Strefa przedsiębiorcy

2021-10-13

Czy Twój komputer jest bezpieczny?



Większość z nas używa komputera niemal codziennie - zarówno do celów prywatnych, jak i służbowych. Ale czy odpowiednio dbamy o jego bezpieczeństwo? Co możesz zrobić, aby Twoje urządzenie nie zostało zainfekowane? Sprawdź to!

Z okazji Dnia Bezpiecznego Komputera przypominamy najważniejsze zasady, jak odpowiednio zabezpieczyć sprzęt - w domu i w pracy. Myślisz, że to trudne albo kosztowne? Nic bardziej mylnego!

Proste rozwiązania techniczne

W ochronie komputerów przed różnego rodzaju zagrożeniami mogą nam pomóc proste rozwiązania techniczne, o których warto pamiętać:

- Przede wszystkim - zabezpiecz dostęp do swojego komputera hasłem lub innym bezpiecznym sposobem (jeśli masz taką możliwość np. odciskiem palca, rozpoznawaniem twarzy).
- Korzystaj z wbudowanej zapory sieciowej (firewall) oraz oprogramowania antywirusowego, które

chroni sprzęt przed szkodliwymi programami, ale także zwiększa ochronę naszej sieci oraz pozwala na filtrowanie stron internetowych pod kątem ich szkodliwości.
- Dbaj o regularne aktualizacje systemu operacyjnego i wszystkich zainstalowanych programów – to może Cię ustrzec przed szkodliwym oprogramowaniem i innymi zagrożeniami w sieci. Jeśli to możliwe, ustaw automatyczne aktualizacje.

WAŻNE! Korzystaj wyłącznie z legalnego oprogramowania, pozyskanego z oficjalnego źródła – od producenta lub dostawcy.

- Dodatkowo - jeśli podłączasz do komputera np. pendrive'y – skanuj je pod kątem wirusów i złośliwego oprogramowania. A najlepiej - nie podłączaj urządzeń, które nie należą do Ciebie – mówi Zuzanna Polak z CSIRT NASK.

Bezpieczne korzystanie z internetu

Internet daje nam dużo możliwości, ale wiąże się też z wieloma zagrożeniami dla naszych komputerów.

Korzystanie na co dzień z wielu urządzeń i usług internetowych może powodować, że stajemy się mniej uważni, a tym samym - bardziej podatni na różnego rodzaju niebezpieczeństwa i ataki, które w naszą stronę kierują cyberprzestępcy. Pamiętajmy o tym, aby w sieci zawsze zachowywać czujność.

Oto kilka podstawowych zasad, które pomogą uchronić Twój komputer przed zainfekowaniem:

- Nie otwieraj podejrzanych załączników i nie klikaj w nietypowe linki – zwłaszcza te, pochodzące od nieznanych nadawców. Mogą zawierać szkodliwe oprogramowanie, które - zanim się obejrzysz - doprowadzą do utraty Twoich plików (np. dokumentów, fotografii), a nawet - danych (np. logowania do bankowości elektronicznej).
- Używaj silnych haseł, a jeśli jest to możliwe - włącz uwierzytelnianie dwuskładnikowe. W przypadku korzystania z portali społecznościowych, nie zapominaj także o ustawieniach prywatności.
- Nie lekceważ komunikatów o zagrożeniach, które - podczas przeglądania stron internetowych - mogą być wyświetlane przez system lub w przeglądarce.
- Nigdy nie podawaj swoich prywatnych danych, zwłaszcza danych logowania, kart płatniczych, nawet jeżeli prosi o nie w sieci osoba, którą znasz. Jej konto mogło zostać zhakowane. Pracownicy banków, urzędów i policji również nigdy nie pytają o takie informacje.

I jeszcze jedno - jeśli trafisz w sieci na podejrzane strony, koniecznie to zgłoś:

- W przypadku nielegalnych treści do Dyżurnet.pl
- W przypadku złośliwych domen do CERT Polska

Bezpieczeństwo Twojej sieci

- Na bezpieczeństwo naszego komputera wpływa nie tylko świadome i rozsądne korzystanie z internetu, ale również sam sprzęt, który pozwala łączyć się z siecią – mówi Zuzanna Polak z CSIRT NASK.

Jak o niego zadbać?

Sprawdź, czy Twój router jest zaktualizowany, jeśli nie – zaktualizuj go. Nie wiesz jak? Markę i model routera znajdziesz na urządzeniu. Następnie poszukaj w internecie instrukcji, jak to zrobić. Aby zwiększyć swoje bezpieczeństwo, koniecznie zmień także fabrycznie nadane hasło. Pamiętaj, aby było ono silne – minimum 15 znaków. Dobrą praktyką jest także posiadanie kilku sieci, np. do pracy, dla gości i dla innych urządzeń.

Chcesz zrobić jeszcze więcej? Oto dodatkowe wskazówki - dla zaawansowanych:

1. Wyłącz dostęp zdalny, który zwiększa ryzyko włamania do sieci domowej z internetu.
2. Wyłącz funkcję Universal Plug and Play (UPnP), która może być wykorzystywana przez cyberprzestępców, w celu ominięcia zabezpieczeń Twojego routera.
3. Aby uniknąć podłączenia nieautoryzowanych urządzeń do Twojej sieci, wyłącz chronioną konfigurację Wi-Fi (WPS).

Instrukcje z podstawowymi ustawieniami routera znajdziesz na stronie producenta. Większość urządzeń można konfigurować przez przeglądarkę. Jeżeli nie potrafisz wykonać konfiguracji samodzielnie, poproś o pomoc - członka rodziny, kolegę z pracy czy znajomego.

Bezpieczeństwo komputera służbowego

Przede wszystkim - nie używaj sprzętu służbowego do spraw prywatnych (ani prywatnego do spraw służbowych). Jest on przeznaczony tylko do Twojego użytku, zatem nie pożyczaj ani nie udostępniaj go nikomu - przechowuj zawsze w bezpiecznym miejscu.

Wiadomości służbowe wysyłaj wyłącznie za pośrednictwem poczty służbowej lub poprzez wyznaczone do tego w Twojej firmie komunikatory. Jeśli odchodzisz od komputera, zablokuj go (zwłaszcza, gdy pracujesz w miejscu publicznym).

Koniecznie zapoznaj się z polityką bezpieczeństwa w Twojej organizacji i wszelkie nieprawidłowości lub problemy techniczne zgłaszaj do odpowiednich osób.

Więcej informacji o tym, jak dbać o swoją cyberhigienę znajdziecie na naszej stronie GOV.pl/cyfryzacja oraz w dostępnej na GOV.pl bazie wiedzy na temat cyberbezpieczeństwa.

Źródło: Cyfryzacja KPRM

Źródło: https://paliwa.pl/strona-startowa/archiwum/czy-twoj-komputer-jest-bezpieczny