Dobre praktyki przy korzystaniu z komputera

Spis treści:

Windows

Zachowywać uwagę przy instalacji oprogramowania

Często strony takie jak dobreprogramy.pl, czy softonic.com oferują możliwość pobierania popularnego oprogramowania z ich stron. Wiąże się to jednak z pobraniem tzw. pomocnika instalacji. Często w tego typu pomocnikach są jednak poukrywane checkboxy, przez nieodznaczenie których zostanie zainstalowane niechciane oprogramowanie, z dołączania którego się utrzymują.

Wiedzieć kiedy zdefragmentować dysk

Aby zwiększyć wydajność dysków talerzowych, często stosuje się tzw. defragmentację, czyli porządkowanie zapisanych danych na dysku. Zwiększa to prędkość zapisu i odczytu z dysku. Operacji tej nie powinno się jednak wykonywać na nośnikach SSD.

Co jakiś czas przeinstalować system

Zdecydowaną wadą systemów Windows jest ich „zapychalność”. Po jakimś czasie nawet najostrożniejszemu użytkownikowi może się zdarzyć, że dysk systemowy nagle z bliżej nieokreślonych przyczyn zacznie nabierać w zajętości, a system będzie uruchamiał się coraz wolniej i wolniej. Warto wtedy zrobić backup wszystkich najważniejszych plików i po prostu zainstalować Windowsa od nowa.

Nie uruchamiać nieznanych aplikacji, plików .reg i .bat

Często mogą to być wirusy lub inne pliki, które mogą przejąć kontrolę lub zniszczyć nasz system.

Instalować poprawki zabezpieczeń

Windows, jak każde duże oprogramowanie, zawsze miał dużo luk. W miarę czasu jednak, Microsoft stara się łatać większość z nich i łatki te wypuszcza pod postacią aktualizacji Windows Update, które powinniśmy zawsze instalować jak tylko się pojawią.

Korzystać z konta użytkownika

Zawsze nasze główne konto powinno być kontem bez uprawnień administratora. Te powinniśmy otrzymywać tylko okazjonalnie, gdy przykładowo chcemy zainstalować nowe oprogramowanie czy zmienić jakieś ustawienia. Konto administratora powinno też być zabezpieczone silnym hasłem.

Szyfrować dyski i zabezpieczyć BIOS

Co nam po zabezpieczaniu kont użytkowników, gdy ktoś w każdej chwili może podłączyć się pod nasz komputer chociażby pendrivem z Linuxem w wersji live i przechwycić wszystkie nasze pliki. Dlatego też wszystkie nasze ważne pliki powinny być zabezpieczone.

Uważać, co udostępniamy

Przez jakiś czas Windows domyślnie udostępniał w sieci domowej cały nasz katalog użytkownika. Było to dosyć niebezpieczne, jeśli nasze hasło było pokroju „12345678”, każdy podłączony do sieci komputer mógł nas znaleźć i jego użytkownik przeglądać chociażby zawartość naszego pulpitu czy zainstalowane programy. Podłączając się do otwartych sieci zawsze powinniśmy ustawić tryb sieci na Publiczny.

Przesiąść się na nowsze wersje

Należy pamiętać, że Windows 7 i starsze nie są już wspierane i istnieje mnóstwo wirusów korzystających z ich luk, które najpewniej nigdy nie zostaną poprawione. Najlepszą opcją jest więc skorzystać z darmowej aktualizacji do Windowsa 10.

Jeśli to możliwe, przesiąść się na Linuxa

System ten jest dużo stabilniejszy i w domowych zastosowaniach dużo rzadziej pada ofiarą ataków. Problemem dla wielu osób jest jednak stosunkowo niewielka ilość oprogramowania tworzonego na ten system w porównaniu z systemem Microsoftu.

Linux

Korzystać tylko z zaufanych repozytoriów

Istnieją repozytoria, które oprócz chcianego oprogramowania dostarczą nam również wirusy czy innego rodzaju malware.

Używać domyślnej umaski

Jeśli ustawimy wszystkim użytkownikom pełne uprawnienia, obecność całego systemu zabezpieczeń plików straci sens. Ponadto możemy przypadkowo wystawić prywatne dane na widok każdego użytkownika komputera i każdego uruchamianego programu.

Używać konta roota tylko, gdy to potrzebne

Wszyscy użytkownicy domyślnie powinni mieć zabronione uprawnienia roota, a te powinny być zabezpieczone silnym hasłem i włączane tylko na specjalne okazje.

Nie „grzebać" w plikach systemowych

W przeciwieństwie do systemu Windows, Linux, o ile mamy uprawienia roota, daje nam praktycznie nieskończone możliwości operowania na plikach, nawet tych najistotniejszych dla systemu, które nigdy nie powinny być modyfikowane. Z tego też powodu nie powinniśmy mieszać się w nie bez odpowiedniej wiedzy i doświadczenia.

Aktualizować system

Podobnie jak w przypadku Windowsa, jest to bardzo proste o nie raz może uratować cały system. W przypadku Linuxa nie musimy nawet restartować komputera (choć jest to zalecane).

Korzystać z wersji LTS

Wersje z długoterminowym wsparciem dadzą nam pewność, że nasz system wystarczy na długo i będzie zawsze aktualny.

Tworzyć kopie zapasowe systemu

Jak już wspomniałem, w Linuxie dużo łatwiej zepsuć cokolwiek, niż w systemie Microsoftu. Z tego powodu warto do kopii zapasowej plików dołączyć także pliki konfiguracyjne systemu, czy cały system.

Zainstalować antywirusa

Systemy rodziny Linux zwykle nie dołączają antywirusów przy instalacji. Powinniśmy więc pomyśleć o jakimś. Dobrym wyborem są przykładowo Sophos lub Comodo.

Wyłączać komputer bezpiecznie

Tzw. hard reset należy przeprowadzać tylko w naprawdę koniecznych wypadkach, zbyt częste jego używanie przyczyni się do uszkodzeń w oprogramowaniu, systemie, a nawet możemy nim uszkodzić dysk twardy.

Dbać o poziom zajętości dysku

Szczególnie nośniki SSD są narażone na „zapchanie", gdyż w miarę nabierania gigabajtów, prędkość zapisu będzie zwalniać i zwalniać. Poziom zajętości dysku nie powinien nigdy przekraczać 60%.