Jak chronić się przed wirusami komputerowymi?

data aktualizacji: 2023.02.15

Zapewne nie wyobrażasz sobie dziś pracy czy rozrywki bez dostępu do Internetu. Doceniając korzyści płynące z sieci, pamiętaj jednak również o zagrożeniach. Sprawdź, jak chronić swój komputer przed wirusami oraz innym rodzajem cyberprzestępczości!

Czym są wirusy komputerowe?

Wirus to program lub fragment kodu, który instaluje się na naszym komputerze bez naszej wiedzy i zgody. Część wirusów jest tylko irytująca i nie działa destrukcyjnie na nasze oprogramowanie lub system, niestety wiele z nich prowadzi do bezpowrotnej utraty danych i uszkodzenia komputera.

Sporo wirusów tworzonych jest po to, żeby zainfekować i przejąć kontrolę nad naszym urządzeniem. Wirusy potrafią się kopiować i w ten sposób rozprzestrzeniać na kolejne urządzenia oraz sieci – podobnie jak wirusy biologiczne. Coraz większy zasięg szybkich sieci oraz niedrogi Internet bez limitu danych, z jednej strony daje duże możliwości, ale z drugiej – zwiększa szansę zainfekowania komputera, laptopa, tabletu czy smartfona niszczącymi wirusami.

Jak rozprzestrzeniają się wirusy?

Wirusy są najczęściej ukryte w powszechnie używanych programach, np. grach, przeglądarkach plików PDF czy innych plikach, które, nieświadom zagrożenia, ściągasz z Internetu. Zainfekowany plik możesz również otrzymać w wiadomości e-mail lub wgrać samodzielnie, np. kopiując pliki z pendrive czy zewnętrznego dysku.

Na szczęście nie musisz biernie przyglądać się destrukcyjnym działaniom wirusów – możesz im zapobiegać. Warto podkreślić, że przed wirusami komputerowymi można, a nawet należy się chronić, stosując przeznaczone do tego celu, dobre oprogramowanie.

Co poza wirusami zagraża naszym urządzeniom?

Wirusy to nie jedyne zagrożenia, na jakie narażone są nasze urządzenia z dostępem do sieci www. Oto inne problemy, z jakimi mierzą się twórcy oprogramowania zapobiegającemu cyberprzestępczości:

- konie trojańskie, czyli oprogramowanie podszywające się pod interesujące użytkownika aplikacje, implementujące szkodliwe, ukryte przed użytkownikiem funkcje,
- exploity – ataki wykorzystujące luki w aplikacji, sieci lub sprzęcie. Atak często jest przeprowadzany z użyciem oprogramowania lub kodu, usiłującego przejąć kontrolę nad systemem lub wykraść dane przechowywane w sieci,
- spam – niechciane lub niepotrzebne wiadomości elektroniczne, najczęściej wysyłane masowo do internautów i rozpowszechniane automatycznie poza ich wiedzą z wykorzystaniem adresów emailowych zapisanych w programie pocztowym,
- phishing – wyłudzanie informacji poprzez wiadomości mailowe podszywając się pod inną osobę lub instytucję,
- cryptolockery (ransomware) – wirusy rozpowszechniane za pomocą narzędzi exploit infiltrujące komputer przy wykorzystaniu luk w zabezpieczeniach przestarzałego, nieaktualizowanego oprogramowania,
- keyloggery – programy szpiegujące, rejestrujące znaki ASCI odpowiadające klawiszom klawiatury wciskanym przez użytkownika – w ten sposób można przechwycić dane logowania.
-

Oczywiście wymienione zagrożenia nie są wszystkimi możliwymi, na które jesteśmy narażeni. W sieci zagraża nam również oprogramowanie szpiegujące (spyware) i inne techniki oraz rodzaje ataków.

Jak skutecznie chronić nasze urządzenia przed cyberprzestępczością?

Wszelkie urządzenia, z których korzystamy, muszą być chronione przed oprogramowaniem złośliwym. Służą do tego przede wszystkim programy antywirusowe, które zapobiegają niekontrolowanemu przekazaniu danych z naszego komputera, ich zniszczeniu a także uszkodzeniu

systemu komputerowego.

Poza zainstalowaniem programu antywirusowego, warto podjąć również szereg działań, dzięki którym zmniejszamy prawdopodobieństwo skutecznego cyberataku. Należy wyróżnić wśród nich w szczególności:

- stosowanie dwuetapowej weryfikacji, zwłaszcza w przypadku dostępów do rachunków bankowych czy innych newralgicznych i istotnych dla nas danych,
- używanie silnych, unikatowych haseł do komputerów i oprogramowania, w tym sieciowego,
- unikanie połączeń z publicznymi sieciami, a jeśli jest to konieczne – korzystanie z VPN czyli Virtual Private Network. VPN tworzy szyfrowany tunel dla danych, chroniąc naszą tożsamość online, ukrywając adres IP i pozwalając na bezpieczne korzystanie z publicznych hotspotów Wi-Fi.
-

Oczywiście nie są to wszystkie możliwe sposoby ochrony przed cyberprzestępczością. Poza korzystaniem z licznych udogodnień, należy zadbać również o podstawowe BHP w pracy z siecią, np. nieudostępnianie własnych haseł osobom trzecim, czy blokowanie dostępu do ekranu albo stosowanie podwójnych zabezpieczeń.

Materiał partnera.

Źródło: https://www.infoilawa.pl/aktualnosci/item/70164-jak-chronic-sie-przed-wirusami-komputerowymi