

Dzień Bezpiecznego Internetu



Dzień Bezpiecznego Internetu

Dzień Bezpiecznego Internetu obchodzony jest co roku w lutym, by promować odpowiedzialne i bezpieczne korzystanie z sieci. To wydarzenie organizowane w wielu krajach, podczas którego podejmowane są działania edukacyjne skierowane do dzieci, młodzieży, rodziców i nauczycieli.

W tym dniu organizowane są warsztaty, konferencje i akcje informacyjne, które mają na celu zwiększenie świadomości na temat zagrożeń w internecie oraz sposobów radzenia sobie z nimi.



Internet



Internet to globalna sieć komputerowa, która łączy miliony urządzeń na całym świecie, umożliwiając komunikację, wymianę informacji i dostęp do zasobów online. Powstał w latach 60. XX wieku jako projekt wojskowy, a obecnie jest jednym z najważniejszych narzędzi w życiu codziennym.

Internet umożliwia szybki dostęp do wiedzy, komunikację z ludźmi na całym świecie, zakupy online, pracę zdalną oraz rozrywkę. Jest także narzędziem edukacyjnym, które ułatwia naukę i rozwój zainteresowań. Jednak korzystanie z internetu wymaga odpowiedzialności i świadomości zagrożeń.

Bezpieczny internet

Internet to przestrzeń, która oferuje wiele możliwości, takich jak nauka, komunikacja i rozrywka. Jednak należy pamiętać, że w sieci czyha wiele zagrożeń. Bezpieczny internet to taki, w którym użytkownicy chronią swoje dane, unikają nieznanych i podejrzanych stron oraz korzystają z odpowiednich zabezpieczeń, takich jak programy antywirusowe czy zapory sieciowe. Warto również pamiętać o kulturze osobistej i przestrzeganiu zasad etykiety internetowej.



Dbaj o swoje bezpieczeństwo



Internet to miejsce, gdzie można znaleźć zarówno prawdziwe, jak i fałszywe informacje. Nie ufaj bezgranicznie każdej treści, którą znajdziesz. Weryfikuj informacje, zwracaj uwagę na źródło i bądź ostrożny wobec wiadomości, które obiecują łatwe zyski, proszą o Twoje dane lub zawierają linki do nieznanych stron. Korzystanie z zaufanych stron to klucz do bezpiecznego surfowania po internecie. Strony takie są oznaczone symbolem kłódki obok adresu URL, posiadają certyfikat SSL i jasno określają swoje zasady ochrony danych.

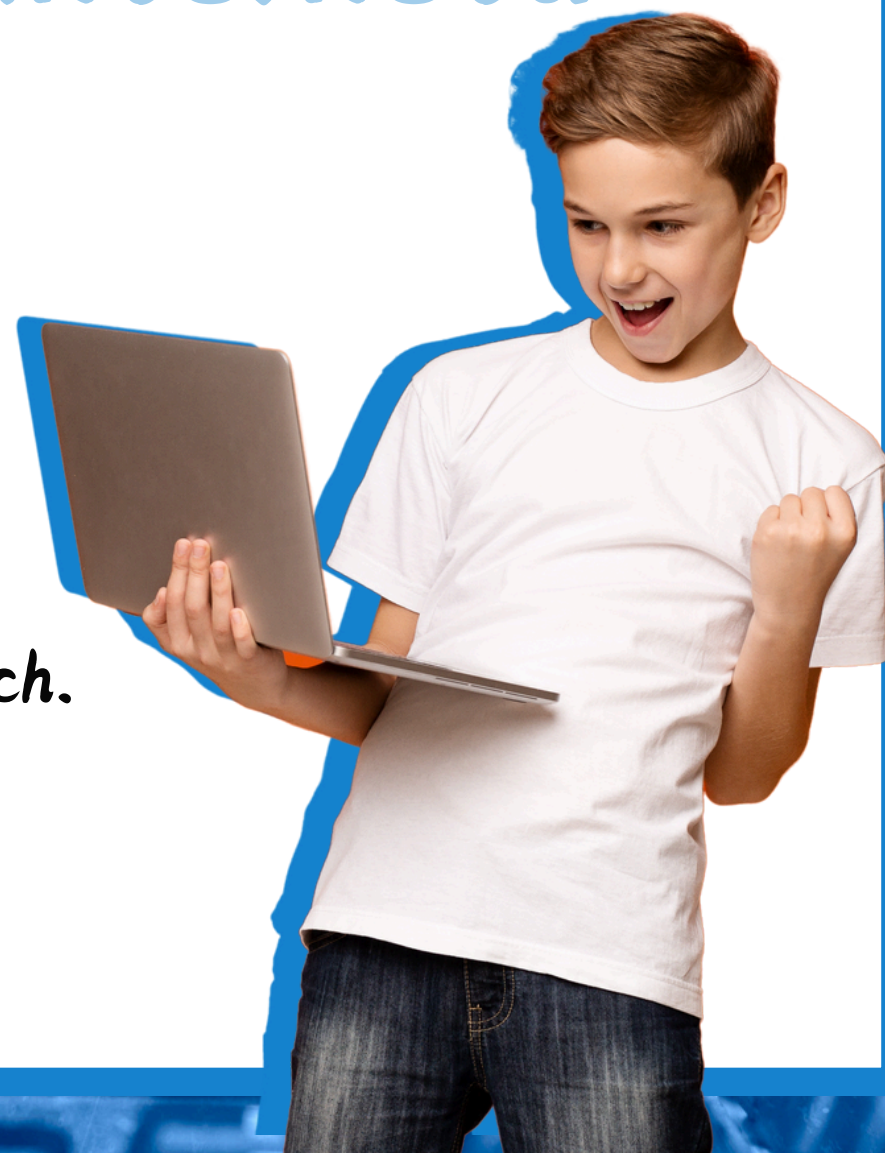
Chroń swoje dane



Twoje dane osobowe są cenne i mogą zostać wykorzystane przez osoby nieuczciwe, np. w celu kradzieży tożsamości. Aby je chronić, nigdy nie podawaj swoich danych osobowych, takich jak adres, numer telefonu czy hasła, na nieznanych stronach internetowych lub w wiadomościach od nieznanomych. Używaj trudnych do odgadnięcia haseł i regularnie je zmieniaj. Korzystaj z ustawień prywatności na portalach społecznościowych, aby kontrolować, kto ma dostęp do Twoich informacji.

Zasady bezpiecznego korzystania z internetu

1. Nie podawaj danych osobowych.
2. Twórz silne hasła.
3. Korzystaj z zaufanych stron.
4. Nie klikaj w podejrzane linki.
5. Aktualizuj oprogramowanie.
6. Używaj programów antywirusowych.
7. Zgłaszaj nieodpowiednie treści.
8. Szanuj innych w sieci.



Szanuj prywatność

Prywatność w internecie to prawo każdego użytkownika. Publikowanie zdjęć, danych czy informacji o innych bez ich zgody jest nie tylko niegrzeczne, ale w wielu przypadkach także nielegalne. Zanim coś opublikujesz, zastanów się, czy nie naruszasz czyjejś prywatności. Szanując granice innych, budujesz kulturę wzajemnego szacunku w sieci.



Hasła dostępu



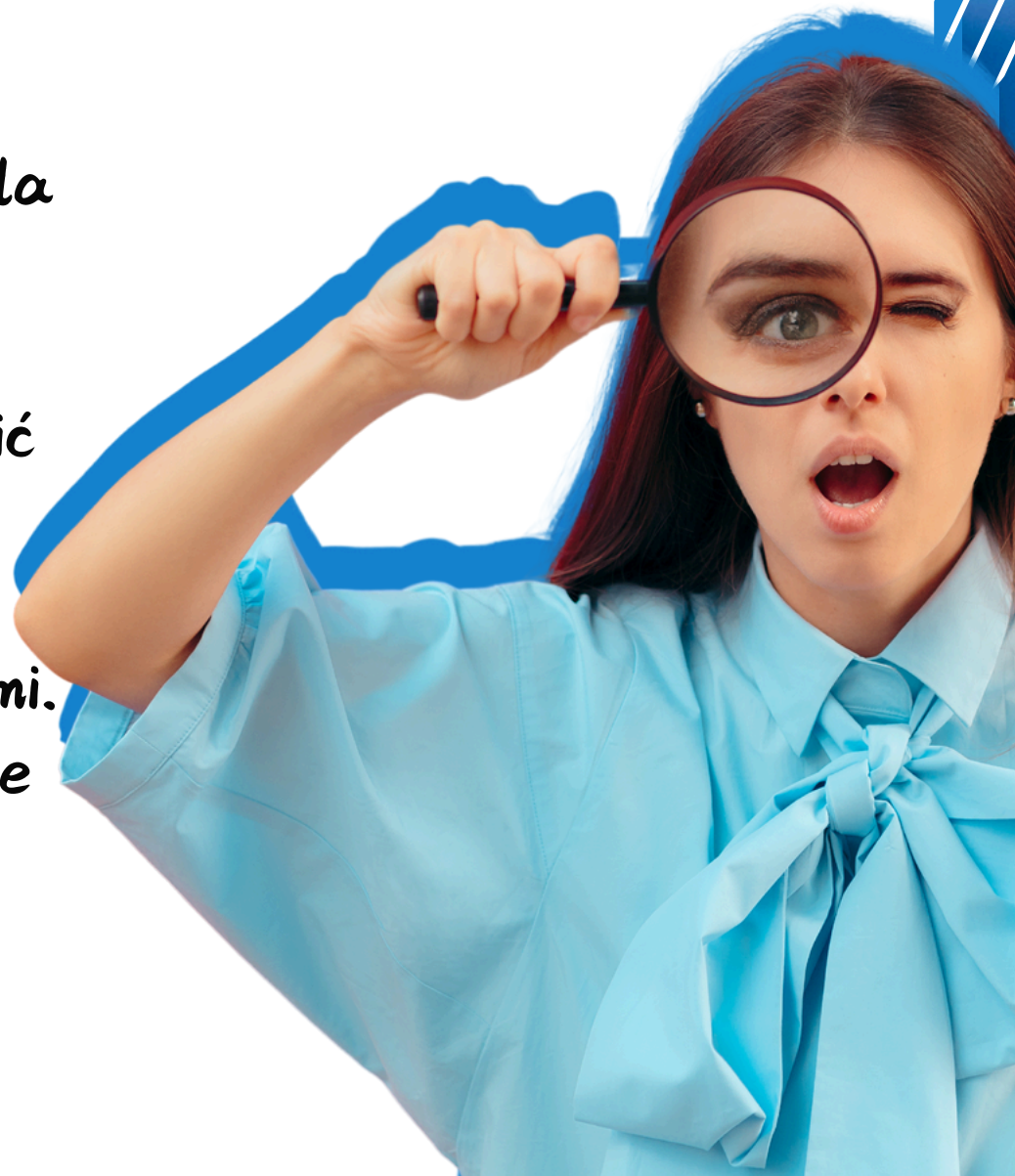
Silne hasło to podstawa bezpieczeństwa w internecie.

Powinno być trudne do odgadnięcia, składać się z co najmniej 12 znaków, w tym liter, cyfr i znaków specjalnych.

Nigdy nie używaj tego samego hasła do różnych kont. Używaj menedżera haseł, aby łatwo zarządzać swoimi hasłami i zapewnić ich bezpieczeństwo.

Tryb prywatny

Tryb prywatny w przeglądarce internetowej to funkcja, która pozwala przeglądać strony bez zapisywania historii, plików cookies czy danych logowania. Dzięki temu możesz chronić swoje dane podczas korzystania z komputerów publicznych lub współdzielonych z innymi użytkownikami. Pamiętaj jednak, że tryb prywatny nie zapewnia pełnej anonimowości w internecie – dostawcy usług internetowych wciąż mogą śledzić Twoje działania.



Wirusy

Wirus komputerowy to złośliwe oprogramowanie, które potrafi się rozprzestrzeniać i uszkadzać pliki lub systemy komputerowe. Wirusy często są ukryte w załącznikach e-mail, plikach pobranych z internetu lub na zainfekowanych stronach. Aby chronić się przed wirusami, korzystaj z programów antywirusowych i nie otwieraj podejrzanych plików.

Ataki hackerskie to działania mające na celu przejęcie kontroli nad systemami komputerowymi, wykradanie danych lub zaktócanie ich działania. Mogą być wymierzone w osoby prywatne, firmy, a nawet rządy. Aby chronić się przed atakami, stosuj silne hasła, aktualizuj oprogramowanie i unikaj podejrzanych linków.



Cyberzagrożenia

Cyberzagrożenia to różnego rodzaju niebezpieczeństwa, które mogą wystąpić podczas korzystania z internetu. Do najczęstszych należą wirusy, ataki hackerskie, phishing czy spyware. Mogą prowadzić do utraty danych, kradzieży pieniędzy lub tożsamości. Aby się chronić, korzystaj z aktualnych programów antywirusowych, unikaj klikania w podejrzane linki i regularnie aktualizuj oprogramowanie.



Scam

Scam to internetowe oszustwo, którego celem jest wyłudzenie pieniędzy lub danych osobowych. Może przyjmować formę fałszywych wiadomości, ofert pracy czy loterii. Zawsze sprawdzaj autentyczność takich ofert i nigdy nie podawaj swoich danych obcym.



SCAM

Hejt w internecie

Hejtowanie to publikowanie w internecie negatywnych komentarzy, które mają na celu sprawienie przykrości lub poniżenie innych. Jest to poważny problem, który może prowadzić do niskiej samooceny i problemów psychicznych u ofiar. Zamiast hejtu, wybieraj słowa wsparcia.



Mowa nienawiści to używanie obraźliwego języka, który poniża lub obraża innych ze względu na ich pochodzenie, religię, wygląd czy przekonania. Reaguj na takie zachowania i zgłaszaj je odpowiednim osobom.

Szacunek

Internet jest miejscem, gdzie spotykają się ludzie z różnych kultur, o różnych poglądach i doświadczeniach. Szanuj ich, tak jak chciałbyś być szanowany. Nie obrażaj, nie wyśmiewaj i nie krytykuj innych bez powodu.



Sztuczna inteligencja – AI

Sztuczna inteligencja (AI) to technologia, która umożliwia maszynom wykonywanie zadań wymagających inteligencji ludzkiej, takich jak rozpoznawanie mowy, analiza danych czy podejmowanie decyzji.



AI ma wiele zalet, takich jak automatyzacja procesów, ale niesie również ryzyko, zwłaszcza jeśli jest używana w nieuczciwych celach, np. do manipulacji informacją lub tworzenia deepfake'ów. Korzystając z AI, zawsze weryfikuj, jakie dane przetwarza i w jakim celu.

AI w rękach oszustów



Sztuczna inteligencja może być używana przez oszustów do tworzenia fałszywych wiadomości, deepfake'ów czy manipulacji informacją. Dlatego ważne jest, aby być czujnym i weryfikować autentyczność treści, które widzisz w internecie. AI jest potężnym narzędziem, które może być używane zarówno w dobrych, jak i złych celach.

Czas przed monitorem

Zbyt długie korzystanie z urządzeń elektronicznych może prowadzić do zmęczenia wzroku, bólu głowy i problemów z koncentracją. Ustal limity czasu spędzanego przed ekranem, rób regularne przerwy i spędzaj czas na aktywnościach fizycznych.

