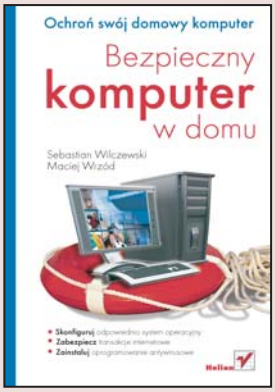
Bezpieczny komputer w domu

Autorzy: Sebastian Wilczewski, Maciej Wrzód
ISBN: 83-246-0681-5
Format: B5, stron: 328



Wszyscy użytkownicy internetu słyszeli już o zagrożeniach czyhających na ich komputery – ataki hakerskie, kradzież danych, przejmowanie numerów kart płatniczych, wirusy, programy szpiegujące, spam... Większość z nas podchodzi do tego z przymrużeniem oka, zakładając, że nas to nie spotka. Tymczasem ofiarą ataku z sieci może paść każdy, często nawet o tym nie wiedząc. Na szczęście na rynku dostępne są narzędzia, których zastosowanie, w połączeniu z odpowiednimi procedurami, może uchronić nas przed niebezpieczeństwami wynikającymi z korzystania z sieci.

„Bezpieczny komputer w domu" to przewodnik dla wszystkich tych, którzy chcą zapewnić sobie komfort psychiczny przy korzystaniu z domowego komputera. Książka ta opisuje zarówno narzędzia, jak i czynności, jakie należy podjąć, by zabezpieczyć komputer przed atakami z sieci. Czytając ją, nauczysz się odpowiednio konfigurować system operacyjny, instalować zaporę sieciową i oprogramowanie antywirusowe oraz korzystać z bezpiecznych transakcji finansowych w sieci. Dowiesz się, czym są programy szpiegujące i jak się przed nimi bronić. Poznasz metody podnoszenia poziomu bezpieczeństwa przeglądarki internetowej i klienta poczty elektronicznej. Przeczytasz także o wykonywaniu kopii danych i przywracaniu systemu po awarii.

- Rodzaje zagrożeń wynikających z korzystania z sieci
- Konfiguracja systemu operacyjnego
- Ochrona dzieci przed niepożądanymi treściami
- Transakcje w internecie
- Usuwanie luk w programach i systemie operacyjnym
- Zabezpieczanie przeglądarki Internet Explorer
- Ochrona przed spamem
- Programy antywirusowe
- Instalacja i konfiguracja zapory sieciowej
- Kopie zapasowe danych

Przekonaj się, że korzystanie z komputera nie musi być źródłem stresu

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

Rozdział 8.

Internet Explorer — bezpieczne surfowanie po internecie

Ten rozdział ma na celu przedstawienie informacji o tym, jak należy korzystać z aplikacji Internet Explorer tak, aby uniknąć niebezpieczeństw, jakie mogą wiązać się z odwiedzaniem różnych stron internetowych. Poznasz również rodzaje tych zagrożeń:

Z tego rozdziału dowiesz się:

- na co zwracać uwagę, odwiedzając strony internetowe,
- po czym poznać strony, które mogą być niebezpieczne,
- czy powinno się zapisywać hasła do stron internetowych w przeglądarce,
- co to są formanty ActiveX i do czego mogą być wykorzystywane,
- jak instalować, aktualizować, wyłączać, usuwać formanty ActiveX i przeglądać informacje o nich,
- czy ciasteczka mogą być dobre,
- jak blokować pobieranie niechcianych plików,
- jak blokować wyskakujące okienka,
- jak chronić swoją prywatność w internecie,
- do czego służą strefy internetowe w aplikacji Internet Explorer,
- jak chronić anonimowość w internecie,
- jak usuwać informacje o swojej aktywności w internecie.

Na co zwracać uwagę, odwiedzając strony internetowe. Które strony nie są bezpieczne

Stronę internetową może założyć praktycznie każdy, kto ma dostęp do internetu. Dodatkowo zawartość strony może być zapisana na serwerze znajdującym się w dowolnym zakątku świata. Przykładowo obywatel Polski może założyć swój serwis internetowy na serwerze w Chinach, a jego treść będzie dostępna dla ludzi z całego świata. To powoduje, że tak naprawdę możemy nie wiedzieć, kto jest właścicielem danego serwisu i z jakiego kraju pochodzi. W internecie nie istnieją granice takie jak w świecie rzeczywistym. Ma to zarówno dobre, jak i złe strony. Dobra strona to możliwość wymiany informacji z całym światem, a zła to… możliwość wymiany informacji z całym światem. Wyobraź sobie, że chcesz przeczytać elektroniczne wydanie lokalnej gazety wydawanej w Nowym Jorku. Możesz to spokojnie zrobić, siadając przed komputerem z dostępem do internetu, znajdującym się w Polsce. Jednocześnie, jeżeli ktoś wpadnie na pomysł stworzenia strony pornograficznej albo pedofilskiej i opublikowania jej na serwerze znajdującym się na egzotycznej wyspie, na której tego typu treści nie są uznawane za nielegalne lub są nielegalne, ale nie są skutecznie ścigane, to serwis ten będzie dostępny dla dowolnej osoby na świecie. Możesz łatwo wysłać rodzinne zdjęcie do znajomych z Stanach Zjednoczonych, ale jednocześnie ktoś ze Stanów Zjednoczonych może próbować wysłać na Twój komputer złośliwe oprogramowanie.

Ściganie przestępstw internetowych może być utrudnione, jeżeli zostały popełnione z użyciem komputerów zlokalizowanych w krajach, które niechętnie współpracują z innymi krajami. Należy mieć to na uwadze, odwiedzając nieznane serwisy internetowe.

Jakich serwisów należy unikać:

- serwisów polskojęzycznych (np. sklepy internetowe), jeśli serwery, na których są umieszczone, znajdują się w innych krajach niż Polska (w rozdziale „Zagadnienia ogólne” zostało opisane, jak określić, gdzie znajduje się komputer);
- serwisów wymagających zainstalowania nietypowego, nieznanego, powszechnie nieużywanego oprogramowania, które ma być rzekomo potrzebne do oglądania treści serwisu (takie oprogramowanie może być wirusem lub złośliwym narzędziem szpiegującym);
- serwisów, które wymagają podania wielu szczegółowych danych osobowych, rzekomo niezbędnych do korzystania z serwisu;
- serwisów, których adres dostałeś od osób nieznajomych;
- serwisów, których nie zna nikt ze znajomych;
- serwisów łudząco podobnych do znanych serwisów aukcyjnych (które jednak nimi nie są);

- serwisów, w których nie został podany adres pocztowy właściciela serwisu (z drugiej strony podany adres może być fałszywy);
- serwisów, które jako kontakt tradycyjny podają skrzynkę pocztową;
- serwisów, które już widziałeś i które występują teraz pod innym adresem, i wiesz, że ten adres często się zmienia;
- serwisów, które nie odpowiadają na pytania wysłane e-mailem (lub gdy takie pytania mimo wielokrotnych prób wysłania nie docierają do nadawcy);
- serwisów, które oferują nielegalną treść lub treść, co do której legalności można mieć poważne wątpliwości;
- serwisów, które oferują atrakcyjne rzeczy za darmo lub w niewiarygodnie niskich cenach;
- serwisów z treścią erotyczną;
- serwisów, które notorycznie wyświetlają niezrozumiałe komunikaty i ostrzeżenia;
- serwisów, które wymagają podania hasła w sposób niezaszyfrowany.

W przypadku takich serwisów istnieje uzasadnione podejrzenie, że mogą być niebezpieczne dla komputera.

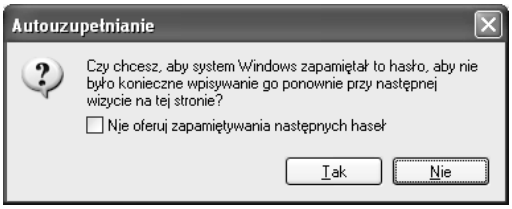
Zapisywanie haseł do stron internetowych. Jakie wiążą się z tym niebezpieczeństwa

Korzystając z komputera i internetu, zapewne korzystasz z wielu serwisów internetowych. Część z nich wymaga założenia konta, aby móc uzyskać dostęp do wybranych treści. Zakładasz kolejne konta i tworzysz kolejne hasła. Zapamiętanie tych haseł może być trudne. Internet Explorer pozwala na zapamiętywanie haseł do witryn internetowych. Znacznie ułatwia to poruszanie się po internecie. Należy jednak zdać sobie sprawę z tego, jakie pociąga to za sobą niebezpieczeństwa, gdyż każde zapisane hasło może być wykradzione przez inne osoby mające dostęp do danego komputera — bezpośredni bądź przez sieć.

Skonfigurowanie programu Internet Explorer tak, aby nie zapisywał haseł do stron internetowych

Rysunek 8.1 przedstawia okno dialogowe, które pokazuje się, kiedy użytkownik po raz pierwszy wpisuje hasło na wybranej stronie. Celem jest zapewnienie maksymalnego bezpieczeństwa. Jeżeli zobaczysz ten komunikat, zaznacz opcję *Nie oferuj zapamiętywania następnych haseł* i wybierz przycisk *Nie*.

Rysunek 8.1.
Autouzupełnianie

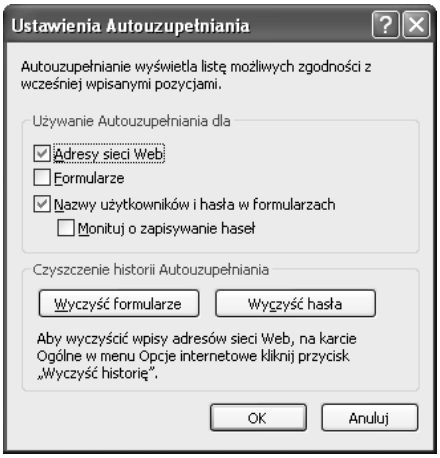


Usuwanie zapisanych haseł Internet Explorera

Aby usunąć zapisane na komputerze hasła do stron internetowych, należy:

1. Uruchomić program Internet Explorer.
2. Z menu *Narzędzia* wybrać polecenie *Opcje internetowe*.
3. Przejść do zakładki *Zawartość*.
4. Wybrać przycisk *Autouzupełnianie…*.
5. W oknie dialogowym *Ustawienia Autouzupełniania* (patrz rysunek 8.2) wybrać przycisk *Wyczyść hasła*.

Rysunek 8.2.
Ustawienia Autouzupełniania



6. Potwierdzić decyzję przyciskiem *OK*.
7. Zamknąć okno *Ustawienia Autouzupełniania* przyciskiem *OK*.
8. Zamknąć okno *Opcje internetowe* przyciskiem *OK*.

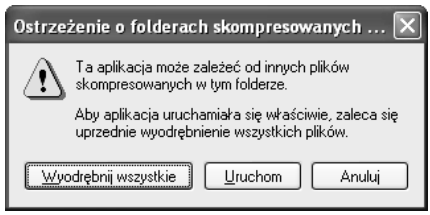
Nie zapisuj haseł do stron internetowych. Mogą zostać wykradzione przez inne osoby mające dostęp do danego komputera. Aby nie zapisywać haseł w oknie dialogowym *Ustawienia Autouzupełniania*, usuń zaznaczenie pola *Nazwy użytkowników i hasła w formularzach*.

Odzyskiwanie haseł do stron internetowych zapisywanych przez Internet Explorera

Hasła zapisane przez Internet Explorera można odzyskać za pomocą różnych aplikacji. Wiele z nich znajdziesz, wpisując w wyszukiwarce *Google* zapytanie `how to recover internet explorer password`. Jedną z takich aplikacji jest *Advanced Internet Explorer Password Recovery*, której wersję testową można pobrać ze strony *http://www.elcomsoft.com/aiepr.html*.

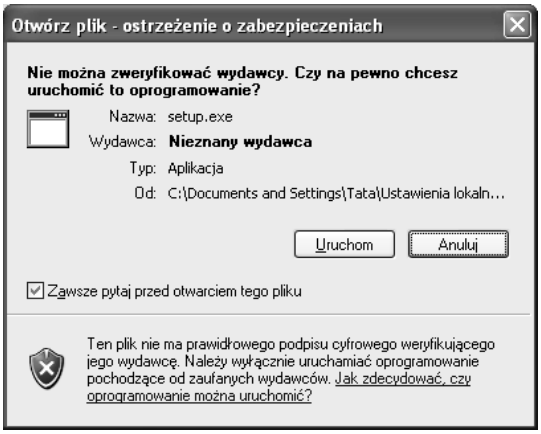
Aby zainstalować tę aplikację i skorzystać z niej, należy:

1. Uruchomić program Internet Explorer.
2. W polu *Adres* wpisać `http://www.elcomsoft.com/aiepr.html` i zatwierdzić wpis klawiszem *Enter*.
3. Kliknąć łącze *Download AIEPR 1.20 (April 5, 2004; 824K)*.
4. W oknie dialogowym *Pobieranie pliku* wybrać przycisk *Otwórz*.
5. Kliknąć dwukrotnie plik *Setup*.
6. W oknie dialogowym *Ostrzeżenie o folderach skompresowanych* (patrz rysunek 8.3) wybrać przycisk *Wyodrębnij wszystkie*.



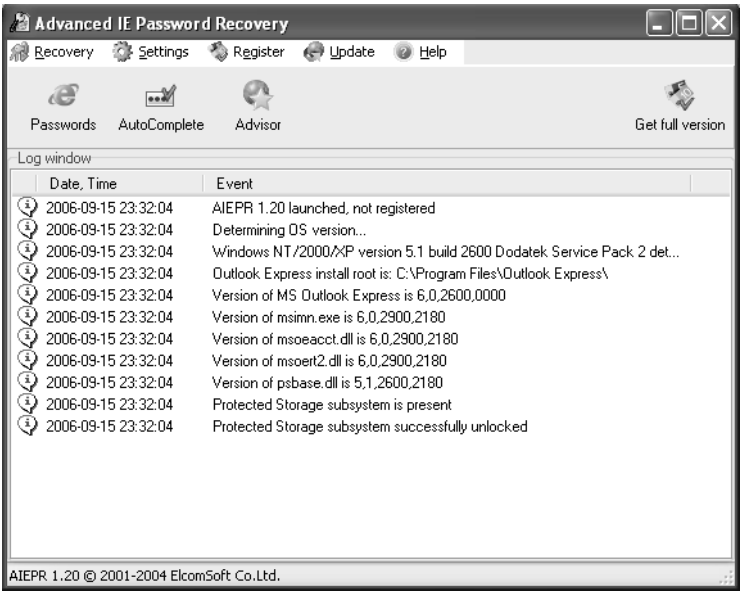
Rysunek 8.3. *Ostrzeżenie o folderach skompresowanych*

7. W oknie dialogowym *Kreator wyodrębniania* wybrać przycisk *Dalej*.
8. W następnym oknie ponownie wybrać *Dalej*.
9. Upewnić się, że w następnym oknie dialogowym zaznaczone jest pole *Pokaż wyodrębnione pliki*, i wybrać przycisk *Zakończ*.
10. Ponownie dwukrotnie kliknąć plik *Setup*.
11. Po pojawieniu się okna dialogowego przedstawionego na rysunku 8.4 wybrać przycisk *Uruchom*.
12. Na kilku następnych ekranach instalatora klikać przycisk *Next*.
13. Na ostatnim ekranie instalatora kliknąć przycisk *Finish*.
14. Z menu *Start* wybrać polecenie *Wszystkie programy*, a następnie pozycję *Advanced IE Password Recovery* oraz ponownie *Advanced IE Password Recovery*.



Rysunek 8.4. *Otwórz plik — ostrzeżenie o zabezpieczeniach*

15. Po uruchomieniu się aplikacji powinien być widoczny ekran jak na rysunku 8.5.



Rysunek 8.5. *Advanced IE Password Recovery*

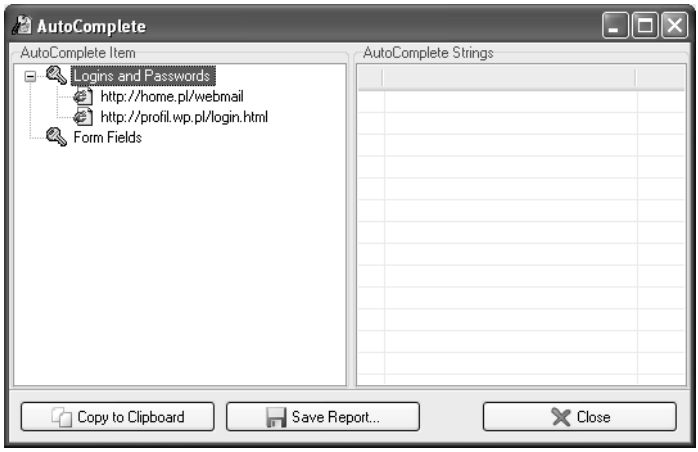
16. Wybrać przycisk *AutoComplete*.

17. Zapoznać się z hasłami i loginami podanymi w oknie dialogowym *AutoComplete* (patrz rysunek 8.6) w sekcji *Logins and Passwords*.

18. Zamknąć okno przyciskiem *Close*.

19. Zamknąć aplikację, wybierając z menu *Recovery* polecenie *Exit*.

Rysunek 8.6.
AutoComplete



Formanty ActiveX — co to jest i jak nimi zarządzać

Formanty i skrypty ActiveX są dodatkami, które mogą być doinstalowane do przeglądarki Internet Explorer po to, aby zwiększyć funkcjonalność stron internetowych. Przykłady kontrolek, z którymi często styka się użytkownik komputera, zostały podanie poniżej:

- *formant Active X dla witryny Microsoft Update* — jest instalowany podczas odwiedzania strony *http://update.microsoft.com/microsoftupdate*, z której można pobrać poprawki do systemów Windows oraz pakietu Office;
- *formant ActiveX dla witryny Windows Update* — jest instalowany podczas odwiedzania strony *http://windowsupdate.microsoft.com/*, z której można pobrać poprawki do systemów Windows;
- *formant ActiveX Shockwave Flash Object* — umożliwia uruchamianie multimedialnych prezentacji wykonanych w technologii Macromedia Flash;
- *formant ActiveX Office Genuine Advantage Validation Tool* — umożliwia pobieranie ze strony firmy Microsoft bezpłatnych dodatków dla posiadaczy legalnego oprogramowania.

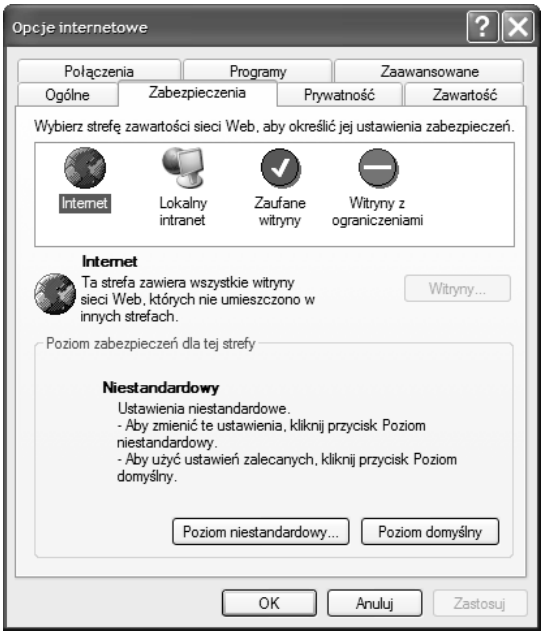
Ponadto wiele stron wymaga zainstalowania formantów ActiveX, aby np. móc przeglądać notowania giełdowe czy korzystać z interaktywnej zawartości. Z powyższego opisu można wnioskować, że formanty ActiveX są pożyteczne. Jednak jeżeli zostaną pobrane z niebezpiecznych stron (niepewnych, nieznanych źródeł), mogą po zainstalowaniu na przykład wysyłać do sieci informacje o tym, jakie operacje wykonuje użytkownik, bez pytania go o zgodę, usuwać dane bądź instalować niepożądane aplikacje, a nawet umożliwić przejęcie zdalnej kontroli nad komputerem.

System Windows XP Home Edition i Professional z zainstalowanym dodatkiem Service Pack 2 ma mechanizmy ochrony przed nieautoryzowaną instalacją formantów ActiveX, pozwalające na wyłączenie lub odinstalowanie dodatków. Proces ustalania zasad instalacji dodatków, samej instalacji dodatków oraz wyłączania i usuwania dodatków zostanie opisany w następnych podrozdziałach.

Ustalanie zasad pobierania formantów ActiveX

Administrator komputera może ustalić zasady pobierania i uruchamiania formantów ActiveX udostępnianych na stronach internetowych. Aby to zrobić, należy:

1. Uruchomić program Internet Explorer.
2. Z menu *Narzędzia* wybrać polecenie *Opcje internetowe*.
3. Przejść do zakładki *Zabezpieczenia*.
4. Kliknąć strefę *Internet* (patrz rysunek 8.7), a następnie przycisk *Poziom niestandardowy…*.

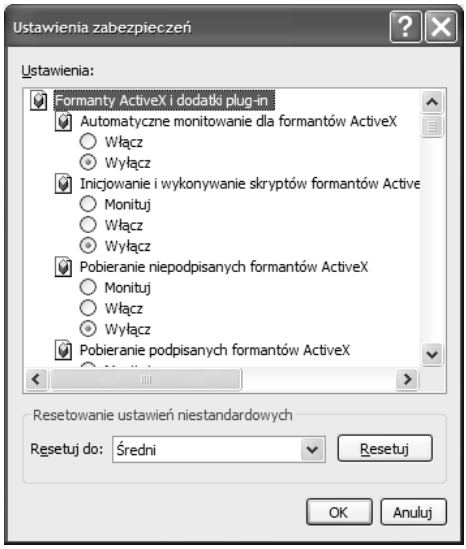


Rysunek 8.7. *Zakładka zabezpieczenia programu Internet Explorer*

5. W oknie dialogowym *Ustawienia zabezpieczeń* (patrz rysunek 8.8) określić ustawienia dotyczące formatek ActiveX.

Z punktu widzenia bezpieczeństwa nie należy zezwalać na automatyczne pobieranie i uruchamianie jakichkolwiek formantów ActiveX. Dlatego należy wybrać opcje *Monituj* lub *Wyłącz*. Wybranie ustawienia *Włącz* może być niebezpieczne dla komputera.

Rysunek 8.8. *Ustawienia zabezpieczeń*



Instalacja formantów ActiveX

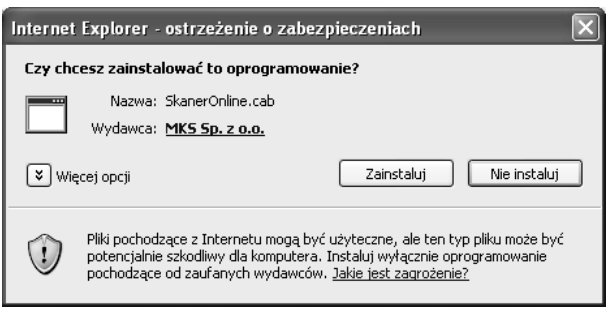
Po odwiedzeniu strony wymagającej zainstalowania formantu ActiveX powinien pojawić się komunikat jak na rysunku 8.9.

Rysunek 8.9. *Informacja o instalacji formantu ActiveX*

Aby zezwolić na instalację formantu, należy:

1. Upewnić się, że strona, z której pobierany jest formant, jest zaufana.
2. Kliknąć komunikat przypominający komunikat pokazany na rysunku 8.9.
3. Wybrać polecenie *Zainstaluj formant ActiveX...*.
4. W oknie dialogowym *Internet Explorer — ostrzeżenie o zabezpieczeniach* (patrz rysunek 8.10) wybrać przycisk *Więcej opcji*.

Rysunek 8.10. *Internet Explorer — ostrzeżenie o zabezpieczeniach*



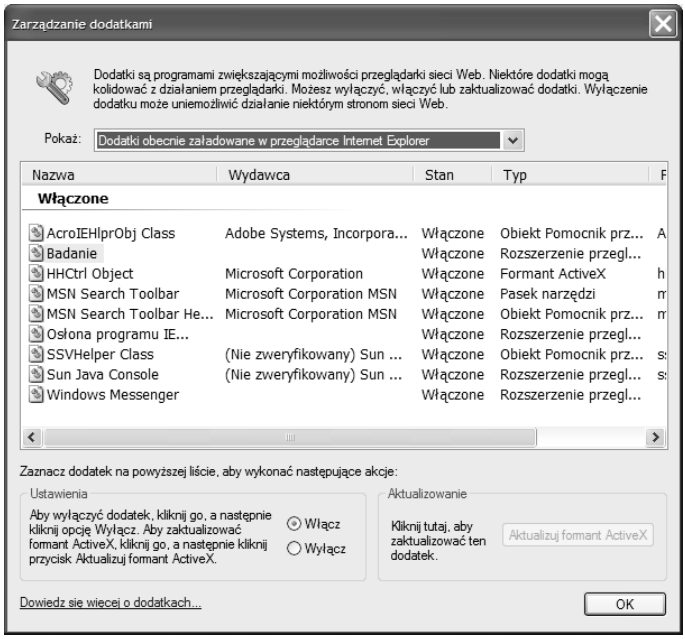
5. Jeżeli formant jest podpisany cyfrowo, kliknąć nazwę wydawcy i zapoznać się z informacjami o podpisie cyfrowym.
6. Zamknąć okno z informacjami o podpisie cyfrowym.
7. Wybrać przycisk *Zainstaluj*.

Przeglądanie informacji o formantach ActiveX

Aby zweryfikować, jakie formanty ActiveX i inne dodatki zostały zainstalowane, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Zarządzaj dodatkami*….
3. Po wyświetleniu okna dialogowego *Zarządzanie dodatkami* można zobaczyć wszystkie zainstalowane dodatki (patrz rysunek 8.11).

Rysunek 8.11. *Zarządzanie dodatkami*



4. W polu *Pokaż* wybrać *Dodatki obecnie załadowane w przeglądarce Internet Explorer*.

   Wyświetlona zostanie lista wszystkich dodatków, które są załadowane w przeglądarce. Zostaną podane następujące informacje:

   - *Nazwa* — w tej kolumnie zostanie podana nazwa dodatku;
   - *Wydawca* — w tej kolumnie zostanie podana nazwa firmy, która stworzyła dodatek;

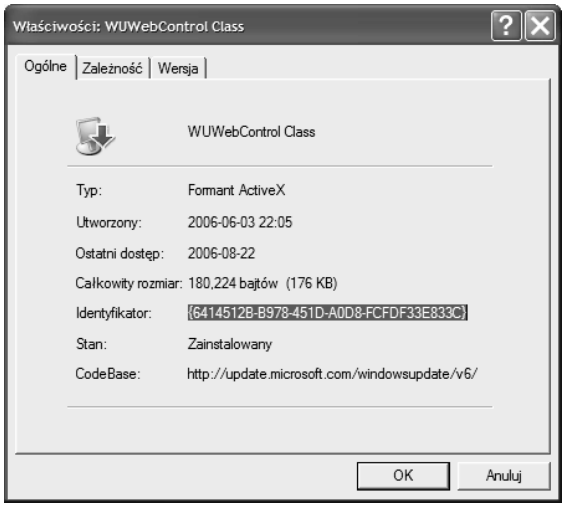
- *Stan* — w tej kolumnie zostanie podany stan dodatku: *Włączone* lub *Wyłączone*;
- *Typ* — w tej kolumnie zostanie podana informacja o typie dodatku; przykładowe typy dodatków podane są poniżej:
  - *Obiekt Pomocnik przeglądarki*,
  - *Rozszerzenie przeglądarki*,
  - *Formant ActiveX*,
  - *Pasek narzędzi*,
- *Plik* — w tej kolumnie podana jest informacja o pliku, w którym zapisany jest dodatek.

5. Po zapoznaniu się z listą dodatków można wybrać opcję *Dodatki, które były używane przez przeglądarkę Internet Explorer*, aby zobaczyć informacje o dodatkach, które były używane (ale niekoniecznie są używane) przez przeglądarkę Internet Explorer.
6. Wybrać przycisk *OK*.

Można również zasięgnąć dokładniejszych informacji o formantach ActiveX. W tym celu należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Opcje internetowe…*.
3. Przejść do zakładki *Ogólne*.
4. Wybrać przycisk *Ustawienia…*.
5. W oknie *Ustawienia* wybrać przycisk *Przeglądaj obiekty…*. Zostanie wyświetlona zawartość folderu *Downloaded Program Files*.
6. Kliknąć prawym przyciskiem myszy wybrany obiekt i wybrać polecenie *Właściwości* (rysunek 8.12 przedstawia informacje o kontrolce *WUWebControl Class*).
7. Przejrzeć zawartość zakładek *Zależność* oraz *Wersja*.
8. Wybrać przycisk *OK*.

Zwróć uwagę na wartość wpisaną w polu *CodeBase* w zakładce *Ogólne*. W tym miejscu wpisany jest adres strony, z której pobrana została formatka ActiveX. Dodatkowo w zakładce *Wersja* w pozycji *Firma* podana jest informacja, jaka firma jest twórcą kontrolki. Znając zawartość pól *Firma* oraz *CodeBase*, można dowiedzieć się, jakie jest pochodzenie formatki.



Rysunek 8.12. *Właściwości obiektu*

Aktualizacja formantu ActiveX

Gdy pojawi się nowa wersja formantu, można ją pobrać. Warto zawsze instalować najbardziej aktualną wersję formantu, aby ustrzec się przed skutkami błędów, które mogą znajdować się w starym formancie.

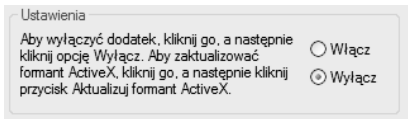
Aby zaktualizować formant, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Zarządzaj dodatkami…*.
3. Po wyświetleniu okna dialogowego *Zarządzanie dodatkami* można wskazać nazwę dodatku i wybrać przycisk *Aktualizuj formant ActiveX*.

Wyłączanie formantów ActiveX

W przypadku gdy istnieje podejrzenie, że kontrolka pochodzi z niepewnego źródła, można ją wyłączyć lub usunąć. Aby wyłączyć formant ActiveX lub inny dodatek programu Internet Explorer, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Zarządzaj dodatkami…*.
3. Po wyświetleniu okna dialogowego *Zarządzanie dodatkami* można wskazać nazwę dodatku i wybrać przycisk *Wyłącz* (patrz rysunek 8.13).



Rysunek 8.13. *Ustawienia dodatku*

Aby formant został rzeczywiście wyłączony, należy zamknąć wszystkie włączone okna Internet Explorera i uruchomić przeglądarkę ponownie.

Usuwanie formantów ActiveX

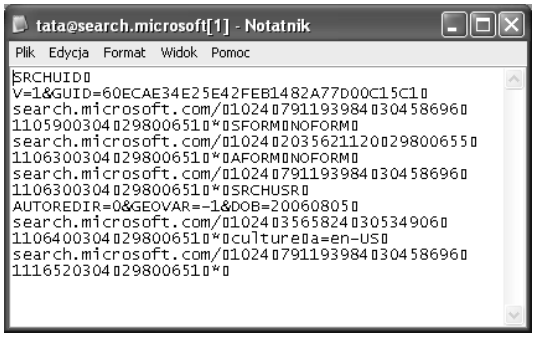
W przypadku gdyby formant został zainstalowany przypadkowo lub pochodził z niepewnego źródła, można go usunąć. Aby to zrobić, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Opcje internetowe…*.
3. Przejść do zakładki *Ogólne*.
4. Wybrać przycisk *Ustawienia…*.
5. W oknie *Ustawienia* wybrać przycisk *Przeglądaj obiekty…*. Zostanie wyświetlona zawartość folderu *Downloaded Program Files*.
6. Kliknąć prawym przyciskiem myszy formant do usunięcia i wybrać polecenie *Usuń*.

Pliki typu cookie (ciasteczka) — do czego służą i jak nimi zarządzać

Pliki typu cookie, nazywane także ciasteczkami, to niewielkie pliki (od kilku do kilkunastu kilobajtów) wysyłane do przeglądarki użytkownika przez serwer WWW i zapisywane lokalnie na komputerze. Zawartość przykładowego pliku cookie przedstawia rysunek 8.14.

Rysunek 8.14. *Zawartość przykładowego pliku cookie*



Należy zdementować pewne błędne opinie na temat plików cookie. Plik cookie może być odczytany tylko przez tę witrynę, która go wysłała. Oznacza to przykładowo, że witryna *wp.pl* nie może odczytać pliku cookie wysłanego przez witrynę *Onet.pl*.

Ze względu na trwałość pliki cookie można podzielić na dwie kategorie:

- Cookies stałe — zostają w komputerze nawet po zamknięciu przeglądarki. Przykładowo, jeżeli jakiś sklep internetowy wykorzystuje mechanizmy stałych cookies do zapisywania informacji o koszyku zakupów i klient zamknie przeglądarkę przed zakończeniem zakupów, a następnie ponownie uruchomi przeglądarkę i ponownie odwiedzi strony tego sklepu, zobaczy w koszyku towary, które uprzednio do niego dodał.
- Cookies tymczasowe — są usuwane z przeglądarki po jej zamknięciu.

Pliki cookie mogą zawierać takie informacje, jak:

- imię i nazwisko osoby odwiedzającej daną witrynę,
- adres pocztowy,
- adres e-mail,
- telefon,
- zainteresowania,
- numer konta bankowego,
- inne dane.

Pliki cookie zawierają poufne informacje. Jednak nie wykradają ich w żaden tajemniczy sposób, a w szczególności nie pobierają ich z innych plików zapisanych na komputerze. Są to po prostu informacje, które użytkownik podał w danej witrynie (np. wypełniając formularz).

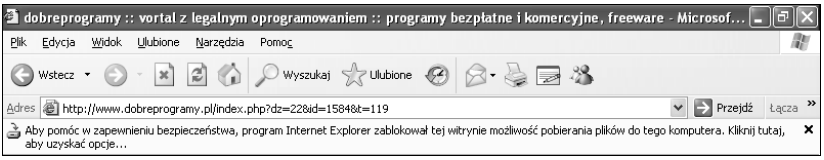
Takie pliki mogą być wykorzystywane do personalizowania wyglądu i zawartości strony. Przykładowo, jeżeli podczas wizyty na jakiejś stronie przeglądarka zapisze cookie zawierający informacje, że interesuje nas gotowanie, to przy następnych odwiedzinach możemy zobaczyć reklamę firmy produkującej przyprawy.

Więcej informacji o tym, jak zarządzać plikami cookie, znajdziesz w podrozdziale „Poziomy prywatności — co to jest, jak je określać".

Blokowanie pobierania niechcianych plików

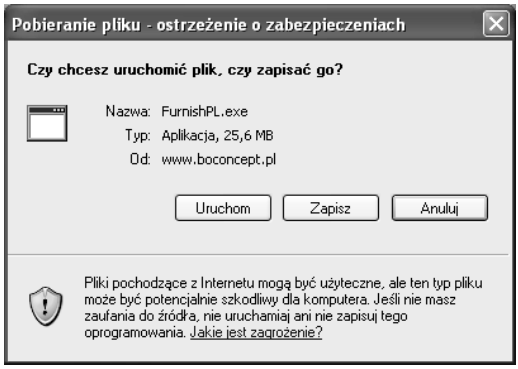
Windows XP z dodatkiem Service Pack 2, zarówno w wersji Home Edition jak i Professional, ma mechanizm blokujący przypadkowe pobieranie plików ze stron internetowych. Jeżeli odwiedzisz stronę, z której można przykładowo pobierać wersje próbne aplikacji, i spróbujesz pobrać plik, powinieneś zobaczyć ostrzeżenie jak na rysunku 8.15.

Rysunek 8.15. *Ostrzeżenie o pobieraniu pliku*



Kliknięcie tego komunikatu pozwoli wybrać polecenie *Pobierz plik*. Po wybraniu polecenia *Pobierz plik* pokaże się okno dialogowe podobne do tego, które przedstawia rysunek 8.16. Dopiero wybranie przycisku *Zapisz* spowoduje pobranie i zapisanie pliku.

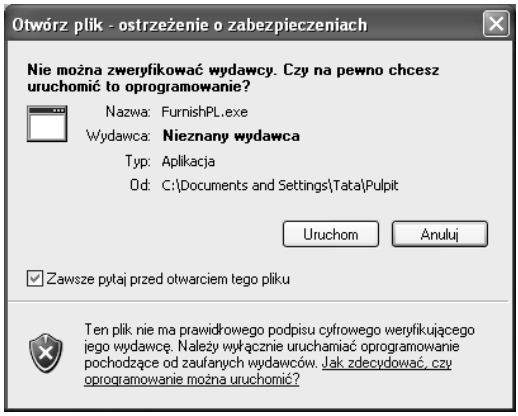
Rysunek 8.16. *Pobieranie pliku — ostrzeżenie o zabezpieczeniach*



Pamiętaj, aby przed zezwoleniem na pobieranie upewnić się, czy plik jest pobierany z zaufanej witryny i nie jest złośliwą (szkodliwą) aplikacją.

Po zapisaniu pobranego pliku system operacyjny wciąż przechowuje informację, że plik pobrany został z internetu. Każda próba jego uruchomienia spowoduje wyświetlenie komunikatu przedstawionego na rysunku 8.17. Dzięki temu nie będzie możliwe przypadkowe uruchomienie pobranego i zapisanego pliku.

Rysunek 8.17. *Otwórz plik — ostrzeżenie o zabezpieczeniach*



Dopiero wybranie przycisku *Uruchom* spowoduje uruchomienie pliku.

Jeżeli jesteś pewien, że plik pochodzi z zaufanego źródła oraz nie jest szkodliwy, a Ty nie chcesz, aby komunikat podany na rysunku 8.17 był dla niego wyświetlany, możesz usunąć zaznaczenie pola *Zawsze pytaj przed otwarciem tego pliku*.

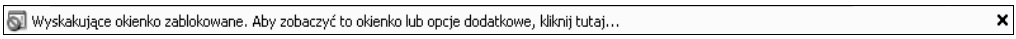
Blokowanie wyskakujących okienek

Wyskakujące okienka są denerwującym dla użytkownika elementem stron WWW. Często zawierają reklamy, których oglądanie może być uciążliwe. System operacyjny Windows XP z zainstalowanym dodatkiem Service Pack 2 ma mechanizm blokowania wyskakujących okien.

Blokowanie wyskakiwania okien jest domyślnie włączone. Jeżeli jednak z jakichś przyczyn zostało ono wyłączone, należy po uruchomieniu przeglądarki Internet Explorer wybrać z menu *Narzędzia* polecenie *Blokowanie wyskakiwania okien*, a następnie *Włącz blokowanie wyskakujących okienek*.

Po wejściu na stronę internetową, która próbuje wyświetlić wyskakujące okienko, powinien ukazać się komunikat podobny do tego przedstawionego na rysunku 8.18. Po kliknięciu komunikatu możliwe będzie wybranie jednego z dwóch poleceń:

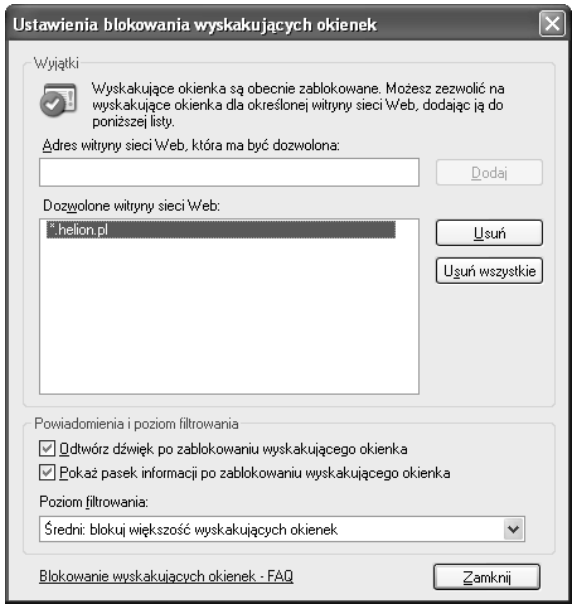
- *Tymczasowo zezwalaj na wyskakujące okienka* — wybranie tego polecenia spowoduje, że wyskakujące okienko zostanie wyświetlone, jednak przy następnej wizycie w tej witrynie konieczne będzie ponowne wyrażenie zgody na wyświetlenie tego okienka;
- *Zawsze zezwalaj na wyskakujące okienka dla tej witryny* — wybranie tego polecenia będzie wymagało potwierdzenia decyzji przez wybranie *Tak* w oknie dialogowym *Czy chcesz zezwalać na wyskakujące okienka dla witryny*. Jeśli zaakceptujesz ten wybór, przy ponownej próbie wywołania wyskakującego okienka przez witrynę ostrzeżenie nie będzie wyświetlane.



Rysunek 8.18. *Ostrzeżenie o wyskakującym okienku*

W przypadku niektórych witryn możesz zdecydować się na dopuszczenie wyświetlania wyskakujących okienek. Aby zezwolić na wyświetlanie wyskakujących okienek na danej witrynie, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Blokowanie wyskakujących okienek*, a następnie *Ustawienia blokowania wyskakujących okienek*....
3. W oknie dialogowym *Ustawienia blokowania wyskakujących okienek* w polu *Adres witryny sieci Web, która ma być dozwolona* wpisać adres oraz wybrać przycisk *Dodaj* (patrz rysunek 8.19).



Rysunek 8.19. *Ustawienia blokowania wyskakujących okienek*

4. Potwierdzić ustawienia przyciskiem *Zamknij*.

W oknie *Ustawienia blokowania wyskakujących okienek* w sekcji *Poziom filtrowania* możesz określić, jak restrykcyjnie Internet Explorer ma traktować wyskakujące okienka. Dostępne są trzy poziomy:

- *Wysoki* — wybranie tego poziomu spowoduje blokowanie wszystkich wyskakujących okien;
- *Średni* — wybranie tego poziomu spowoduje blokowanie większości wyskakujących okien;
- *Niski* — wybranie tego poziomu spowoduje blokowanie większości wyskakujących okien, nie będą jednak blokowane wyskakujące okna z bezpiecznych witryn.

Dla własnej wygody powinieneś stosować poziom *Wysoki*.

Strefy internetowe

Co to są strefy internetowe

Korzystając z programu Internet Explorer, możesz odwiedzać wiele witryn internetowych. Każda z witryn należy do jednej z czterech stref internetowych. Przypisanie witryny do wybranej strefy zależy od tego, jak bardzo ufamy witrynie. Strefy internetowe opisane zostały poniżej:

- *Internet* — Internet Explorer przypisuje do tej strefy wszystkie witryny, które nie są w strefie *Zaufane witryny*, nie są witrynami intranetowymi lub nie są przypisane do innej strefy. W tej strefie są na przykład witryny portalu *Onet.pl* czy *Wirtualna Polska*. Nie możesz dodać żadnej witryny do tej strefy.
- *Lokalny intranet* — do tej strefy należą wszystkie strony, do których dostęp nie wymaga korzystania z *serwera proxy* lub domyślnej bramy. Do tej strefy należą witryny określone w zakładce *Połączenia*, ścieżki sieciowe (np. *\\nazwa_serwera\udział*) i lokalne witryny intranetowe. Do tej strefy można dodawać witryny.
- *Zaufane witryny* — domyślnie do tej strefy nie należy żadna witryna. Należy do niej dodawać tylko witryny bezpieczne, którym się ufa, gdyż Internet Explorer przypisuje do niej niski poziom zabezpieczeń, więc witryny zaufane mogą pobierać i zapisywać na komputerze wiele informacji.
- *Witryny z ograniczeniami* — domyślnie do tej strefy nie należy żadna witryna. Należy do niej dodawać witryny, którym się nie ufa, czyli takie witryny, co do których istnieje ryzyko, że pobrane z nich pliki mogą być niebezpieczne dla komputera i zainstalowanych na nim aplikacji

Ustawienia stref zabezpieczeń

Do każdej ze stref internetowych przypisane są domyślnie określone poziomy zabezpieczeń (poziom zabezpieczeń to zestaw informacji, jakie czynności lub akcje znajdująca się w danej strefie witryna może podejmować). Poziomy zabezpieczeń przypisane do poszczególnych stref przedstawia tabela 8.1.

Tabela 8.1. *Strefy internetowe i domyślne poziomy zabezpieczeń*

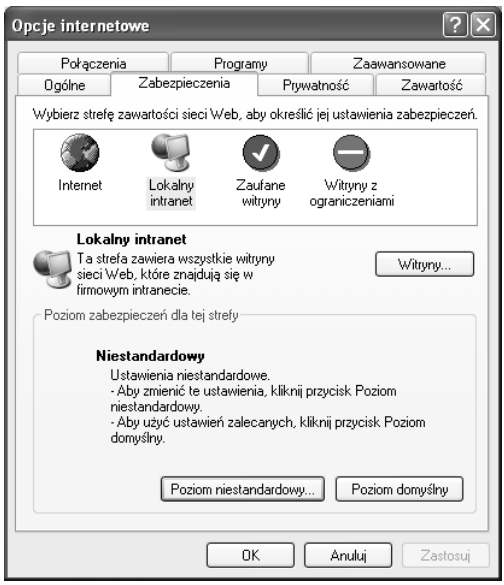
Nazwa strefy	Domyślny poziom zabezpieczeń
Internet	Średni
Lokalny intranet	Średni
Zaufane witryny	Niski
Witryny z ograniczeniami	Wysoki

Modyfikacja zabezpieczeń dla stref internetowych

Aby zmodyfikować zabezpieczenia dla strefy, należy:

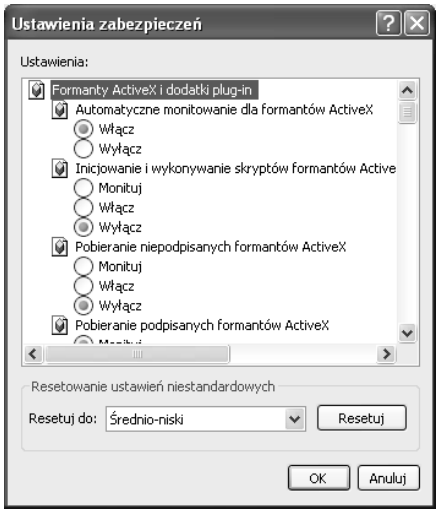
1. Uruchomić program Internet Explorer.
2. Z menu *Narzędzia* wybrać polecenie *Opcje*.
3. Przejść do zakładki *Zabezpieczenia* (patrz rysunek 8.20).
4. Kliknąć nazwę strefy.
5. Kliknąć przycisk *Poziom niestandardowy…*.

Rysunek 8.20. *Zakładka zabezpieczenia*



6. W oknie *Ustawienia zabezpieczeń* (patrz rysunek 8.21) zmienić odpowiednie ustawienia.

Rysunek 8.21. *Ustawienia zabezpieczeń*



Jeżeli dokonałeś wielu zmian w ustawieniach zabezpieczeń dla danej strefy i nie jesteś już pewien, co zmieniłeś, możesz przypomnieć sobie domyślne ustawienia, korzystając z tabeli 8.1, i w oknie dialogowym *Ustawienia zabezpieczeń* w polu *Resetuj do:* wybrać właściwy poziom i zatwierdzić przyciskiem *Resetuj*.

7. Potwierdzić swoją decyzję przyciskiem *OK*.

8. Ponownie wybrać przycisk *OK*.

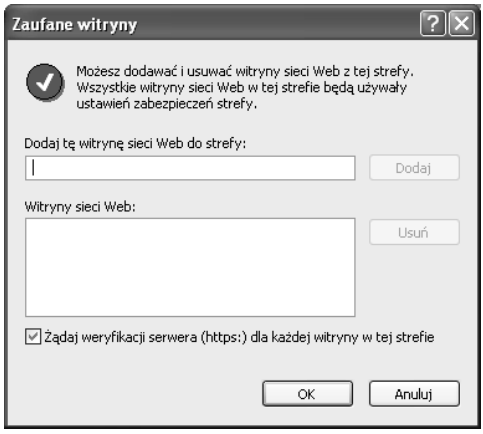
Raczej powinno się wprowadzać bardziej restrykcyjne ustawienia dla danej strefy, niż je łagodzić. Zanim podejdziesz bardziej liberalnie do zabezpieczeń dla danej strefy, dobrze się zastanów, jakie będą z tego korzyści i jakie niebezpieczeństwa. Być może zamiast obniżać poziom zabezpieczeń dla danej strefy, lepiej będzie przenieść jedną lub parę witryn z tej strefy do innej, o niższym poziomie zabezpieczeń.

Dodawanie i usuwanie witryn ze stref internetowych

Aby dodać witrynę do strefy zabezpieczeń, należy:

1. Uruchomić program Internet Explorer.
2. Z menu *Narzędzia* wybrać polecenie *Opcje*.
3. Przejść do zakładki *Zabezpieczenia*.
4. Kliknąć nazwę strefy.
5. Wybrać przycisk *Witryny...*.
6. W następnym oknie dialogowym (patrz rysunek 8.22) w polu *Dodaj tę witrynę sieci Web do strefy* wpisz adres witryny i kliknij przycisk *Dodaj*.

Rysunek 8.22. *Zaufane witryny*



Możesz również usunąć witrynę z danej strefy, wskazując ją na liście witryn i wybierając przycisk *Usuń*.

7. Potwierdzić decyzję przyciskiem *OK*.

Jeżeli adres witryny nie zaczyna się od *https:*, powinieneś przed wybraniem przycisku *OK* usunąć zaznaczenie pola *Żądaj weryfikacji serwera (https:) dla każdej witryny w tej strefie*.

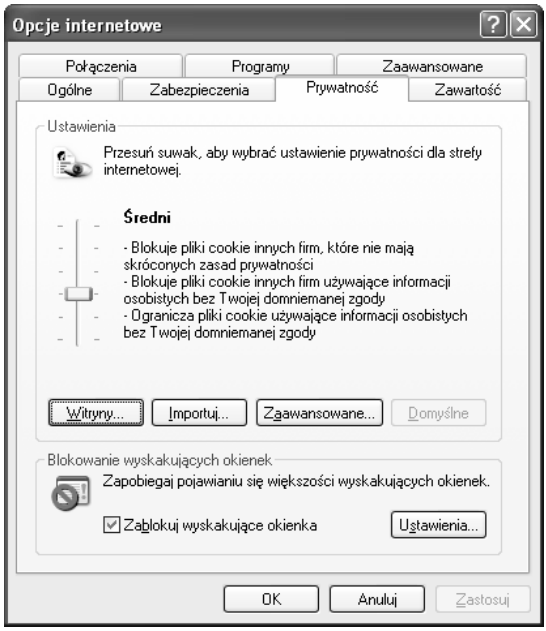
8. Ponownie wybrać przycisk *OK*.

Poziomy prywatności — co to jest, jak je określać

Program Internet Explorer pozwala na określenie poziomów prywatności podczas surfowania po internecie. Poziom prywatności określa, jak dużo informacji Internet Explorer przekazuje serwerowi, na którym zapisane są strony odwiedzane przez użytkownika.

Aby określić poziom prywatności, należy

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Opcje internetowe*.
3. Przejść do zakładki *Prywatność* (patrz rysunek 8.23).



Rysunek 8.23. *Zakładka Prywatność*

4. Przesuwając suwak w środkowej części ekranu, wybrać jedno z ustawień.

Jeżeli ustawisz poziom prywatności na taki, który blokuje wszystkie pliki cookie, nie będziesz mógł na przykład korzystać ze stron banków internetowych, które wymagają, aby pliki cookie były obsługiwane przez przeglądarkę. Podobnie może być ze stronami służącymi do obsługi poczty elektronicznej. Dodatkowo wiele serwisów internetowych korzysta z plików cookie, aby dostosować wyświetlaną zawartość do preferencji użytkownika.

5. Wybrać przycisk *OK*.

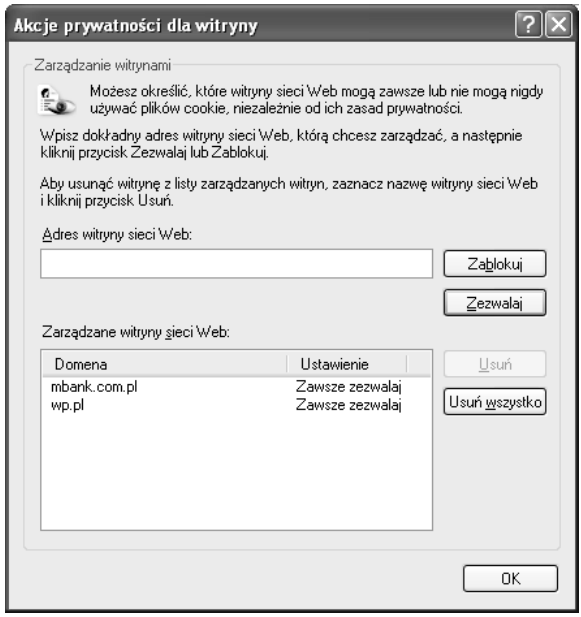
Poniżej opisano wszystkie dostępne poziomy prywatności:

- *Blokowanie wszystkich plików cookie* — wybierając ten poziom, zablokujesz pliki cookie ze wszystkich witryn sieci WWW oraz uniemożliwisz odczytywanie plików cookie zapisanych na komputerze.
- *Wysoki* — wybierając ten poziom, zablokujesz wszystkie pliki cookie ze wszystkich stron internetowych, które nie mają określonych skróconych zasad, oraz zablokujesz pliki cookie ze wszystkich stron, które korzystają z informacji osobistych użytkownika bez jego wyraźnej zgody.
- *Średnioniski* — po wybraniu tego poziomu przeglądarka będzie zachowywała się jak przy poziomie *Wysoki* oraz będzie blokować pliki cookie ze stron, które korzystają z informacji osobistych użytkownika bez jego domniemanej zgody.
- *Średni* — wybierając ten poziom, zablokujesz pliki cookie ze stron, które nie mają określonych skróconych zasad prywatności, oraz pliki cookie ze stron, które korzystają z informacji osobistych użytkownika bez jego domniemanej zgody, a także usuniesz po zamknięciu przeglądarki pliki cookie ze stron, które korzystają z informacji osobistych użytkownika bez jego domniemanej zgody.
- *Niski* — wybierając ten poziom, zablokujesz pliki cookie ze stron, które nie mają określonych skróconych zasad prywatności, oraz usuniesz po zamknięciu przeglądarki pliki cookie ze stron, które korzystają z informacji osobistych użytkownika bez jego domniemanej zgody.
- *Akceptowanie wszystkich plików cookie* — wybierając ten poziom, pozwolisz, aby wszystkie pliki cookie były zapisywane na komputerze i mogły być odczytywane wyłącznie przez witryny sieci WWW, które je utworzyły.

Aby chronić swoją prywatność, ustal poziom prywatności na jak najwyższym poziomie. W przypadku gdyby zaufane, dobrze znane i bezpieczne witryny przestały funkcjonować przez niemożność korzystania z plików cookie, możesz w aplikacji Internet Explorer stworzyć listę witryn, które mimo ustawienia wysokiego poziomu prywatności będą mogły korzystać z plików cookie. Aby to zrobić, należy:

1. Uruchomić program *Internet Explorer*.
2. Wybrać z menu *Narzędzia* polecenie *Opcje internetowe*.
3. Przejść do zakładki *Prywatność*.
4. Wybrać przycisk *Witryny…*.
5. W oknie dialogowym *Akcje prywatności dla witryn* (patrz rysunek 8.24) w polu *Adres witryny sieci Web:* wpisać adres strony, dla której nie mają być blokowane pliki cookie, i wybrać przycisk *Zezwalaj*.

Możesz również wybrać przycisk *Zablokuj*, aby zablokować wybraną stronę niezależnie od ustawień określonych w zakładce *Prywatność*.



Rysunek 8.24. *Akcje prywatności dla witryny*

Jak chronić swoją anonimowość w internecie. Steganos Internet Anonym Pro 6

W poprzednich podrozdziałach dowiedziałeś się o zapisywaniu haseł przez przeglądarkę Internet Explorer, plikach cookie oraz innych elementach, które mogą świadczyć o rodzaju Twojej aktywności w internecie. Dodatkowo w rozdziale 2. przedstawiono informacje, jak zidentyfikować, skąd nawiązano połączenie. W tym rozdziale przedstawiona zostanie aplikacja *Steganos Internet Anonym Pro 6*. Jest to jedna z wielu aplikacji pozwalających poruszać się w internecie bardziej anonimowo.

Nie istnieje całkowita anonimowość w internecie. Aplikacje, które mają ją zapewnić, tylko utrudniają zidentyfikowanie komputera. Stwierdzenie „zapewnienie anonimowości" używane w tym rozdziale jest tylko skrótem myślowym i oznacza maksymalne utrudnienie identyfikacji internauty.

Aplikację *Steganos Internet Anonym Pro 6* możesz pobrać w wersji testowej ze strony *http://www.programs.pl/program,493.html* lub ze strony producenta: *https:\\www.steganos.com*. Procedura instalacyjna nie została opisana w tym rozdziale, gdyż jest intuicyjna i przypomina instalację innych opisanych programów.

Anonimowe poruszanie się po internecie

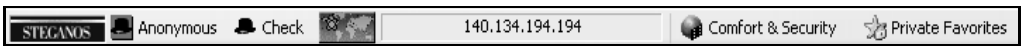
Aby zapewnić sobie anonimowe poruszanie się po internecie, należy:

1. Wybrać z menu *Start* polecenie *Wszystkie programy*, następnie *Steganos Internet Anonym Pro 6* i ponownie *Steganos Internet Anonym Pro 6*.
2. Po chwili uruchomi się aplikacja *Steganos Internet Anonym Pro 6* (patrz rysunek 8.25).

Rysunek 8.25. *Steganos Internet Anonym Pro 6*

Aplikacja *Steganos Internet Anonym Pro 6* działa w ten sposób, że korzystając z niej, nie łączysz się z witryną bezpośrednio, lecz za pośrednictwem *serwerów proxy* firm współpracujących z firmą Steganos. Dlatego serwer (np. serwer, na którym działa Wirtualna Polska) nie zarejestruje informacji o tym, że ktoś się z nim łączył z Twojego adresu — będzie to adres serwera firmy współpracującej z firmą Steganos. Co więcej, Twoje połączenie będzie nieustannie przełączane pomiędzy tymi serwerami. To znacznie utrudni identyfikację, ale jej nie uniemożliwi, gdyż firma Steganos będzie wiedziała, kto łączy się z ich serwerami; nie będzie tego wiedziała np. Wirtualna Polska. Dynamicznie zmieniane serwery firmy Steganos będą po prostu pośredniczyły w połączeniu pomiędzy komputerem domowym a określonym serwisem internetowym.

3. Uruchomić program Internet Explorer.
4. Sprawdzić, czy w aplikacji Internet Explorer pojawił się pasek narzędzi podobny do tego na rysunku 8.26.



Rysunek 8.26. *Steganos Internet Anonym Pro 6*

5. Sprawdzić, czy na pasku narzędzi dynamicznie zmienia się adres IP, a na miniaturce mapy świata — lokalizacja serwera proxy, przez który nawiązywane jest połączenie.

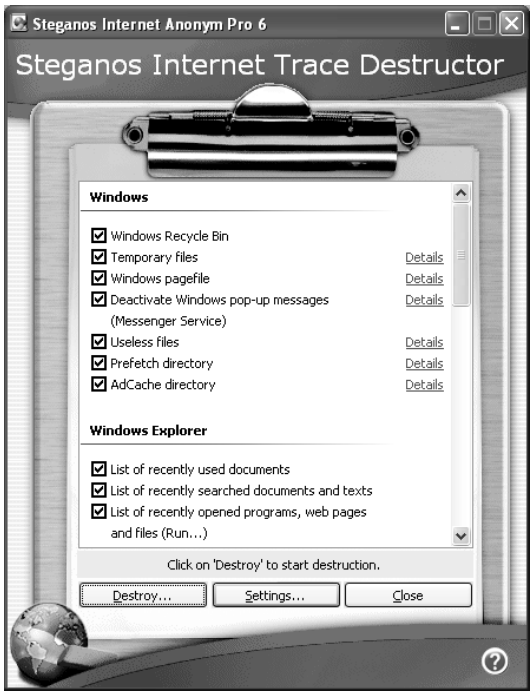
W związku z dynamicznym przełączaniem się pomiędzy serwerami proxy na całym świecie początkowo wywoływane strony internetowe będą wczytywały się wolno. Z czasem czas ładowania stron powinien się skrócić.

Usuwanie poufnych danych z komputera

Aby usunąć poufne informacje (w tym informacje o aktywności w internecie), należy:

1. Wybrać z menu *Start* polecenie *Wszystkie programy*, następnie *Steganos Internet Anonym Pro 6* i *Internet Trace Destructor*.
2. Gdy po chwili uruchomi się aplikacja *Steganos Internet Trace Destructor* (patrz rysunek 8.27), zaznaczyć wszystkie elementy, które mają być usunięte.

Rysunek 8.27. *Steganos Internet Trace Destructor*



3. Wybrać przycisk *Destroy*....
4. Potwierdzić decyzję przyciskiem *Yes*, a następnie *OK*.

Program *Steganos Internet Anonym Pro 6* między innymi usunął pliki zawierające informacje o tym, jakie strony w internecie odwiedzałeś. Ważne jest, abyś wiedział, że usunięte w ten sposób pliki wciąż można odzyskać za pomocą specjalistycznych narzędzi. Do trwałego usuwania danych z komputera służą specjalistyczne aplikacje. Jedną z takich aplikacji jest *System Mechanic Incinerator* (więcej informacji o tej aplikacji znajdziesz na stronie *http://www.iolo.com/*).

5. Po pojawieniu się komunikatu jak na rysunku 8.28, informującym o konieczności restartu komputera, wybrać przycisk *Yes*.

Rysunek 8.28. *Steganos Internet Trace Destructor*

Usuwanie informacji o swojej aktywności w internecie z wykorzystaniem Internet Explorera

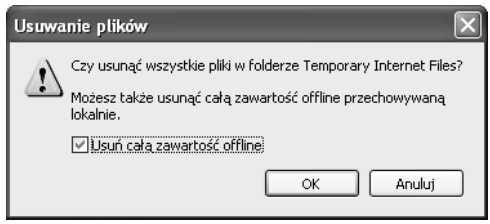
Aby usunąć informacje o swojej aktywności w internecie, należy:

1. Uruchomić program Internet Explorer.
2. Wybrać z menu *Narzędzia* polecenie *Opcje internetowe*.
3. Przejść do zakładki *Ogólne* (patrz rysunek 8.29).

Rysunek 8.29. *Zakładka Ogólne*

4. Wybrać przycisk *Usuń pliki cookie…*.
5. W okienku *Usuwanie plików cookie* wybrać przycisk *OK*.
6. Wybrać przycisk *Usuń pliki…*.
7. W oknie dialogowym *Usuwanie plików* zaznaczyć pole *Usuń całą zawartość offline* i wybrać przycisk *OK* (patrz rysunek 8.30).

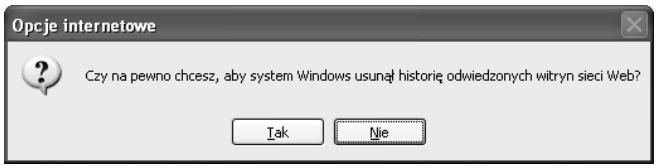
Rysunek 8.30.
Usuwanie plików



Tymczasowe pliki internetowe są zapisywane na komputerze podczas odwiedzania stron internetowych. Pliki te przechowują zawartość odwiedzanych stron. Domyślnie są zapisywane w folderze *C:\Documents and Settings**nazwa użytkownika**\Ustawienia lokalne\Temporary Internet Files*. Możesz je również samodzielnie usunąć z tej lokalizacji.

8. Wybrać przycisk *Wyczyść historię*.
9. W oknie dialogowym *Opcje internetowe* (patrz rysunek 8.31) wybrać przycisk *Tak*.

Rysunek 8.31.
Opcje internetowe



Pozostałe zagadnienia i podsumowanie

Internet został wynaleziony po to, aby ułatwić dostęp do informacji. Jednak z czasem jest on coraz częściej wykorzystywany do wyrządzania szkody jego użytkownikom. Aby zapewnić sobie bezpieczeństwo podczas korzystania z zasobów internetu, należy właściwie korzystać z przeglądarki.

- Pamiętaj, że na stronach mogą znajdować się skrypty, programy i formatki, których pobranie i (lub) uruchomienie może być niebezpieczne dla danych przechowywanych na komputerze.
- Nie pobieraj programów i skryptów, które znajdują się na stronach niezaufanych.

- Nie uruchamiaj programów i skryptów, które pobrałeś ze stron niezaufanych (jeżeli mimo wszystko już je pobrałeś).
- Nie pobieraj żadnych plików z nieznanych stron.
- Nie korzystaj z internetu, jeżeli zalogowałeś się do komputera z uprawnieniami administratorskimi, zamiast tego załóż sobie konto o ograniczonych uprawnieniach, które będziesz wykorzystywał do poruszania się w internecie. Jeżeli ktoś przejmie kontrolę nad komputerem, to najpewniej zrobi to na uprawnieniach tego właśnie użytkownika, a nie administratora.
- Nie klikaj łączy do stron internetowych podesłanych przez nieznane osoby.
- Czytaj uważnie wszystkie komunikaty i ostrzeżenia, które wyświetla przeglądarka.
- Pamiętaj, że informacje podawane na stronach internetowych mogą być nieprawdziwe, a nawet stanowić próbę wprowadzenia użytkownika w błąd.
- Zasada ograniczonego zaufania jest dobra i na ulicy, i w internecie.
- Zanim klikniesz przycisk *OK*, *Cancel*, *Tak* itp., upewnij się, że właściwie zrozumiałeś treść komunikatu.
- Najpewniejszym sposobem na zamknięcie okna, które się pokazało, jest wybranie kombinacji klawiszy *Alt+F4*. Przycisk *Cancel* nie zawsze ma takie znaczenie, jak się nam wydaje.
- Ustaw przeglądarkę tak, aby zapewniała jak najwyższy poziom prywatności danych. Jeżeli niezaufane witryny nie będą chciały współpracować z przeglądarką, ignoruj je. Jeżeli ważne dla Ciebie i jednocześnie zaufane witryny wymagają obsługi plików cookie, dodaj jest do listy wyjątków.
- Całkowita anonimowość w internecie jest fikcją, ale możesz korzystać z programów, które ją w dużym stopniu (choć nie do końca) zapewniają.
- Jeżeli łączysz się z określoną witryną, to serwery, przez które przechodzi Twoje połączenie, rejestrują adres IP, z którego zostało zainicjowane. Umożliwia to odnalezienie osoby, która np. umieściła obraźliwy wpis na forum internetowym.

Czy zdajesz sobie sprawę, z jak wielu serwerów musisz skorzystać, aby nawiązać połączenie np. z witryną Wirtualnej Polski? Aby sprawdzić, przez jakie serwery przechodzi połączenie, wybierz z menu *Start* polecenie *Uruchom.* Wpisz polecenie `cmd` i zatwierdź klawiszem *Enter*. W oknie, które się pojawi, wpisz polecenie `tracert wp.pl` i potwierdź klawiszem *Enter*. Po chwili uzyskasz listę serwerów, przez które przechodziły pakiety. Każdy z nich odnotował, kto zainicjował to połączenie.

- Nie wykonuj bez zastanowienia i zrozumienia czynności, o które ktoś prosi na stronie internetowej (czy w rzeczywistym świecie na prośbę złodzieja zostawiłbyś otwarte drzwi do domu?).
- Jeżeli czegoś nie rozumiesz, zapytaj się specjalisty.

- Jeżeli zapiszesz w systemie hasło do witryny internetowej, może się okazać, że nie tylko Ty je odczytasz, ale również inna osoba, która ma dostęp do komputera.
- Jeżeli korzystasz z komputera publicznego (np. w kafejce internetowej), to zapisanie hasła w systemie może spowodować, że każda następna osoba, która zasiądzie do komputera, będzie mogła bez podawania hasła dostać się na przykład do Twojej poczty — nie zapisuj więc haseł w systemie.
- Jeżeli korzystasz jeszcze z modemu, zablokuj połączenia typu 0-700 i 0-400 oraz połączenia międzynarodowe, aby zabezpieczyć się przed działaniem dialerów.
- Do przeglądarki, tak jak do systemu operacyjnego, musisz pobierać poprawki, aby zabezpieczyć się przed wykorzystaniem obecnych w niej błędów. Poprawki do przeglądarki Internet Explorer pobierasz tak samo jak poprawki do systemu operacyjnego Windows.
- Staraj się nie obniżać poziomu zabezpieczeń dla stref internetowych — raczej je podwyższaj.