**Internauto! Czy wiesz jak dbać o swoje cyberbezpieczeństwo?**

**Każdego dnia tysiące użytkowników internetu staje się ofiarami cyberprzestępstw. Kradzież danych, wyłudzenia czy złamanie zabezpieczeń do kont bankowych to tylko wierzchołek góry lodowej. Problem jest na tyle rozległy, że może dotknąć wszystkich - niezależnie od wieku, płci czy statusu społecznego. Jak się przed nim chronić? Jak dbać o swoje cyberbezpieczeństwo?**

**Cyberbezpieczeństwo - o co w tym chodzi?**

**Cyberbezpieczeństwo** to nic innego, jak zbiór metod mających na celu zapobieganie cybernetycznym atakom i złośliwemu oprogramowaniu komputerowemu. Obejmuje ono różne praktyki, w tym szyfrowanie danych, wdrażanie programów antywirusowych, stosowanie haseł i innych metod uwierzytelniania, a także przestrzeganie określonych procedur związanych z ochroną danych. Współcześnie, gdy technologia jest coraz bardziej powszechna w codziennym życiu, zagrożenia związane z cyberprzestępczością każdego dnia stają się coraz większe.



Dobre praktyki związane z bezpieczeństwem cyfrowym pomagają nie tylko chronić dane przed atakami, ale również **budować zaufanie klientów** w firmach, w których są one stosowane. Dodatkowo, można dzięki nim uniknąć dodatkowych kosztów związanych z odzyskiwaniem plików i utratą renomy w oczach swoich kontrahentów. Warto zatem mieć na uwadze, że cyberbezpieczeństwo jest nieodłącznym elementem działalności w dobie postępu technologicznego i powinno być traktowane z należytą uwagą.

**Największe zagrożenia w sieci**

W dzisiejszych czasach, jednym z największych zagrożeń dla użytkowników internetu są **ataki phishingowe**. Ich celem jest wyłudzenie danych poufnych, takich jak hasła czy numery kart kredytowych, poprzez podszycie się pod istniejącą firmę, zachęcenie do kliknięcia w link wysłany mailem lub wykorzystanie innych metod manipulacji. Na ten moment bardzo często spotykamy się również z **atakami malware**, a więc atakami przeprowadzanymi przy użyciu złośliwego oprogramowania ([wirusy](https://cyberszkolenia.pl/trojan-jak-chronic-sie-przed-niebezpiecznym-wirusem/)). Mogą one nie tylko blokować urządzenia bądź sieci, ale nawet doprowadzić do kradzieży danych czy wyłudzeń finansowych. Osoby korzystające z publicznego, niezabezpieczonego WiFi, obarczone są dodatkowym ryzykiem.

**Jak podnieść poziom swojego cyberbezpieczeństwa?**

Istnieje wiele sposobów na zwiększenie swojego bezpieczeństwa podczas korzystania z internetu. Kluczowe jest **regularne aktualizowanie oprogramowania** i sprzętu, co pozwoli uniknąć wykorzystania znanych już cyberprzestępcom luk w zabezpieczeniach. Równie ważną rolę odgrywa także **tworzenie mocnych haseł**, które powinny zostać zbudowane z różnorodnego ciągu znaków. Nie trzeba być hakerem, aby złamać hasło pokroju “12345” czy “11111” - warto mieć to na uwadze.

W celu zwiększenia poziomu cyberbezpieczeństwa dobrze jest zainstalować na swoim komputerze lub urządzeniu mobilnym **antywirusa**, który będzie je chronić przed wieloma zagrożeniami. Korzystanie z wirtualnej sieci prywatnej (VPN) dodatkowo zwiększy bezpieczeństwo transmisji danych. Nie należy również zapominać o regularnym tworzeniu kopii zapasowych - w przypadku kradzieży danych, mając ich backup łatwo będzie można je odzyskać.

Ostatnim, ale nie mniej ważnym elementem wchodzącym w skład cyberbezpieczeństwa jest **świadomość**. Choć może wydawać się to banalne, należy regularnie edukować się z zakresu zagrożeń w sieci, aby móc skutecznie rozpoznawać czyhające na każdym kroku oszustwa. W tym celu można zajrzeć do internetu lub, jeśli jesteś przedsiębiorcą i chcesz uświadomić swój zespół, możesz zdecydować się na dedykowane [cyber szkolenia](https://cyberszkolenia.pl/) z tego zakresu.