

# Chroń się przed programami szpiegującymi

Autor: Marek  
14.11.2008.

Oto pięć łatwych kroków, służących do zabezpieczenia się przed programami szpiegującymi.

Źródło: [netsecurity.about.com](http://netsecurity.about.com)

Źumaczenie: Julianna Wieczorek, Częstochowa

Jeśli nie jedna rzecz, to inna. Jest to jedna z tych niedorzecznych fraz, której w zasadzie nie trzeba powtarzać. Tak samo jak "gdziekolwiek pójdziesz, tam jesteś". Ale w tym wypadku wydaje się to właściwe.

Komputery w Internecie są niemal nieustannie bombardowane wirusami i innymi złośliwymi programami, tak więc użytkownicy muszą zaopatrzyć się w oprogramowanie antywirusowe, aby się chronić. Skrzynki mailowe są stale zalewane coraz bardziej niebezpiecznym spamem, dlatego też użytkownicy zaopatrują się w programy anty-spamowe i stosują różne techniki w celu ochrony. Jak tylko pomyślisz, że masz wszystko pod kontrolą, okazuje się, że Twój system posiada wiele programów szpiegujących i programów typu "adware", działających dyskretnie w tle, monitorujących i raportujących Twoją pracę na komputerze. I dlatego też: "jeśli nie jedna rzecz, to inna".

Im bliżej program szpiegujący czy program typu "adware" monitoruje i śledzi strony, które odwiedzasz w Internecie, tym łatwiej określić zwyczaj użytkownika i spróbować zidentyfikować działania marketingowe. Jednak wiele form szpiegowania wykracza poza proste śledzenie i faktycznie monitoruje naciśnięcie klawisza czy wychwytywanie hasła i inne funkcje, przekraczając tym samym linię i stwarzając konkretne zagrożenie bezpieczeństwa.

Jak można zabezpieczyć się przed takimi podstępными programami? Paradoksalnie, wielu użytkowników niewiedząco zgadza się na ich zainstalowanie. W rzeczywistości, usunięcie niektórych programów szpiegujących i adware może oznaczać, że niektóre programy freeware lub shareware staną się niebezpieczne. Poniżej opiszę 5 prostych kroków, według których należy postępować, aby uniknąć, a jeśli nie da się uniknąć, to przynajmniej wykryć i usunąć te programy z systemu komputera.

Zabezpieczenie 1:

¼ ostrożny w czasie śledzenia: pozbawione skrupułów programy często pochodzą z pozbawionych skrupułów stron.

Jeśli szukasz programów typu „freeware” lub „shareware”; w określonym celu, spróbuj szukać ich w znanych miejscach, takich jak [tucows.com](http://tucows.com) lub [download.com](http://download.com).

#### Zabezpieczenie 2:

Przeczytaj umowę EULA: zapytasz: „Co to jest EULA?”; End User License Agreement, czyli Umowa Licencyjna Użytkownika Oprogramowania. Dotyczy ona całego technicznego i prawnego aspektu, a znajduje się w polu powyżej przycisku opcji, gdzie trzeba powiedzieć: „Nie, nie akceptuję” lub „Tak, przeczytałem i akceptuję warunki”;. Dla większości osób jest to uciążliwe i klikają oni na „tak”;, nie czytając ani słowa. EULA jest prawną umową, jaką zawierasz z dostawcą oprogramowania. Bez jej przeczytania możesz nieświadomie wyrazić zgodę na zainstalowanie oprogramowania szpiegującego lub uruchomienie wielu innych wstpliwych działań, których sobie nie życzysz. Czasami lepiej jest odpowiedzieć „Nie, nie zgadzam”;

#### Zabezpieczenie 3:

Przeczytaj zanim klikniesz: Czasami podczas odwiedzania witryny internetowej, wyskakuje pole tekstowe. Podobnie jak przy EULA, wielu użytkowników po prostu uznaje to za uciążliwe i klika, aby pole zniknęło. Użytkownicy klikają przycisk „tak” lub „ok”; bez zwracania uwagi na to, że w rzeczywistości to pole mówi: „Czy chcesz zainstalować nasz program szpiegujący?”; Ok, wprowadzając nie dzieje się to tak bezpośrednio, ale taka możliwość dostarcza kolejnego powodu, aby przeczytać informację przed kliknięciem przycisku „OK”;

#### Zabezpieczenie 4:

Chroń swój system: Oprogramowanie antywirusowe w dzisiejszych czasach jest w pewnym stopniu błędnie nazywane. Wirusy są jedynie niewielką częścią złośliwego kodu, przed którym chronią programy antywirusowe. Pod słowem „antywirus” kryją się teraz także robaki, trojany, programy wykorzystujące luki oraz dowcipy i żarty, a nawet programy typu „spyware”; i „adware”;. Jeśli Twój program antywirusowy nie wykrywa i nie blokuje programów szpiegujących, możesz spróbować produktu, takiego jak AdAware Pro, który będzie chronił Twój system przed programami „spyware”; i „adware”; w czasie rzeczywistym.

#### Zabezpieczenie 4:

Skanuj swój system: nawet posiadając oprogramowanie antywirusowe, zapory i inne środki ochronne, niektóre programy „spyware”; lub „adware”; mogą dostać się do systemu. Chociaż produkt taki jak AdAware Pro wymieniony w kroku 4 będzie chronił system, monitorując go w czasie rzeczywistym, to trochę kosztuje. Twórcy AdAware Pro, Lavasoft wypuściła także wersję darmową, przeznaczoną dla użytku osobistego. AdAware nie będzie monitorował w czasie rzeczywistym, ale okresowo można ręcznie skanować system w celu wykrycia i usunięcia wszelkich programów szpiegujących. Innym doskonałym wyborem jest Spybot Search & Destroy, który jest również dostępny za darmo.

Dzięki postępowaniu według tych pięciu kroków, Twój system będzie aktywnie chroniony przed programami szpiegującymi, a wszystko, co zdoła dostać się do systemu, będzie wykrywane i usuwane. Powodzenia!

Źródło: [netsecurity.about.com](http://netsecurity.about.com)

Źródło: Julianna Wieczorek, Częstochowa