

JAK CHRONIĆ KOMPUTER PRZED WIRUSAMI?

1. Zainstaluj program antywirusowy.

Program antywirusowy jest niezbędny, gdy dojdzie do infekcji komputera. Pozwoli ci on namierzyć, rozpoznać i usunąć szkodliwe oprogramowanie.

Nie musisz od razu kupować programu antywirusowego. Producenci udostępniają na swoich stronach testowe wersje, dzięki którym będziesz mógł/mogła zdecydować, który antywirus odpowiada ci najbardziej. Istnieje także wiele dobrych darmowych programów antywirusowych, między innymi: Avast! Free Antivirus i Comodo Antivirus.

2. Zainstaluj zaporę sieciową.

Zadaniem zapory sieciowej jest uniemożliwienie wirusom przedostanie się do twojego komputera. Jest niezbędna, gdy jesteś podłączony do Internetu. Zapory sieciowej nie należy jednak wyłączać, nawet jeżeli w danym momencie nie łączysz się z siecią.

3. Regularnie aktualizuj bazy danych wirusów i skanuj dysk.

Programy antywirusowe zawsze przypominają użytkownikowi o niezbędnych aktualizacjach. Postępuj zgodnie z ich wskazówkami. Raz na tydzień, czyli mniej więcej po każdej kolejnej aktualizacji bazy danych wirusów, wykonuj skan systemu.

4. Nie instaluj kilku programów antywirusowych i zapór sieciowych na jednym komputerze.

Instalowanie kilku antywirusów i zapór sieciowych wcale nie poprawi bezpieczeństwa twojego komputera. Wręcz przeciwnie – może wywołać wiele niepożądanych zachowań systemu. Obecność kilku firewallei może na przykład całkowicie zablokować dostęp do Internetu. Programy antywirusowe mogą natomiast wzajemnie się zwalczać.

5. Regularnie aktualizuj oprogramowanie.

Nowe wersje oprogramowania są nie tylko bardziej funkcjonalne, ale i bezpieczniejsze.

6. Zwracaj uwagę na źródło oprogramowania.

Dostępne w Internecie oprogramowanie ściągać tylko z zaufanych stron.

7. Nie otwieraj załączników mailowych od nieznanymi nadawców.

W załącznikach kryć się mogą konie trojańskie. Często praktyką jest także wysyłanie tak zwanych łańcuszków, zawierających rzekomo porady dotyczące ochrony komputera przed wirusami. Przed wcieleniem tych porad w życie należy zawsze sprawdzić ich autentyczność.

8. Korzystaj ostrożnie z sieci P2P.

Wymienianie się plikami w sieci peer to peer nie jest bezpieczne. Często zdarza się, że nazwy plików nie odpowiadają ich rzeczywistej zawartości. Jeśli posiadacz interesujących cię plików nie wydaje ci się godny zaufania, zrezygnuj z ich ściągania.

9. Nie bagatelizuj komunikatów firewallea i programów antywirusowych.

Nie odpowiadaj mechanicznie na zapytania firewallea. Zawsze dokładnie czytaj ich treść.

Źródło: <http://wirtualna-rodzinka.pl/wirusy-komputerowe---jak-dzialaja-i-co-powoduja.html>