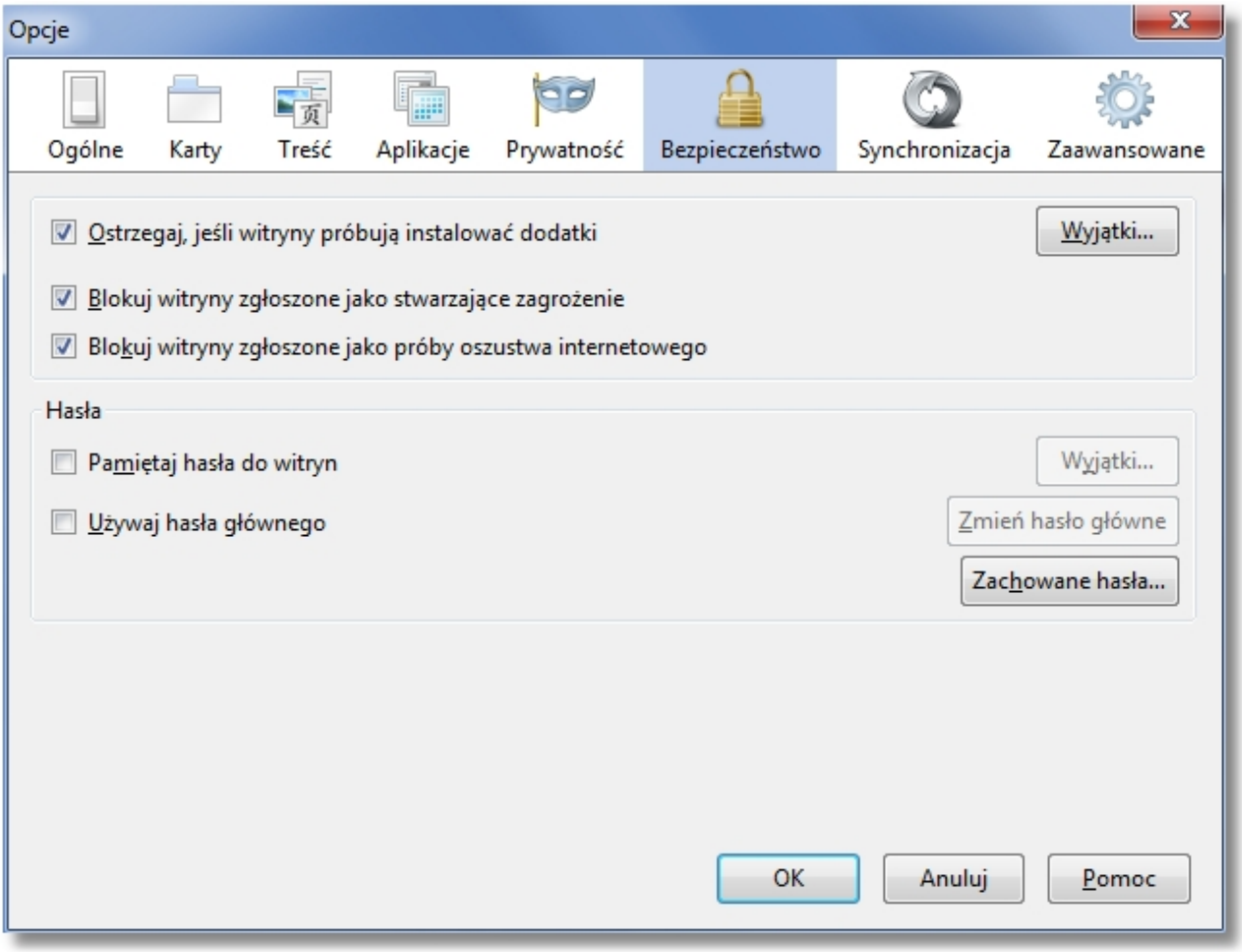
Domyślnie przeglądarka Firefox w wersji 32.0 nie pokazuje paska menu. W celu wyświetlenia paska menu należy ustawić kursor myszy na pasku menu, kliknąć prawy przycisk myszy oraz zaznaczyć opcję *Pasek menu*. Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.



W celu poprawnego skonfigurowania przeglądarki, z górnego menu przeglądarki należy wybrać *Narzędzia* a następnie *Opcje* i skonfigurować jak poniżej:



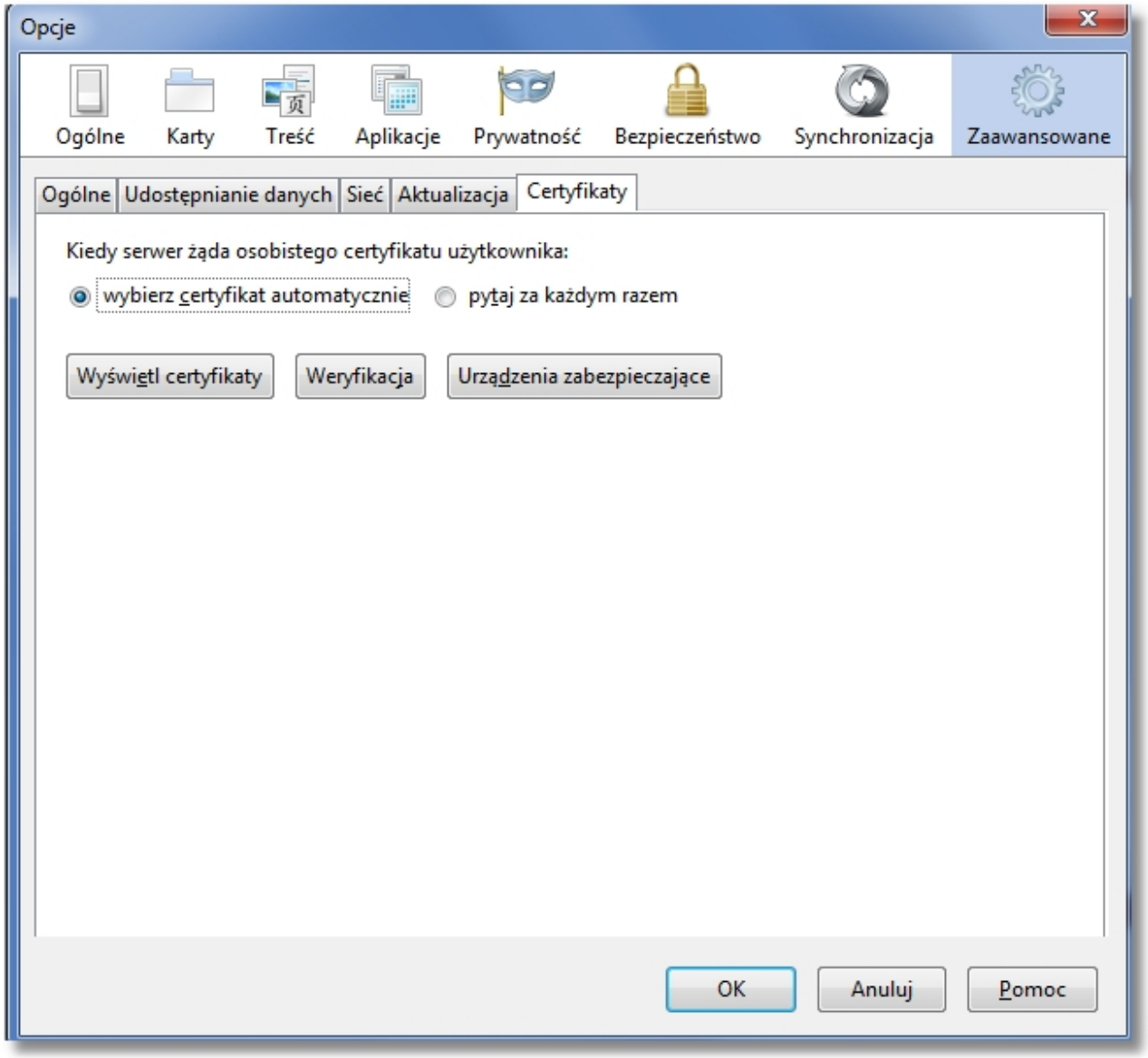
W opcji *Bezpieczeństwo* należy:
- zaznaczyć opcję *Ostrzegaj, kiedy witryny próbują instalować dodatki*,
- zaznaczyć opcję *Blokuj zgłoszone witryny stwarzające zagrożenie*,
- zaznaczyć opcję *Blokuj zgłoszone próby oszustwa internetowego*,
- w sekcji **Hasła** odznaczyć opcje: *Pamiętaj hasła do witryn* oraz *Używaj hasła głównego*.



Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

W opcji *Zaawansowane* zakładka *Certyfikaty* należy:

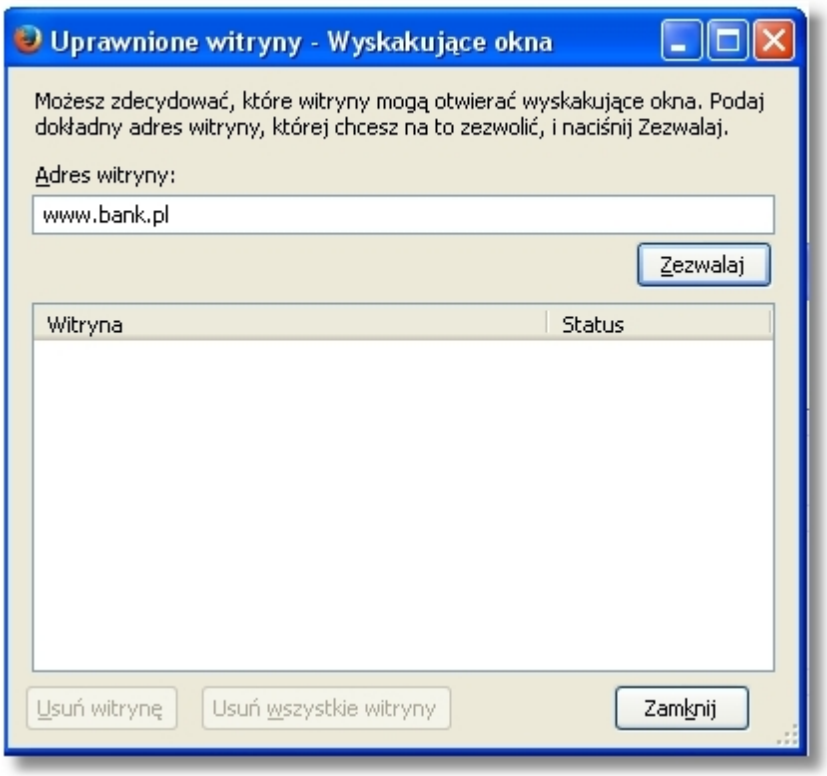
- w sekcji **Certyfikaty**: Kiedy serwer żąda osobistego certyfikatu użytkownika włączyć: *wybierz certyfikat automatycznie.*



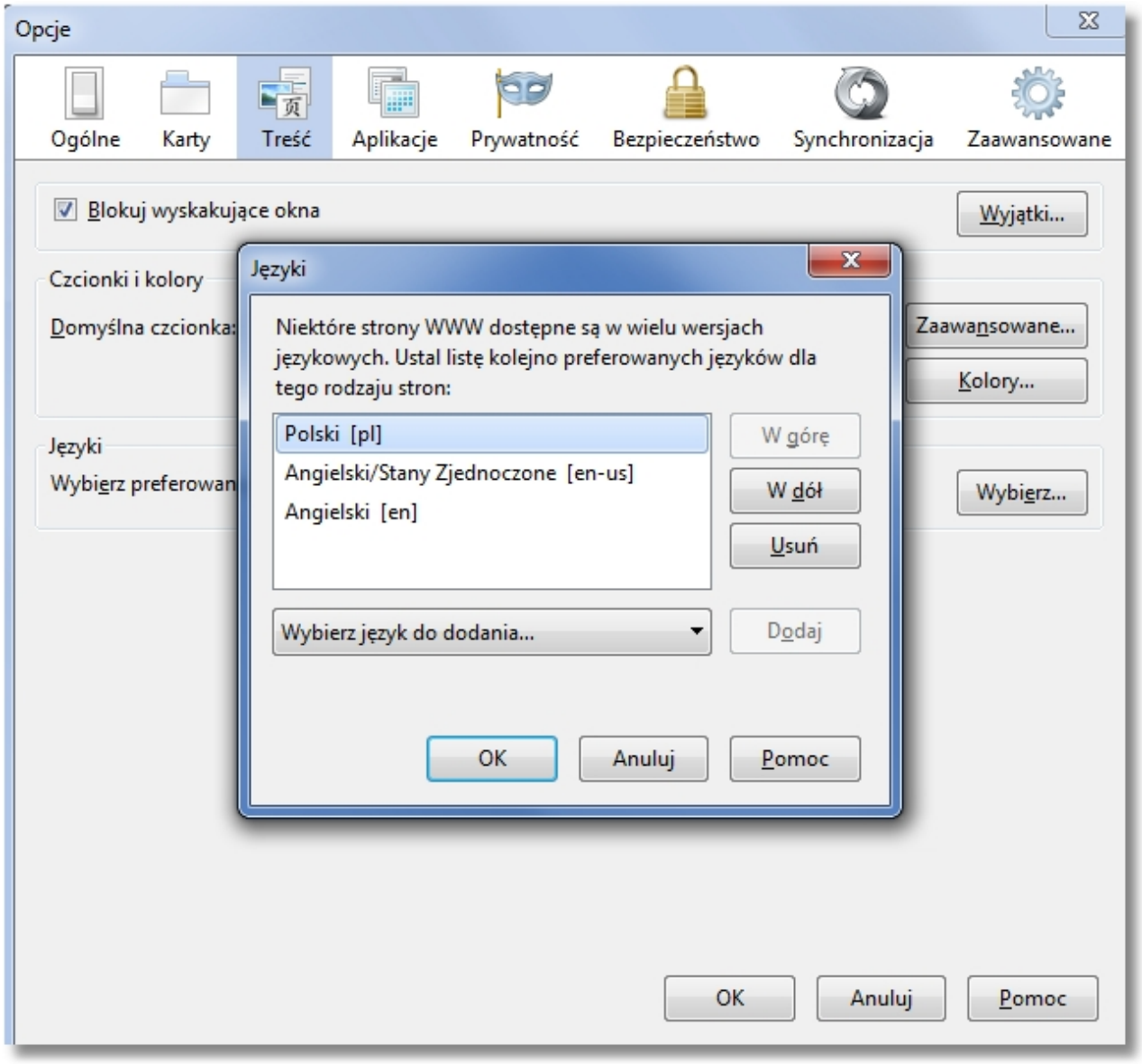
Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

W opcji *Treść* należy:

- zaznaczyć parametr **Zablokuj wyskakujące okna**. Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy w opcji *Wyjątki...* wpisać adres strony banku internetowego a następnie zezwolić na wyskakujące okienka dla tej strony przyciskiem [Zezwól].



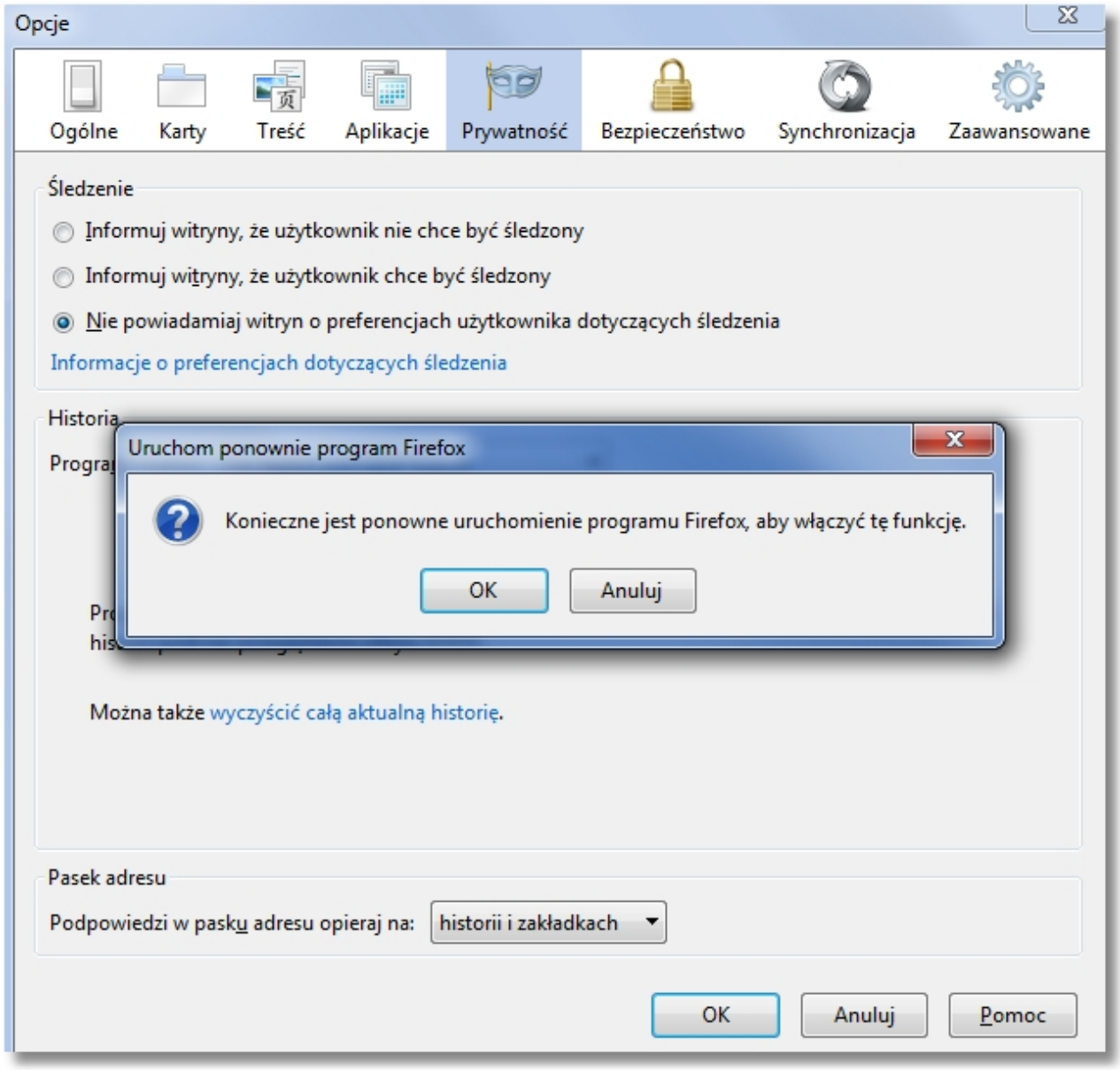
w sekcji **Języki** kliknąć na przycisk [Wybierz...], z listy wybrać Polski [pl] i dodać go do listy języków za pomocą przycisku [Dodaj] a następnie za pomocą przycisku [W górę] ustawić Polski [pl] jako pierwszy element na liście.



Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

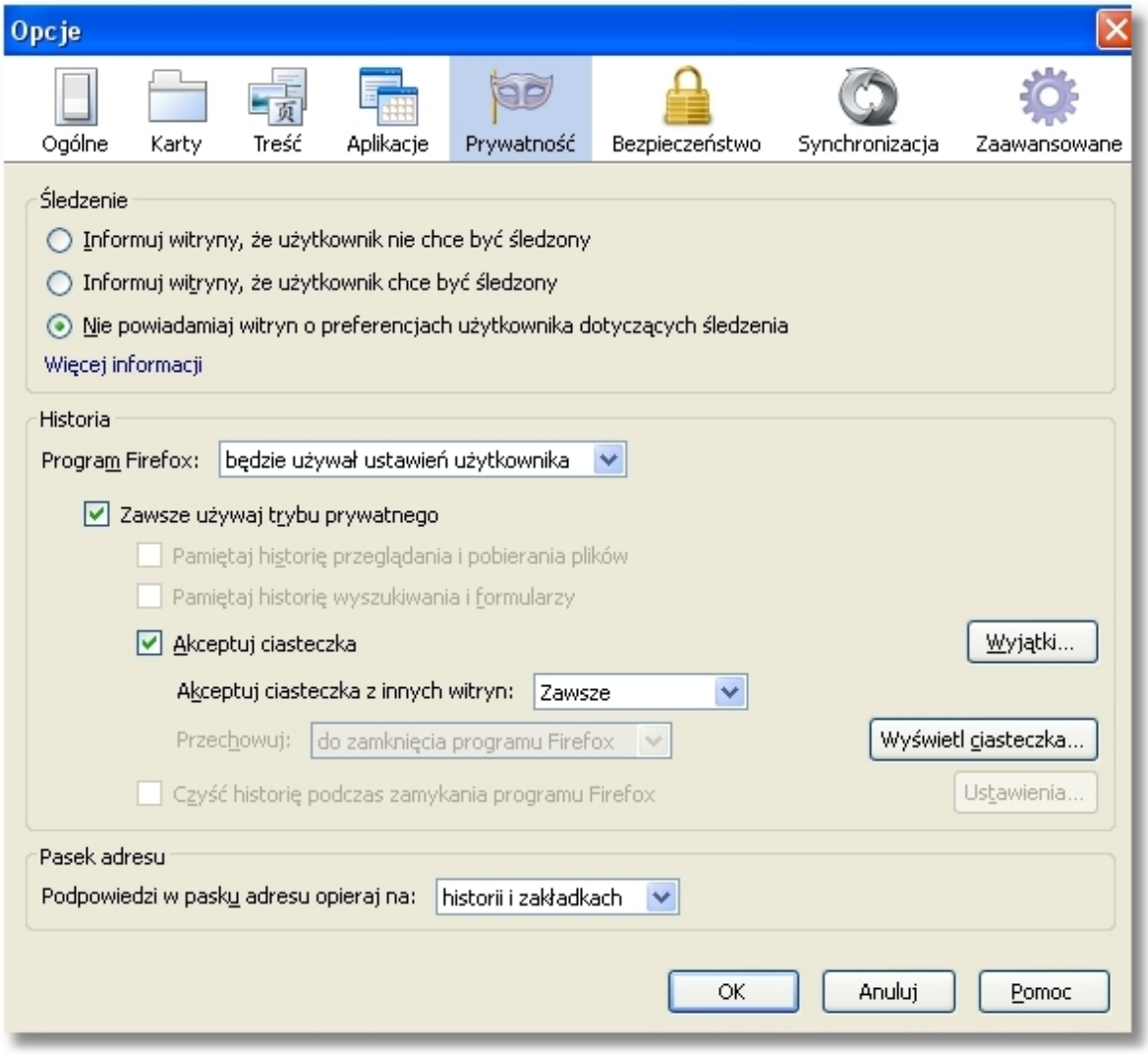
W opcji *Prywatność* w sekcji **Historia** należy:

- wybrać opcję: *nie będzie pamiętał historii*. W przypadku wyboru tej opcji program Firefox będzie używał tych samych ustawień co w trybie prywatnym i nie będzie zapisywał historii podczas przeglądania stron WWW.



lub

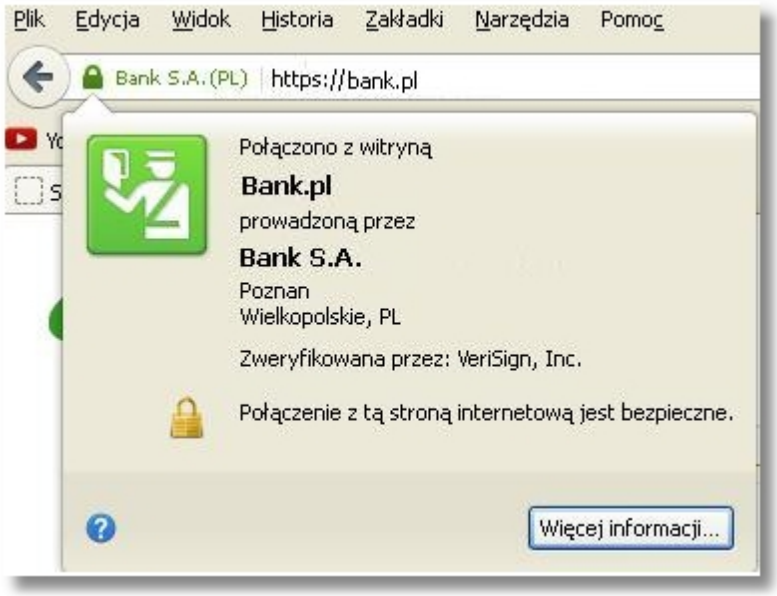
- w przypadku wyboru opcji: *będzie używał ustawień użytkownika* dla pola **Program Firefox** należy zaznaczyć opcję: *Zawsze używaj trybu prywatnego* oraz *Akceptuj ciasteczka* a następnie wybrać [OK].

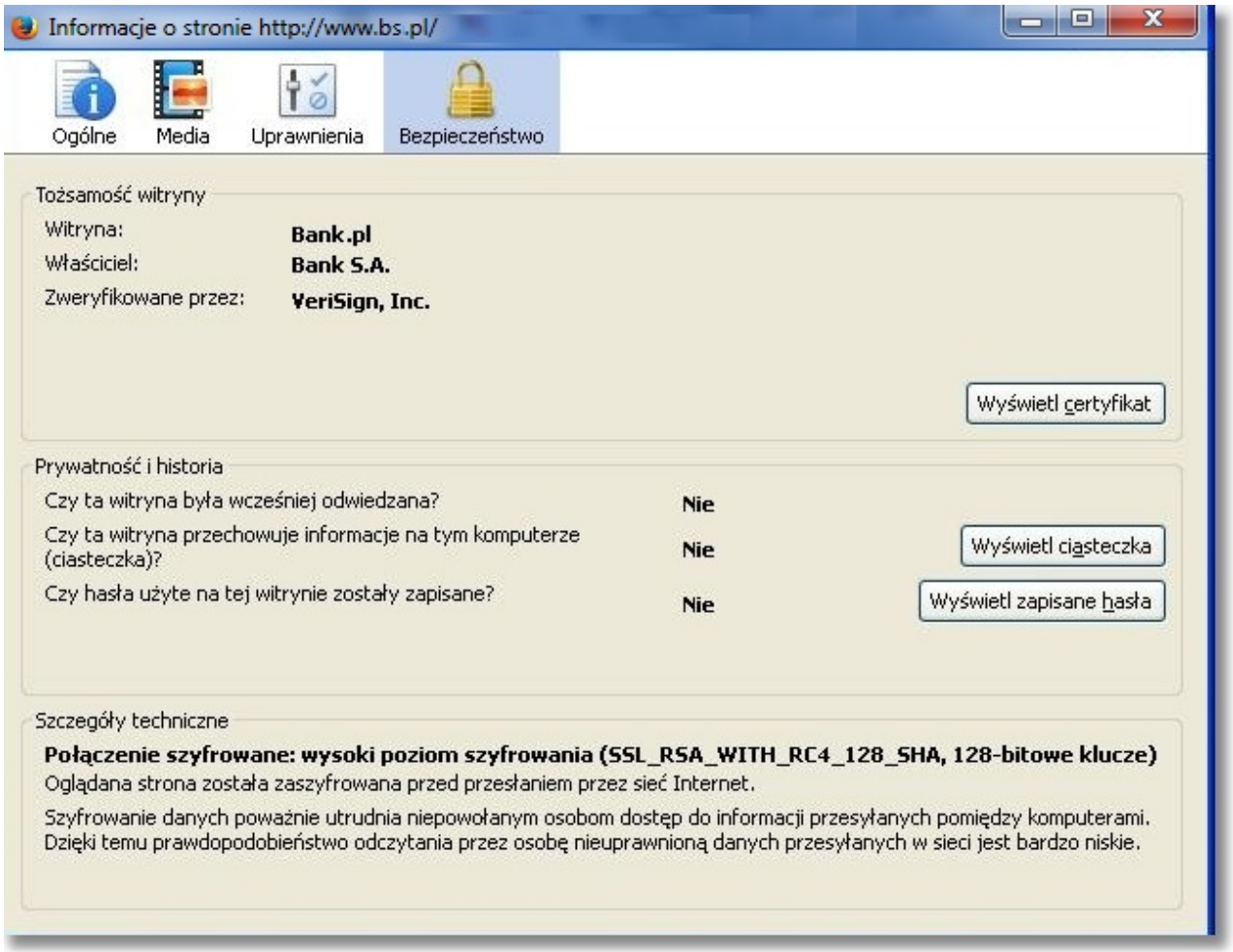


Wybór opcji opisanych powyżej spowoduje wyświetlenie komunikatu o treści: *"Konieczne jest ponowne uruchomienie programu Firefox, aby włączyć tę funkcję."*

Jeżeli z jakiegoś powodu opisane ustawienia ciasteczek nie są odpowiednie dla wszystkich stron przeglądanych przez użytkownika, zapamiętywaniem ciasteczek można sterować indywidualnie dla wybranych stron.
W tym celu po zalogowaniu do systemu bankowości internetowej należy wybrać z menu *Narzędzia* opcję *Informacje o stronie*. W oknie informacji należy wybrać *Uprawnienia*, następnie upewnić się, że poniżej wyświetlony jest napis przykładowo: *"Uprawnienia dla: www.bank.pl"* i w sekcji **Zapisywanie ciasteczek** usunąć zaznaczenie *Użyj domyślnych* i wybrać opcję *Zezwalaj na czas sesji*.

W celu wyświetlenia informacji o zabezpieczeniach związanych z szyfrowaniem witryny należy w przeglądarce Firefox w wersji 32.0 kliknąć na pasek adresu a dokładne w ikonkę strony a następnie wybrać przycisk [Więcej informacji ...] jak na poniższym ekranie.


Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
Bank S.A. (PL) https://bank.pl
Połączono z witryną
Bank.pl
prowadzoną przez
Bank S.A.
Poznan
Wielkopolskie, PL
Zweryfikowana przez: VeriSign, Inc.
Połączenie z tą stroną internetową jest bezpieczne.
Więcej informacji...

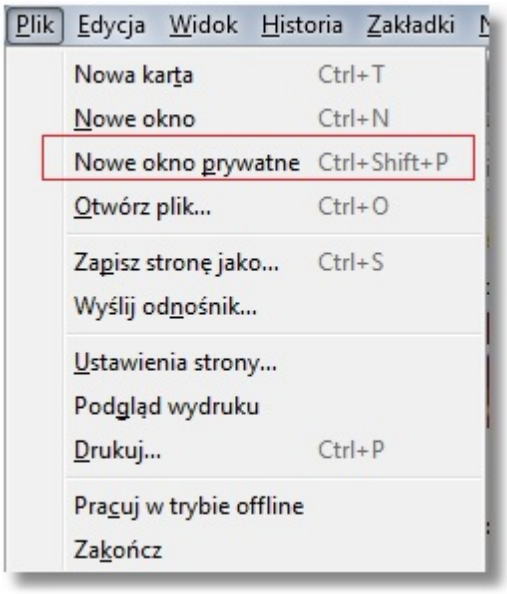

Informacje o stronie http://www.bs.pl/
Ogólne
Media
Uprawnienia
Bezpieczeństwo
Tożsamość witryny
Witryna: Bank.pl
Właściciel: Bank S.A.
Zweryfikowane przez: VeriSign, Inc.
Wyświetl certyfikat
Prywatność i historia
Czy ta witryna była wcześniej odwiedzana? Nie
Czy ta witryna przechowuje informacje na tym komputerze (ciasteczka)? Nie
Wyświetl ciasteczka
Czy hasła użyte na tej witrynie zostały zapisane? Nie
Wyświetl zapisane hasła
Szczegóły techniczne
Połączenie szyfrowane: wysoki poziom szyfrowania (SSL_RSA_WITH_RC4_128_SHA, 128-bitowe klucze)
Oglądana strona została zaszyfrowana przed przesłaniem przez sieć Internet.
Szyfrowanie danych poważnie utrudnia niepowołanym osobom dostęp do informacji przesyłanych pomiędzy komputerami. Dzięki temu prawdopodobieństwo odczytania przez osobę nieuprawnioną danych przesyłanych w sieci jest bardzo niskie.

Rozdział 9. Konfiguracja przeglądarki Firefox 37.0.2

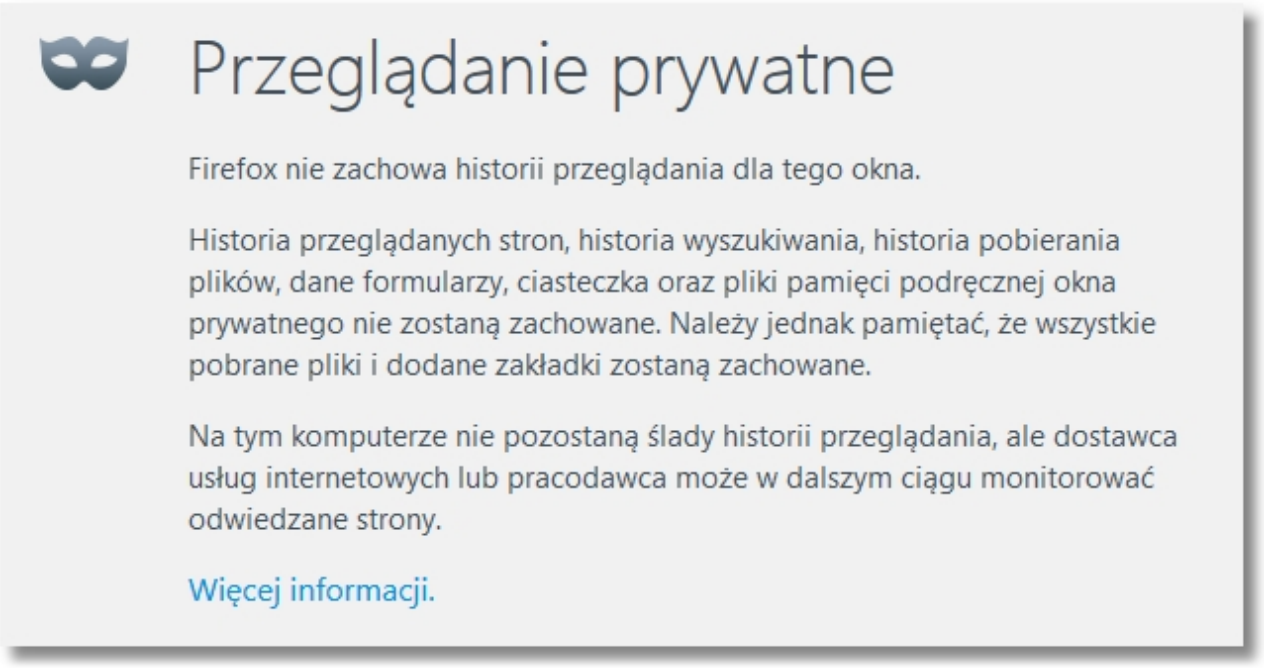
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Firefox w wersji 37.0.2 wspiera następujące systemy operacyjne: Windows 2000 / XP / Vista / Windows7 / XP64 / Vista64 / Windows7 64 / Windows8 / Windows8 64.
Znacznie poprawiony został tryb prywatności, między innymi możliwe jest kasowanie wszystkich prywatnych danych przy zamknięciu przeglądarki. W trybie prywatnym Firefox nie zachowa historii przeglądanych stron, historii wyszukiwania, historii pobierania plików, danych formularzy, ciasteczek oraz plików pamięci podręcznej.
Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład jest to komputer, z którego w firmie korzystają inni pracownicy lub publiczny komputer w kafejce internetowej, bibliotece itp.) zalecane jest:

- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej przejście w prywatny tryb przeglądania sieci, zaś po zakończonej sesji - jego wyłączenie lub zamknięcie przeglądarki.
- Jeśli nie użyto trybu prywatnego, zalecane jest po zakończonej pracy wejście w historię przeglądania i usunięcie wpisu dotyczącego Systemu Bankowości Internetowej przez wybranie opcji *usuń całą witrynę*.
- Alternatywnie można usunąć całość historii przeglądania z ostatnich kilku godzin lub całego dnia.

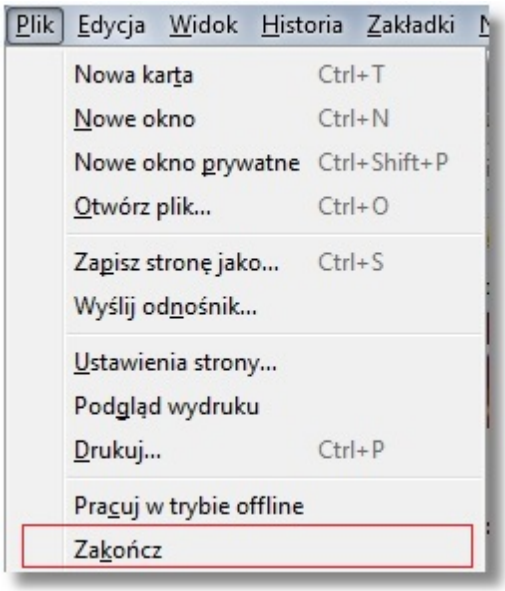
Prywatny tryb przeglądania sieci upraszcza ochronę informacji prywatnych. By go włączyć należy wybrać z menu *Plik*, następnie wybrać *Nowe okno prywatne* lub nacisnąć [Crtl]+[Shift]+[P]. W chwili przejścia do tego trybu przeglądarka zapamiętuje aktualnie otwarte karty, po czym zamyka je i otwiera tylko jedną, czystą kartę.



Od tej pory wszystkie czynności użytkownika podlegają specjalnej ochronie. Firefox nie zachowa historii przeglądanych stron, historii wyszukiwania, historii pobierania plików, danych formularzy, ciasteczek (cookies) oraz plików pamięci podręcznej. W ten sposób wrażliwe dane użytkownika po zakończeniu korzystania z sieci Internet nie zostaną narażone na nawet przypadkowe ujawnienie.

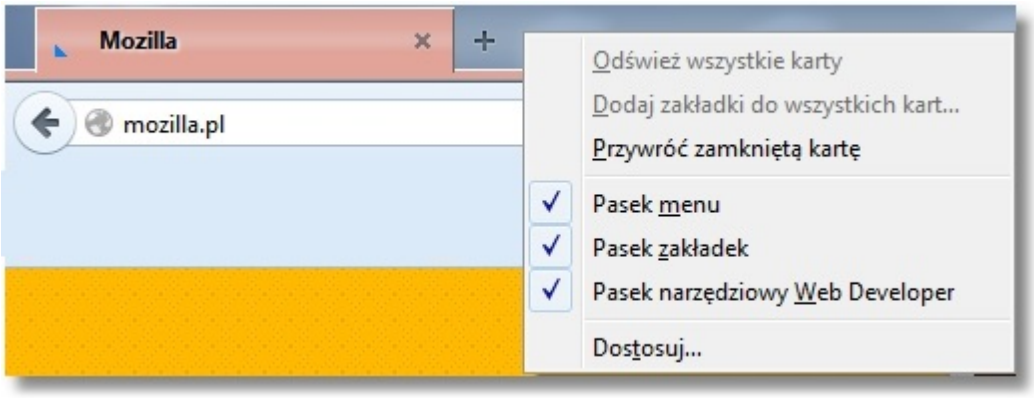


Po zakończeniu pracy w trybie prywatnym (w menu *Plik*) należy wybrać opcję *Zakończ*. Informacje związane z przeglądanymi stronami zostaną bezpiecznie usunięte, a zapamiętane wcześniej karty zostaną ponownie otwarte.

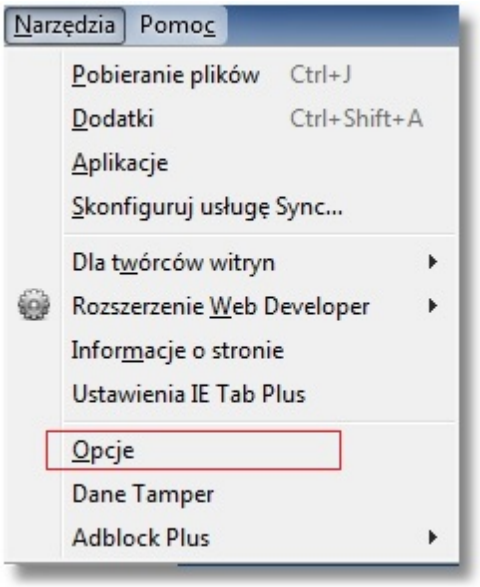


Usuwanie całej witryny z historii przeglądania jest przydatne, jeśli chcemy by przeglądarka "zapominała", że dana witryna była odwiedzana. W celu usunięcia całej witryny z historii przeglądania należy otworzyć historię przeglądania (wybrać z menu *Historia*), następnie opcję *Wyświetl całą historię* albo nacisnąć [Crtl]+[H] i kliknąć prawym przyciskiem myszy w stronę, której chcemy się pozbyć. Następnie należy wybrać z menu kontekstowego *Usuń całą witrynę*.
Zachęcamy do korzystania z trybu prywatnego – pomaga on poprawić bezpieczeństwo i chroni wrażliwe dane użytkownika przed przypadkowym ujawnieniem.

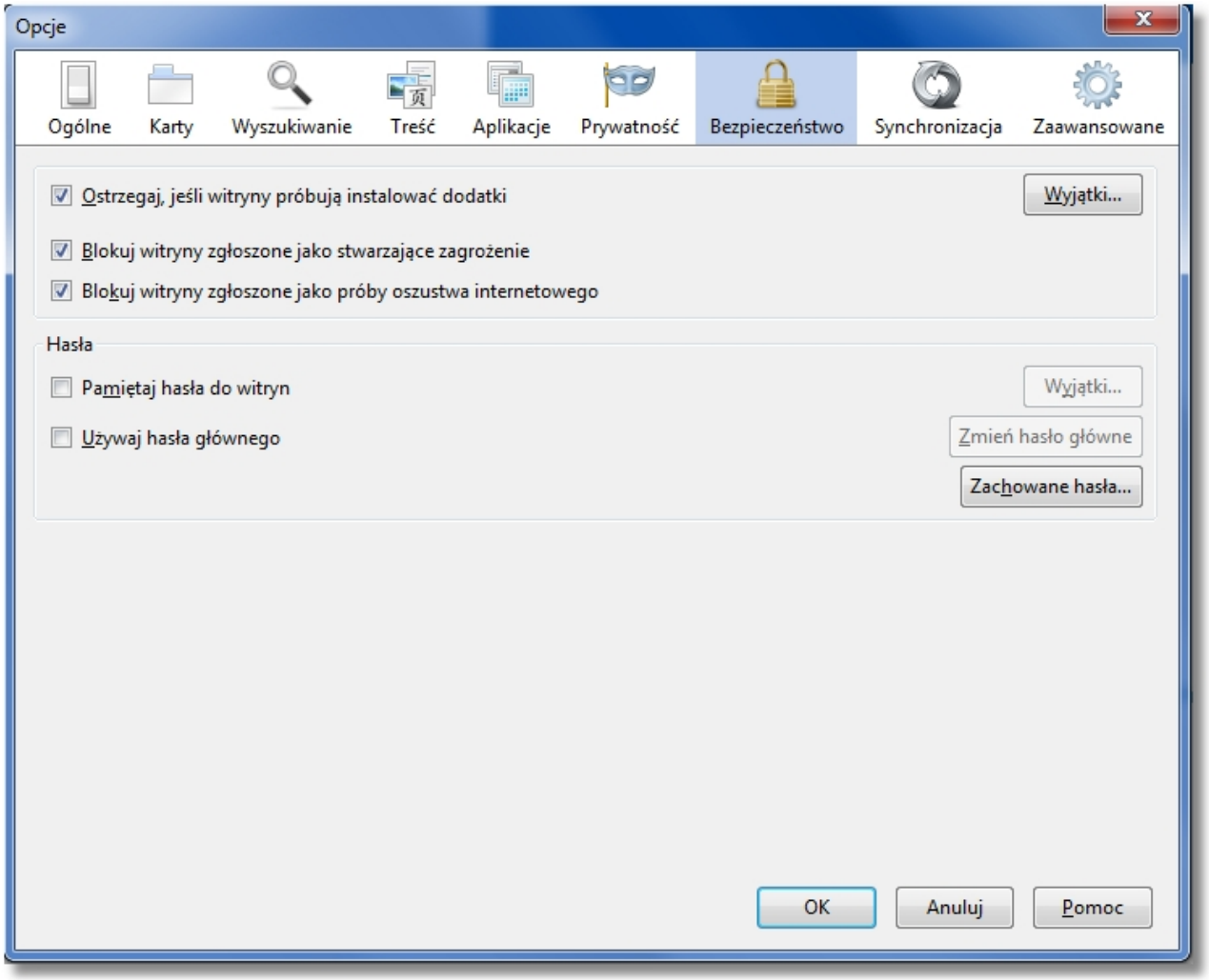
Domyślnie przeglądarka Firefox w wersji 37.0.2 nie pokazuje paska menu. W celu wyświetlenia paska menu należy ustawić kursor myszy na pasku menu, kliknąć prawy przycisk myszy oraz zaznaczyć opcję *Pasek menu*. Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.



W celu poprawnego skonfigurowania przeglądarki, z górnego menu przeglądarki należy wybrać *Narzędzia* a następnie *Opcje* i skonfigurować jak poniżej:



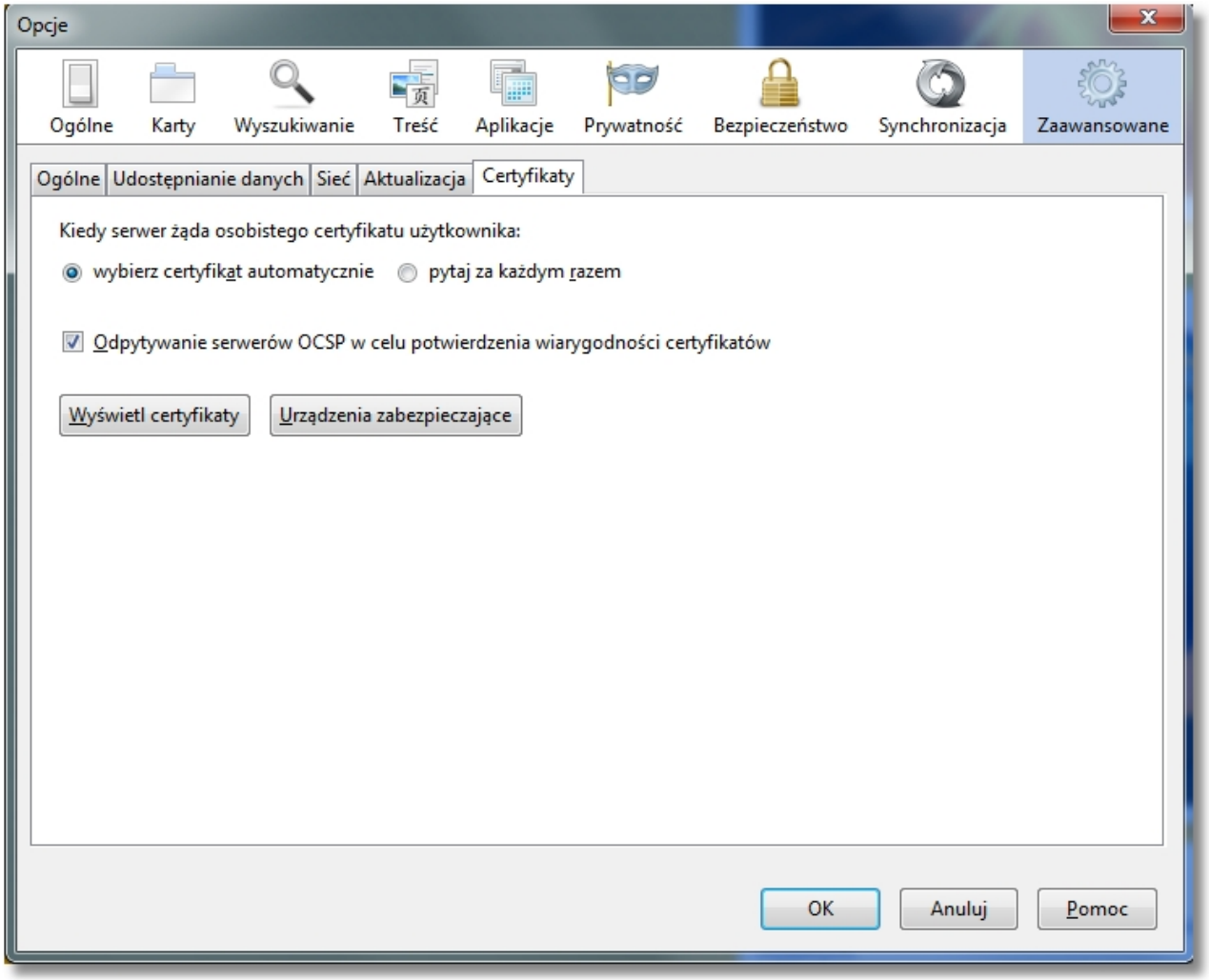
W opcji *Bezpieczeństwo* należy:
- zaznaczyć opcję *Ostrzegaj, kiedy witryny próbują instalować dodatki*,
- zaznaczyć opcję *Blokuj zgłoszone witryny stwarzające zagrożenie*,
- zaznaczyć opcję *Blokuj zgłoszone próby oszustwa internetowego*,
- w sekcji **Hasła** odznaczyć opcje: *Pamiętaj hasła do witryn* oraz *Używaj hasła głównego*.



Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

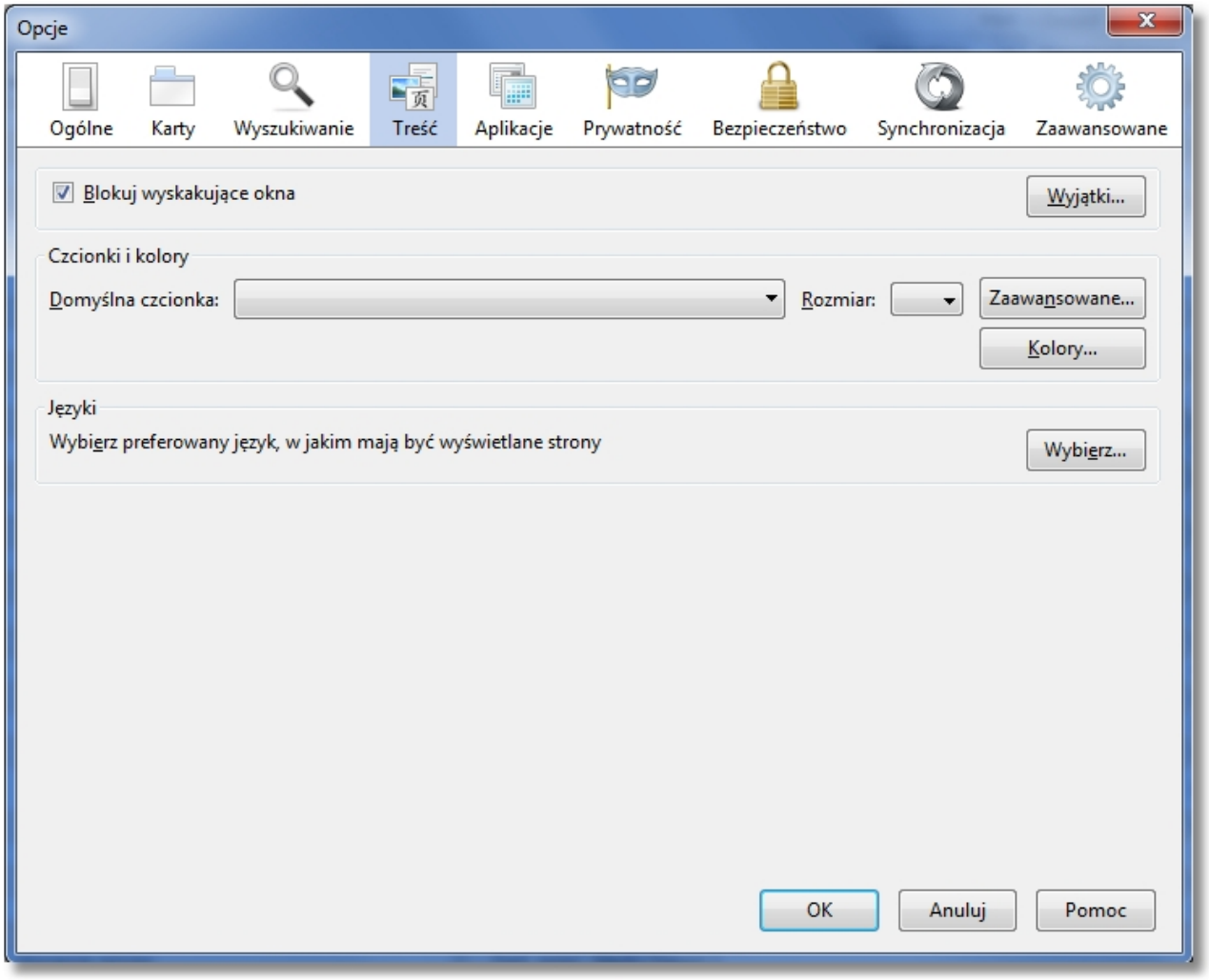
W opcji *Zaawansowane* zakładka *Certyfikaty* należy:

- w sekcji **Certyfikaty**: Kiedy serwer żąda osobistego certyfikatu użytkownika włączyć: *wybierz certyfikat automatycznie.*

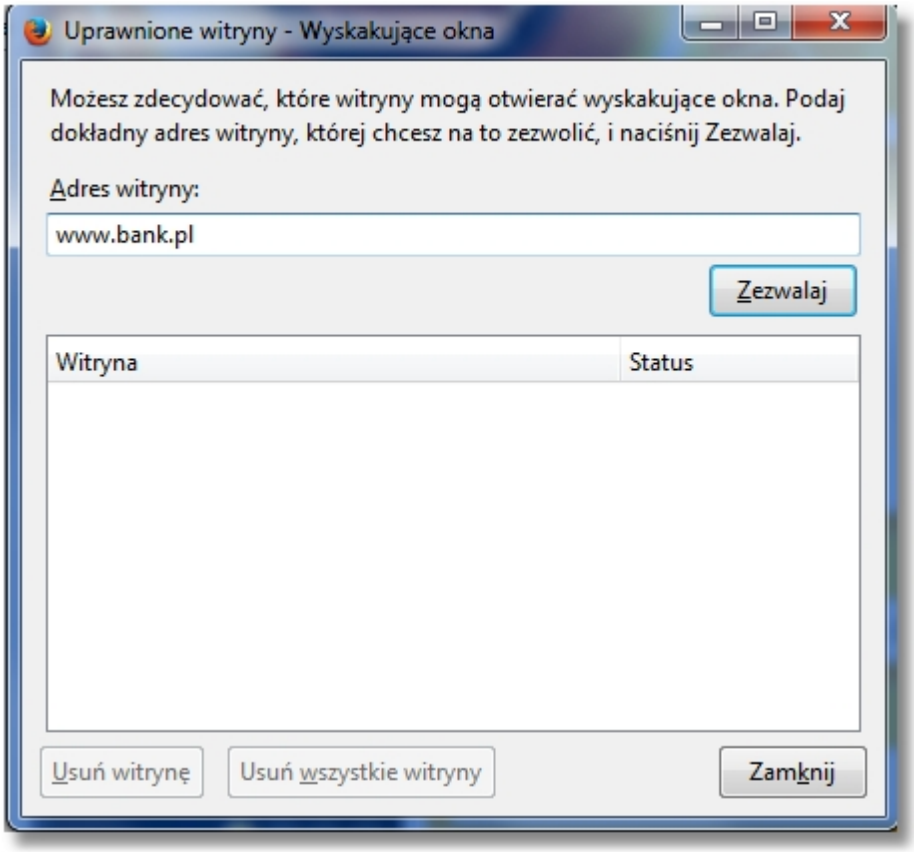


Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

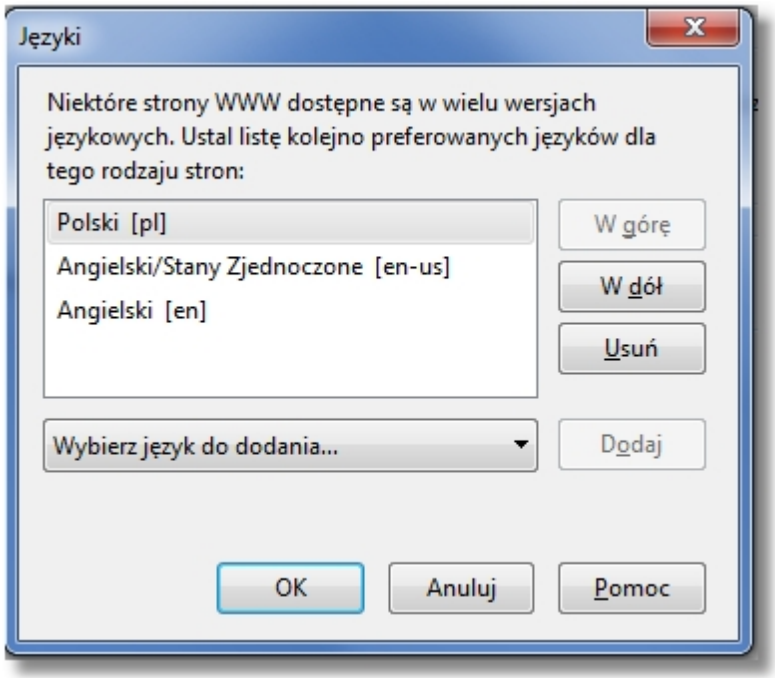
W opcji *Treść* należy:
- zaznaczyć opcję *Blokuj wyskakujące okna*.



Z uwagi na fakt, że w aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy w opcji *Wyjątki...* wpisać adres strony banku internetowego a następnie zezwolić na wyskakujące okienka dla tej strony przyciskiem [Zezwól].

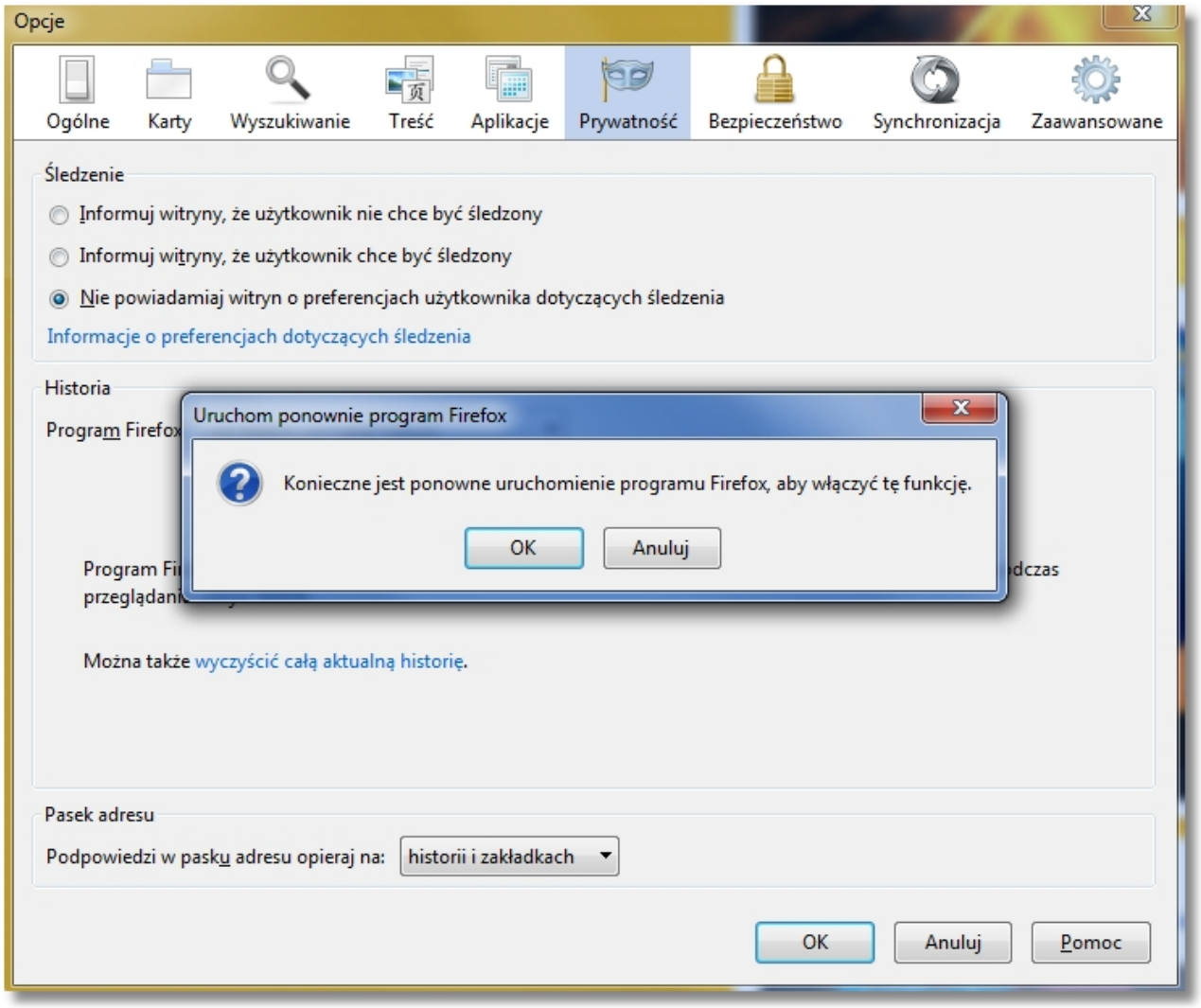


- W opcji *Treść* w sekcji **Języki** kliknąć na przycisk [Wybierz...], z listy wybrać Polski [pl] i dodać go do listy języków za pomocą przycisku [Dodaj], a następnie za pomocą przycisku [W górę] ustawić Polski [pl] jako pierwszy element na liście.



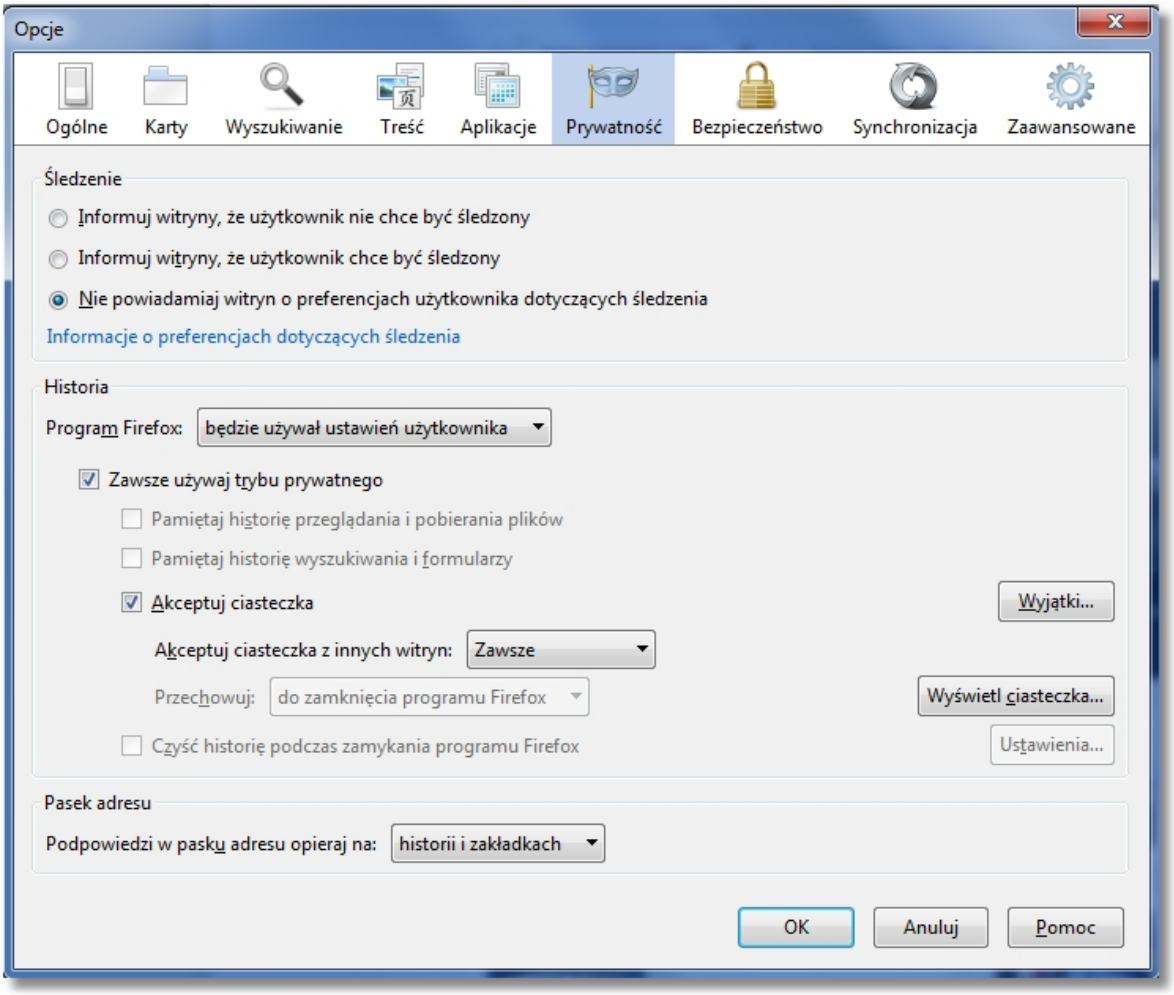
Wprowadzone zmiany należy zaakceptować przyciskiem [OK].

W opcji *Prywatność* w sekcji **Historia** należy:
- wybrać opcję: *nie będzie pamiętał historii*. W przypadku wyboru tej opcji program Firefox będzie używał tych samych ustawień co w trybie prywatnym i nie będzie zapisywał historii podczas przeglądania stron WWW.



lub

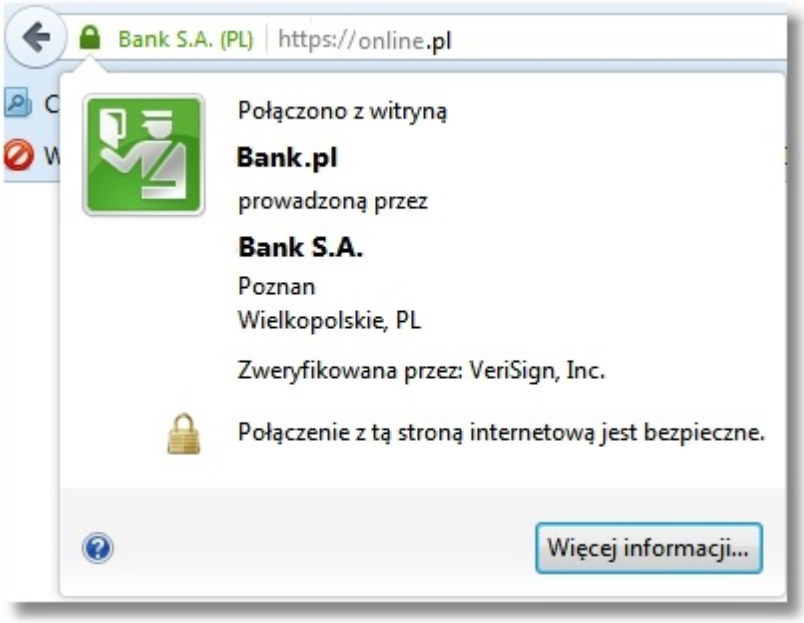
- w przypadku wyboru opcji: *będzie używał ustawień użytkownika* dla pola **Program Firefox** należy zaznaczyć opcję: *Zawsze używaj trybu prywatnego* oraz *Akceptuj ciasteczka* a następnie wybrać [OK].

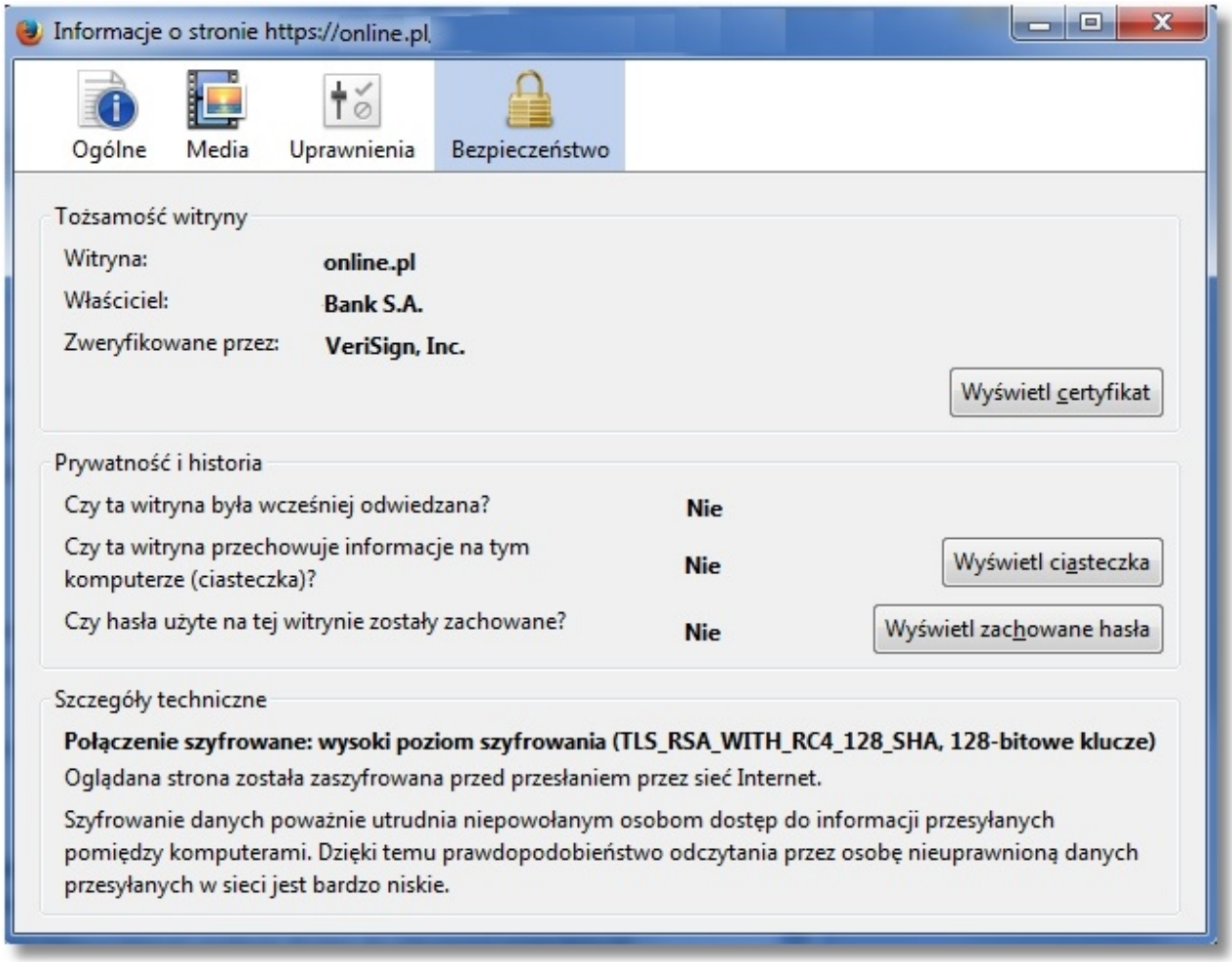


Wybór opcji opisanych powyżej spowoduje wyświetlenie komunikatu o treści: *"Konieczne jest ponowne uruchomienie programu Firefox, aby włączyć tę funkcję."*

Jeżeli z jakiegoś powodu opisane ustawienia ciasteczek nie są odpowiednie dla wszystkich stron przeglądanych przez użytkownika, zapamiętywaniem ciasteczek można sterować indywidualnie dla wybranych stron.
W tym celu po zalogowaniu do systemu bankowości internetowej należy wybrać z menu *Narzędzia* opcję *Informacje o stronie*. W oknie informacji należy wybrać *Uprawnienia*, następnie upewnić się, że poniżej wyświetlony jest napis przykładowo: *"Uprawnienia dla: www.bank.pl"* i w sekcji **Zapisywanie ciasteczek** usunąć zaznaczenie *Użyj domyślnych* i wybrać opcję *Zezwalaj na czas sesji*.

W celu wyświetlenia informacji o zabezpieczeniach związanych z szyfrowaniem witryny należy w przeglądarce Firefox w wersji 37.0.2 kliknąć na pasek adresu a dokładne w ikonkę strony a następnie wybrać przycisk [Więcej informacji ...] jak na poniższym ekranie.

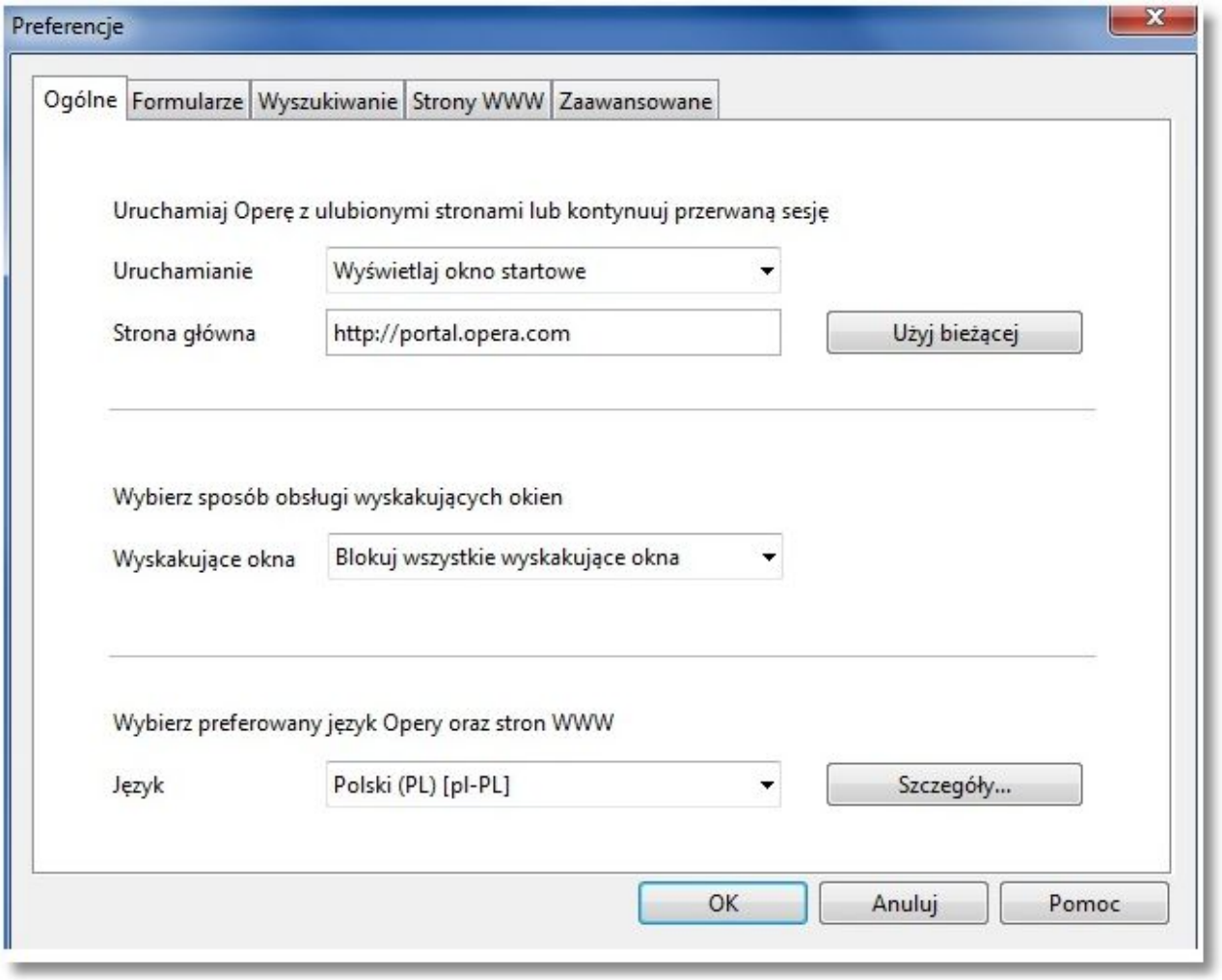

Bank S.A. (PL)
https://online.pl
Połączono z witryną
Bank.pl
prowadzoną przez
Bank S.A.
Poznan
Wielkopolskie, PL
Zweryfikowana przez: VeriSign, Inc.
Połączenie z tą stroną internetową jest bezpieczne.
Więcej informacji...


Informacje o stronie https://online.pl
Ogólne
Media
Uprawnienia
Bezpieczeństwo
Tożsamość witryny
Witryna: online.pl
Właściciel: Bank S.A.
Zweryfikowane przez: VeriSign, Inc.
Wyświetl certyfikat
Prywatność i historia
Czy ta witryna była wcześniej odwiedzana? Nie
Czy ta witryna przechowuje informacje na tym komputerze (ciasteczka)? Nie
Wyświetl ciasteczka
Czy hasła użyte na tej witrynie zostały zachowane? Nie
Wyświetl zachowane hasła
Szczegóły techniczne
Połączenie szyfrowane: wysoki poziom szyfrowania (TLS_RSA_WITH_RC4_128_SHA, 128-bitowe klucze)
Oglądana strona została zaszyfrowana przed przesłaniem przez sieć Internet.
Szyfrowanie danych poważnie utrudnia niepowołanym osobom dostęp do informacji przesyłanych pomiędzy komputerami. Dzięki temu prawdopodobieństwo odczytania przez osobę nieuprawnioną danych przesyłanych w sieci jest bardzo niskie.

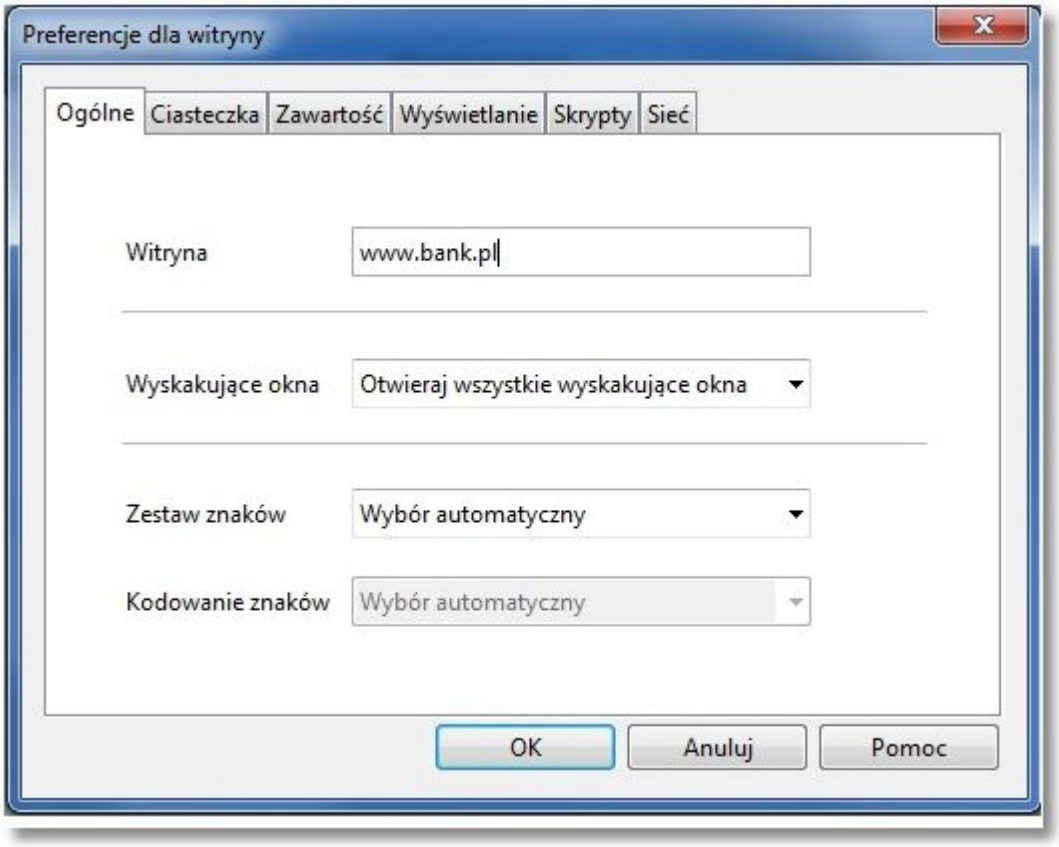
Rozdział 10. Konfiguracja przeglądarki Opera 11.51

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki. W przypadku, gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Aby poprawnie skonfigurować przeglądarkę należy:

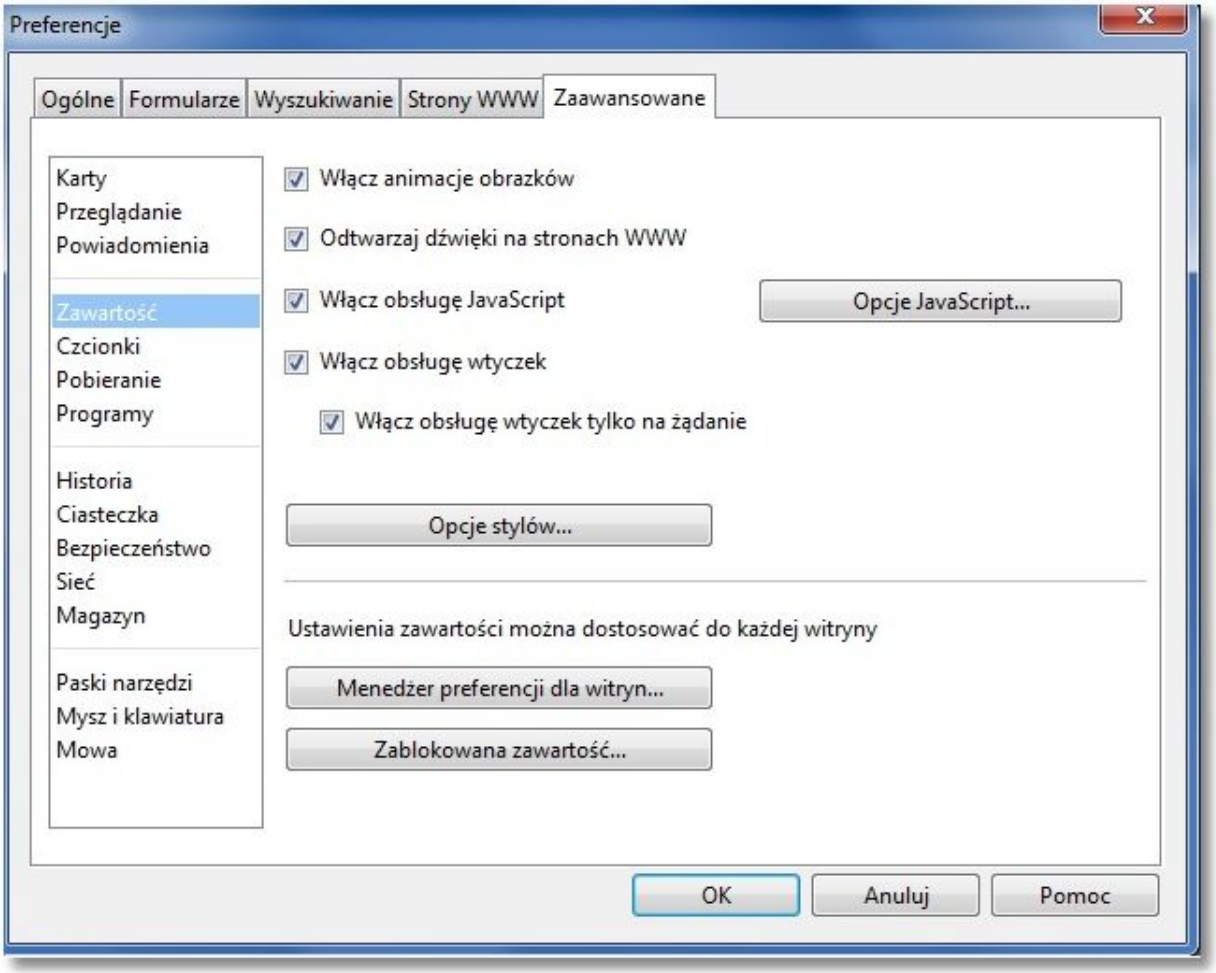
- z menu *Ogólne* wybrać *Preferencje...*



W zakładce *Ogólne* należy ustawić pole **Wyskakujące okna** na wartość *Blokuj wszystkie wyskakujące okna*. Z uwagi na fakt, że w aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy z menu *Narzędzia* wybrać opcję *Szybka konfiguracja*, a następnie *Preferencje dla witryny ...* W następnym kroku w zakładce *Ogólne* w sekcji **Witryna** wpisać adres strony banku internetowego a w sekcji **Wyskakujące okna** ustawić wartość *Otwieraj wszystkie wyskakujące okna* i zaakceptować wprowadzone dane przyciskiem [OK].



W zakładce *Formularze* należy odznaczyć opcję *Włącz menedżera haseł*.
W zakładce *Strony WWW* należy ustawić parametr **Obrazki** na wartość *Wyświetlaj obrazki*.
W zakładce *Zaawansowane* w opcji *Przeglądanie* w celu ułatwienia pracy z długimi listami zalecane jest zaznaczenie opcji *Pokaż paski przewijania*.
W zakładce *Zaawansowane* w opcji *Zawartość* należy zaznaczyć następujące opcje:

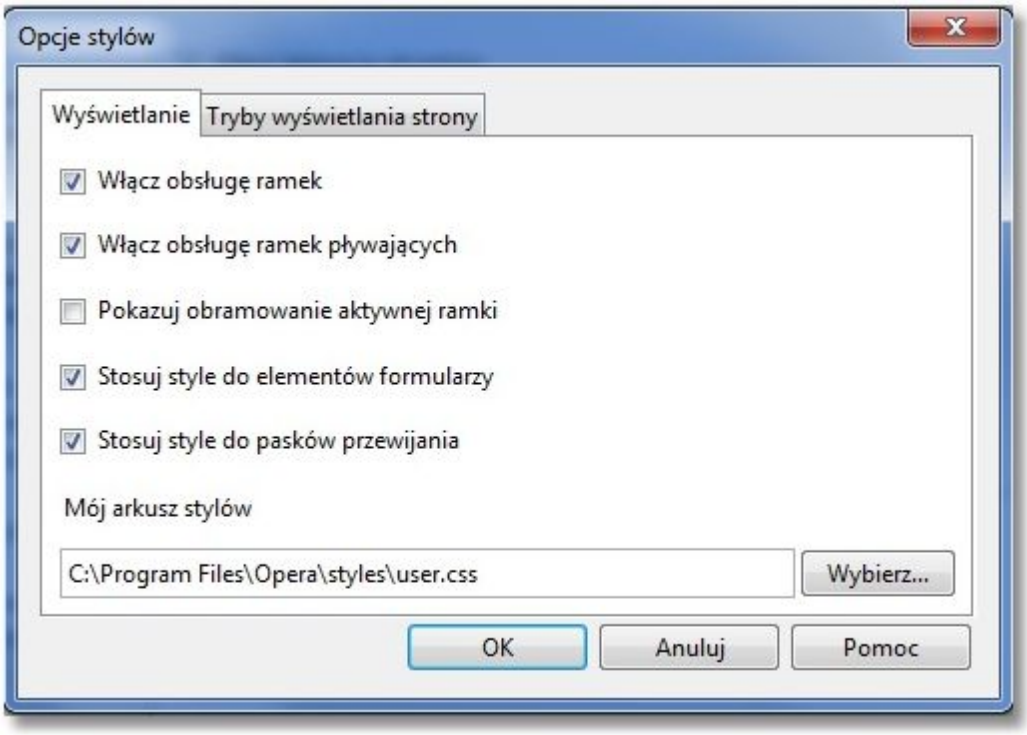


Włącz obsługę JavaScript - po kliknięciu przycisku [Opcje JavaScript...] należy zaznaczyć następujące parametry:

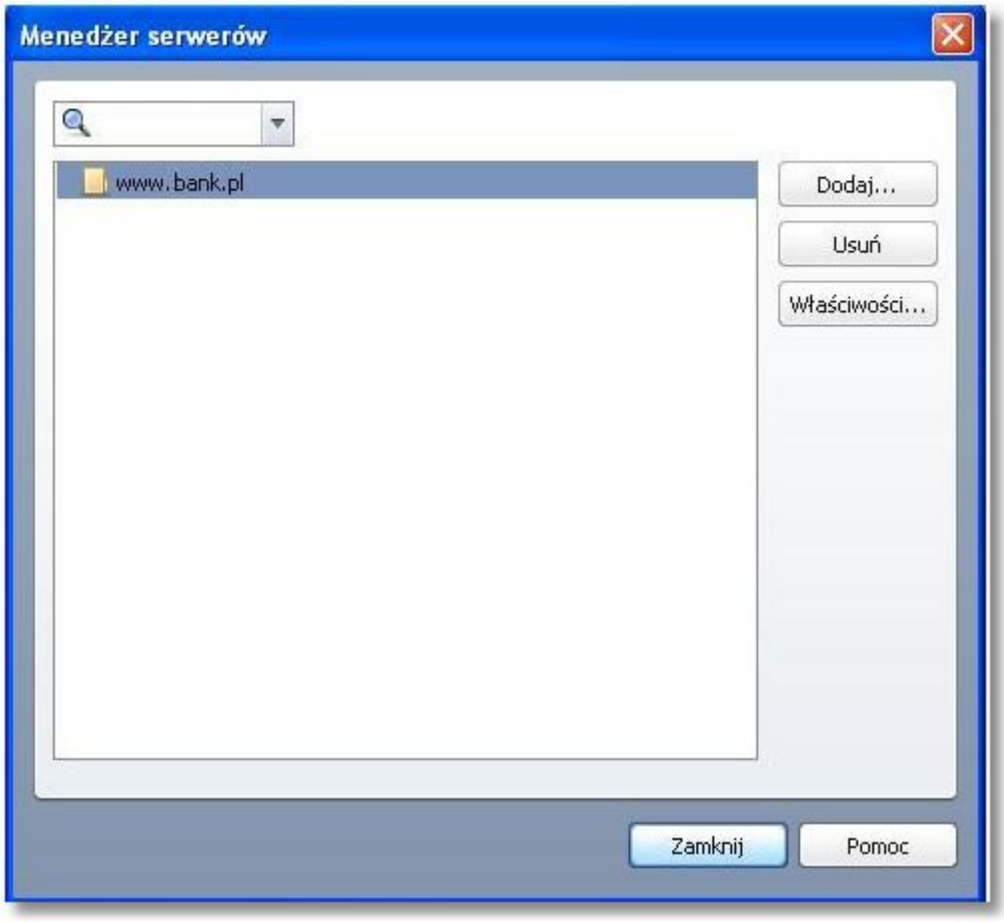
- Pozwól na zmianę rozmiaru okien,
- Pozwól na przesuwanie okien,
- Pozwól na przenoszenie okien na pierwszy plan,
- Pozwól na przenoszenie okien na ostatni plan,
- Pozwól na zmianę zawartości pola stanu

po kliknięciu przycisku [Opcje stylów] należy zaznaczyć parametry:

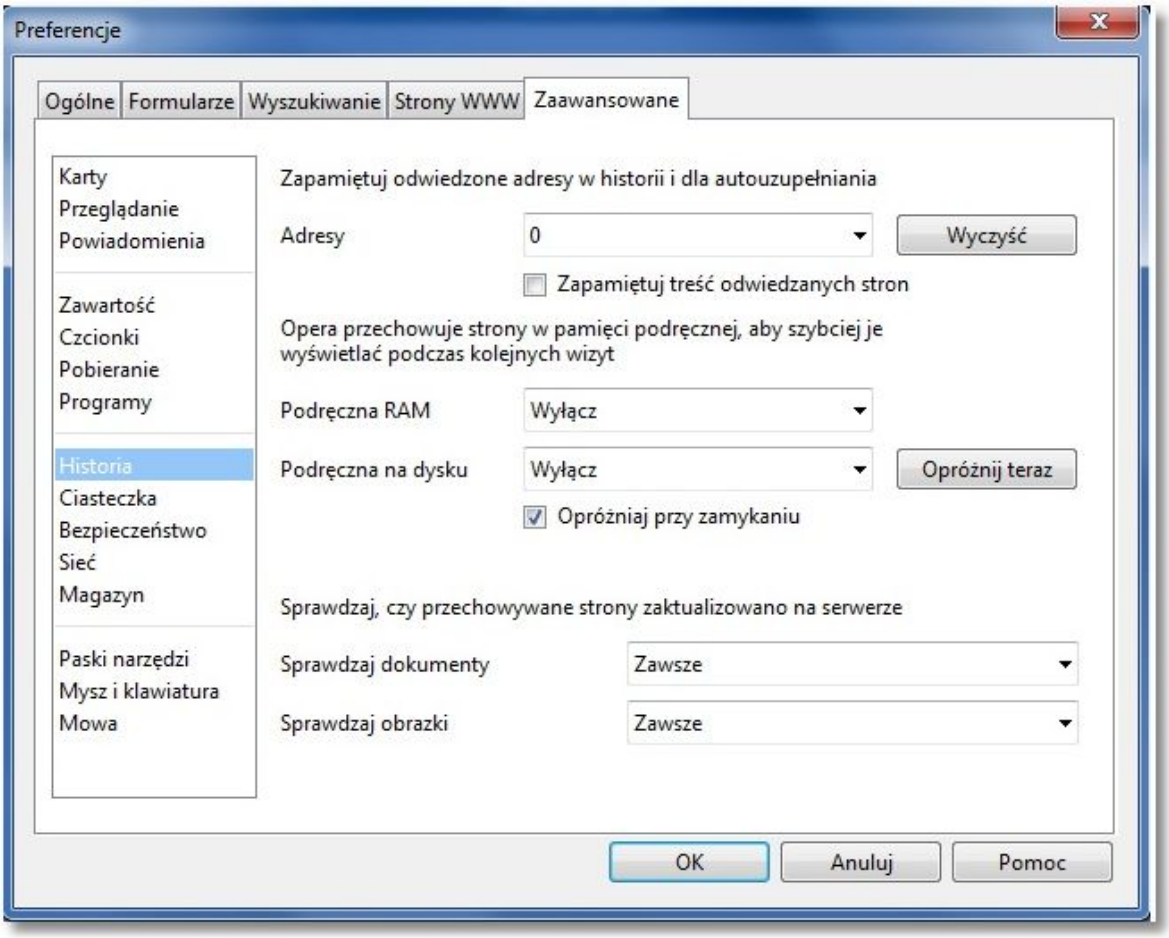
- Włącz obsługę ramek,
- Włącz obsługę ramek pływających,
- Stosuj style do elementów formularzy,
- Stosuj style do pasków przewijania.



Po kliknięciu przycisku [Menedżer preferencji witryn ...] dostępnego na zakładce *Zaawansowane* istnieje możliwość ustawienia parametrów dla określonej witryny.
Należy nacisnąć przycisk [Dodaj], a następnie wpisać adres wybranej witryny oraz określić preferencje.



W zakładce *Zaawansowane* w opcji *Historia* należy:
- ustawić Adresy na 0 oraz kliknąć przycisk [Wyczyść] w celu opróżnienia historii,
- odznaczyć pole **Zapamiętuj treść odwiedzanych stron**,
- ustawić Pamięć podręczna RAM na *Wyłącz*,
- ustawić Pamięć podręczna na dysku na *Wyłącz* oraz kliknąć przycisk [Opróżnij teraz] aby opróżnić pamięć podręczną,
- zaznaczyć opcję *Opróżniaj przy zamykaniu*,
- ustawić: *Sprawdzaj dokumenty na Zawsze, Sprawdzaj obrazki na Zawsze*.



W zakładce *Zaawansowane* w opcji *Ciasteczka* należy:
- ustawić Ciasteczka na Akceptuj ciasteczka.

W zakładce *Zaawansowane* w opcji *Bezpieczeństwo* należy zaznaczyć parametr **Włącz ochronę przed oszustami**. Zaznaczenie parametru stanowi zabezpieczenie przed stronami podszywającymi się pod inne serwisy i wykradającymi dane użytkowników.

W zakładce *Zaawansowane* w opcji *Bezpieczeństwo* należy po kliknięciu na przycisk [Protokoły zabezpieczające] odznaczyć: *Włącz SSL 3*.

W zakładce *Zaawansowane* w opcji *Sieć* należy:
- zaznaczyć *Pozwól na automatyczne przekierowywanie*,
- zaznaczyć *Przekazuj dane stron odsyłających*.

W celu akceptacji danych wprowadzonych w zakładce *Zaawansowane* należy wybrać przycisk [OK].

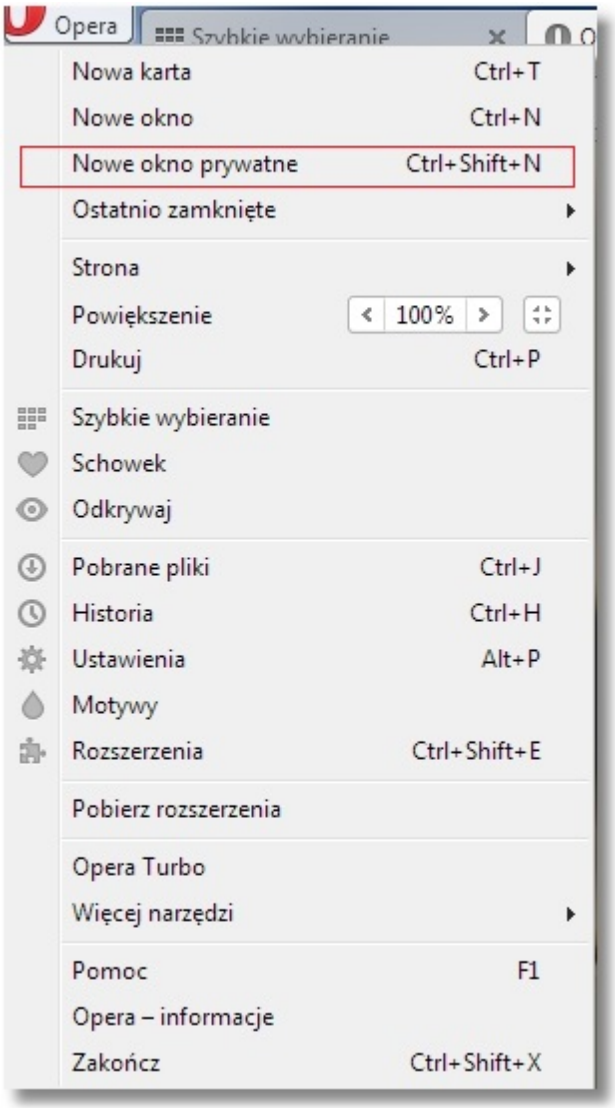
Z menu *Plik* wybrać *Opcje wydruku...* i zaznaczyć parametr **Drukuj tło strony**.

Rozdział 11. Konfiguracja przeglądarki Opera 24.0

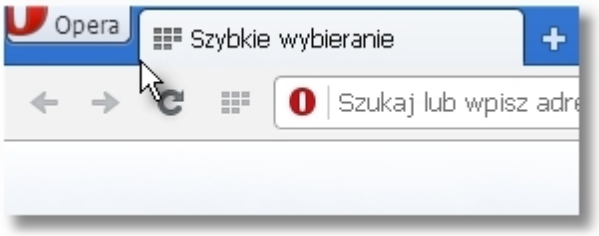
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Opera zawiera dodatkowe udogodnienia zwiększające bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wrażliwe lub wymagające szczególnej ochrony - takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą zalecane jest:

- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej przejście w prywatny tryb przeglądania sieci, zaś po zakończonej sesji zamknięcie przeglądarki.
- Jeśli nie użyto trybu prywatnego, zalecane jest po zakończonej pracy wejście w historię przeglądania i usunięcie wpisu dotyczącego Systemu Bankowości Internetowej przez wybranie przycisku [Wyczyść dane przeglądania ...].
- Alternatywnie można usunąć całość historii przeglądania z ostatnich kilku godzin lub całego dnia.

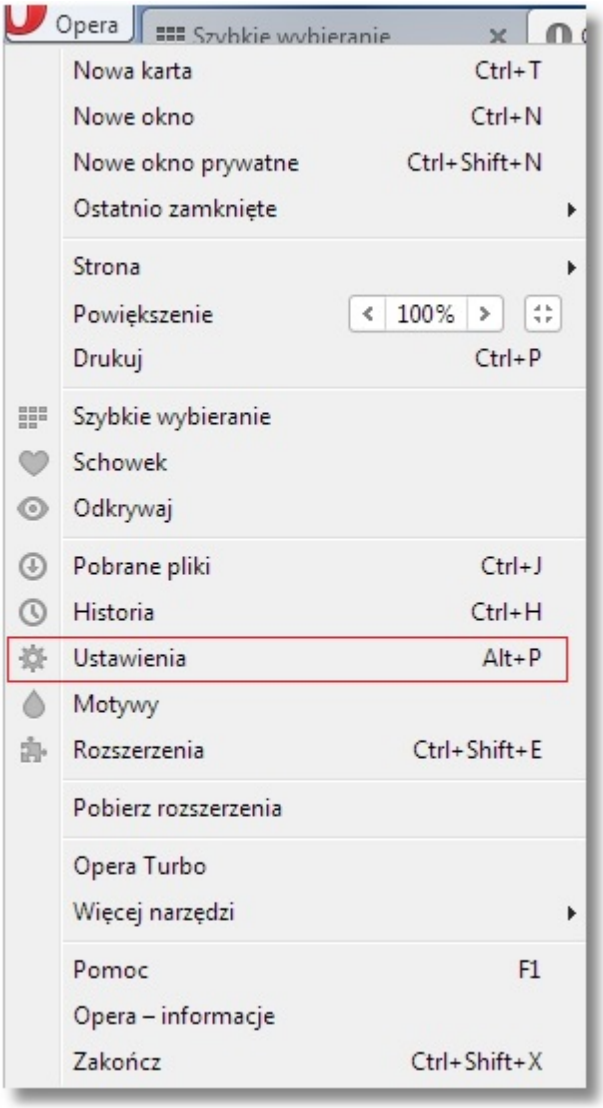
Prywatny tryb przeglądania sieci upraszcza ochronę informacji prywatnych. By go włączyć należy wybrać z menu głównego wybrać *Nowe okno prywatne* lub nacisnąć [Crtl]+[Shift]+[N]. W chwili przejścia do tego trybu przeglądarka zapamiętuje aktualnie otwarte karty, po czym zamyka je i otwiera tylko jedną, czystą kartę.



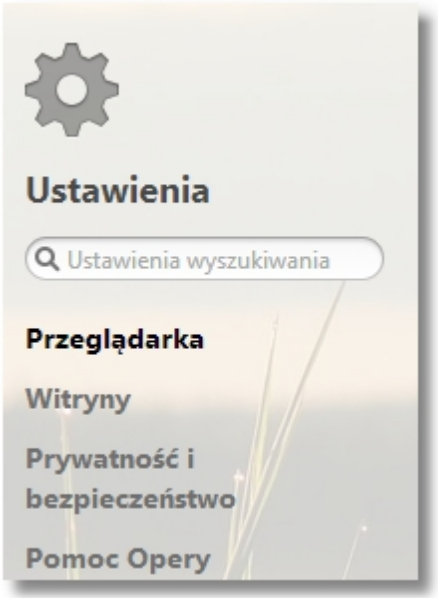
Aby poprawnie skonfigurować przeglądarkę należy w pierwszym kroku kliknąć w ikonkę Opera.



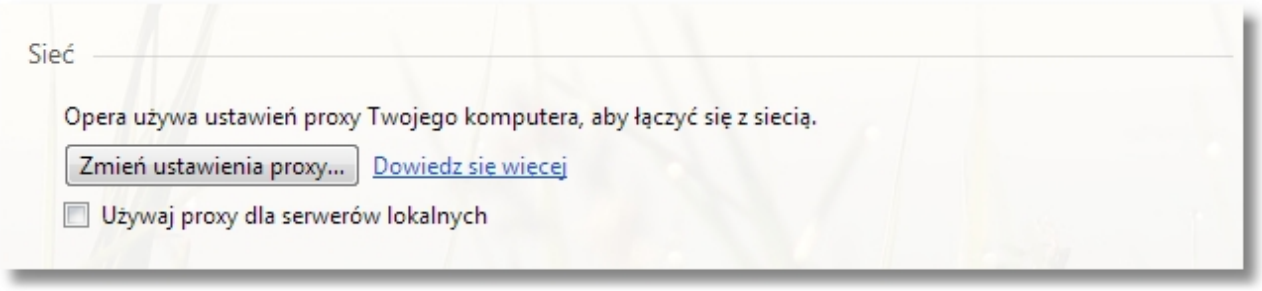
Z menu głównego wybrać opcję *Ustawienia* lub nacisnąć klawisze [Alt+P].



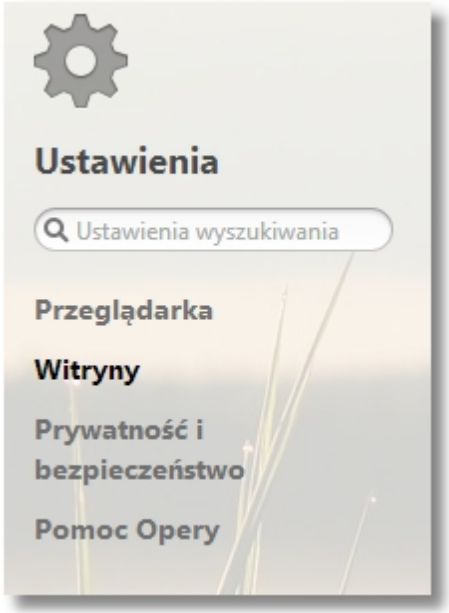
Zostanie zaprezentowane menu z dostępnymi zakładkami.



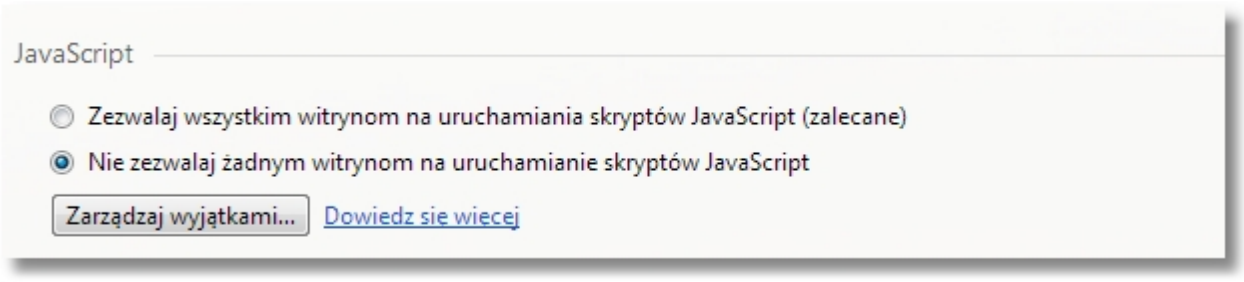
Należy wybrać zakładkę *Przeglądarka* oraz skonfigurować następujące ustawienia.
W sekcji **Sieć** wybrać przycisk [Zmień ustawienia proxy...] a następnie w zakładce *Zaawansowane* w sekcji **Zabezpieczenia** zaznaczyć opcje: *Użyj TLS 1.* Zaleca się wyłączenie opcji *Użyj SSL 3.0.*



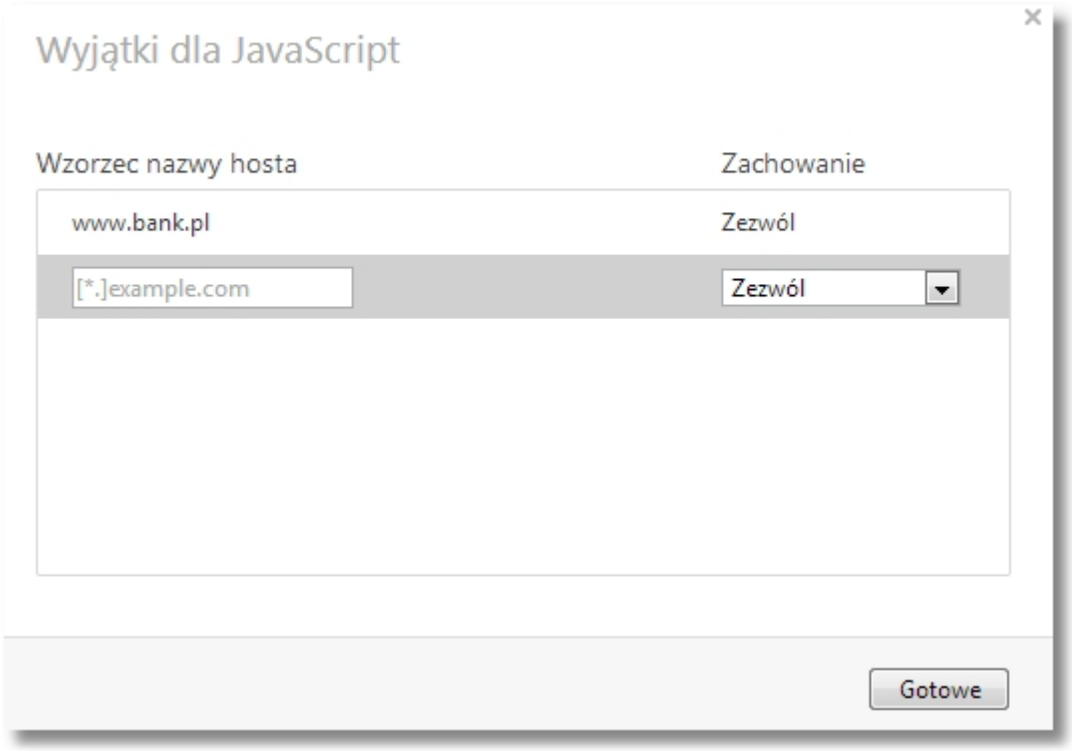
Wybrać *Witryny* oraz skonfigurować odpowiednio ustawienia.



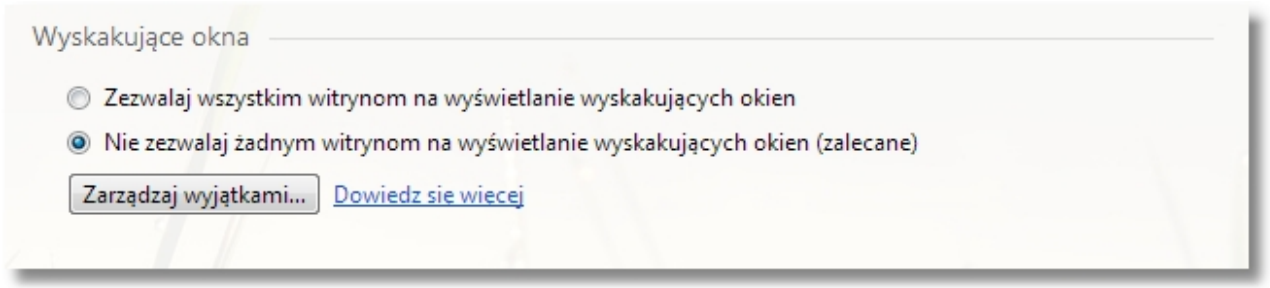
W sekcji **JavaScript** należy zaznaczyć opcję *Nie zezwalaj żadnym witrynom na uruchamianie skryptów JavaScript.*



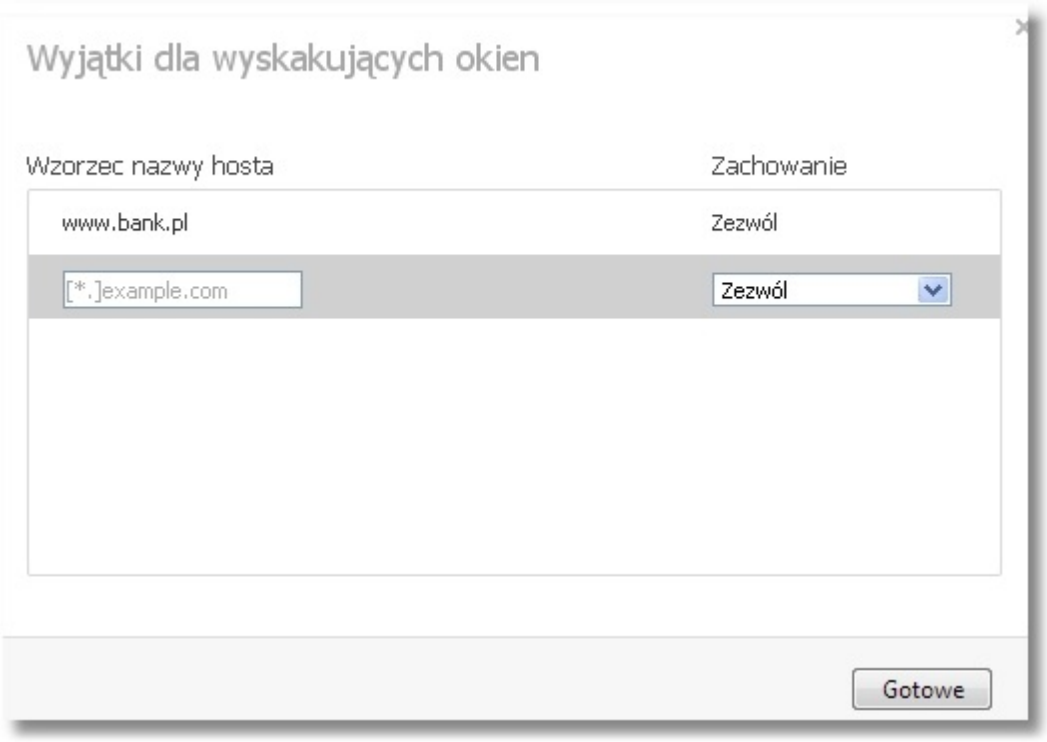
W przypadku całkowitego wyłączeniu obsługi JavaScript, niektóre strony przestaną działać prawidłowo. W celu wyboru sposobu obsługi skryptów JavaScript na poszczególnych witryn należy wybrać przycisk [Zarządzaj wyjątkami...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].



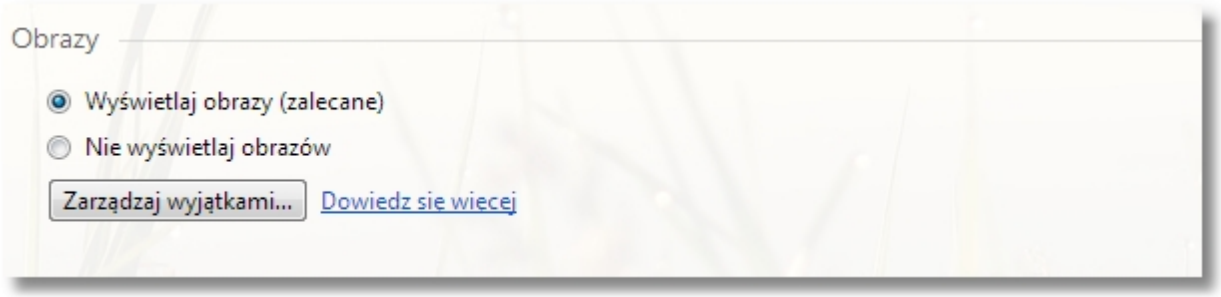
W sekcji **Wyskakujące okna** należy zaznaczyć opcję *Nie zezwalaj żadnym witrynom na wyświetlanie wyskakujących okien (zalecane).*



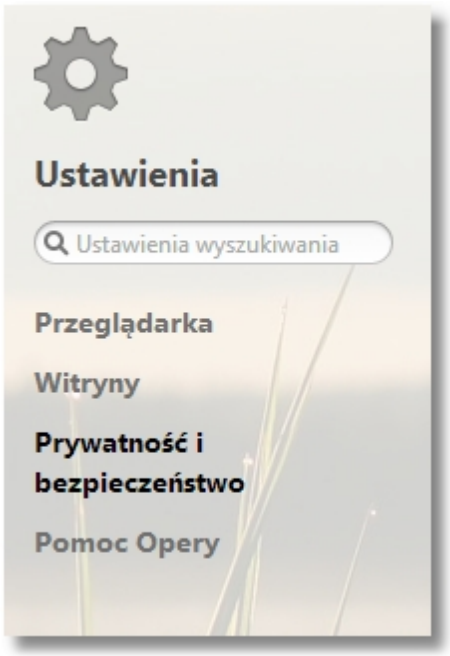
Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy wybrać przycisk [Zarządzaj wyjątkami ...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].



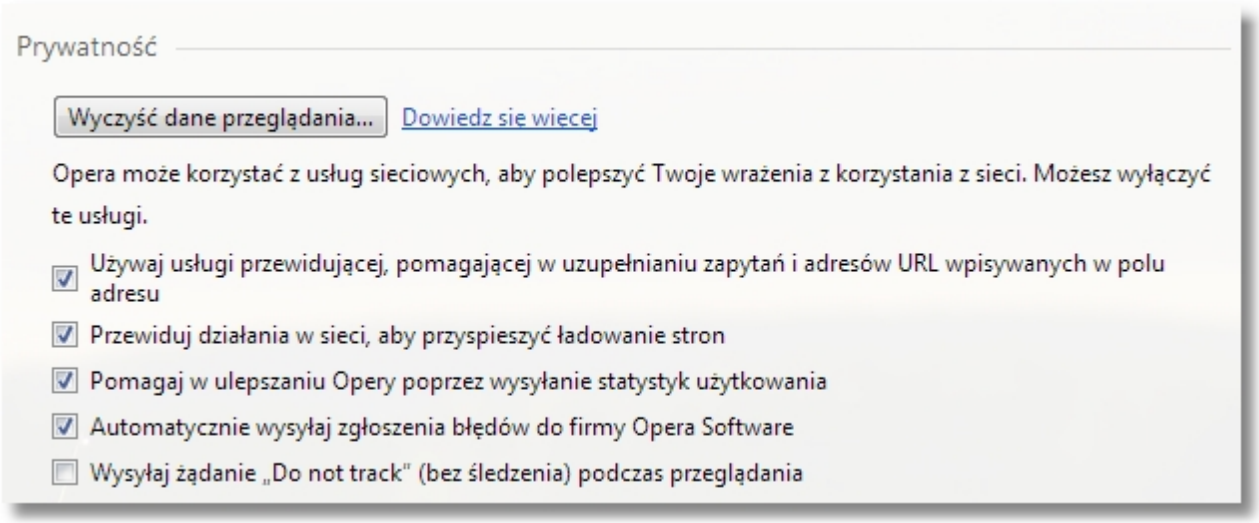
W sekcji **Obrazy** należy zaznaczyć opcję *Wyświetlaj obrazy (zalecane)*.



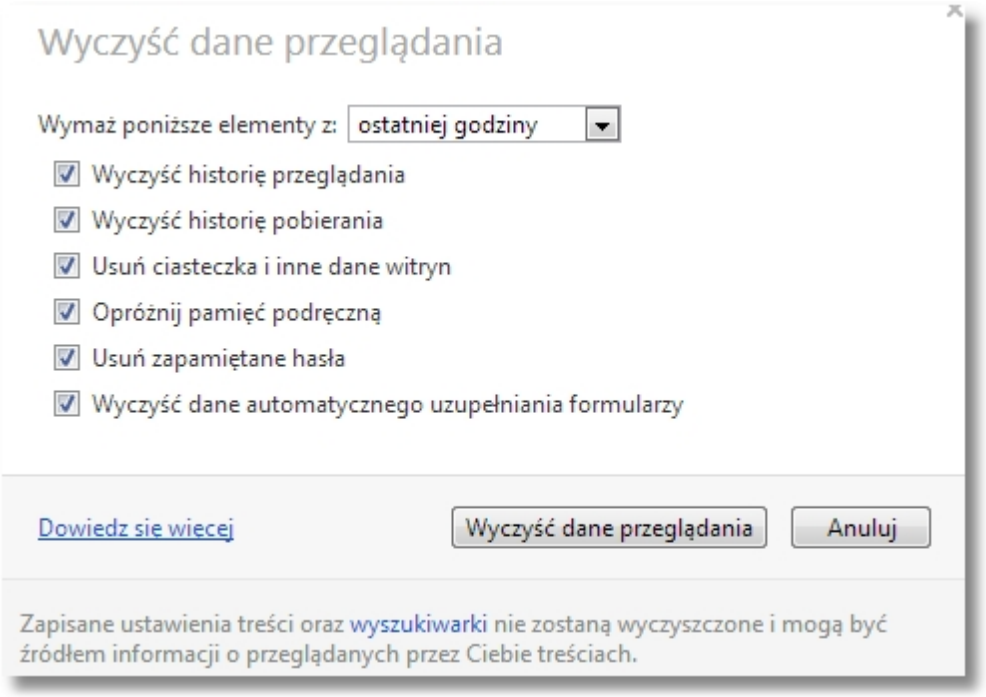
Wybrać zakładkę *Prywatność i bezpieczeństwo* oraz skonfigurować odpowiednio ustawienia.



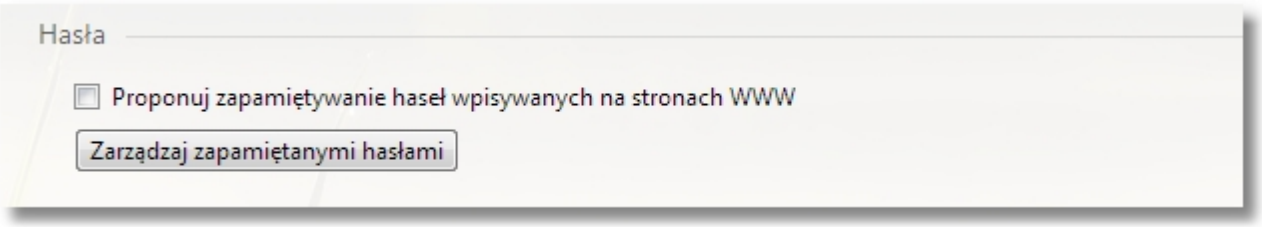
W sekcji **Prywatność** należy wybrać przycisk [Wyczyść dane przeglądania...]



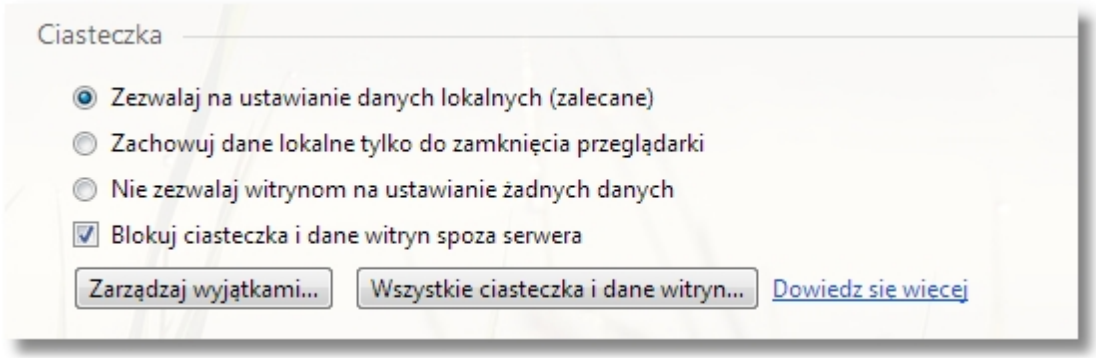
Zaznaczyć opcje jak poniżej oraz wybrać przycisk [Wyczyść dane przeglądania]. Wyczyszczenie historii przeglądania spowoduje usunięcie wszystkich informacji o odwiedzonych stronach, takich jak adresy i czasy odwiedzin.



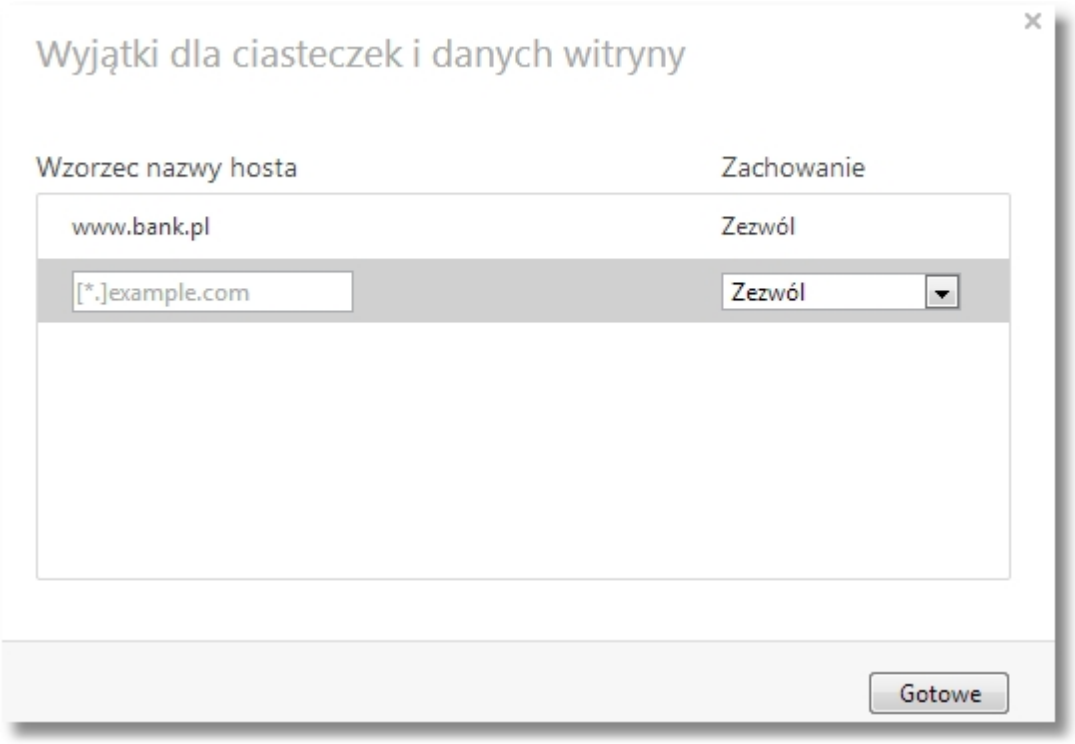
W sekcji **Hasła** należy odznaczyć opcję *Proponuj zapamiętywanie haseł wpisywanych na stronach WWW*.



W sekcji **Ciasteczka** należy zaznaczyć opcję *Blokuj ciasteczka i dane witryn spoza serwera*.



Określenie ustawień ciasteczek daje kontrolę nad sposobem ich obsługi przez Operę. W związku z tym użytkownik ma możliwość określenia wyjątków dla ciasteczek i danych witryny. W tym celu należy wybrać przycisk [Zarządzaj wyjątkami...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].

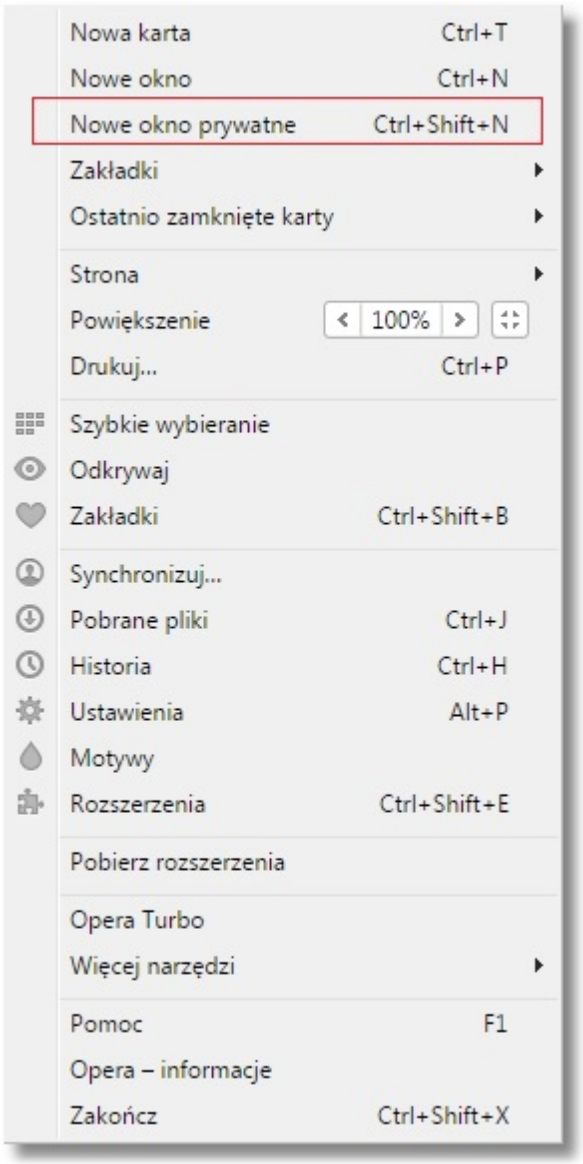

Wyjątki dla ciasteczek i danych witryny
Wzorzec nazwy hosta
Zachowanie
www.bank.pl
Zezwól
[*.]example.com
Zezwól
Gotowe

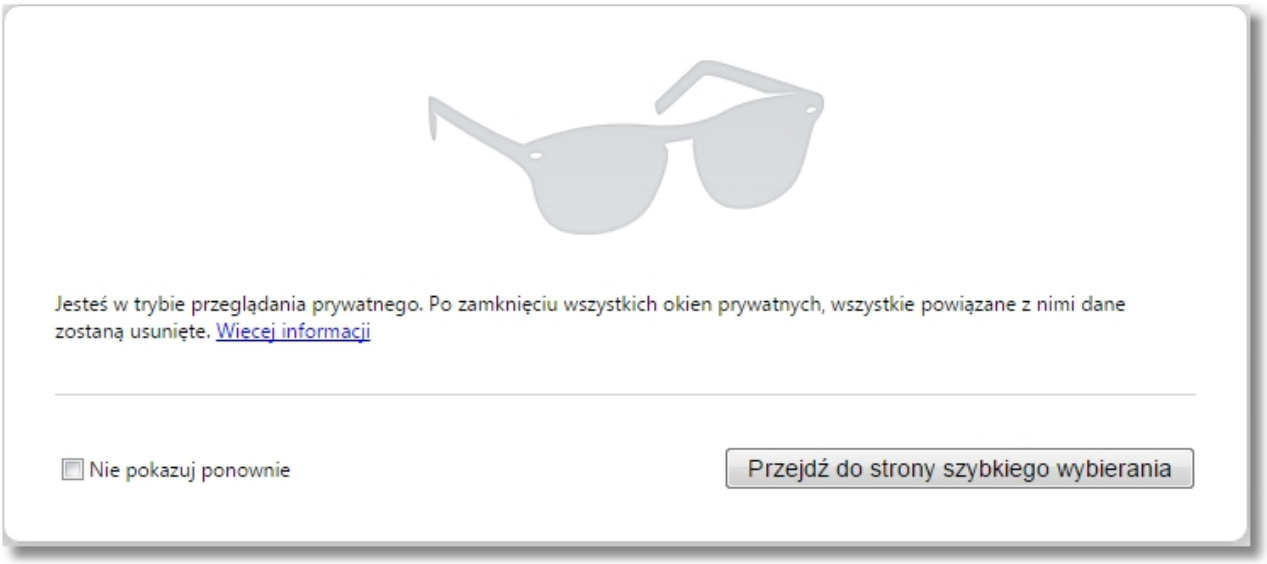
Rozdział 12. Konfiguracja przeglądarki Opera 29.0

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana.
Przeglądarka Opera zawiera dodatkowe udogodnienia zwiększające bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wrażliwe lub wymagające szczególnej ochrony - takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą zalecane jest:

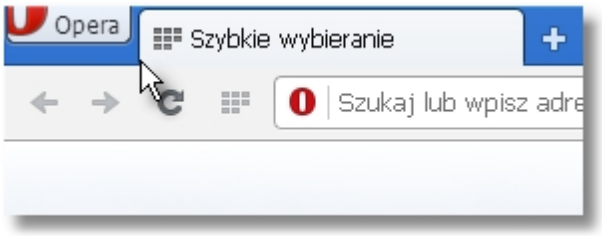
- Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej przejście w prywatny tryb przeglądania sieci, zaś po zakończonej sesji zamknięcie przeglądarki.
- Jeśli nie użyto trybu prywatnego, zalecane jest po zakończonej pracy wejście w historię przeglądania i usunięcie wpisu dotyczącego Systemu Bankowości Internetowej przez wybranie przycisku [Wyczyść dane przeglądania ...].
- Alternatywnie można usunąć całość historii przeglądania z ostatnich kilku godzin lub całego dnia.

Prywatny tryb przeglądania sieci upraszcza ochronę informacji prywatnych. W celu włączenia tego trybu należy wybrać z menu głównego opcję *Nowe okno prywatne* lub nacisnąć [Crtl]+[Shift]+[N]. W chwili przejścia do tego trybu przeglądarka zapamiętuje aktualnie otwarte karty, po czym zamyka je i otwiera tylko jedną czystą kartę.

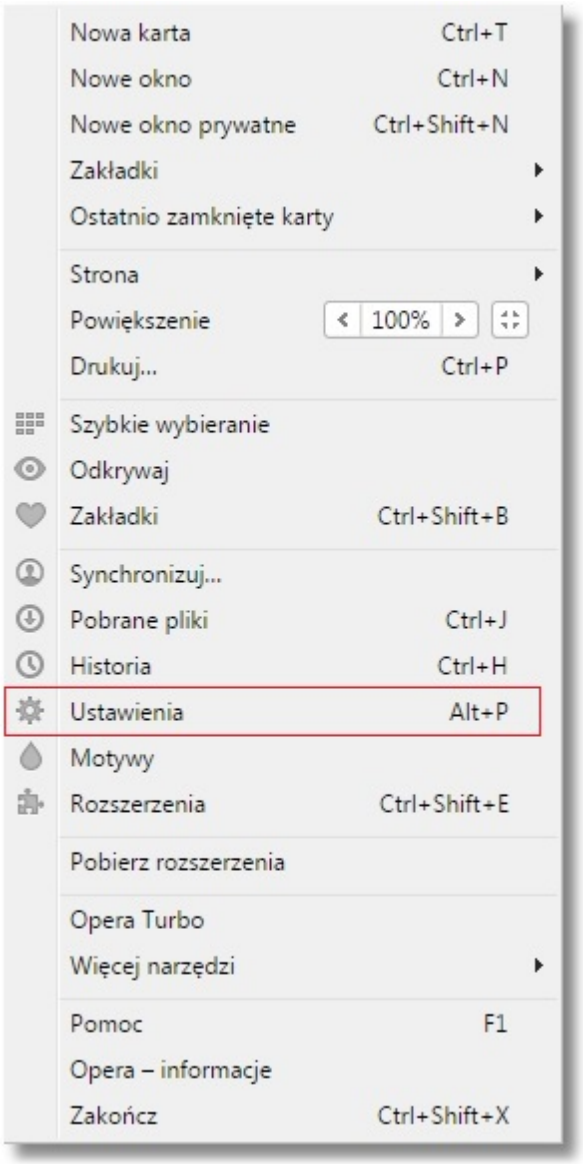




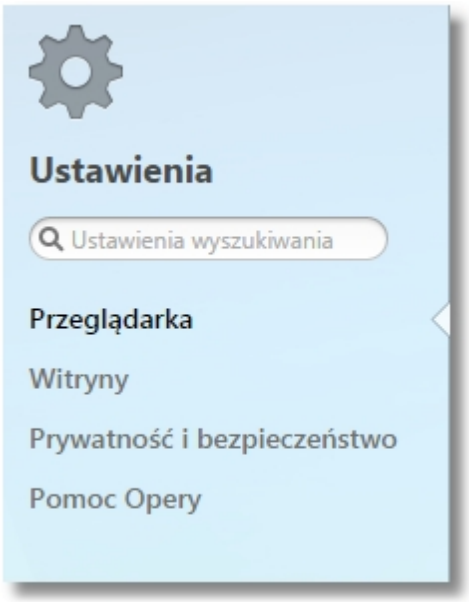
Aby poprawnie skonfigurować przeglądarkę należy w pierwszym kroku kliknąć w ikonkę Opera.



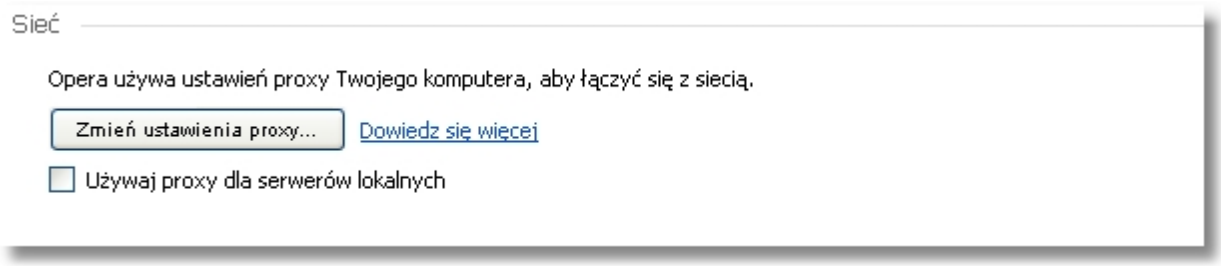
Z menu głównego wybrać opcję *Ustawienia* lub nacisnąć klawisze [Alt+P].



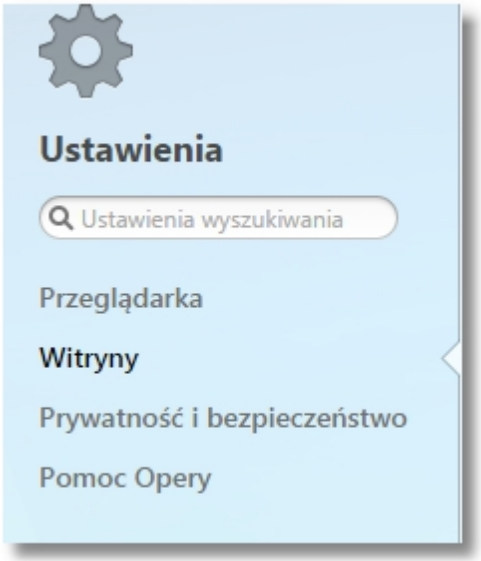
Zostanie zaprezentowane menu z dostępnymi zakładkami.



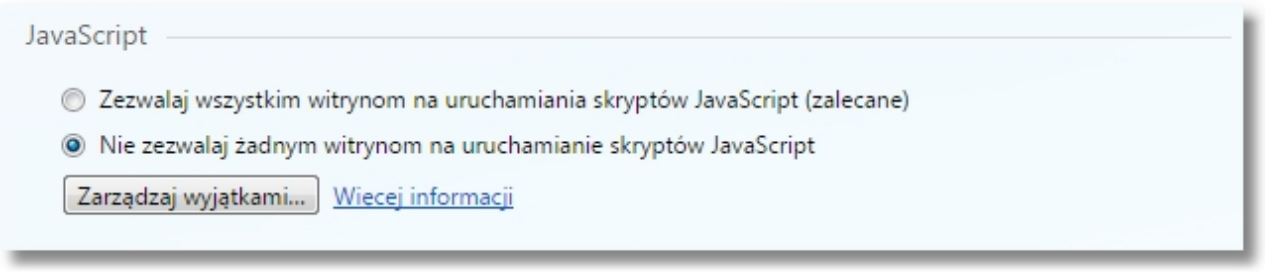
Należy wybrać zakładkę *Przeglądarka* oraz skonfigurować następujące ustawienia.
W sekcji **Sieć** wybrać przycisk [Zmień ustawienia proxy...] a następnie w zakładce *Zaawansowane* w sekcji **Zabezpieczenia** zaznaczyć opcje: *Użyj szyfrowania TLS 1.1, Użyj szyfrowania TLS 1.2, Użyj TLS 1.* Zaleca się wyłączenie opcji *Użyj SSL 3.0.*



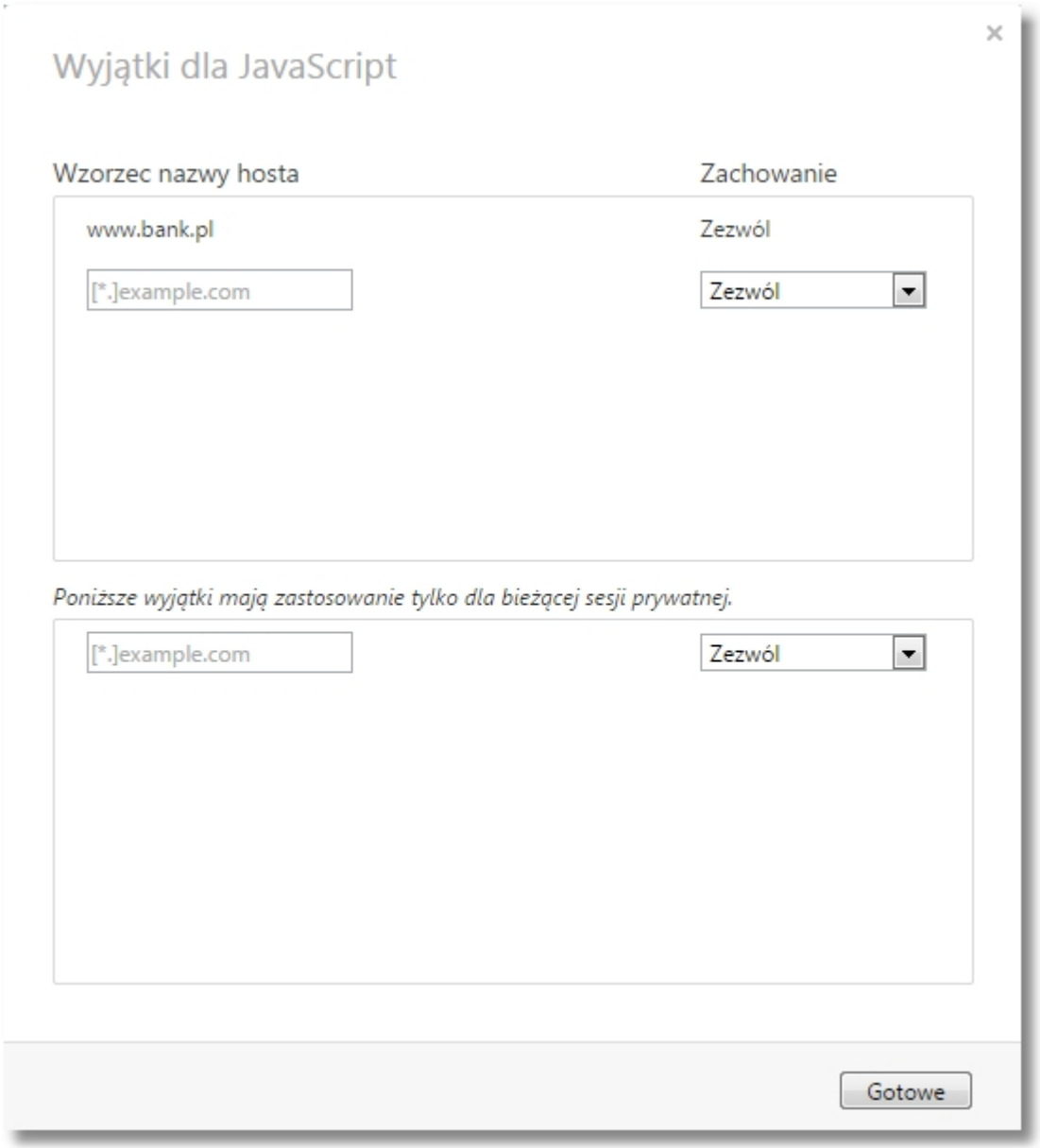
Wybrać zakładkę *Witryny* oraz skonfigurować odpowiednio ustawienia.



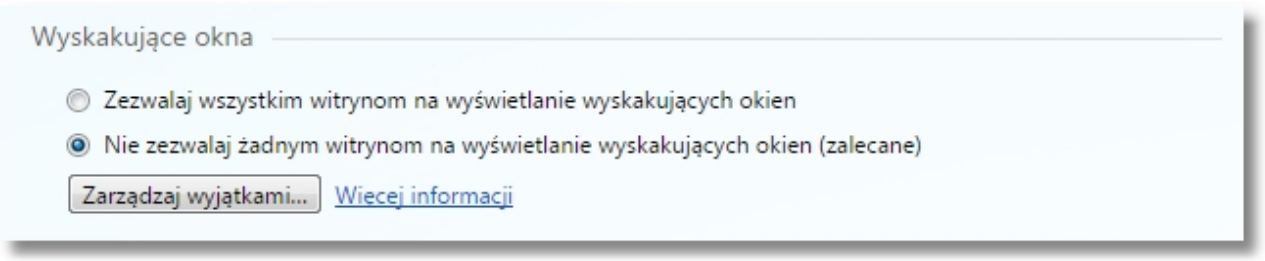
W sekcji **JavaScript** należy zaznaczyć opcję *Nie zezwalaj żadnym witrynom na uruchamianie skryptów JavaScript.*



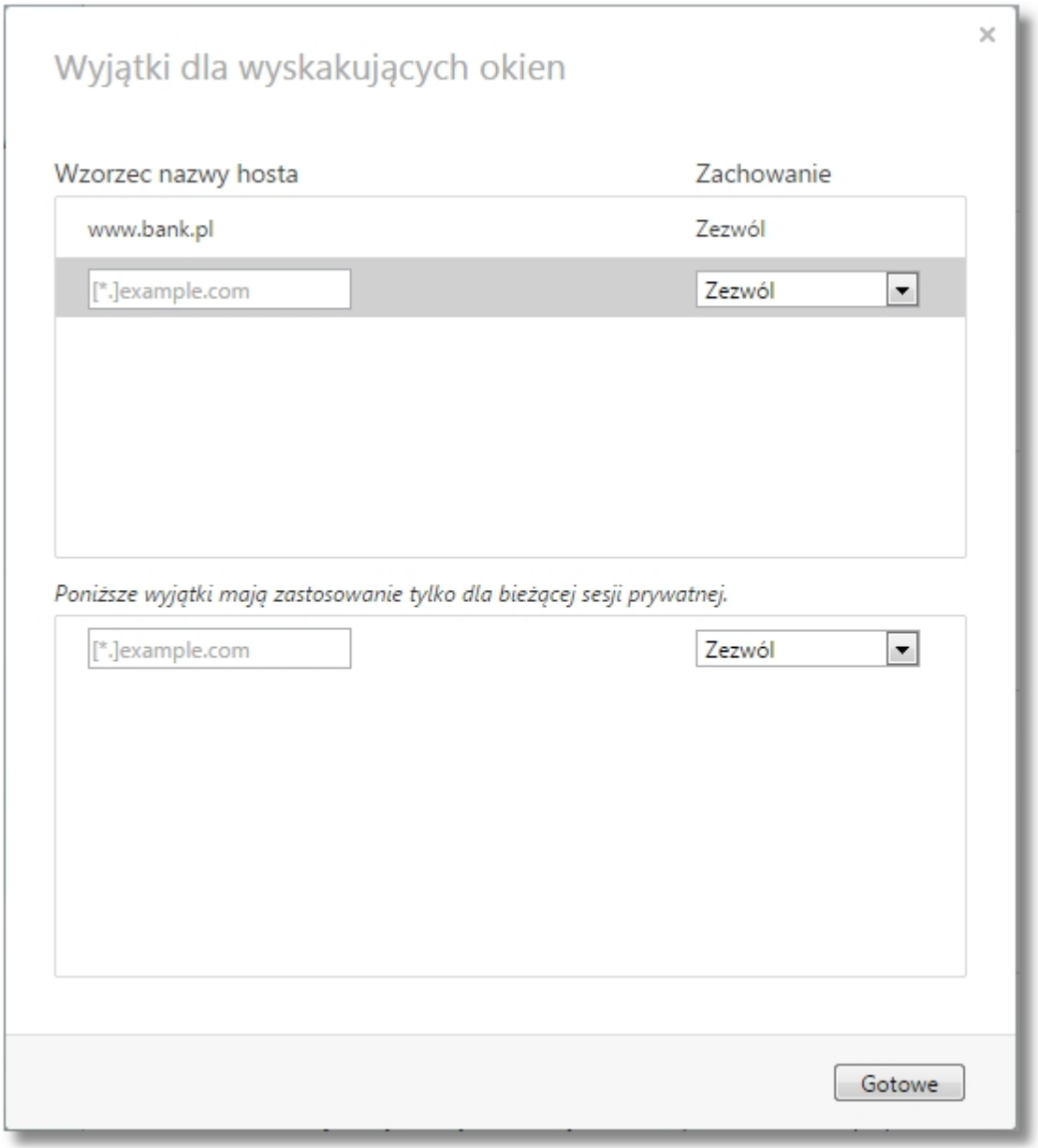
W przypadku całkowitego wyłączeniu obsługi JavaScript, niektóre strony przestaną działać prawidłowo. W celu wyboru sposobu obsługi skryptów JavaScript na poszczególnych witryn należy wybrać przycisk [Zarządzaj wyjątkami ...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].



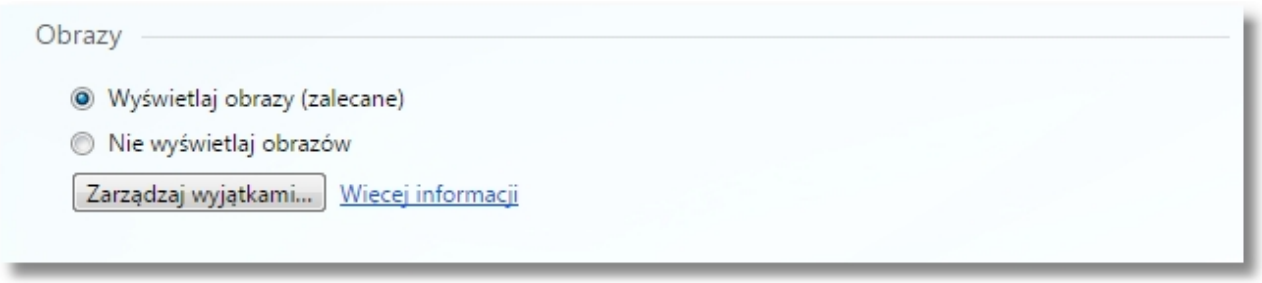
W sekcji **Wyskakujące okna** należy zaznaczyć opcję *Nie zezwalaj żadnym witrynom na wyświetlanie wyskakujących okien (zalecane).*



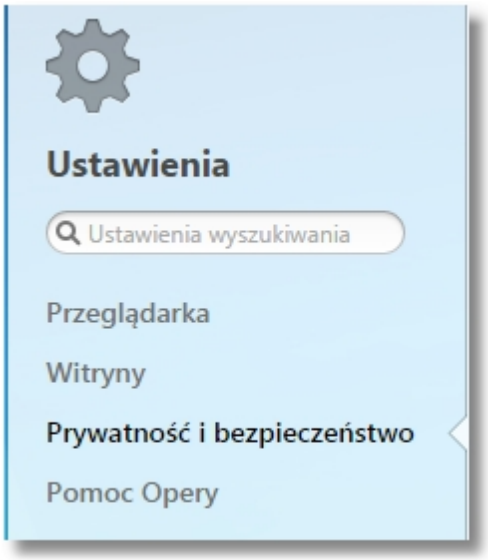
Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy wybrać przycisk [Zarządzaj wyjątkami ...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].



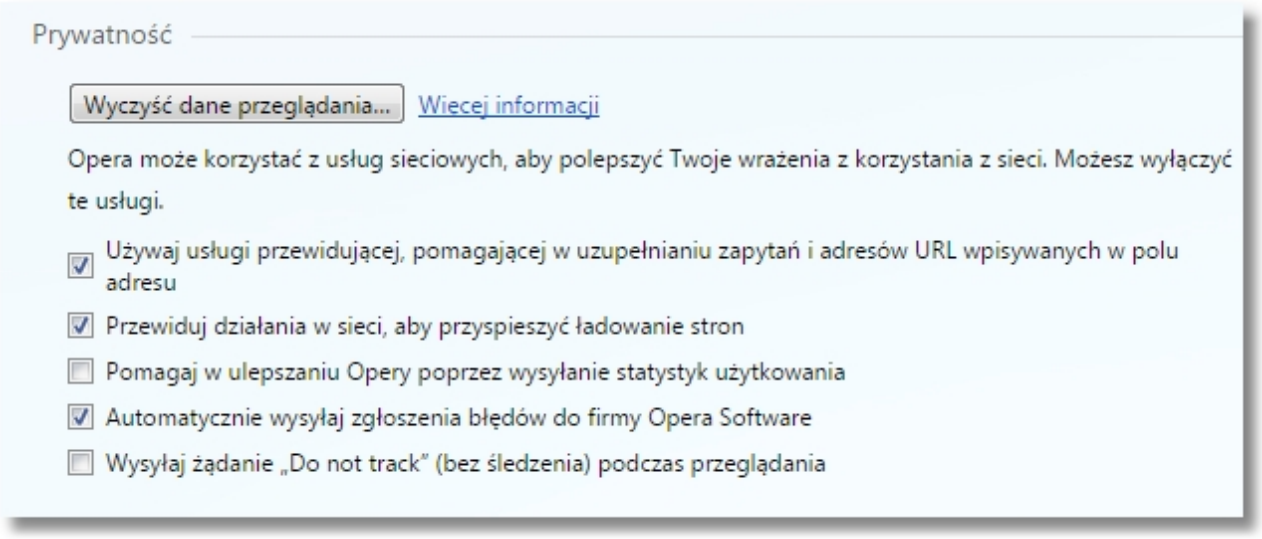
W sekcji **Obrazy** należy zaznaczyć opcję *Wyświetlaj obrazy (zalecane)*.



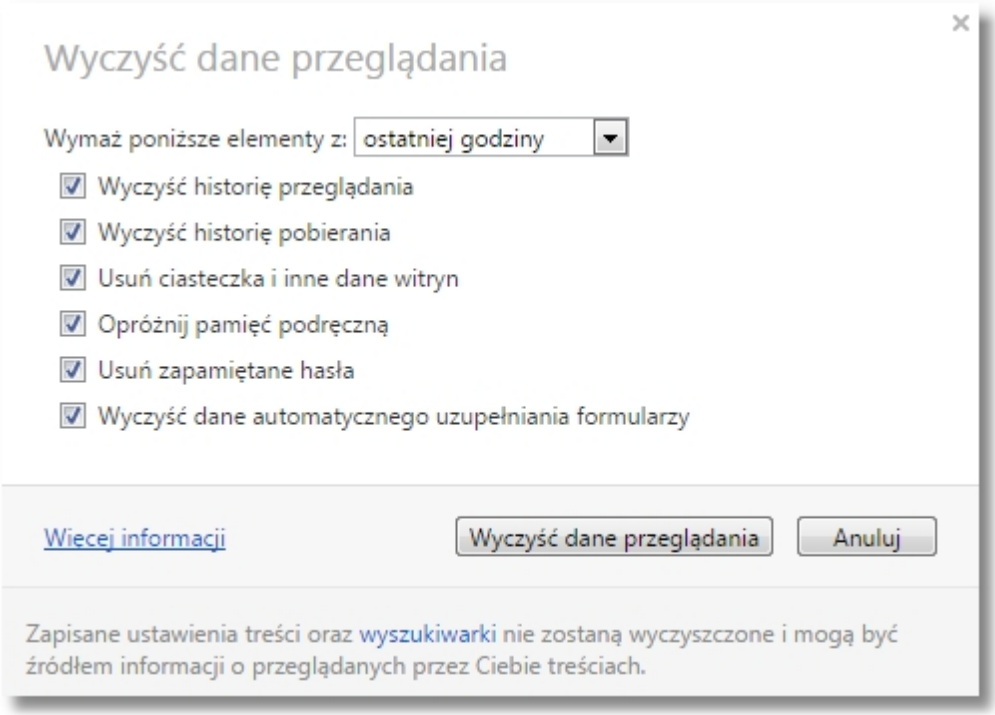
Wybrać zakładkę *Prywatność i bezpieczeństwo* oraz skonfigurować odpowiednio ustawienia.



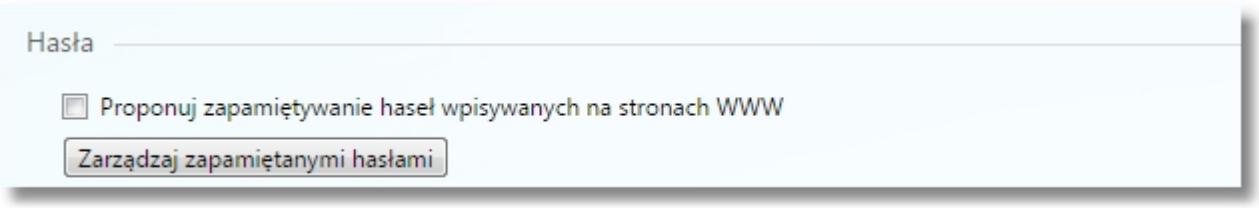
W sekcji **Prywatność** należy wybrać przycisk [Wyczyść dane przeglądania ...]



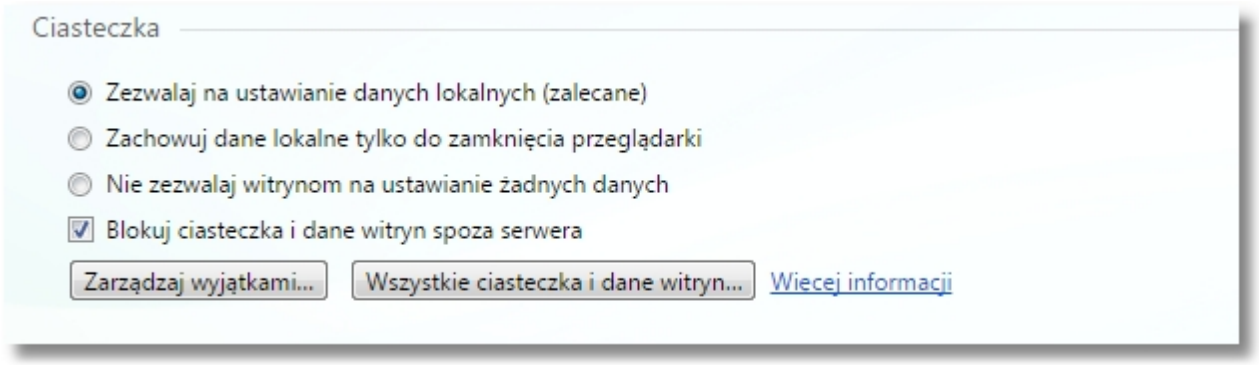
Zaznaczyć opcje jak poniżej oraz wybrać przycisk [Wyczyść dane przeglądania]. Wyczyszczenie historii przeglądania spowoduje usunięcie wszystkich informacji o odwiedzonych stronach, takich jak adresy i czasy odwiedzin.



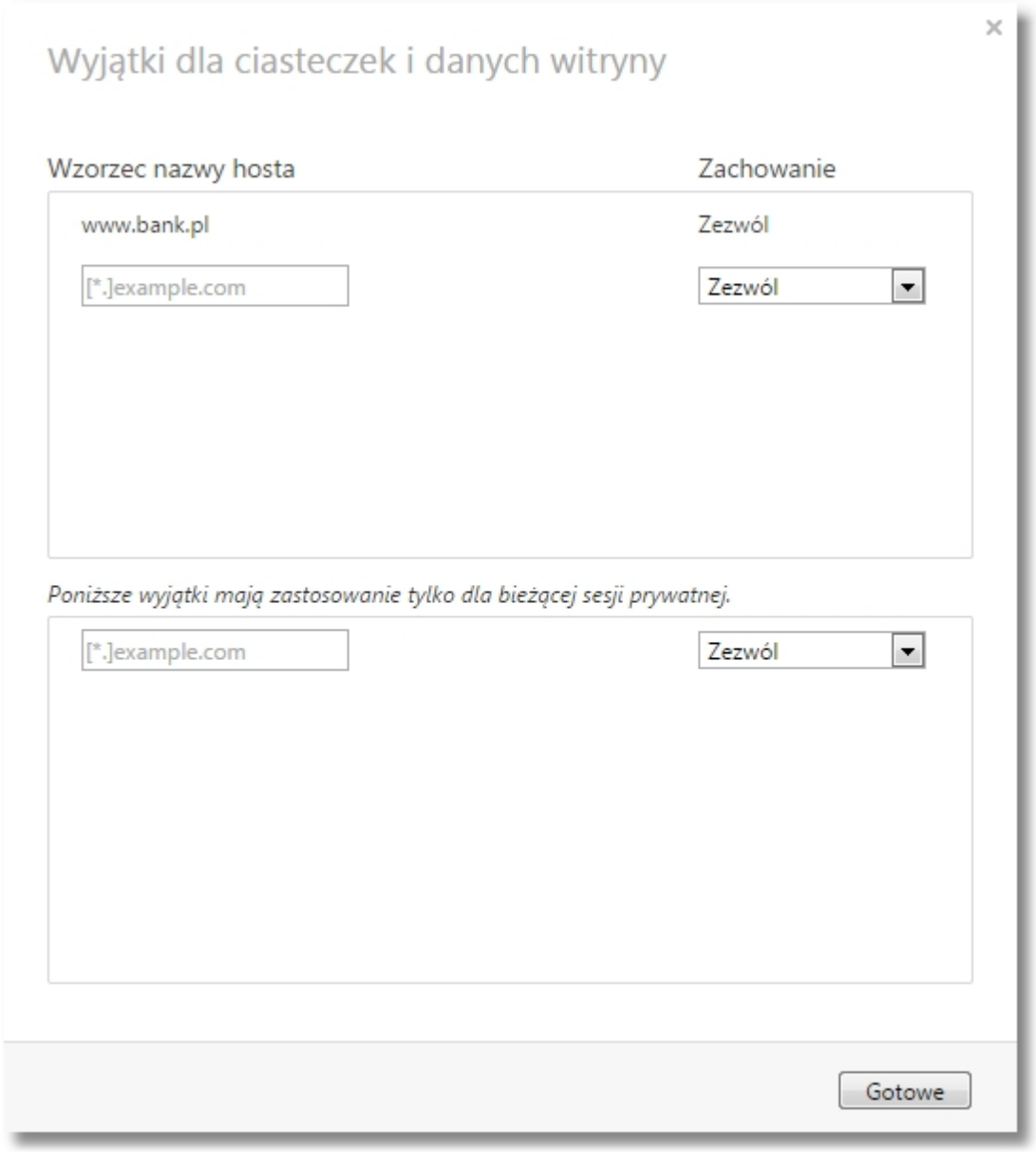
W sekcji **Hasła** należy odznaczyć opcję *Proponuj zapamiętywanie haseł wpisywanych na stronach WWW*.



W sekcji **Ciasteczka** należy zaznaczyć opcję *Blokuj ciasteczka i dane witryn spoza serwera*.



Określenie ustawień ciasteczek daje kontrolę nad sposobem ich obsługi przez Operę. W związku z tym użytkownik ma możliwość określenia wyjątków dla ciasteczek i danych witryny. W tym celu należy wybrać przycisk [Zarządzaj wyjątkami...] wpisać adres strony banku internetowego, w kolumnie **Zachowanie** ustawić wartość *Zezwól* i zaakceptować wprowadzone dane przyciskiem [Gotowe].

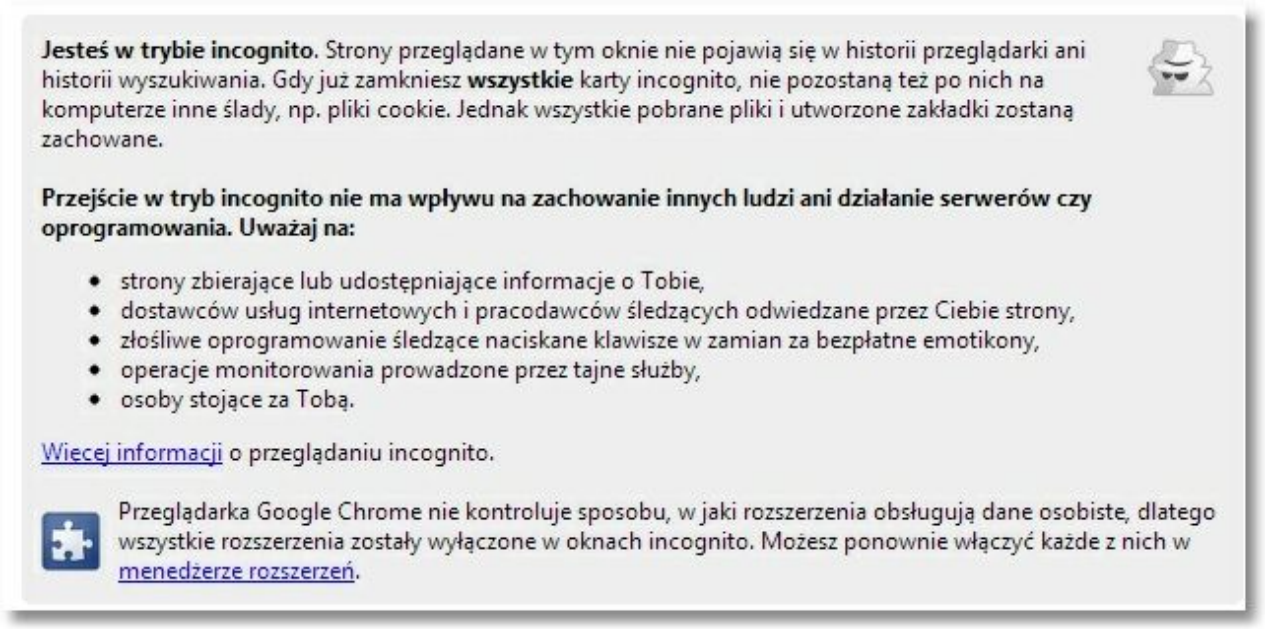

Wyjątki dla ciasteczek i danych witryny
Wzorzec nazwy hosta
Zachowanie
www.bank.pl
Zezwól
[*.]example.com
Zezwól
Poniższe wyjątki mają zastosowanie tylko dla bieżącej sesji prywatnej.
[*.]example.com
Zezwól
Gotowe

Rozdział 13. Konfiguracja przeglądarki Google Chrome 22.0.1229.96

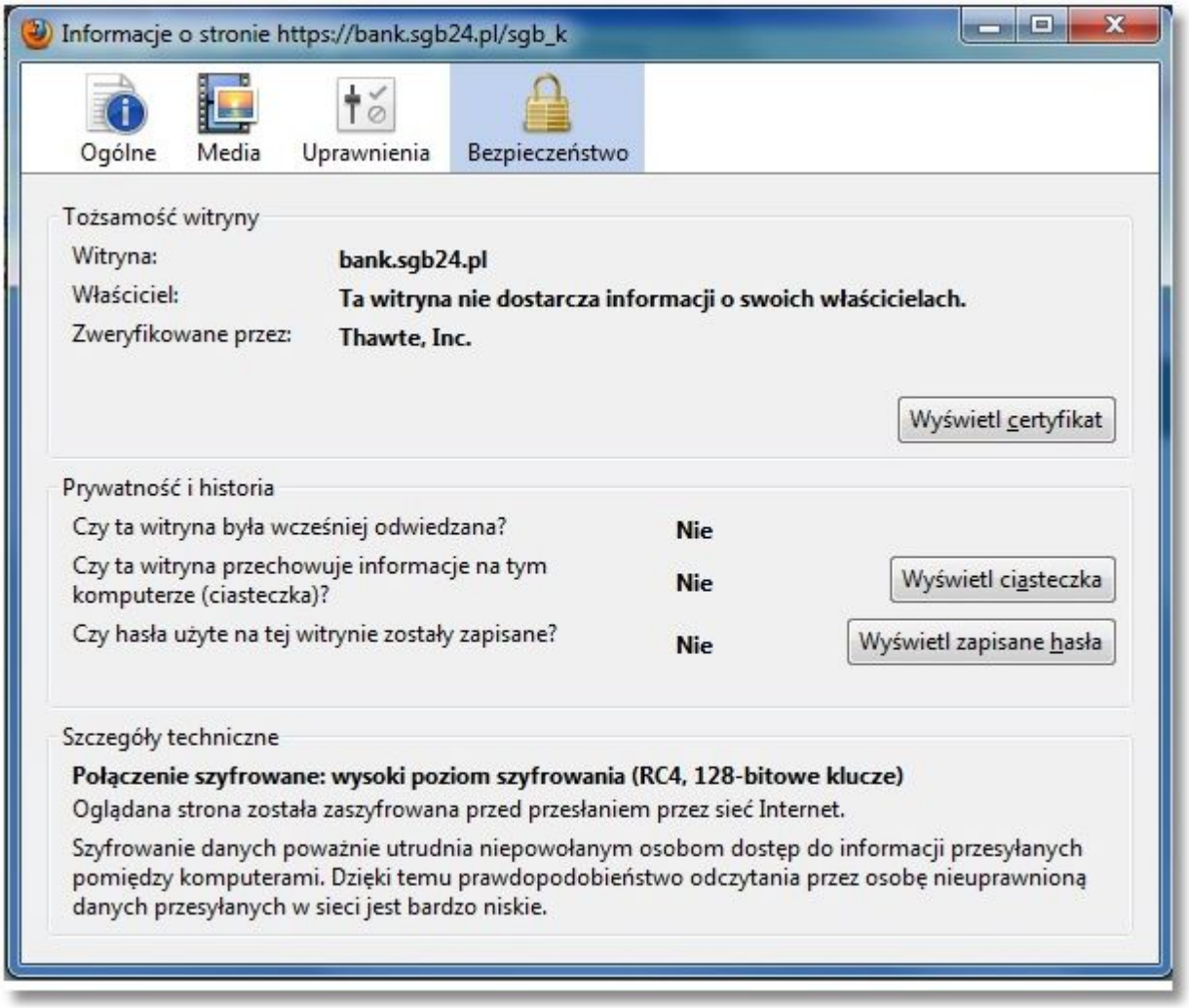
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki. W przypadku, gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana. Przeglądarka Google Chrome w wersji 22.0.1229.96 wspiera następujące systemy operacyjne: Windows Vistax32, Windows Vistax64, Windows 7x32, Windows 7x64.
Przeglądarka Google Chrome zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecana jest praca w trybie incognito. Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję **Nowe okno incognito.** Otworzy się nowe okno z ikoną incognito  . W innym oknie można dalej przeglądać strony w normalnym trybie.

Aby otworzyć okno incognito, można też użyć skrótu klawiaturowego <CTRL>+<SHIFT>+<N>.

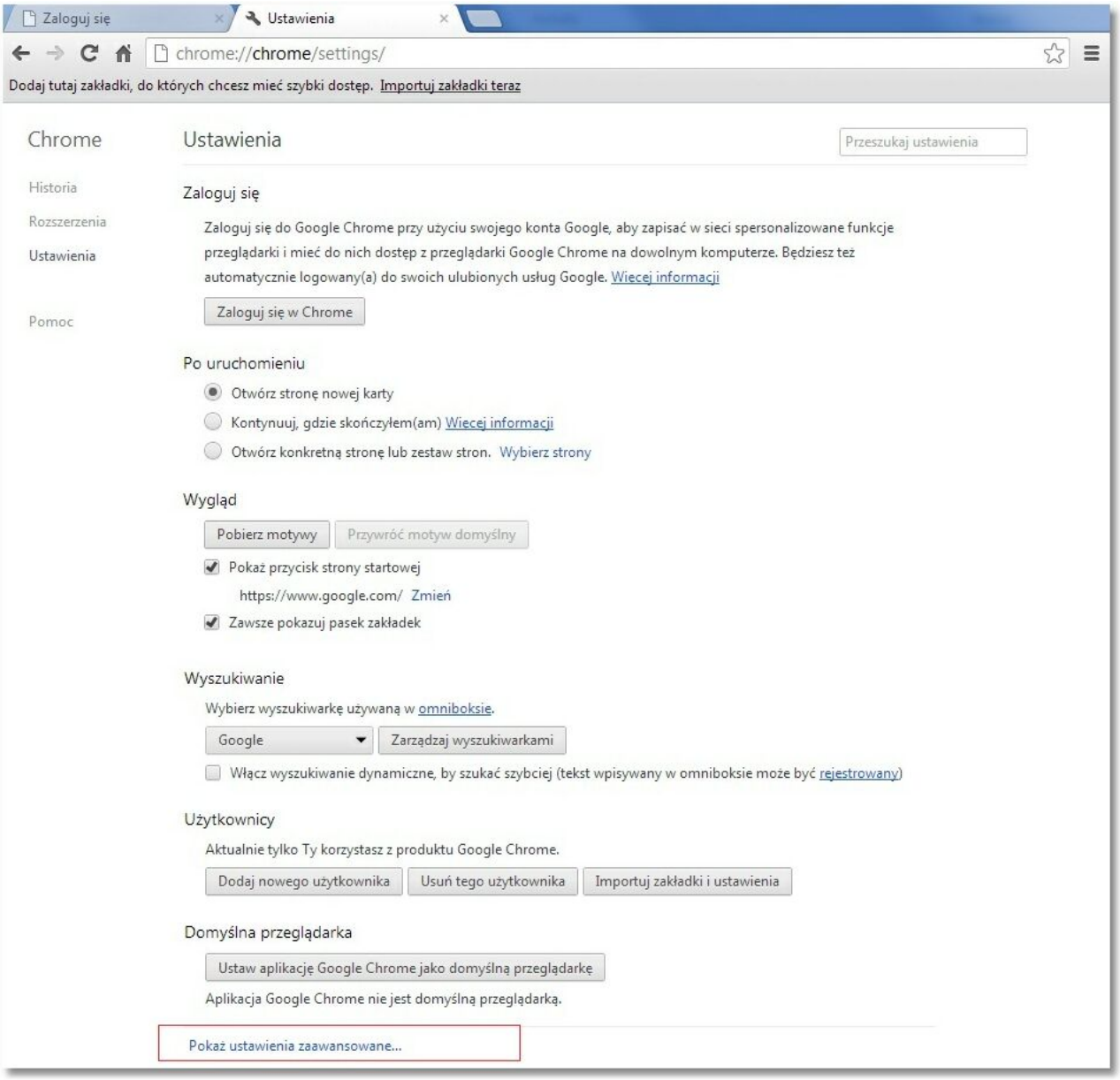
W trybie incognito otwierane strony oraz pobierane pliki nie są rejestrowane w historiach przeglądania i pobierania. Wszystkie nowe pliki cookie są kasowane po zamknięciu wszystkich otwartych okien incognito. Zmiany w zakładkach i ogólnych ustawieniach Google Chrome wprowadzone w trybie incognito są zawsze zapisywane.



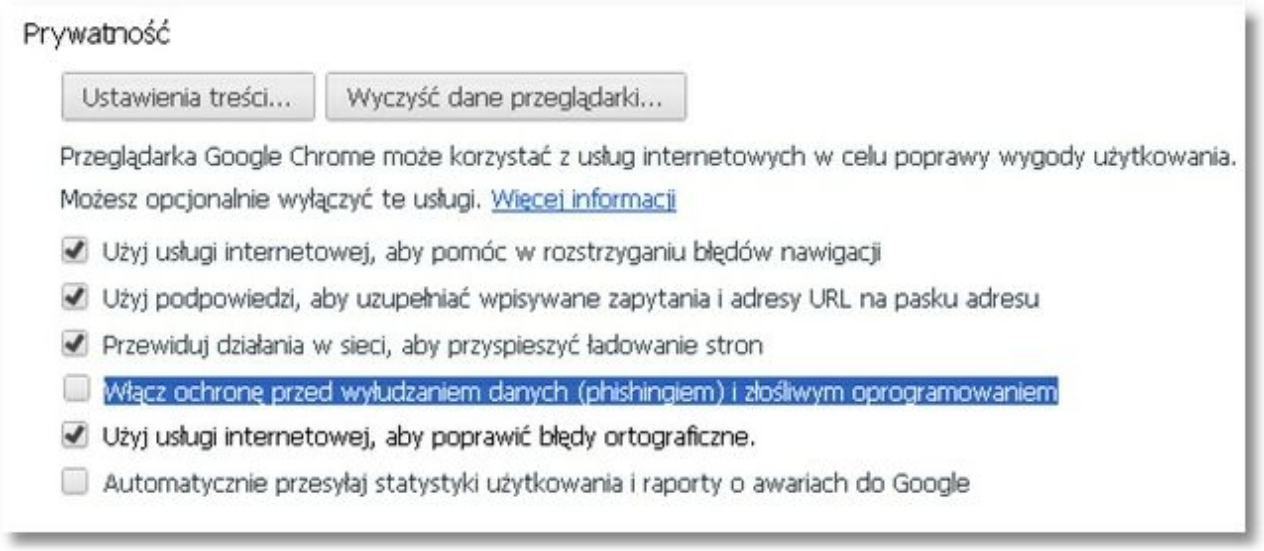
Aby poprawnie skonfigurować przeglądarkę Google Chrome należy w pierwszym kroku kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać menu **Ustawienia**.



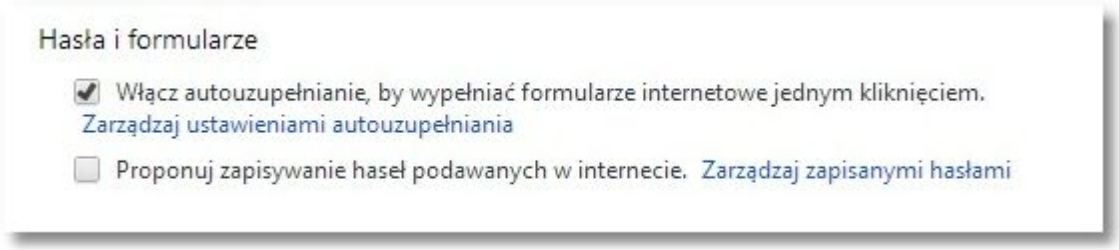
- z menu **Ustawienia** wybrać odnośnik Pokaż ustawienia zaawansowane ...



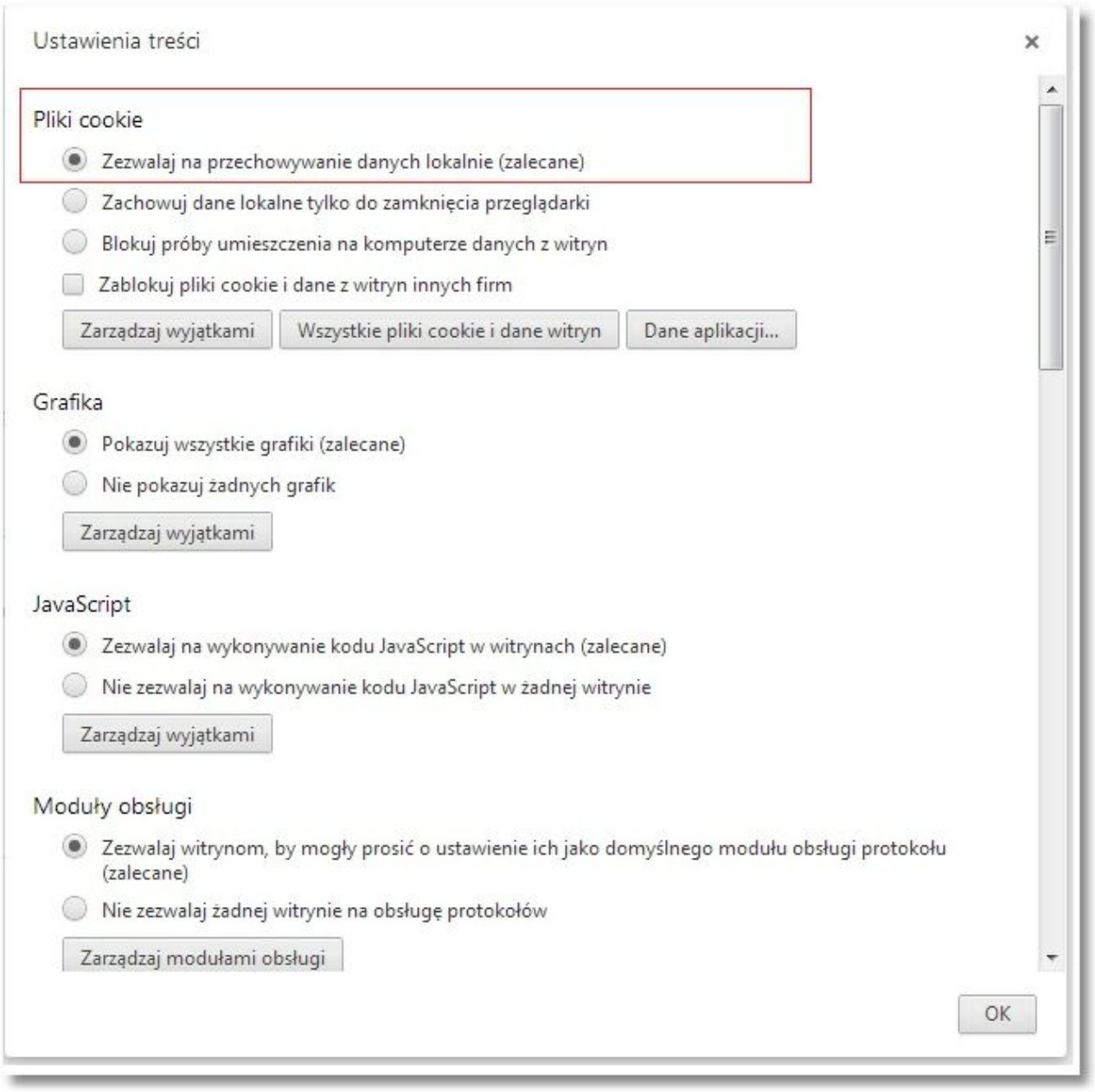
- w sekcji **Prywatność** odznaczyć pole **Włącz ochronę przed wyłudzaniem danych (phishingiem) i złośliwym oprogramowaniem**.



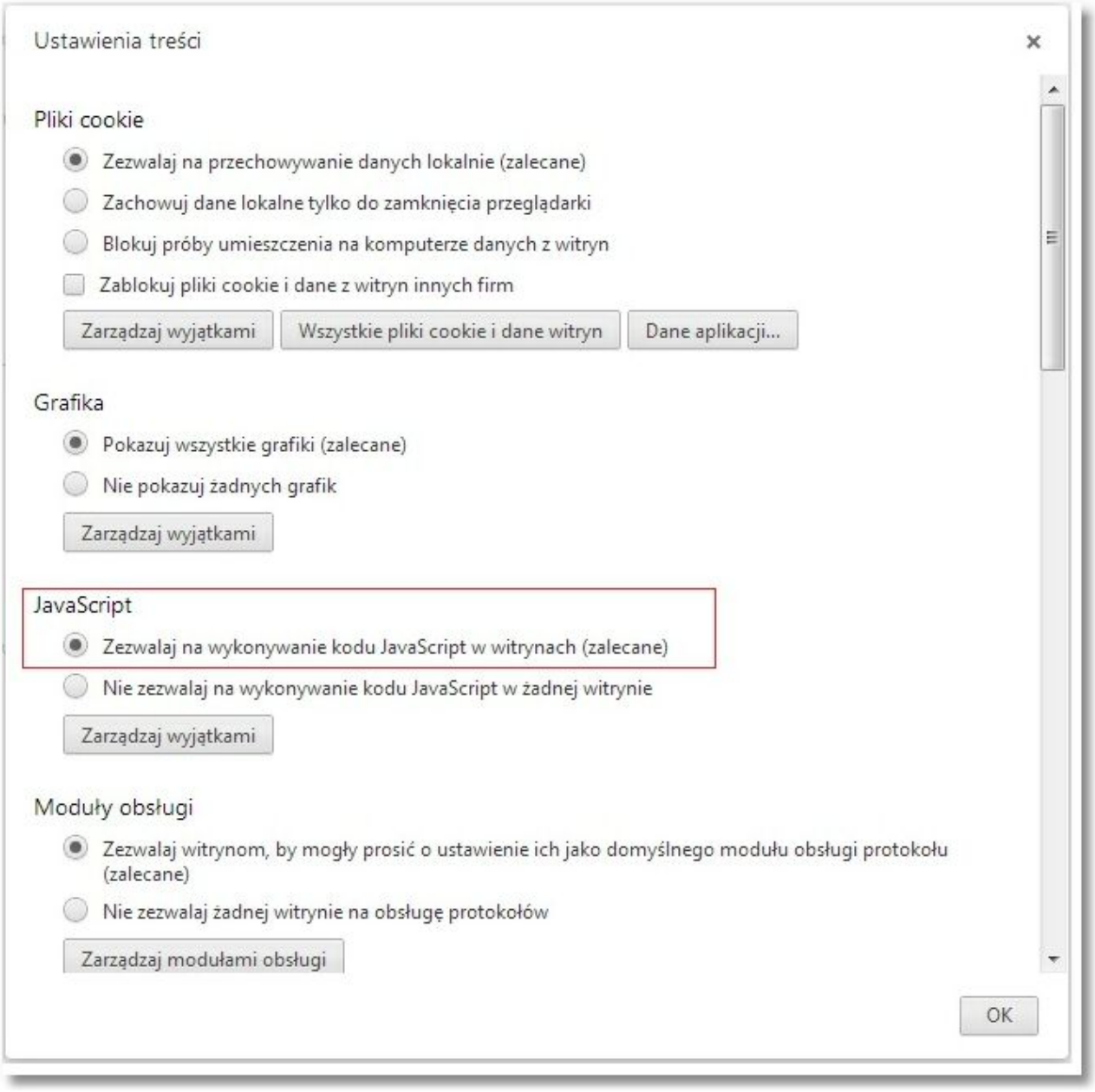
- w sekcji **Hasła i formularze** odznaczyć pole **Proponuj zapisywanie haseł podawanych w internecie**.



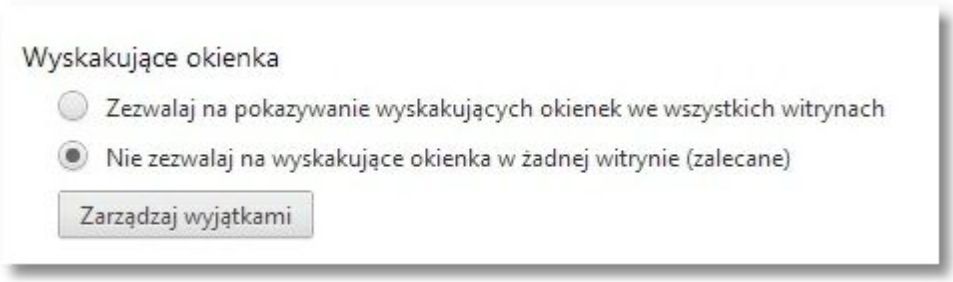
W sekcji **Prywatność** wybrać odnośnik **Ustawienia treści**, a następnie w sekcji **Pliki cookie** zweryfikować, czy zaznaczona jest opcja *Zezwalaj na przechowywanie danych lokalnie (zalecane)*, aby umożliwić dostęp plikom cookie własnej firmy i innych firm.



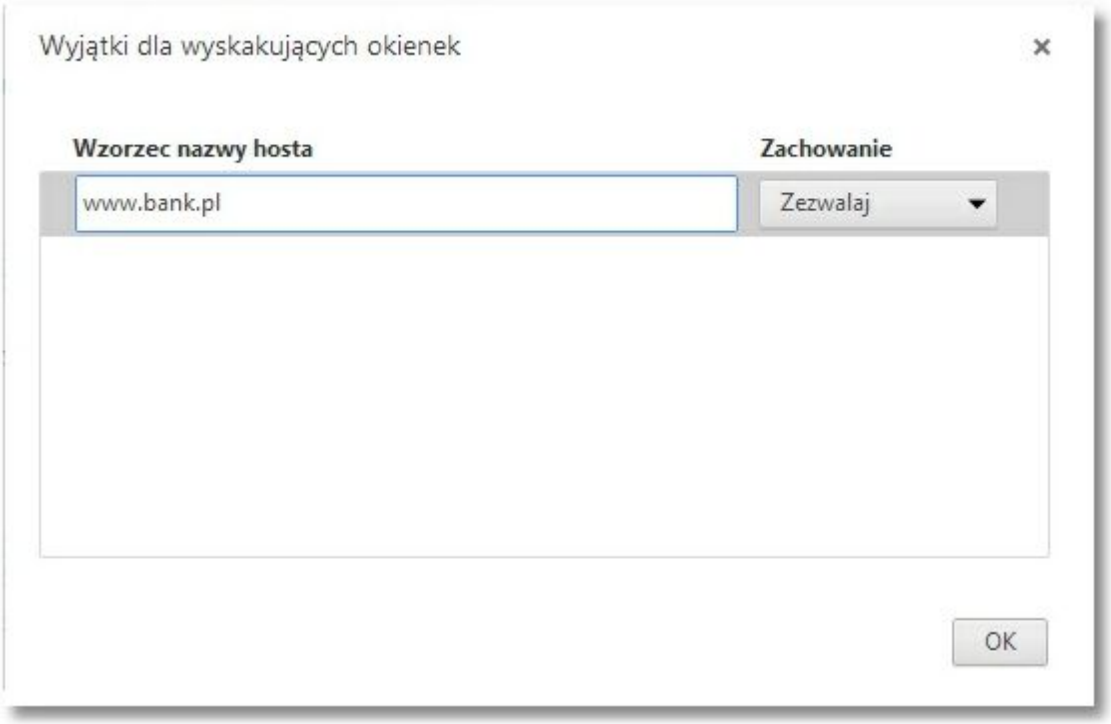
W sekcji **Prywatność** wybrać odnośnik **Ustawienia treści**, a następnie w sekcji **JavaScript** zaznaczyć pole **Zezwalaj na wykonywanie kodu JavaScript w witrynach (zalecane)**, aby włączyć obsługę JavaScript w przeglądarce.



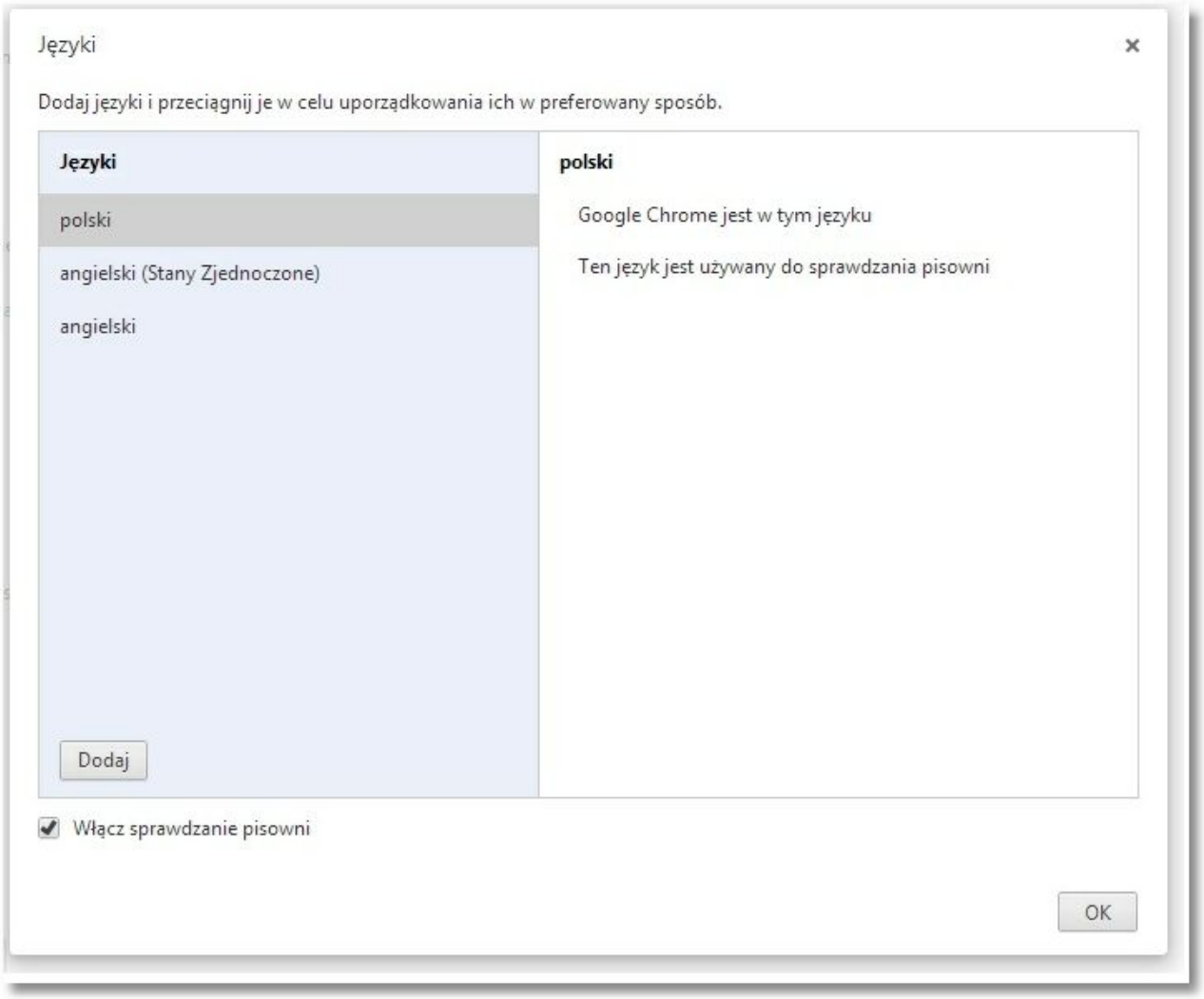
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści, a następnie w sekcji **Wyskakujące okienka** należy zaznaczyć pole **Nie zezwalaj na wyskakujące okienka w żadnej witrynie (zalecane)**.



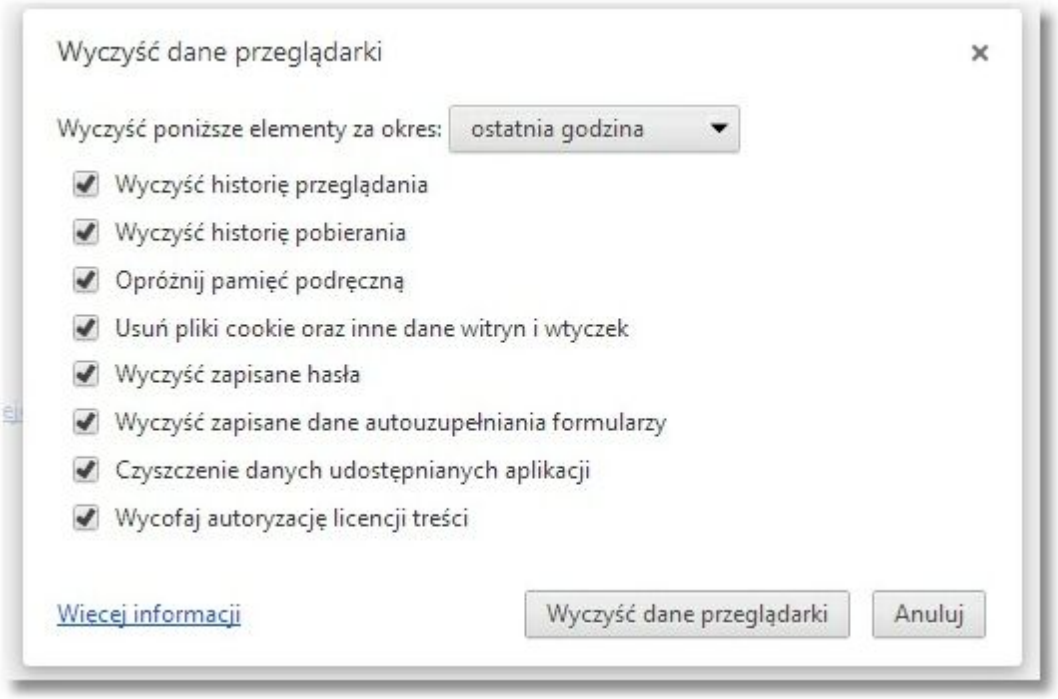
Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy w sekcji **Wyskakujące okienka** wybrać odnośnik Zarządzaj wyjątkami, a następnie w sekcji **Wzorzec nazwy hosta wpisać** adres strony banku internetowego i zaakceptować wprowadzone dane przyciskiem [OK].



- w zakładce **Ustawienia** w sekcji **Języki** kliknąć na odnośnik Ustawienia języków i sprawdzania pisowni oraz wybrać z listy polski i dodać go do listy języków za pomocą przycisku [Dodaj] oraz zatwierdzić przyciskiem [OK]. Pozycja będzie prezentowana jako pierwszy element na liście.



W celu wyczyszczenia pamięci podręcznej przeglądarki należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję *Narzędzia -> Wyczyść dane przeglądania*.
Na poniższym formularzu zaznaczyć wszystkie pozycje oraz wybrać przycisk [Wyczyść dane przeglądarki].


Wyczyść dane przeglądarki
Wyczyść poniższe elementy za okres:
ostatnia godzina
Wyczyść historię przeglądania
Wyczyść historię pobierania
Opróżnij pamięć podręczną
Usuń pliki cookie oraz inne dane witryn i wtyczek
Wyczyść zapisane hasła
Wyczyść zapisane dane autouzupełniania formularzy
Czyszczenie danych udostępnianych aplikacji
Wycofaj autoryzację licencji treści
Więcej informacji
Wyczyść dane przeglądarki
Anuluj

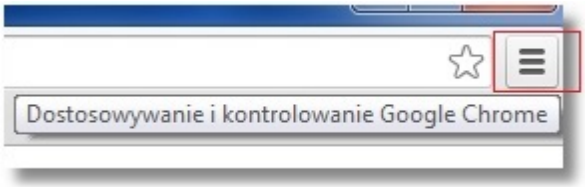
Rozdział 14. Konfiguracja przeglądarki Google Chrome 37.0.2062.103

Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana. Przeglądarka Google Chrome w wersji 37.0.2062.103 wspiera następujące systemy operacyjne: Windows Vistax32, Windows Vistax64, Windows 7x32, Windows 7x64.
Przeglądarka Google Chrome zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecana jest praca w trybie incognito. Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję **Nowe okno incognito.** Otworzy się nowe okno z ikoną incognito  . W innym oknie można dalej przeglądać strony w normalnym trybie.

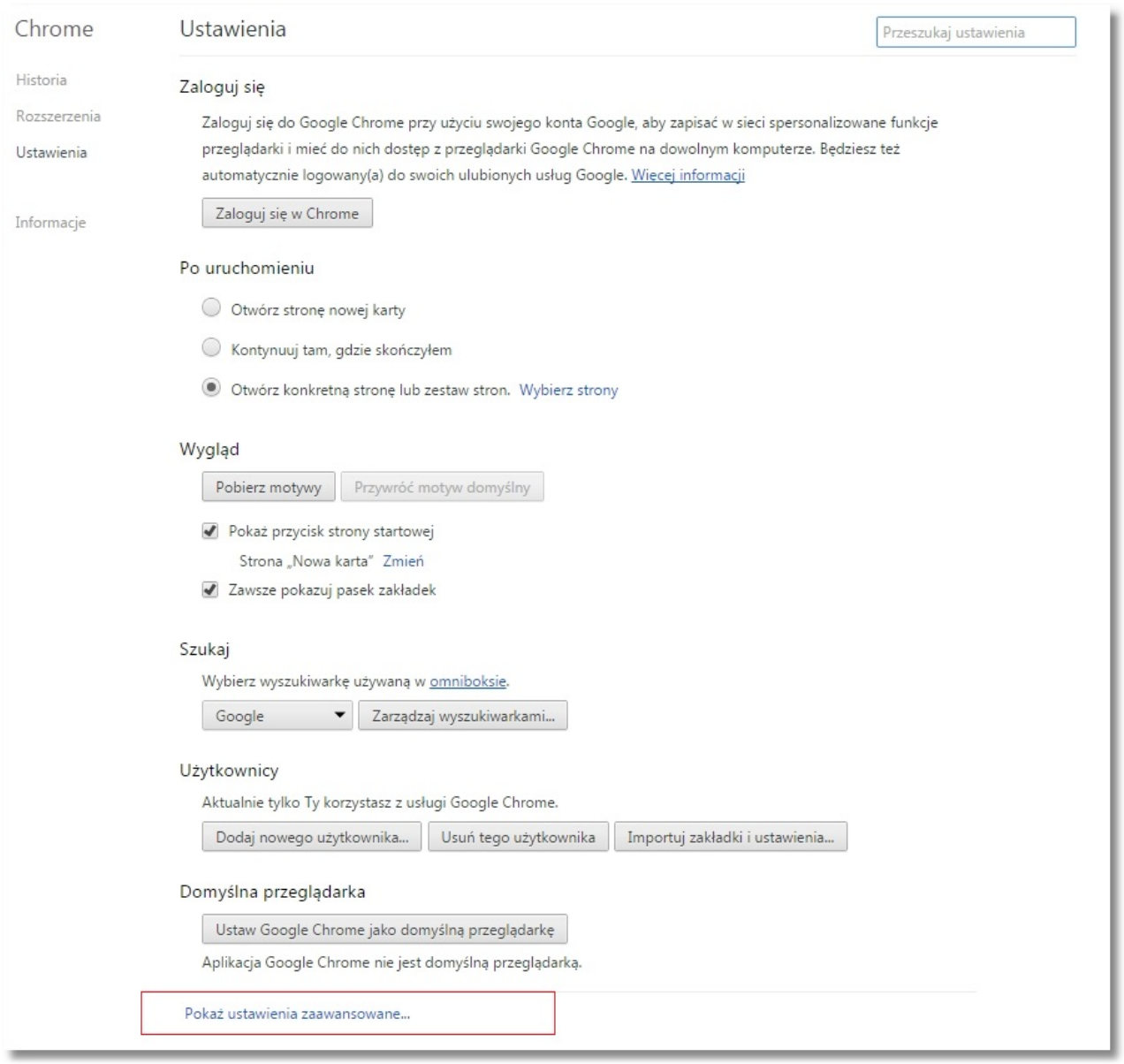
Aby otworzyć okno incognito, można też użyć skrótu klawiaturowego Ctrl+Shift+N.

W trybie incognito otwierane strony oraz pobierane pliki nie są rejestrowane w historiach przeglądania i pobierania. Wszystkie nowe pliki cookie są kasowane po zamknięciu wszystkich otwartych okien incognito. Zmiany w zakładkach i ogólnych ustawieniach Google Chrome wprowadzone w trybie incognito są zawsze zapisywane.

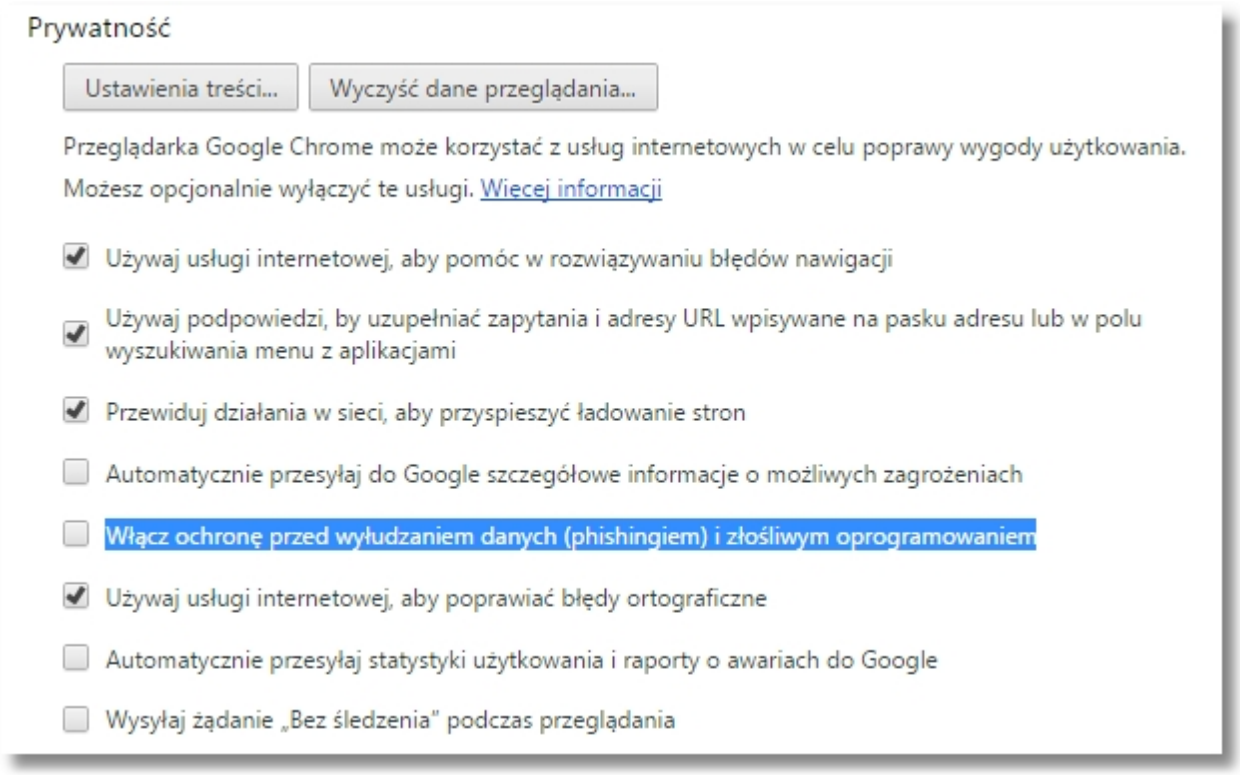
Aby poprawnie skonfigurować przeglądarkę Google Chrome należy w pierwszym kroku kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać menu **Ustawienia**.



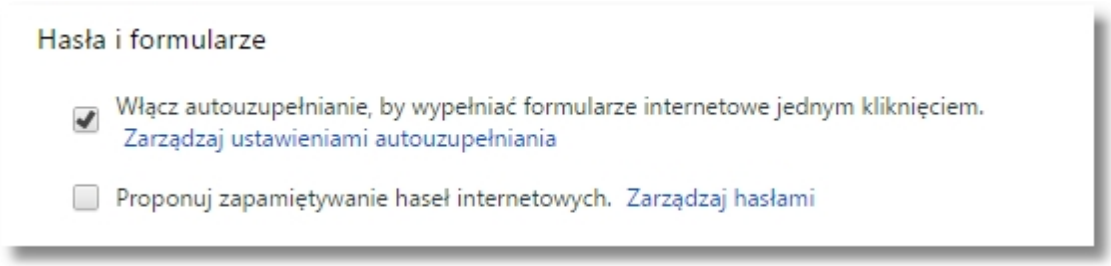
- z menu **Ustawienia** wybrać odnośnik Pokaż ustawienia zaawansowane...



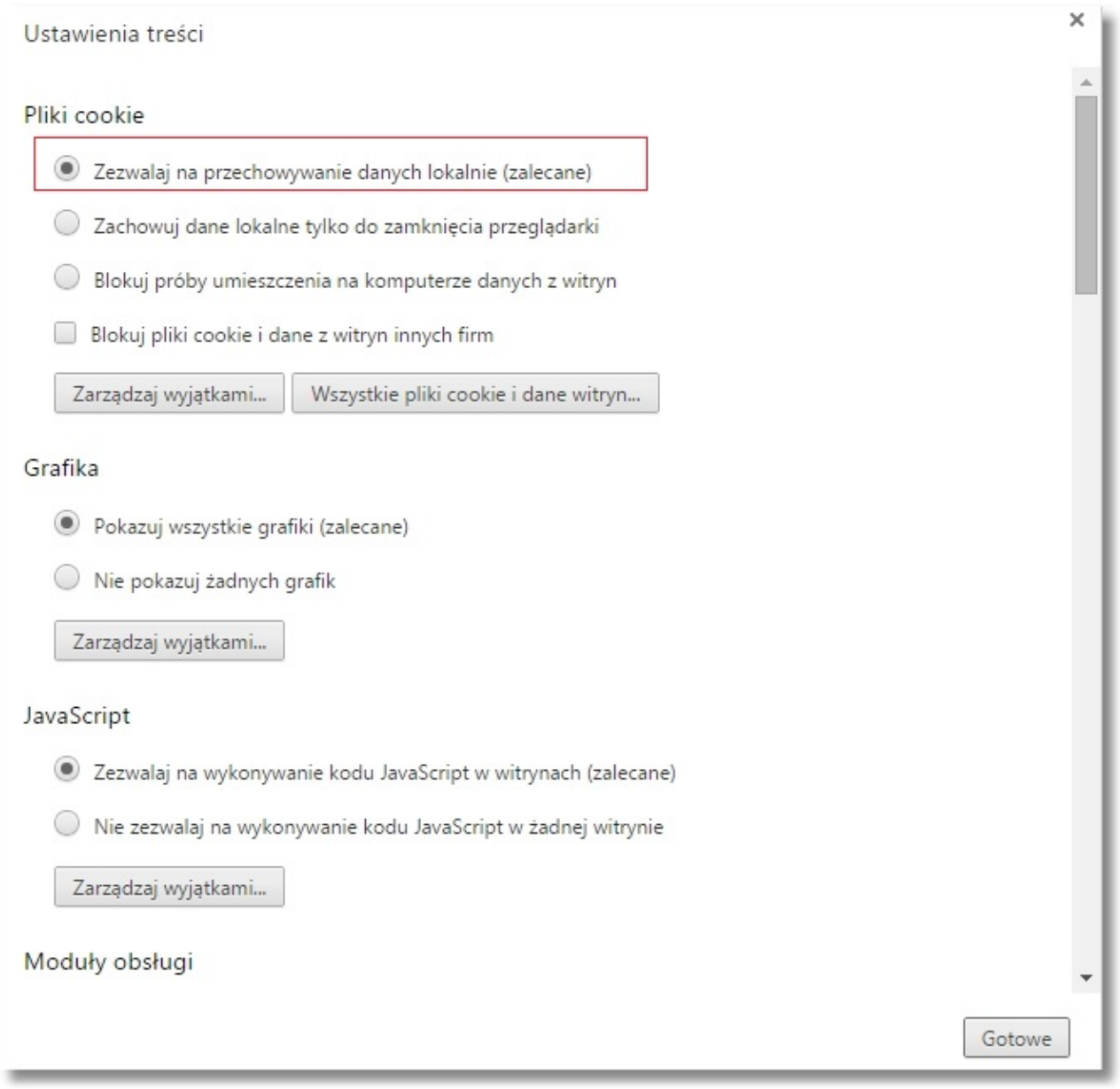
- w sekcji **Prywatność** odznaczyć pole **Włącz ochronę przed wyłudzaniem danych (phishingiem) i złośliwym oprogramowaniem**.



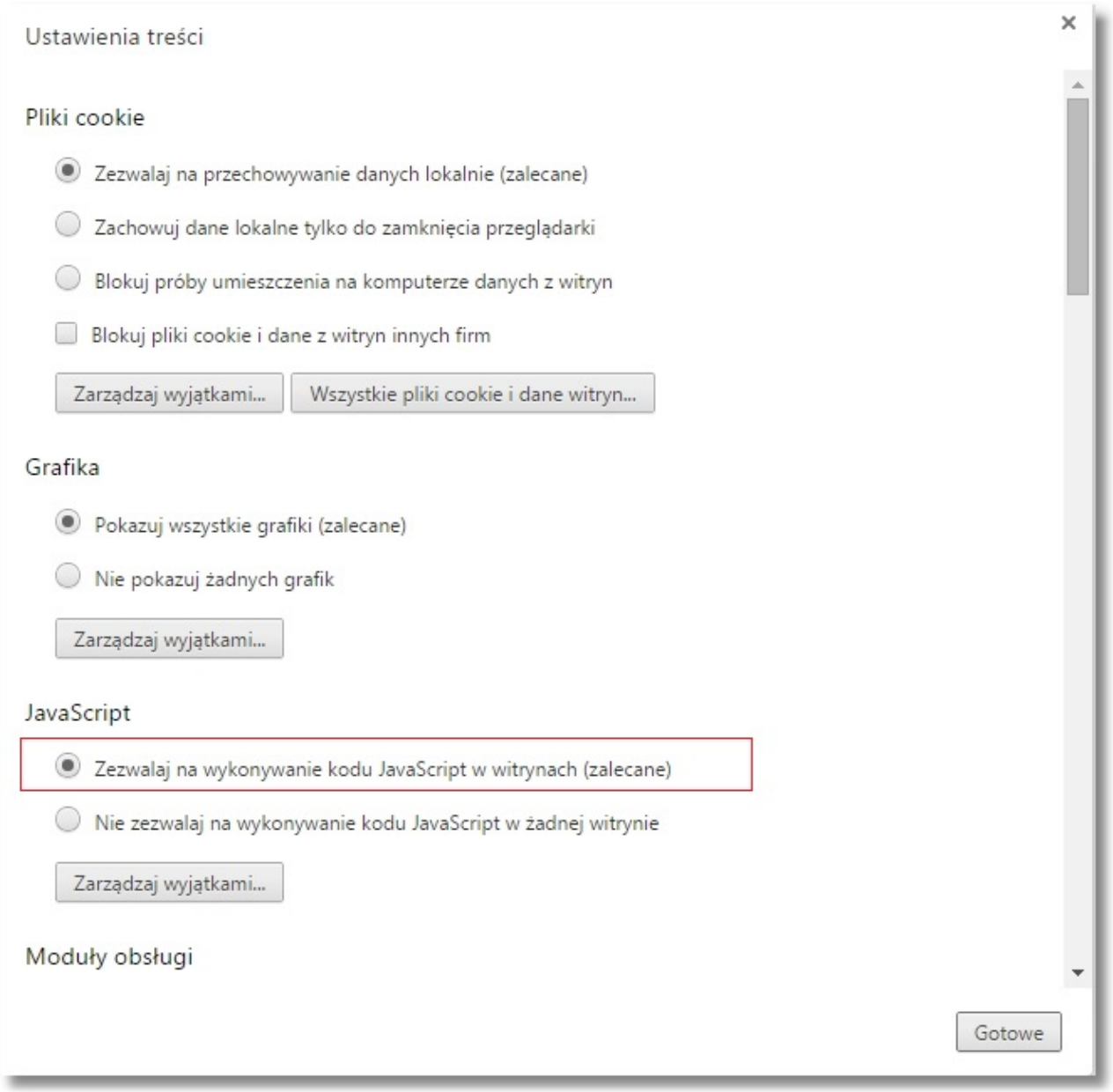
- w sekcji **Hasła i formularze** odznaczyć pole **Proponuj zapisywanie haseł podawanych w internecie**.



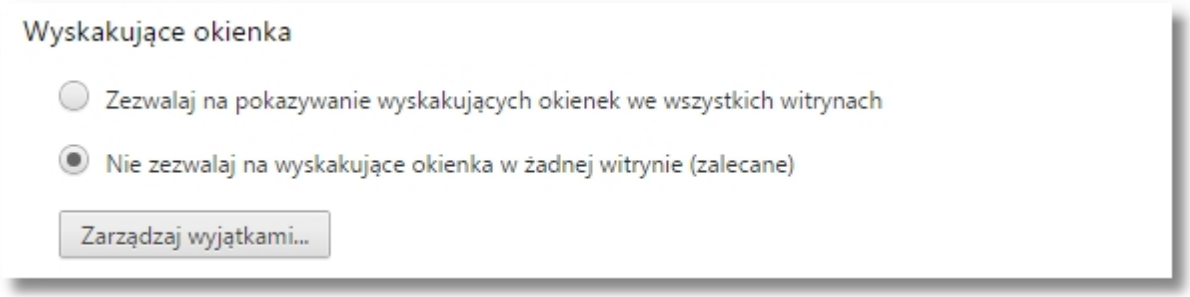
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści, a następnie w sekcji **Pliki cookie** zweryfikować, czy zaznaczona jest opcja *Zezwalaj na przechowywanie danych lokalnie (zalecane)*, aby umożliwić dostęp plikom cookie własnej firmy i innych firm.



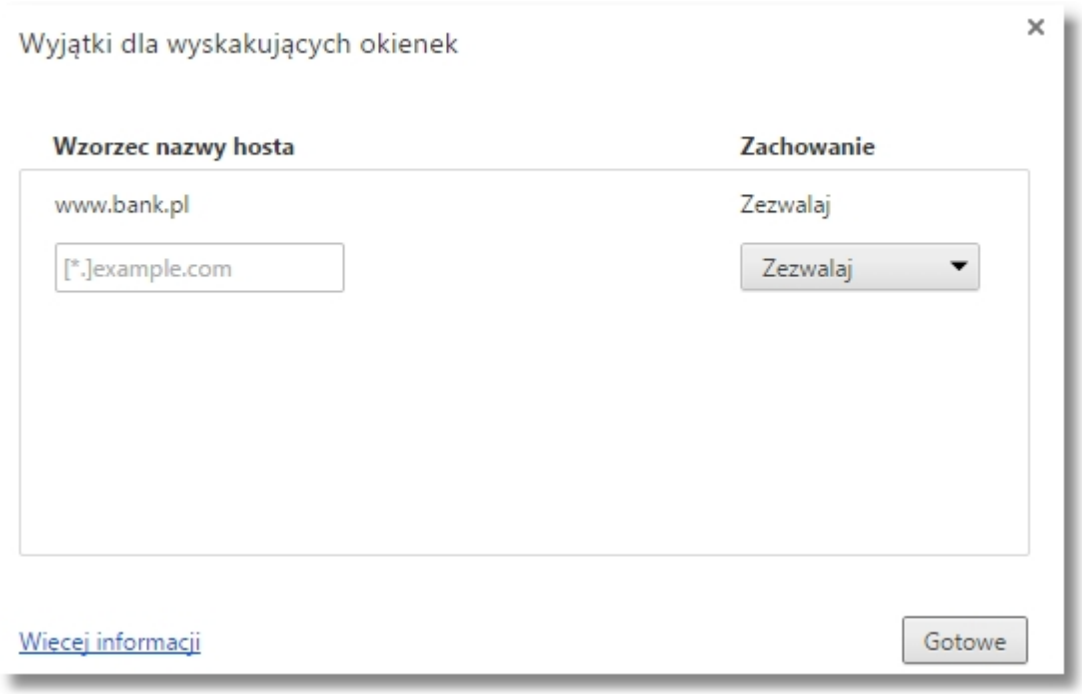
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści, a następnie w sekcji **JavaScript** zaznaczyć pole **Zezwalaj na wykonywanie kodu JavaScript w witrynach (zalecane)**, aby włączyć obsługę JavaScript w przeglądarce.



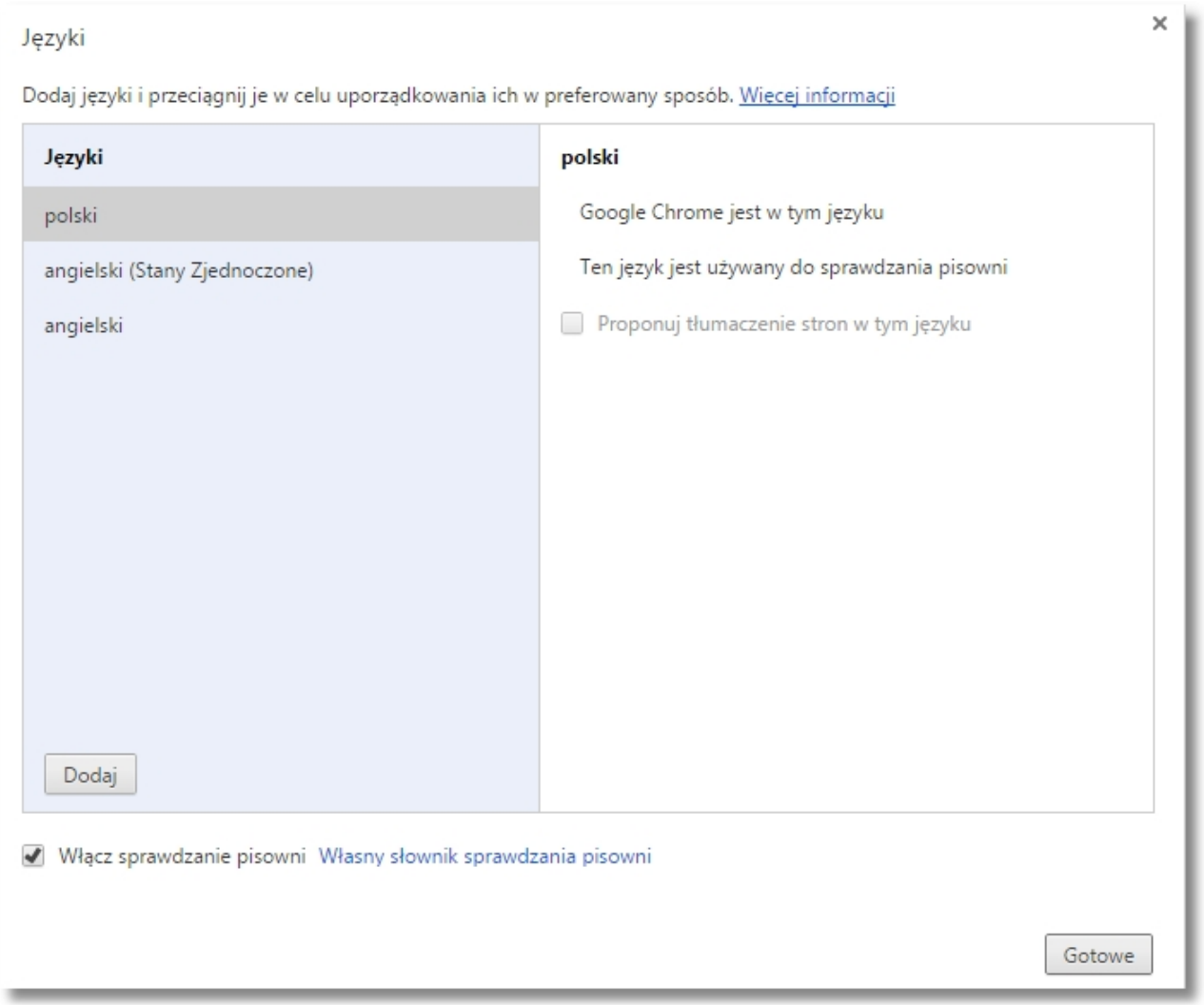
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści, a następnie w sekcji **Wyskakujące okienka** należy zaznaczyć pole **Nie zezwalaj na wyskakujące okienka w żadnej witrynie (zalecane)**.



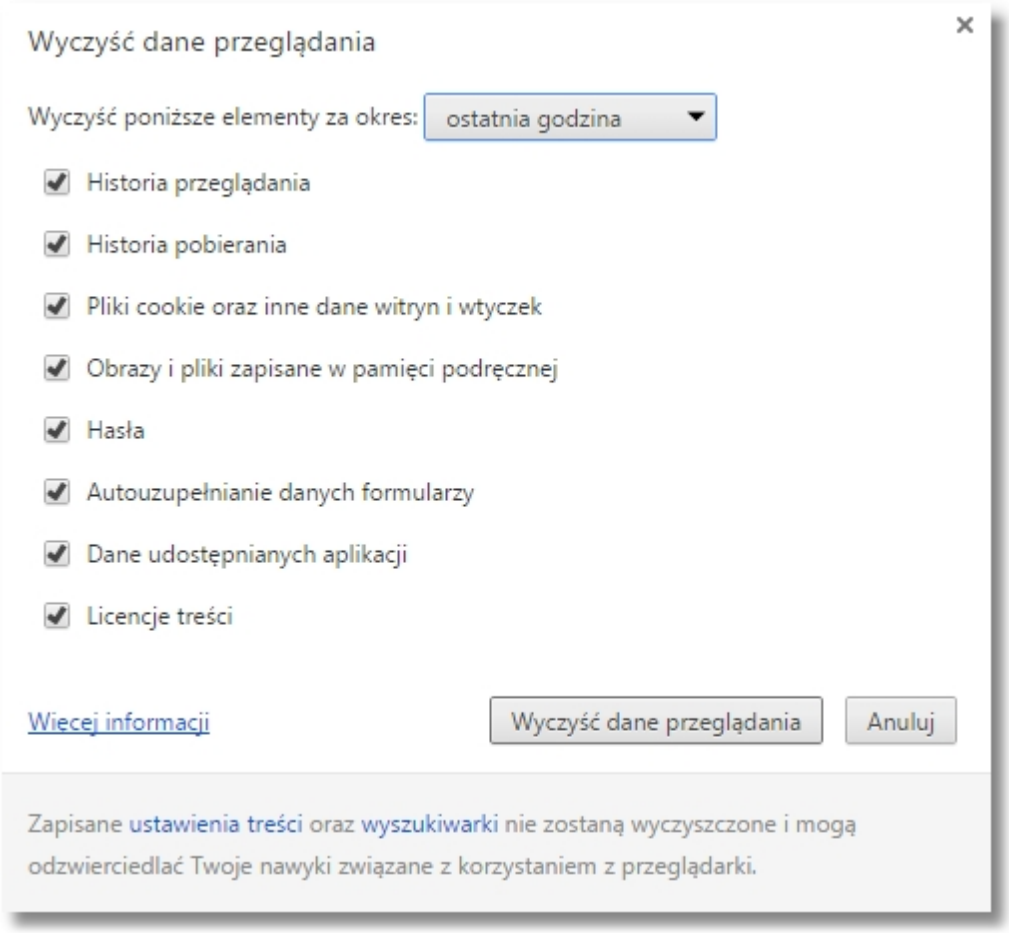
Z uwagi na fakt, że w Aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy w sekcji **Wyskakujące okienka** wybrać odnośnik Zarządzaj wyjątkami, a następnie w sekcji **Wzorzec nazwy hosta wpisać** adres strony banku internetowego i zaakceptować wprowadzone dane przyciskiem [Gotowe].



- w zakładce *Ustawienia* w sekcji **Języki** kliknąć na odnośnik Ustawienia języków i sprawdzania pisowni oraz wybrać z listy polski i dodać go do listy języków za pomocą przycisku [Dodaj] oraz zatwierdzić przyciskiem [Gotowe]. Pozycja będzie prezentowana jako pierwszy element na liście.



W celu wyczyszczenia pamięci podręcznej przeglądarki należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję *Narzędzia -> Wyczyść dane przeglądania*.
Na poniższym formularzu zaznaczyć wszystkie pozycje oraz wybrać przycisk [Wyczyść dane przeglądania].

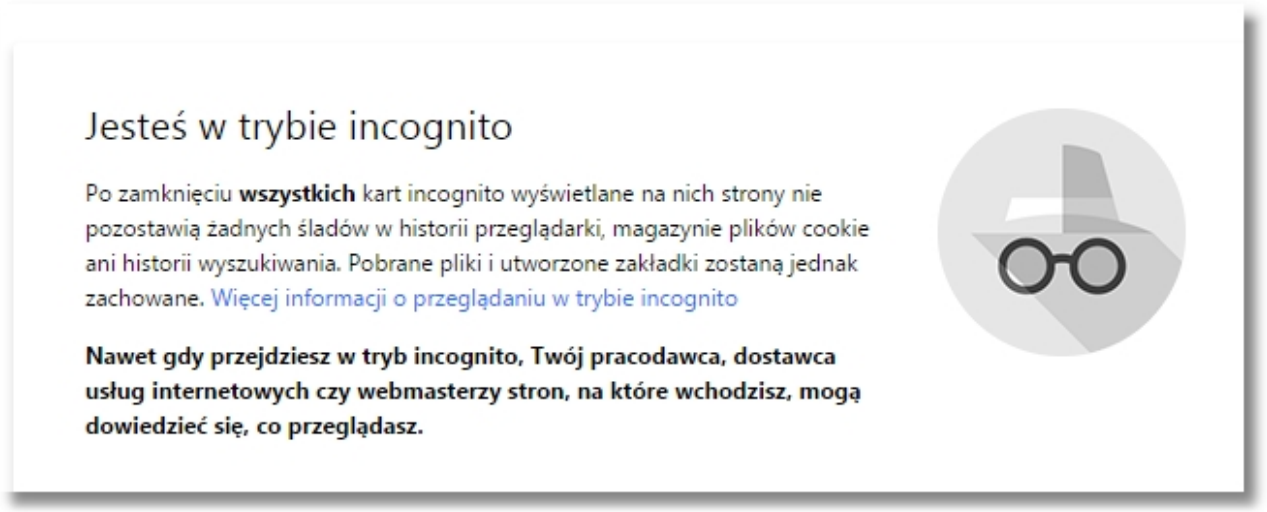

Wyczyść dane przeglądania
Wyczyść poniższe elementy za okres:
ostatnia godzina
Historia przeglądania
Historia pobierania
Pliki cookie oraz inne dane witryn i wtyczek
Obrazy i pliki zapisane w pamięci podręcznej
Hasła
Autouzupełnianie danych formularzy
Dane udostępnianych aplikacji
Licencje treści
Więcej informacji
Wyczyść dane przeglądania
Anuluj
Zapisane ustawienia treści oraz wyszukiwarki nie zostaną wyczyszczone i mogą odzwierciedlać Twoje nawyki związane z korzystaniem z przeglądarki.

Rozdział 15. Konfiguracja przeglądarki Google Chrome 42.0.2311.152

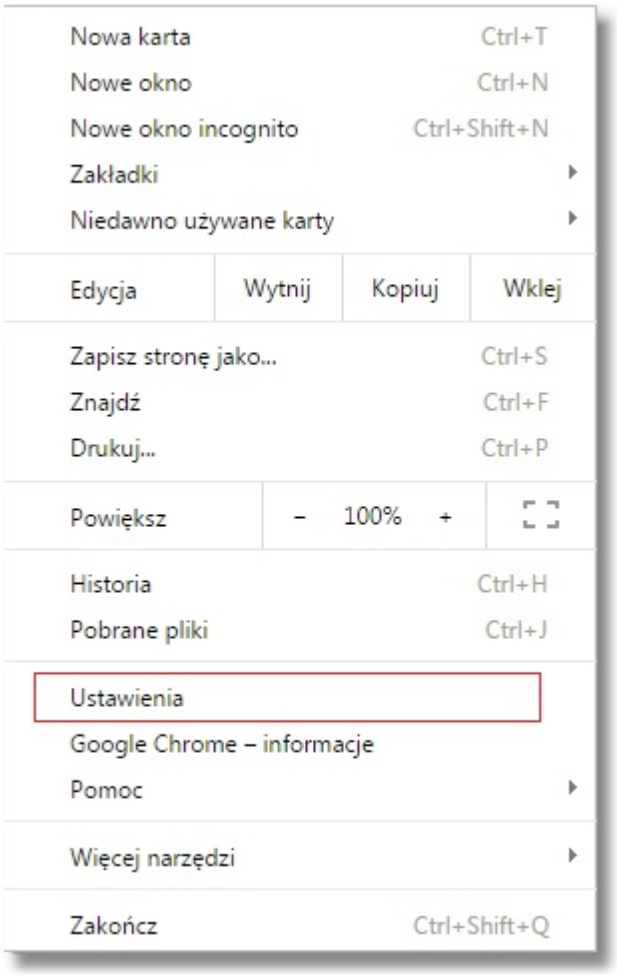
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki, w przypadku gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana. Przeglądarka Google Chrome w wersji 42.0.22311.90 wspiera następujące systemy operacyjne: Windows Vistax32, Windows Vistax64, Windows 7x32, Windows 7x64, Windows 8x32, Windows 8x64, Windows XP. Przeglądarka Google Chrome zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony - takimi jak Serwis Bankowości Internetowej. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecana jest praca w trybie incognito. Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję **Nowe okno incognito.** Otworzy się nowe okno z ikoną incognito  . W innym oknie można dalej przeglądać strony w normalnym trybie.

Aby otworzyć okno incognito, można też użyć skrótu klawiaturowego Ctrl+Shift+N.

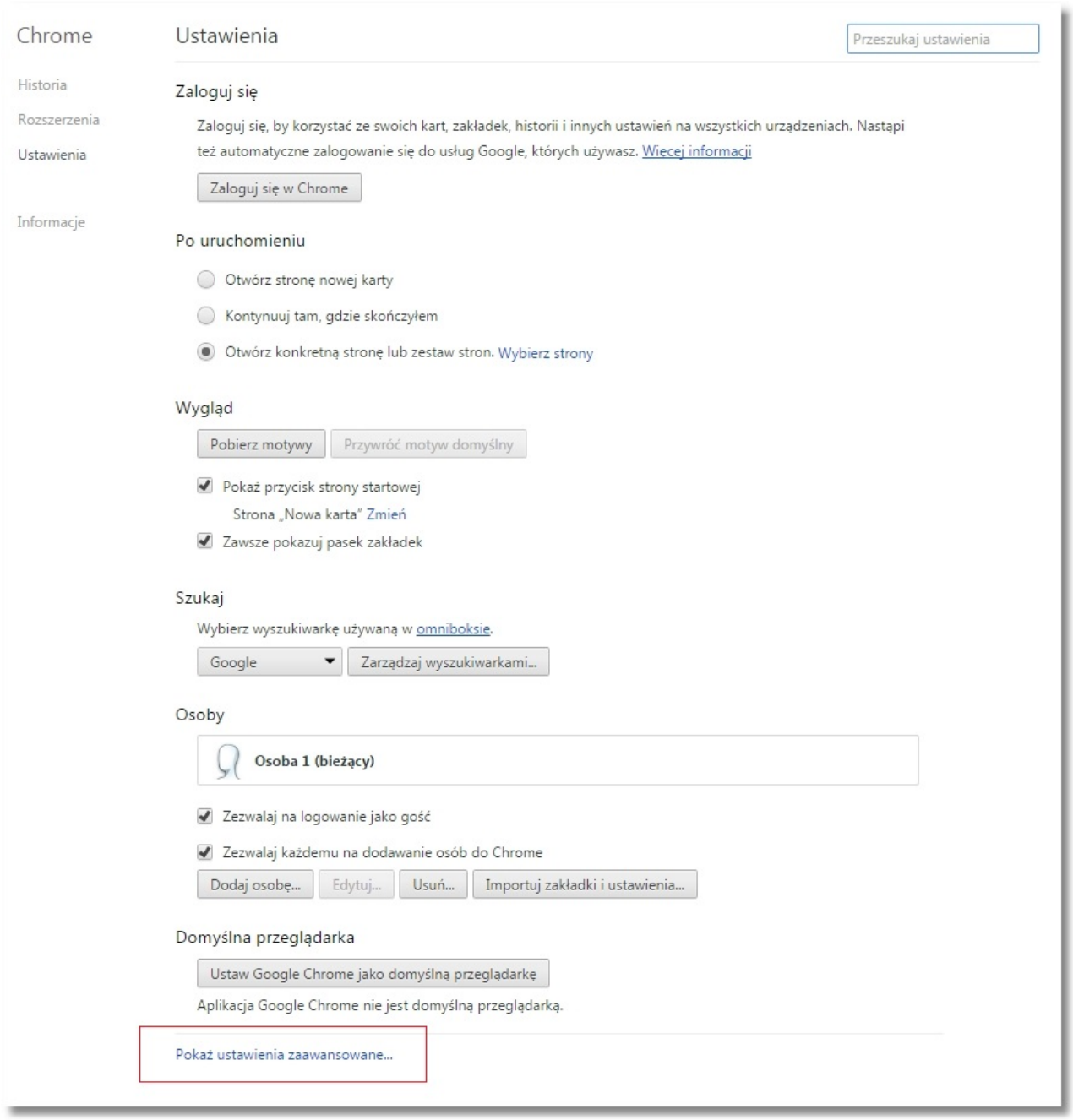
W trybie incognito otwierane strony oraz pobierane pliki nie są rejestrowane w historiach przeglądania i pobierania. Wszystkie nowe pliki cookie są kasowane po zamknięciu wszystkich otwartych okien incognito. Zmiany w zakładkach i ogólnych ustawieniach Google Chrome wprowadzone w trybie incognito są zawsze zapisywane.



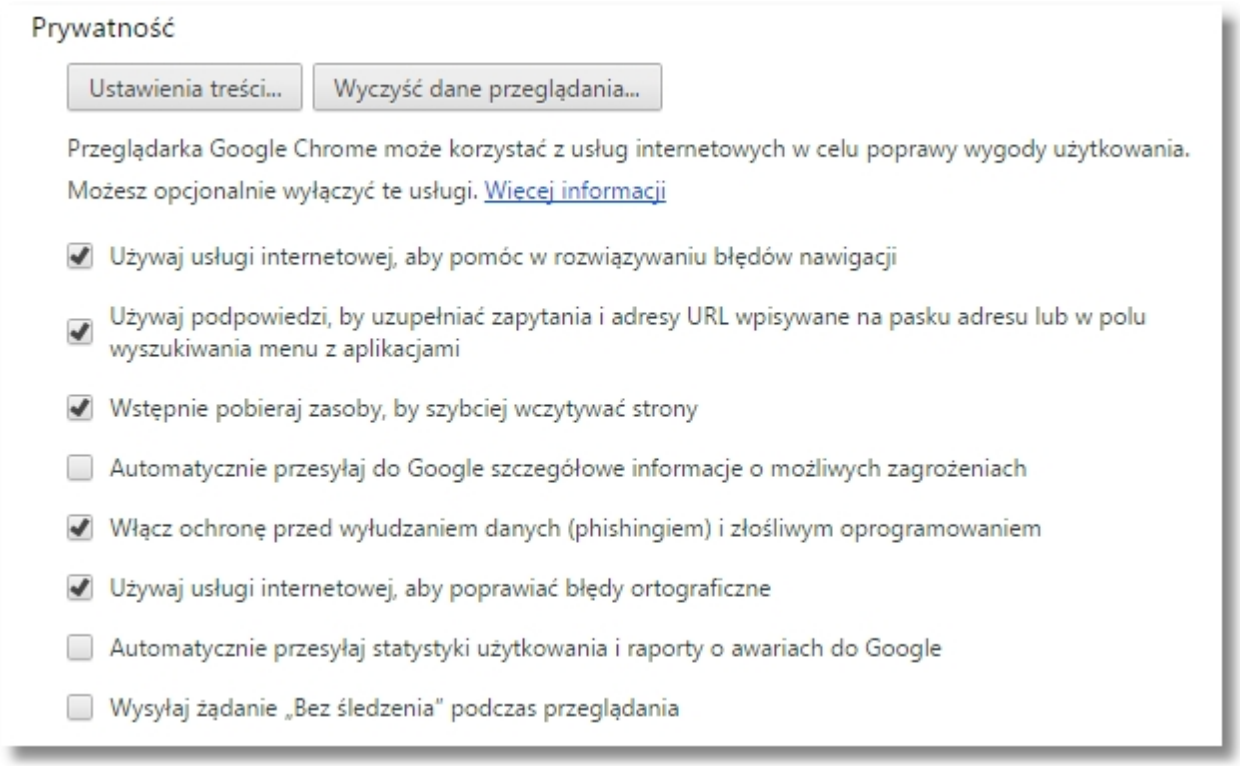
Aby poprawnie skonfigurować przeglądarkę Google Chrome należy w pierwszym kroku kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać menu **Ustawienia**.



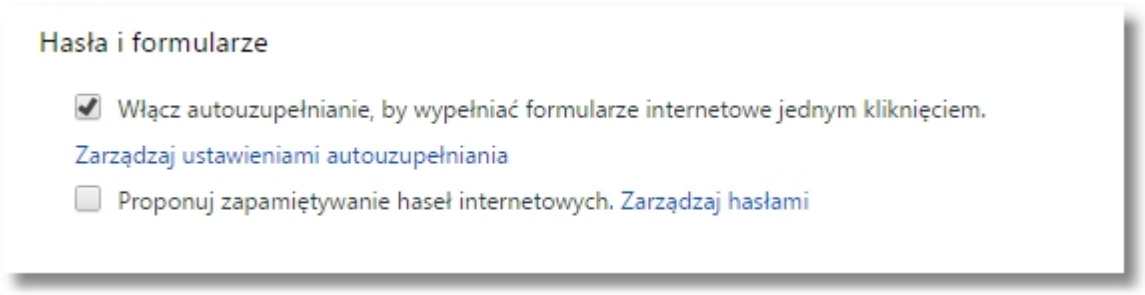
- z menu **Ustawienia** wybrać odnośnik Pokaż ustawienia zaawansowane...



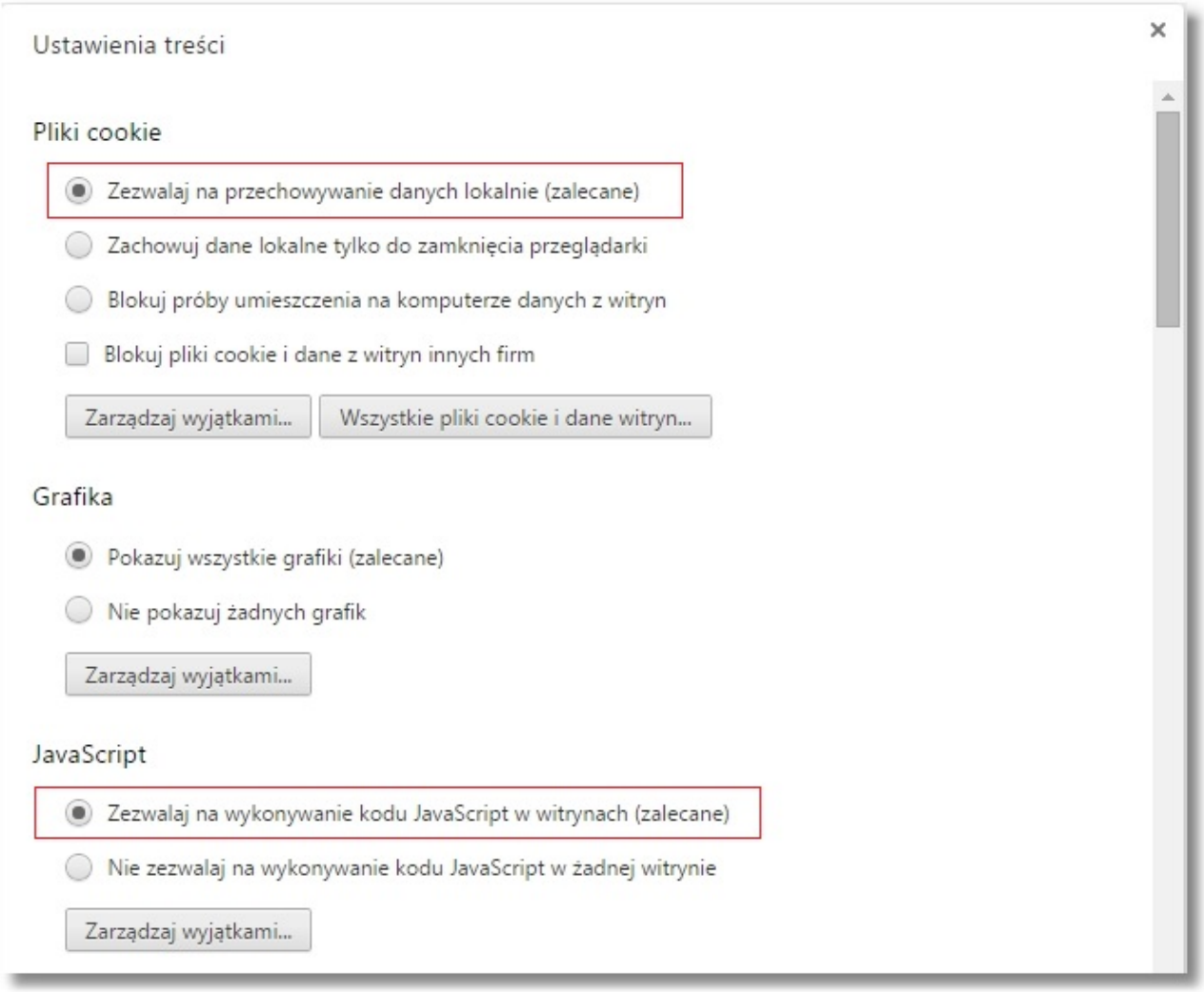
- w sekcji **Prywatność** zaznaczyć pole **Włącz ochronę przed wyłudzaniem danych (phishingiem) i złośliwym oprogramowaniem**.



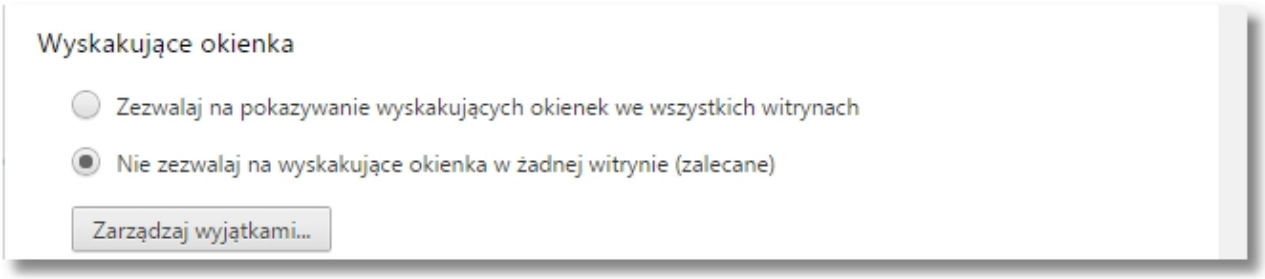
- w sekcji **Hasła i formularze** odznaczyć pole **Proponuj zapisywanie haseł podawanych w internecie**.



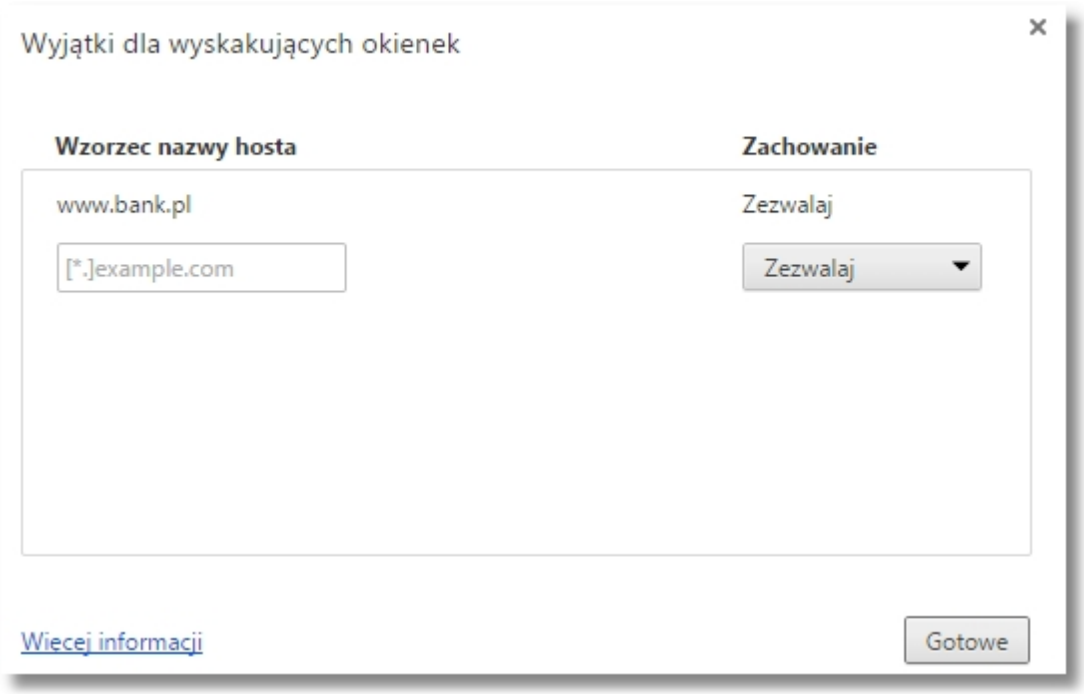
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści a następnie w sekcji **Pliki cookie** zweryfikować, czy zaznaczona jest opcja *Zezwalaj na przechowywanie danych lokalnie (zalecane)*, aby umożliwić dostęp plikom cookie własnej firmy i innych firm.
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści a następnie w sekcji **JavaScript** zaznaczyć pole **Zezwalaj na wykonywanie kodu JavaScript w witrynach (zalecane)**, aby włączyć obsługę JavaScript w przeglądarce.



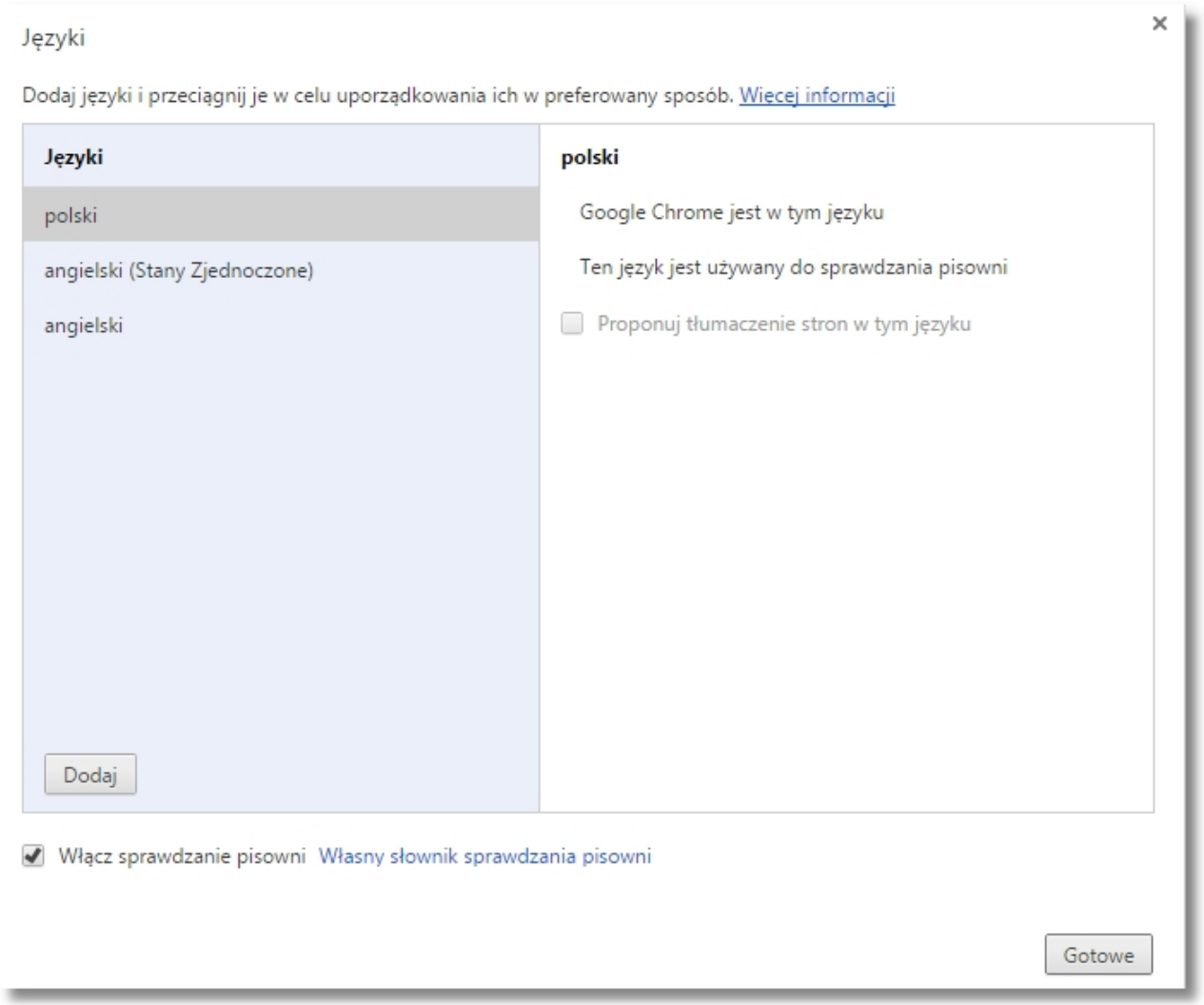
W sekcji **Prywatność** wybrać odnośnik Ustawienia treści a następnie w sekcji **Wyskakujące okienka** należy zaznaczyć pole **Nie zezwalaj na wyskakujące okienka w żadnej witrynie (zalecane)**.



Z uwagi na fakt, że w aplikacjach występują wyskakujące okienka istnieje konieczność zezwolenia na wyskakujące okienka dla Aplikacji. W tym celu należy w sekcji **Wyskakujące okienka** wybrać odnośnik Zarządzaj wyjątkami, a następnie w sekcji **Wzorzec nazwy hosta wpisać** adres strony banku internetowego i zaakceptować wprowadzone dane przyciskiem [Gotowe].

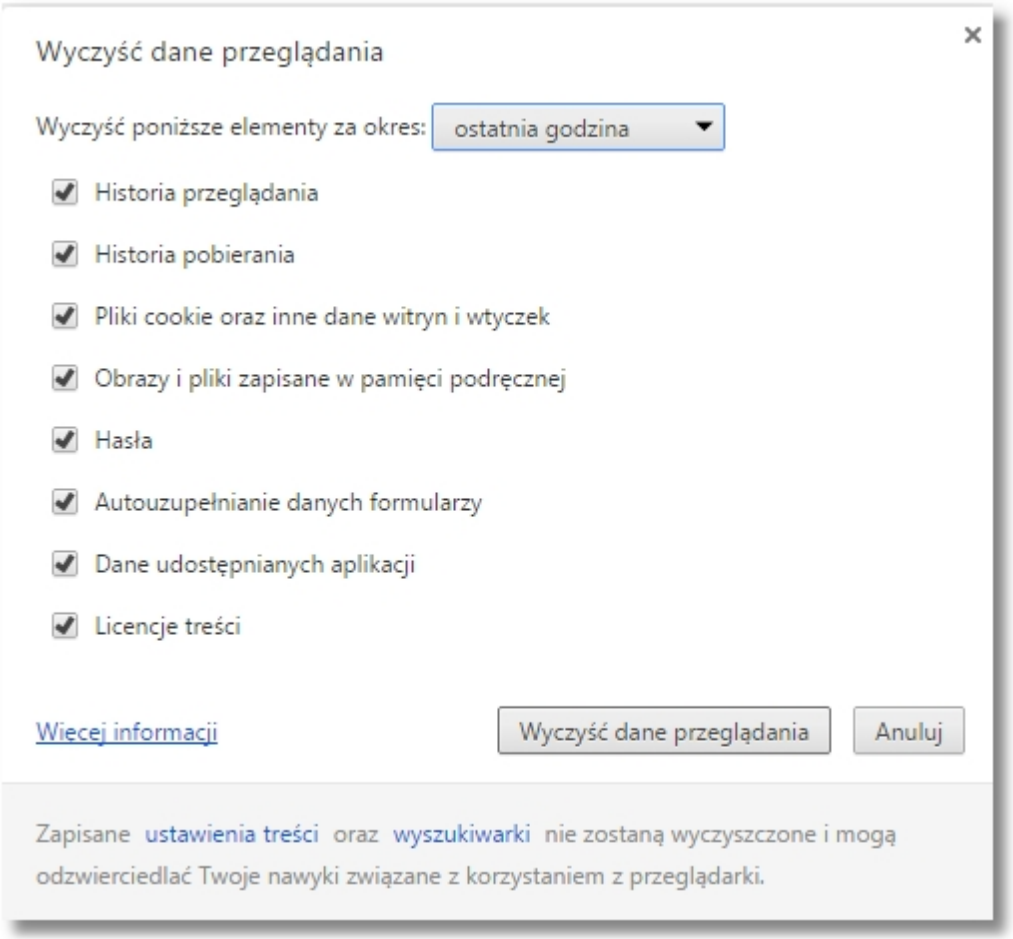


- w zakładce *Ustawienia* w sekcji **Języki** kliknąć na odnośnik Ustawienia języków i sprawdzania pisowni oraz wybrać z listy polski i dodać go do listy języków za pomocą przycisku [Dodaj] oraz zatwierdzić przyciskiem [Gotowe]. Pozycja będzie prezentowana jako pierwszy element na liście.



Po zdefiniowaniu powyższych ustawień należy wybrać przycisk [Gotowe].

W celu wyczyszczenia pamięci podręcznej przeglądarki należy kliknąć ikonkę  na pasku narzędzi przeglądarki oraz wybrać pozycję *Więcej narzędzi -> Wyczyść dane przeglądania*.
Na poniższym formularzu zaznaczyć wszystkie pozycje oraz wybrać przycisk [Wyczyść dane przeglądania].



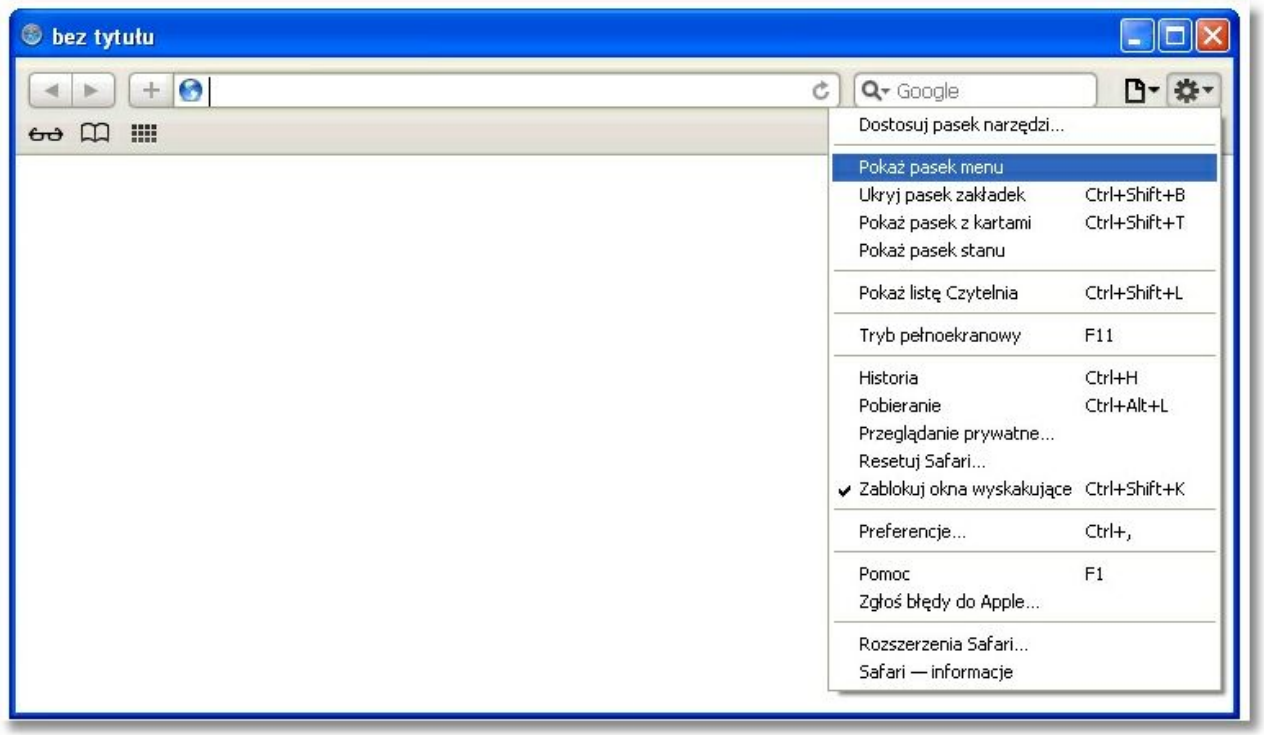
Włączanie obsługi NPAPI w przeglądarce Chrome w wersji 42 lub nowszej

W celu korzystania z wtyczek opartych na NPAPI w przeglądarce Chrome w werji 42 lub wyższej należy wykonać dodatkowy krok konfiguracyjny:
Na pasku adresów URL wpisać:
chrome://flags/#enable-npapi
Kliknąć na łączu Włącz dla opcji konfiguracyjnej Włącz NPAPI.
Nacisnąć przycisk [Uruchom ponownie teraz], który pojawił się na dole strony konfiguracyjnej.

Rozdział 16. Konfiguracja przeglądarki Safari 5.1.7

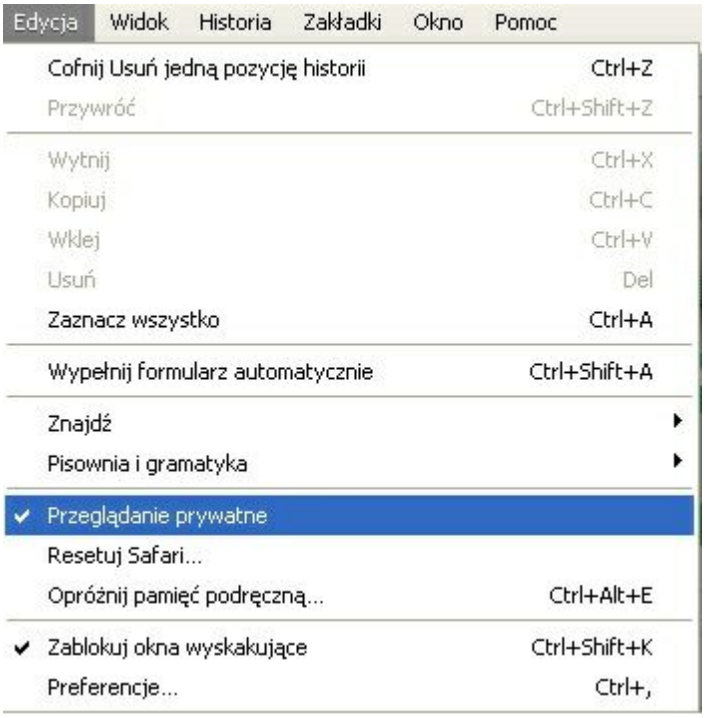
Konfiguracja przedstawiona w niniejszym rozdziale odnosi się do konfiguracji domyślnej przeglądarki. W przypadku, gdy konfiguracja jakiejś opcji nie jest tu opisana przyjmujemy, że nie została ona zmieniana. Przeglądarka Safari w wersji 5.1.7 wspiera następujące systemy operacyjne: Windows, MacOSX oraz Linux.

Przeglądarka Safari zawiera udogodnienia podnoszące bezpieczeństwo pracy ze stronami internetowymi zawierającymi dane wymagające szczególnej ochrony – takimi jak Serwis Bankowości Internetowej. Poprzez udostępnienie funkcji przeglądania prywatnego przeglądarka pozwala chronić informacje osobiste. Jeśli użytkownik musi skorzystać z komputera, który nie jest pod jego wyłączną kontrolą (na przykład współdzielony komputer w miejscu pracy lub publiczny komputer w kafejce internetowej itp.) zalecana jest praca w trybie prywatnym. Kiedy funkcja **Przeglądanie prywatne** zostanie włączona, przeglądarka Safari nie będzie pamiętać odwiedzanych stron, historii wyszukiwania i informacji funkcji automatycznego wypełniania.
Domyślnie przeglądarka Safari nie pokazuje paska menu. W celu wyświetlenia paska menu należy kliknąć ikonkę  oraz zaznaczyć pozycję **Pokaż pasek menu**.



Od tego momentu pasek menu będzie prezentowany przy każdym uruchomieniu przeglądarki.

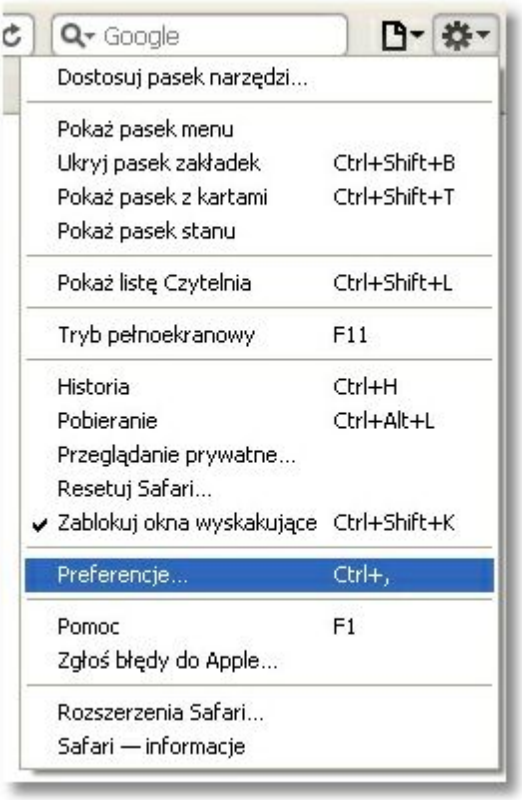
Przed rozpoczęciem pracy z Serwisem Bankowości Internetowej należy wybrać zakładkę *Edycja*, a następnie pozycję *Przeglądanie prywatne.*



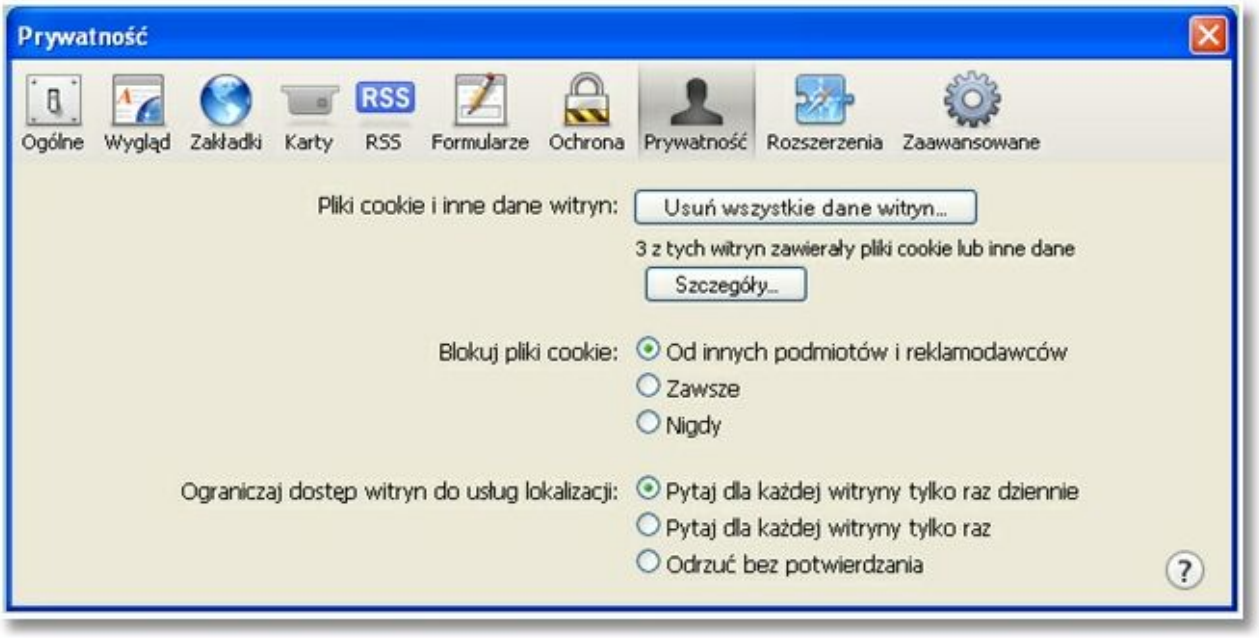
Otworzy się nowe okno, na którym należy potwierdzić włączenie przeglądania w trybie prywatnym poprzez wybór przycisku [OK].

Aby poprawnie skonfigurować przeglądarkę Safari należy wykonać następujące czynności:

- W celu wyczyszczenia historii przeglądania należy kliknąć ikonkę  oraz wybrać pozycję *Preferencje*.

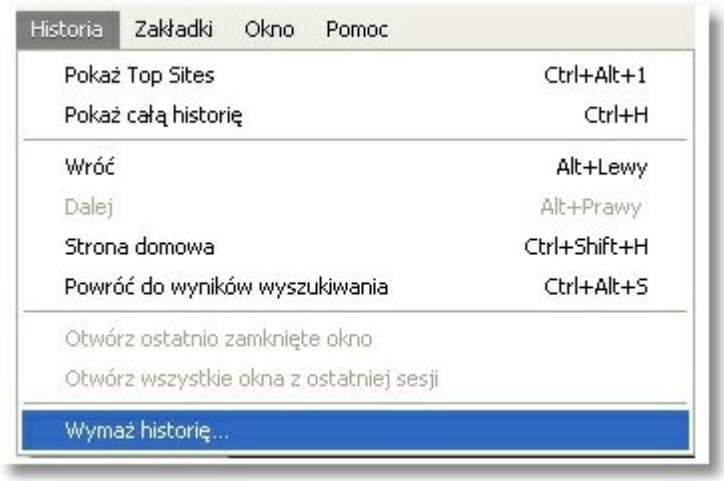


Następnie na zakładce *Prywatność* wybrać przycisk [Usuń wszystkie dane witryn ...].



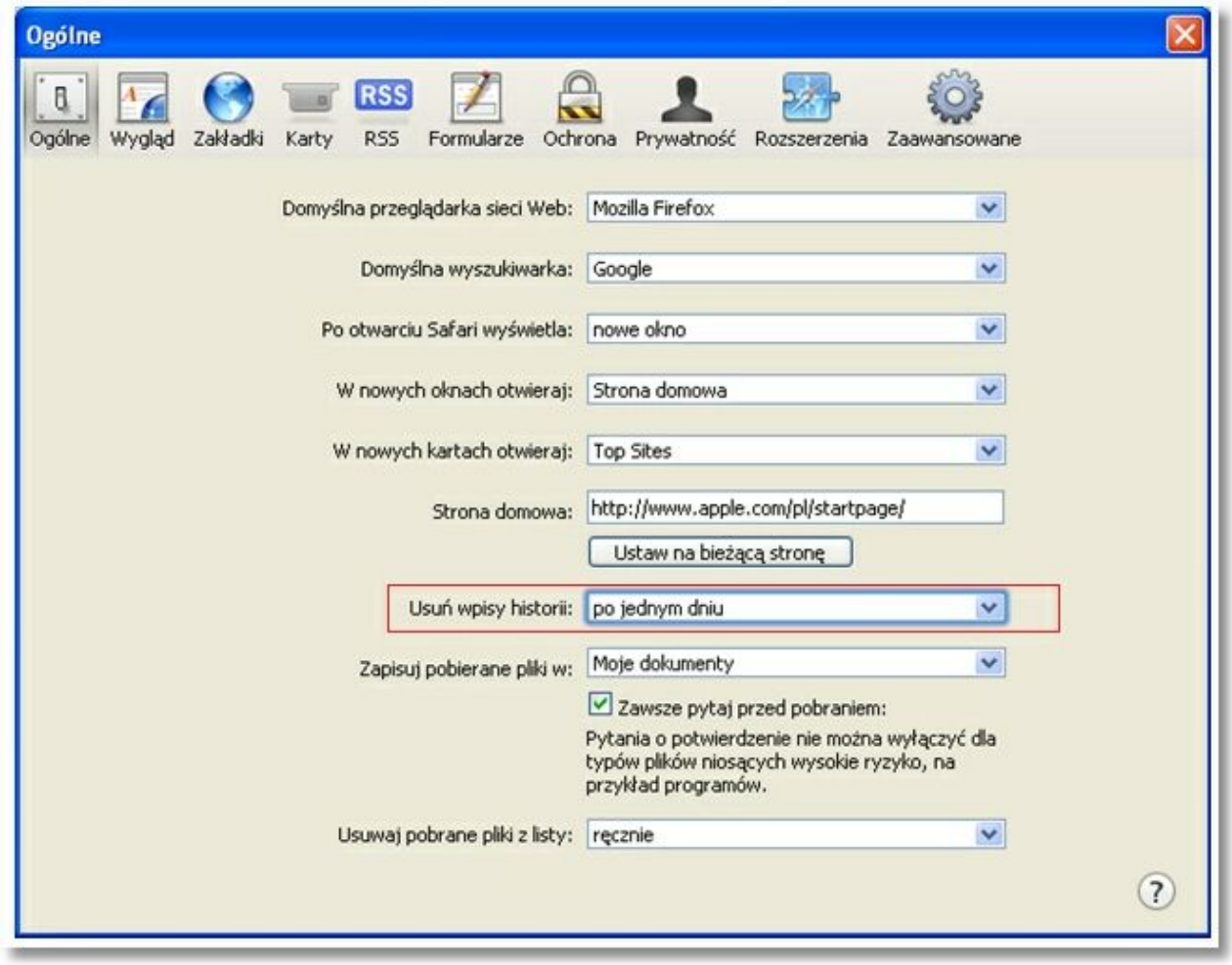
W celu potwierdzenia usunięcia danych zachowanych przez strony www na komputerze należy wybrać przycisk [Usuń teraz].

Czyszczenie historii przeglądania możliwe jest również po wyborze pozycji *Wymaż historię ...* dostępnej w menu *Historia.*

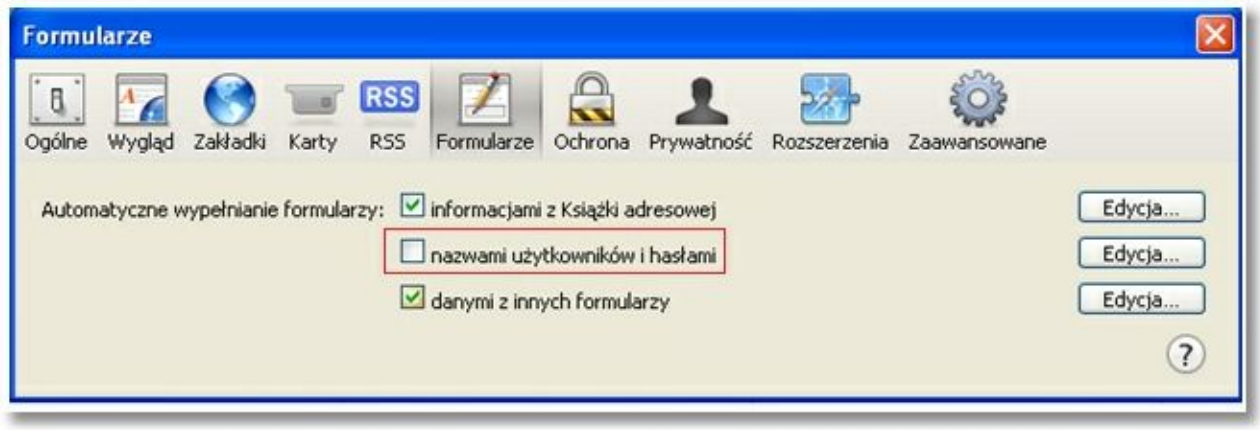


W celu potwierdzenia usunięcia historii przeglądania danych należy wybrać przycisk [Wymaż].

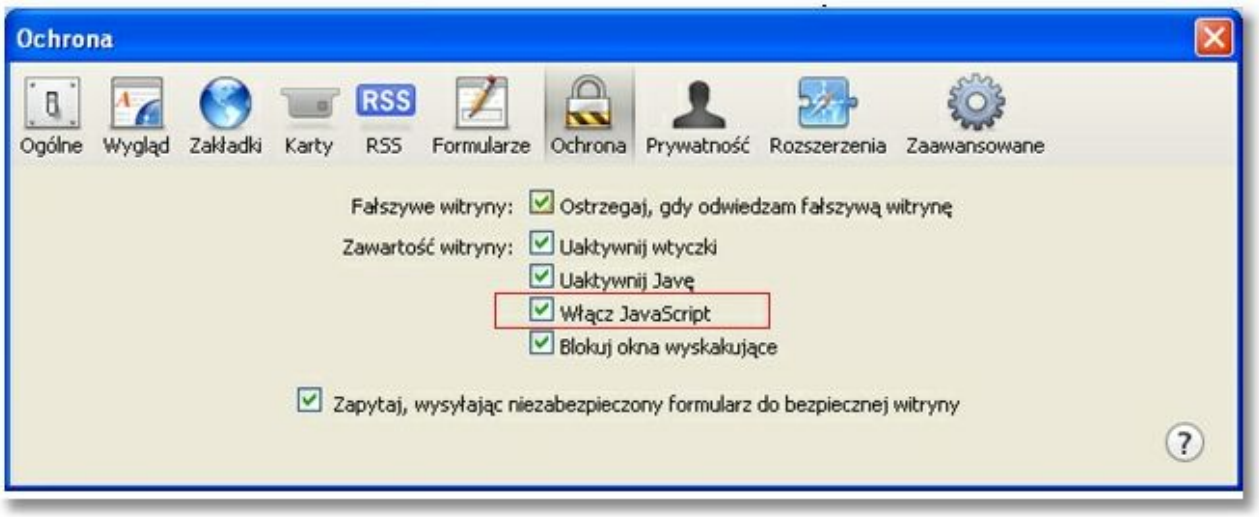
W celu ustawienia czyszczenia historii "po jednym dniu" należy w zakładce *Ogólne* dla pola **Usuń wpisy w historii** ustawić wartość *po jednym dniu*.



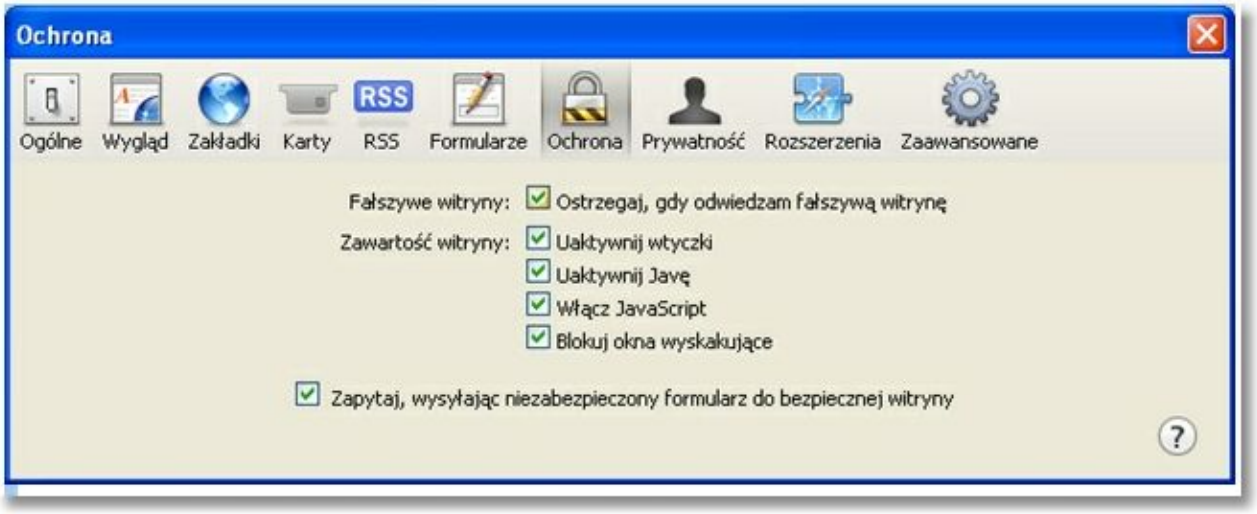
- W celu wyłączenia zapamiętywania haseł należy na zakładce *Formularze* odznaczyć pozycję *nazwami użytkowników i hasłami*.



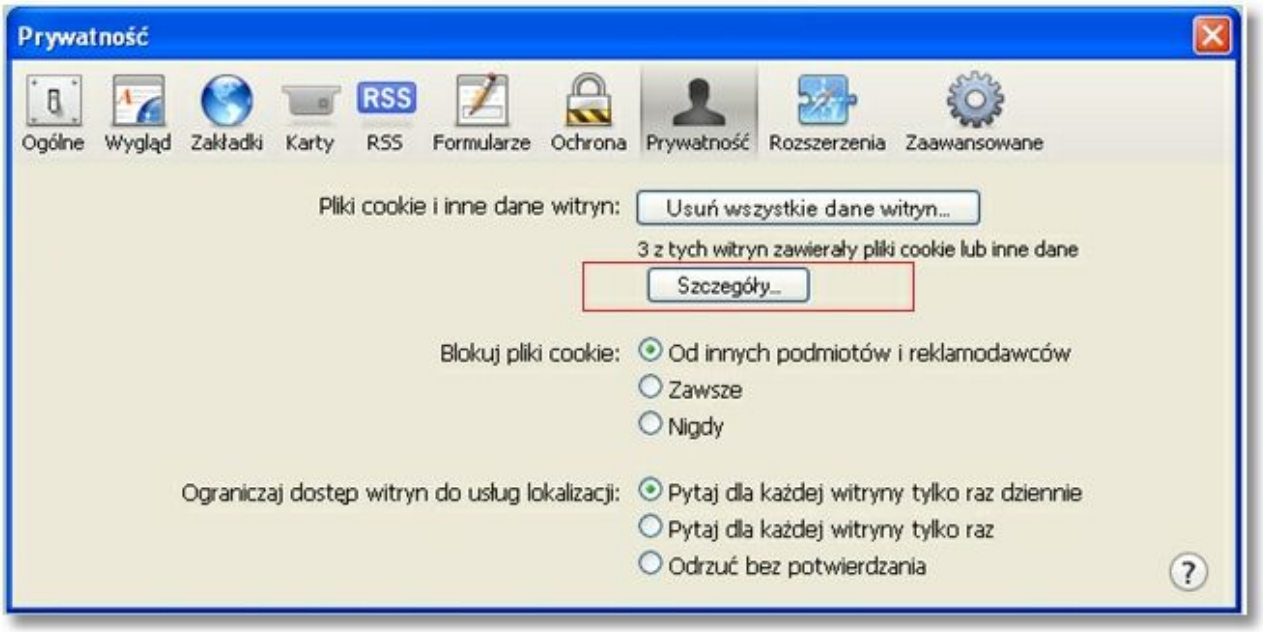
- W celu aktywacji Java Script należy w zakładce *Ochrona* zaznaczyć pole **Włącz JavaScript**.

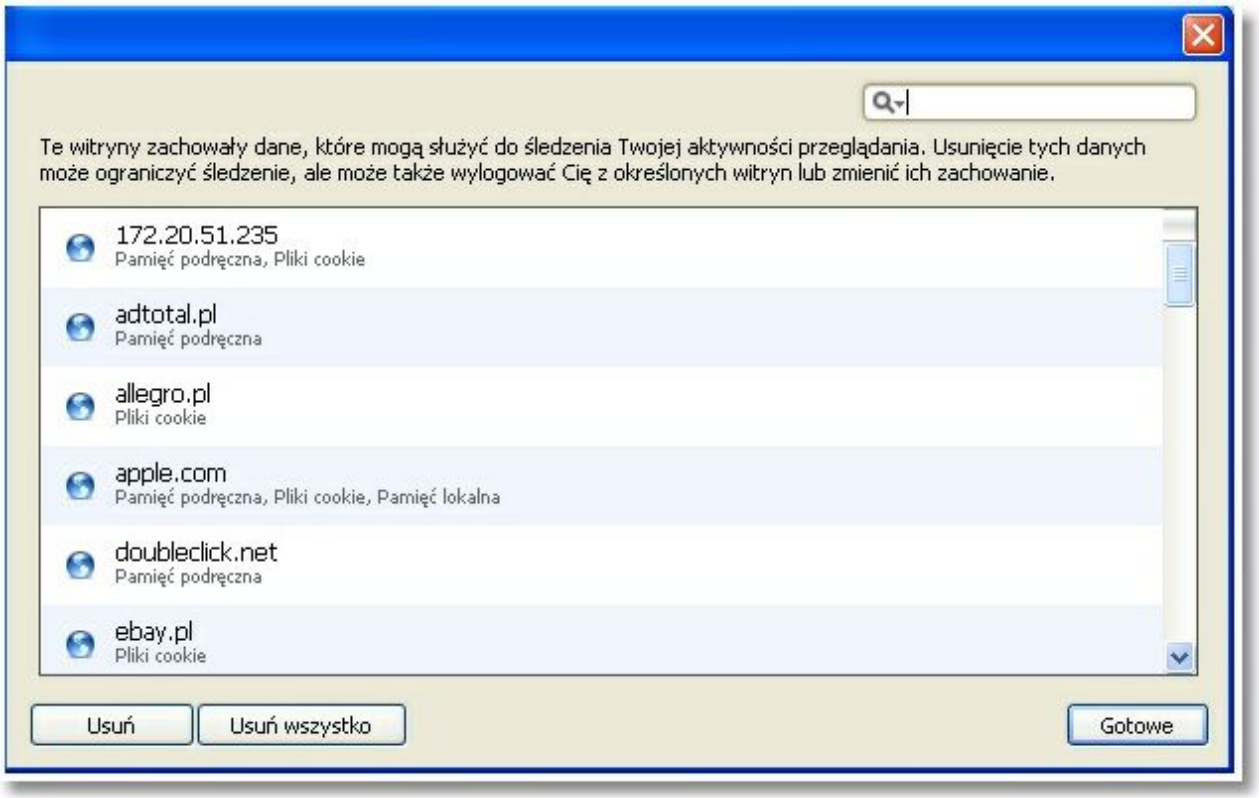


- W zakładce *Ochrona* należy zaznaczyć pole **Blokuj okna wyskakujące**.



- W celu wyczyszczenia ciasteczek po zakończeniu pracy należy w zakładce *Prywatność* wybrać przycisk [Szczegóły], a następnie nacisnąć przycisk [Usuń wszystko].


Prywatność
Ogólne
Wygląd
Zakładki
Karty
RSS
Formularze
Ochrona
Prywatność
Rozszerzenia
Zaawansowane
Pliki cookie i inne dane witryn:
Usuń wszystkie dane witryn...
3 z tych witryn zawierały pliki cookie lub inne dane
Szczegóły...
Blokuj pliki cookie:
Od innych podmiotów i reklamodawców
Zawsze
Nigdy
Ograniczaj dostęp witryn do usług lokalizacji:
Pytaj dla każdej witryny tylko raz dziennie
Pytaj dla każdej witryny tylko raz
Odrzuć bez potwierdzania


Te witryny zachowały dane, które mogą służyć do śledzenia Twojej aktywności przeglądania. Usunięcie tych danych może ograniczyć śledzenie, ale może także wylogować Cię z określonych witryn lub zmienić ich zachowanie.
172.20.51.235
Pamięć podręczna, Pliki cookie
adtotal.pl
Pamięć podręczna
allegro.pl
Pliki cookie
apple.com
Pamięć podręczna, Pliki cookie, Pamięć lokalna
doubleclick.net
Pamięć podręczna
ebay.pl
Pliki cookie
Usuń
Usuń wszystko
Gotowe

Rozdział 17. Konfiguracja przeglądarki Safari 6.0 dedykowanej na urządzenia mobilne

Przeglądarka Safari w wersji 6.0 dedykowana jest wyłącznie pod system OS X Lion (i jest zintegrowana z OS X Mountain Lion).

Ustawienia sieci WWW w przeglądarce Safari na urządzeniu mobilnym

Pewne typy zawartości stron WWW (filmy, animacje i aplikacje internetowe) są domyślnie wyświetlane przez przeglądarkę Safari. Niektóre z tych funkcji można wyłączyć w celu ochrony prywatności oraz zabezpieczenia urządzenia przed potencjalnymi zagrożeniami występującymi w Internecie.

Aby zmienić ustawienia zabezpieczeń należy wybrać kolejno opcje *Ustawienia -> Safari*. Więcej informacji na temat przeglądarki Safari w systemie iOS zawiera podręcznik użytkownika.

Włączanie ochrony przed phishingiem

Aby włączyć ochronę przed phishingiem należy wybrać kolejno *Ustawienia -> Safari* a następnie włączyć opcję *Alerty o fałszywych witrynach*. Jeśli w ustawieniach przeglądarki Safari zostanie włączona funkcja ochrony przed phishingiem, w razie odwiedzenia witryny podejrzanej o wyłudzanie informacji na ekranie pojawi się ostrzeżenie. Aby wyłączyć tę funkcję należy ponownie wybrać opcję *Alerty o fałszywych witrynach*.

Phishing to próba wyłudzenia osobistych danych, takich jak hasło, informacje o koncie czy nazwa użytkownika. Fałszywa witryna może się podszyć pod prawdziwą, na przykład pod witrynę banku, instytucji finansowej lub dostawcy usług poczty e-mail.

Blokowanie plików cookie

Aby zdecydować, czy przeglądarka Safari ma blokować pliki cookie w systemie iOS 8 należy kolejno wybrać opcje *Ustawienia > Safari > Blokuj cookie* a następnie opcję *Zawsze pozwalaj*, *Z odwiedzonych wi*tryn, *Tylko z bieżącej witryny* lub *Zawsze blokuj*. W systemie iOS 7 lub starszym należy wybrać opcję *Nigdy*, *Od innych podmiotów i reklamodawców* lub *Zawsze*.

Zezwalanie na wykonywanie skryptów JavaScript

Cookie to mały plik z danymi umieszczany na urządzeniu przez witrynę internetową. Pozwala on witrynie rozpoznać użytkownika przy kolejnej wizycie i dostosować się do jego preferencji na podstawie podanych przez niego informacji. Niektóre strony mogą nie działać, dopóki nie zostaną zaakceptowane pliki cookie.

Aby zmienić ustawienia należy wybrać kolejno opcje *Ustawienia -> Safari -> Zaawansowane* i włączyć opcję *JavaScript*.

Wymazywanie informacji z urządzenia

Aby wymazać historię i pliki cookie z przeglądarki Safari w systemie iOS 8 należy wybrać kolejno opcje *Ustawienia -> Safari -> Wymaż historię i dane witryn*. W systemie iOS 7 lub starszym należy wybrać opcję *Wymaż historię* oraz *Wymaż pliki cookie i dane*.

Aby wymazać pozostałe informacje przechowywane przez przeglądarkę Safari należy wybrać kolejno opcję *Ustawienia -> Safari -> Zaawansowane -> Dane witryn -> Usuń wszystkie dane witryn*.

Włączanie i wyłączanie przeglądania prywatnego na urządzeniu mobilnym

Aby wyłączyć zapamiętywanie odwiedzanych witryn w historii należy włączyć przeglądanie prywatne.
Korzystając z przeglądania prywatnego można odwiedzać witryny bez zachowywania ich w historii.
Tryb przeglądania prywatnego chroni informacje prywatne oraz uniemożliwia niektórym witrynom internetowym śledzenie zachowania użytkownika. Przeglądarka Safari nie będzie zapamiętywała odwiedzanych stron, historii wyszukiwania ani informacji wpisywanych w formularzach.

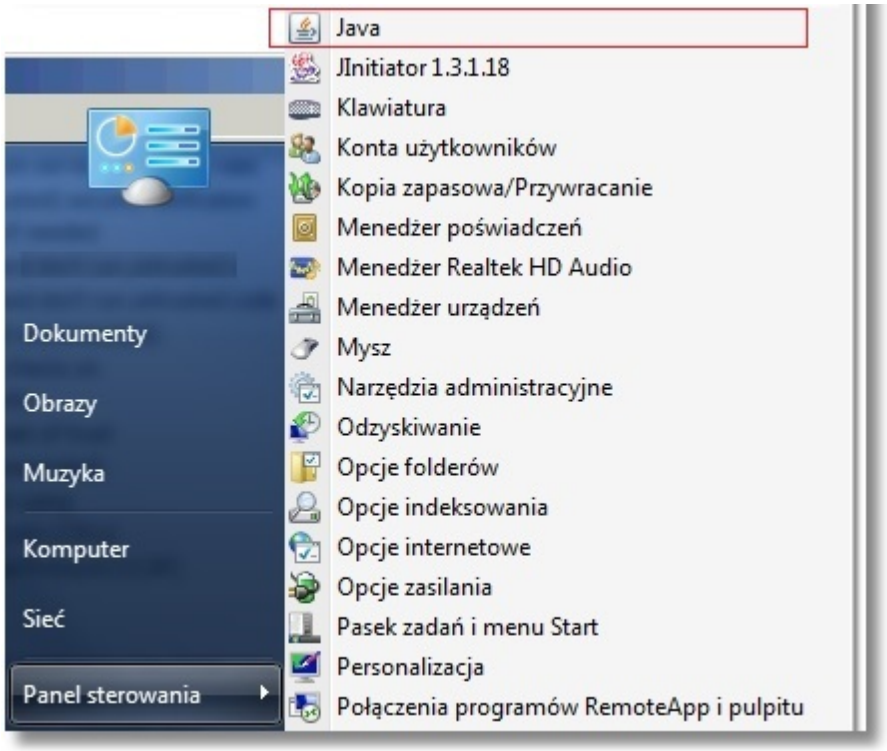
W celu włączenia przeglądania prywatnego na urządzeniu mobilnym należy wybrać w przeglądarce Safari ikonę Strony, następnie opcję *Prywatne.* Przy włączonej funkcji przeglądania prywatnego schemat kolorów przeglądarki Safari zmienia się z białego lub szarego na czarny lub ciemny.

W przypadku używania systemu iOS 7 lub starszego na iPadzie należy otworzyć przeglądarkę Safari stuknąć w ikonę **Plus** w celu otwarcia nowej karty a następnie stuknąć w opcję *Prywatne*.
W celu wyłączenia trybu przeglądania prywatnego należy na telefonie iPhone, iPadzie lub iPodzie touch otworzyć przeglądarkę Safari, wybrać ikonę **Strony** a następnie wybrać w opcję *Prywatne.*

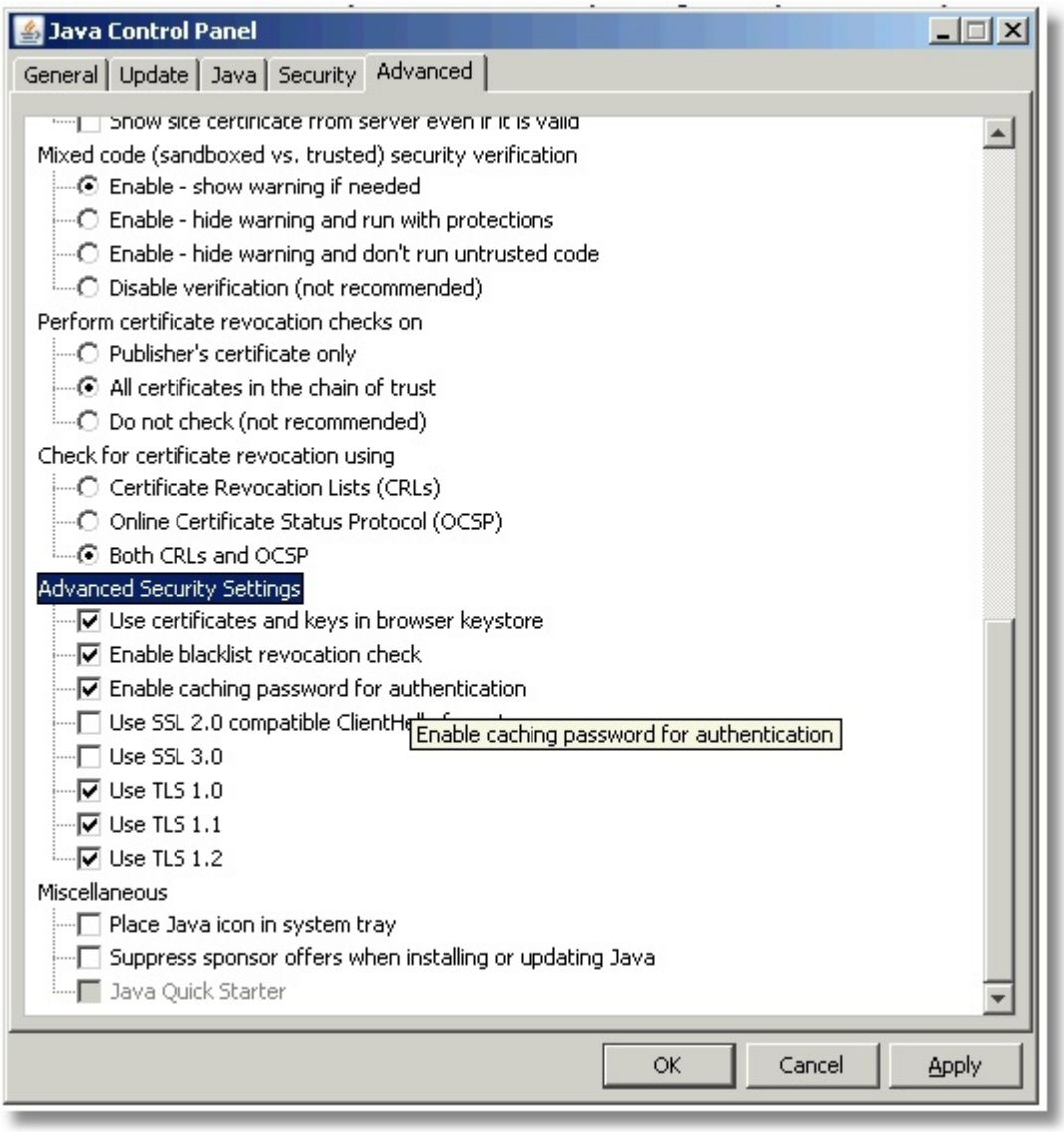
W przypadku systemu iOS 7 lub starszego na iPadzie należy wybrać ikonę **Plus** w celu otwarcia nowej karty a następnie wybrać opcję *Prywatne*.

Rozdział 18. Dodatkowa konfiguracja Javy w wersji 1.7.0

Z menu podręcznego dostępnego pod przyciskiem [Start] należy wybrać opcję *Panel sterowania -> Java* (dla widoku ikon).



Na formatce *Java Control Panel* wybrać zakładkę *Advanced* a następnie w sekcji **Advanced Security Settings** należy zaznaczyć opcję *Use TLS 1.0*, *Use TLS 1.1* oraz *Use TLS 1.2*. Zaleca się wyłączenie opcji *Użyj SSL 3.0.* Zmiany na formatce należy zatwierdzić poprzez przycisk [Apply].


Java Control Panel
General
Update
Java
Security
Advanced
Show site certificate from server even if it is valid
Mixed code (sandboxed vs. trusted) security verification
Enable - show warning if needed
Enable - hide warning and run with protections
Enable - hide warning and don't run untrusted code
Disable verification (not recommended)
Perform certificate revocation checks on
Publisher's certificate only
All certificates in the chain of trust
Do not check (not recommended)
Check for certificate revocation using
Certificate Revocation Lists (CRLs)
Online Certificate Status Protocol (OCSP)
Both CRLs and OCSP
Advanced Security Settings
Use certificates and keys in browser keystore
Enable blacklist revocation check
Enable caching password for authentication
Use SSL 2.0 compatible ClientHe
Enable caching password for authentication
Use SSL 3.0
Use TLS 1.0
Use TLS 1.1
Use TLS 1.2
Miscellaneous
Place Java icon in system tray
Suppress sponsor offers when installing or updating Java
Java Quick Starter
OK
Cancel
Apply

Asseco Poland SA
ul. Olchowa 14
35-322 Rzeszów
tel.: +48 17 888 55 55
fax: +48 17 888 55 50
info@asseco.pl
www.asseco.pl

Autor: Zespół Dokumentowania/ Pion Banków Komercyjnych

Data wydania dokumentu: 2015-05-18

Identyfikator dokumentu: DOC.UZT_def3000_CEB_def2500_REB_Konfiguracja_Przegladarek_Internetowych