**Najczęstsze błędy użytkowników internetu, które prawdopodobnie popełniasz**

**Żyjemy w erze cyfrowej, gdzie nasze codzienne życie, praca, a nawet relacje osobiste są nierozerwalnie związane z internetem. Choć to potężne narzędzie otwiera przed społeczeństwem niezliczone możliwości, to niestety, wymaga od swoich użytkowników odpowiedzialnego podejścia i ostrożności, o czym nie wszyscy zdają się pamiętać.**

Cyberbezpieczeństwo nie jest już zagadnieniem zarezerwowanym tylko dla specjalistów [IT](https://cyberszkolenia.pl/oferta/konsulting-i-audyty-it/). Każdy z nas, jako użytkownik internetu, powinien mieć chociażby podstawową świadomość zagrożeń w sieci oraz znać zasady, które pomogą mu się bezpiecznie po niej poruszać. Wydawać by się mogło, że obecnie społeczeństwo wie na ten temat więcej, niż kiedykolwiek wcześniej. Niestety, mimo to wielu użytkowników internetu popełnia liczne błędy na porządku dziennym, co stanowi spore zagrożenie nie tylko dla ich sprzętu elektronicznego, ale również danych osobowych.

**Błąd 1: Tworzenie banalnych haseł**

**Błędem popełnianym notoryczne zarówno przez nowych, jak i starych użytkowników internetu, jest stosowanie łatwych do odgadnięcia haseł.** Proste ciągi znaków (“12345”, “hasło”), czy powszechnie dostępne osobiste informacje (imię, nazwisko, data urodzenia, imię zwierzaka) nie sprawiają problemu w zapamiętaniu, jednak stanowią słabe zabezpieczenie przed cyberprzestępcami. Tak nieskomplikowane hasła hakerzy - przy użyciu odpowiednich programów - są w stanie złamać w zaledwie kilka sekund, uzyskując tym samym dostęp do Twoich prywatnych danych, w tym tych dotyczących finansów lub miejsca zamieszkania.

*Polecamy:* [Jak stworzyć bezpieczne hasło? | Praktyczny poradnik dla każdego](https://cyberszkolenia.pl/jak-stworzyc-bezpieczne-haslo/)

**Błąd 2: Używanie niezabezpieczonych sieci Wi-Fi**

**Korzystanie z publicznych sieci Wi-Fi, na przykład w kawiarniach, hotelach czy na lotniskach, jest kolejnym błędem, który może narazić nas na cyberzagrożenia.** Chociaż rozwiązanie to jest niezwykle wygodne oraz oczywiście darmowe, stanowi również łatwy cel dla hakerów. Publiczne Wi-Fi pozbawione jest jakichkolwiek zabezpieczeń, co pozwala cyberprzestępcom przechwycić wszystkie dane, które przesyłasz w trakcie korzystania z sieci - w tym hasła i informacje o karcie kredytowej.



**Błąd 3: Klikanie w podejrzane linki**

**Klikanie w podejrzane linki w e-mailach lub na stronach internetowych to kolejny, bardzo powszechny błąd, który najczęściej popełniają osoby starsze.** Cyberprzestępcy często korzystają z różnego rodzaju socjotechnik, takich jak [phishing](https://cyberszkolenia.pl/phishing-czyli-najpopularniejsze-oszustwo-internetowe-ostatnich-lat/), aby skłonić użytkowników sieci do kliknięcia w zainfekowany adres URL. Link ten może zainstalować złośliwe oprogramowanie na urządzeniu lub przenieść do fałszywej witryny internetowej, która będzie próbować wykraść Twoje dane do logowania oraz inne informacje.

**Błąd 4: Brak aktualizacji**

**Nieaktualizowanie swoich systemów i wykorzystywanego oprogramowania jest dość powszechnym błędem w kontekście bezpieczeństwa cybernetycznego.** Wbrew pozorom, aktualizacje nie służą tylko do wprowadzania nowych funkcji i usprawnień. Ich rola nie kończy się również na zwiększeniu wydajności aplikacji. Zazwyczaj zawierają one łatki bezpieczeństwa, które usuwają znane luki, przez które hakerzy mogą dostać się do Twojego systemu. Ignorowanie nowych wersji posiadanych programów to zatem jak pozostawienie otwartych drzwi do domu dla potencjalnych włamywaczy.

**Błąd 5: Brak antywirusa**

**Pomimo wielu kampanii mających szerzyć świadomość cybernetyczną, wielu użytkowników internetu wciąż nie korzysta z ochrony antywirusowej na swoich urządzeniach.** W dzisiejszych czasach, zagrożenia online są bardziej zaawansowanie i zróżnicowane, niż kiedykolwiek wcześniej. Złośliwe oprogramowanie - malware -, może przybierać wiele różnych form, od [trojanów](https://cyberszkolenia.pl/trojan-jak-chronic-sie-przed-niebezpiecznym-wirusem/) i robaków, aż po [ransomware](https://cyberszkolenia.pl/ransomware-co-to-jest/) czy spyware. Bez odpowiedniej tarczy ochronnej w postaci programu antywirusowego, jako internauta jesteś narażony z ich ramienia na utratę danych, kradzież informacji osobistych, włamanie na konto bankowe, a także zdalne przejęcie kontroli nad Twoim komputerem przez nieautoryzowane osoby.

**Błąd 6: Brak dyskrecji na social media**

**Choć social media stały się integralną częścią naszego codziennego życia, to często nie zdajemy sobie sprawy z zagrożeń, które mogą nieść za sobą.** Udostępnianie zbyt dużej ilości informacji prywatnych w mediach społecznościowych, takich jak Facebook, Instagram, Twitter czy LinkedIn, może prowadzić do nieprzyjemnych konsekwencji. Dane osobowe, w tym pełne imię i nazwisko, data urodzenia, adres domowy, miejsce pracy, informacje o rodzinie, a nawet Twoje zwyczaje i hobby, mogą zostać wykorzystane przez osoby o złych zamiarach w różnoraki sposób.

**Błąd 7: Samowolne instalacje**

**Samowolne instalacje oprogramowania lub aplikacji bez weryfikacji to kolejna powszechna pułapka, w którą łatwo wpadają internauci w każdym wieku.** Cyberprzestępcy ukrywają złośliwe pliki w atrakcyjnych pakietach - na przykład w darmowych grach lub fałszywych aktualizacjach oprogramowania. Osoby, które nie sprawdzają dokładnie źródeł, z których ściągają programy, w ten sposób instalują na swoich komputerach wirusy, które działając w tle szkodzą całemu systemowi.

Ponadto, niektóre programy, nawet te z zaufanych źródeł, mogą zawierać tzw. "**bundleware**". Są to dodatkowe aplikacje, które są pobierane razem z głównym programem, chyba, że użytkownik zdecyduje się je odznaczyć podczas procesu instalacji. Często te dodatkowe aplikacje są niepotrzebne, a niekiedy nawet i szkodliwe.

**Błąd 8: Niewylogowanie z kont**

**Pozostawianie swoich kont internetowych zalogowanych, zwłaszcza na publicznych lub współdzielonych urządzeniach, jest poważnym błędem, który może prowadzić do nieautoryzowanego dostępu osób trzecich do Twoich prywatnych informacji.** Nawet jeżeli uważasz, że komputer z którego korzystasz jest bezpieczny, nigdy nie wiadomo, czy nie zostanie skradziony. Wówczas zalogowane konta na nim pozostawione mogą stać się bardzo łatwym celem dla złodziei.

**Błąd 9: Brak szkoleń**

**Brak regularnych szkoleń z zakresu cyberbezpieczeństwa dla pracowników jest jednym z największych błędów, które może popełnić jakakolwiek firma.** Personel to jednocześnie pierwsza linia obrony, jak i najsłabsze ogniwo w kontekście ataków hakerskich, ponieważ wiele z nich opiera się na wykorzystaniu ludzkich błędów. Cyberprzestępcy mogą na przykład podszywać się pod zaufane osoby lub organizacje, aby nakłonić pracowników danej placówki do ujawnienia poufnych informacji lub do kliknięcia w złośliwy link. Bez odpowiedniego [cyberszkolenia](https://cyberszkolenia.pl/), Twoi podwładni mogą nie być świadomi czyhających w sieci zagrożeń i nie wiedzieć, jak na nie reagować.

**Podsumowanie**

Podsumowując, cyberbezpieczeństwo to obszar, który wymaga od nas wszystkich ciągłego zaangażowania i czujności. Wymienione w artykule błędy, chociaż częste, są łatwe do uniknięcia, jeśli podejdziemy do nich z odpowiednią ostrożnością i wiedzą. Pamiętajmy, że w erze cyfrowej nasze bezpieczeństwo w sieci jest równie ważne, co to fizyczne. Edukacja i zapobiegawczość są najważniejszymi narzędziami w walce z cyberprzestępczością. Kontynuuj więc naukę, szkolenia i praktykowanie bezpiecznych nawyków online, aby zawsze być o krok przed hakerami.

**Bezpieczeństwo w Internecie zaczyna się od Ciebie.**