2023

CYBER BEZPIECZNE DZIECIAKI

CYBERBEZPIECZEŃSTWO

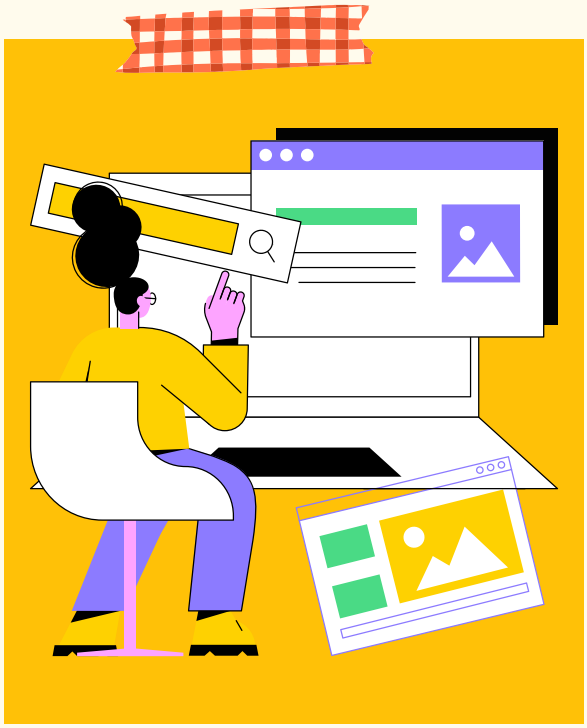
Projekt realizowany przy wsparciu finansowym Województwa Małopolskiego.

MAŁOPOLSKA

FUNDACJA FYLION

INTERNET

Witajcie w fascynującym świecie internetu! Dzięki niemu możemy odkrywać nowe miejsca, poznawać ciekawych ludzi i zdobywać niesamowitą wiedzę. Ale czy wiecie, że w tym wirtualnym świecie tak samo, jak w rzeczywistości, ważne jest, aby dbać o swoje bezpieczeństwo?



Internet to miejsce pełne możliwości, ale również ukrytych zagrożeń. To jak podróż do nieznanego kraju – potrzebujemy mapy, aby znaleźć właściwą drogę, oraz przewodnika, aby unikać niebezpieczeństw. To właśnie w tym celu istnieje pojęcie "cyberbezpieczeństwa".

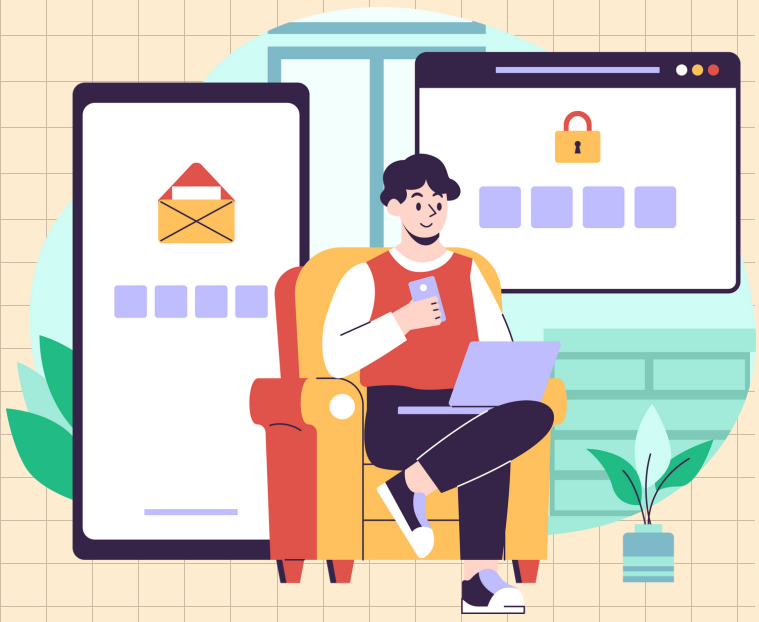
CZEGO SIĘ DOWIESZ:

- CO TO JEST CYBERBEZPIECZEŃSTWO?
- CZY KAŻDY W INTERNECIE JEST ANONIMOWY?
- JAK CHRONIĆ SIĘ W INTERNECIE
- CZY TO CO WIDZIMY W SIECI JEST PRAWDZIWE
- JAK REAGOWAĆ NA CYBERPRZEMOC
- SŁOWNIK POJĘĆ I ZNAKÓW

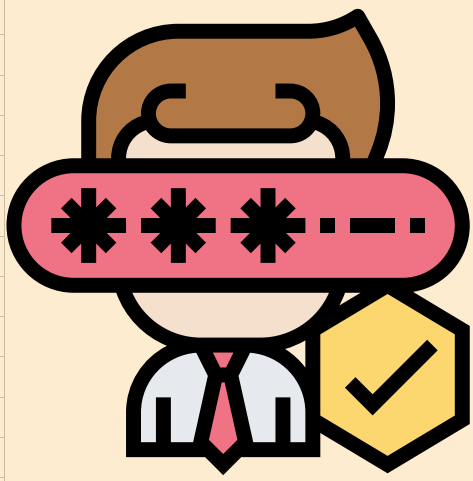
CYBER BEZPIECZEŃSTWO

Cyberbezpieczeństwo to zestaw zasad, technik i działań, które pomagają nam zachować bezpieczeństwo w sieci.

Dzięki niemu możemy unikać oszustw, chronić nasze dane oraz wiedzieć, jak reagować w przypadku niebezpieczeństwa. To jak tarcza, która nas ochrania przed nieznanych wrogami w wirtualnym świecie.



GŁÓWNE ZASADY CEBERBEZPIECZEŃSTWA



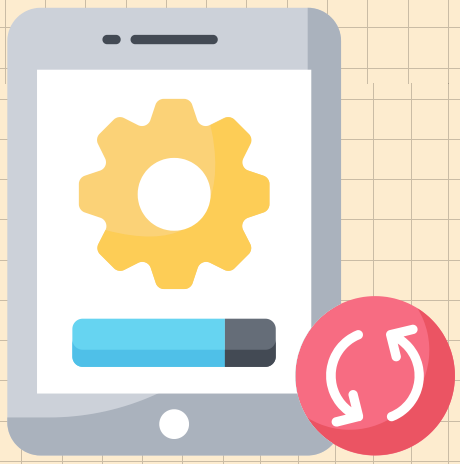
1. **Ostrzegawcze Linki:** Zanim klikniesz w link, dokładnie się przyjrzyj jego adresowi. Czasami oszuści udają, że prowadzą do znanych stron, ale w rzeczywistości mogą Cię skierować na fałszywą stronę, gdzie mogą próbować wykraść Twoje dane. Jeśli nie jesteś pewny, czy link jest bezpieczny, lepiej go nie otwieraj.

2. Mocne Hasła: Twórz hasła jak superbohater! Używaj długich kombinacji liter, cyfr i znaków specjalnych. Unikaj haseł łatwych do zgadnięcia, takich jak "123456" czy "haslo123".

3. Przyjaciele Online: Wirtualny świat ma wiele cudownych możliwości, ale nie każdy, kto tam się pojawia, jest tym, za kogo się podaje. Uważaj na osoby, które próbują nawiązać kontakt, szczególnie jeśli nie znasz ich osobiście. Nie dodawaj nikogo do znajomych, jeśli nie jesteś pewny, że jest to bezpieczne.

GŁÓWNE ZASADY CEBERBEZPIECZEŃSTWA

5. Aktualizacje to Klucz: Twój komputer, tablet czy telefon potrzebują regularnych aktualizacji oprogramowania. Dzięki nim twój sprzęt jest chroniony przed nowymi zagrożeniami. Często cyberprzestępcy wykorzystują luki w zabezpieczeniach, więc trzymaj się z dala od przestarzałych wersji oprogramowania.



6.Dziel Się Mądrze: Twoje dane osobowe, takie jak imię, adres czy numer telefonu, są cenne. Nie udostępniaj ich publicznie w internecie. Kiedy rejestrujesz się na stronach czy w aplikacjach, udostępnij tylko niezbędne informacje. Dzielenie się za dużą ilością danych może uczynić Cię narażonym na oszustwa lub kradzież tożsamości.

7. Ustawienia Prywatności: Znajdź ustawienia prywatności w swoich kontach online. Decyduj, kto może widzieć Twoje treści.

Anonimowość w Internecie:
Bądź Ostrożnym Odkrywcą

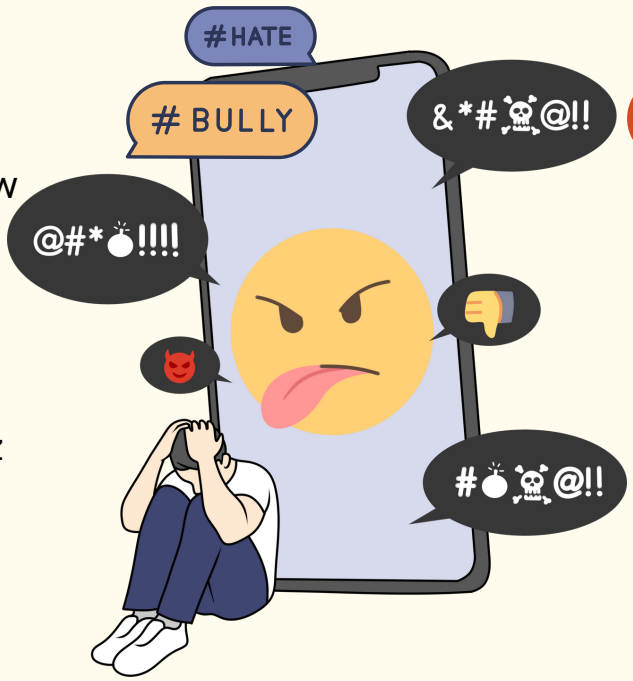
Wirtualny świat może wydawać się tajemniczy i niewidzialny, ale pamiętaj, że **nikt nie jest całkowicie anonimowy w sieci.** Jeśli zrobisz coś nieodpowiedniego lub złego, istnieje ryzyko, że zostaniesz wykryty.

Dlaczego nie jesteś całkowicie anonimowy:

1.**Ślady Cyfrowe:** Twoje działania online pozostawiają ślady. Komentarze, posty, wiadomości - to wszystko może być przypisane do Ciebie.

2. Adres IP: Każde urządzenie podłączone do internetu ma swój unikalny adres IP. To jak numer seryjny Twojego urządzenia, który można wykorzystać do identyfikacji.

3. Konta: Większość stron wymaga rejestracji. Jeśli posiadasz konto, zostawiasz swoje dane, a to może pomóc w ustaleniu tożsamości.



4. Związane Dane: Czasami osoby lub instytucje mają możliwość połączenia danych z różnych źródeł, co może prowadzić do ujawnienia tożsamości.

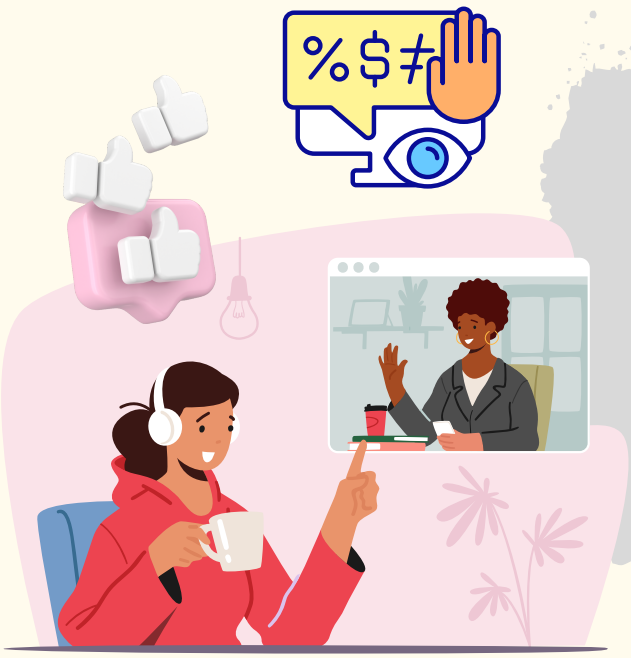
Jak zachować bezpieczeństwo:

Odpowiedzialność w Działaniach: Pamiętaj, że to, co robisz online, ma konsekwencje. Unikaj negatywnych komentarzy czy nieodpowiednich postów.

Ostrożność w Kontach: Nie próbuj przejmować kont innych osób ani nie dawaj swoich danych nieznajomym. To może narazić Ciebie i innych na ryzyko.

Zdjęcia i Prywatność: Nie wysyłaj czy nie udostępniaj zdjęć innych osób bez ich zgody. Szanuj czyjąś prywatność, tak jak oczekujesz, że ktoś zrobi to samo dla Ciebie.

Zachowaj Dobre Słowa: Twórz treści pozytywne i konstruktywne. Słowa mają moc, a to, co piszesz, może mieć wpływ na innych.



Pamiętaj, że bezpieczne zachowanie w sieci to oznaka odpowiedzialności i szacunku dla innych. Bądź mądrym odkrywcą, a Twój ślad w wirtualnym świecie będzie pełen pozytywnych doświadczeń! 🌐🛡️

Jak zachować bezpieczeństwo:

ROZMOWY

Z OBCYMI PRZEZ INTERNET

Rozmowa z obcymi w sieci to delikatna sprawa, a zachowanie bezpieczeństwa jest kluczowe. Poniżej znajdziesz ważne wskazówki na temat tego, o czym nie rozmawiać i jakich informacji nie przekazywać w rozmowach online:

Hasła i Uwierzytelnianie: Nigdy nie udostępniaj swoich haseł, PIN-ów ani innych danych do logowania. To prywatne informacje, które mogą dać dostęp do twoich kont.

Dane Osobowe: Unikaj podawania swojego pełnego imienia, nazwiska, adresu zamieszkania, numeru telefonu, daty urodzenia czy numeru dowodu osobistego. To informacje, które mogą być wykorzystane do kradzieży tożsamości.

Dane Finansowe: Nie przekazuj nikomu swoich numerów kart kredytowych, kodów CVV czy innych informacji finansowych. To może prowadzić do oszustwa finansowego.

Adresy i Plany: Unikaj mówienia o swoim dokładnym miejscu zamieszkania, szkole czy innych miejscach, gdzie się znajdujesz. Również unikaj mówienia o swoich planach na przyszłość.

Prywatne Zdjęcia: Nie udostępniaj swoich prywatnych zdjęć osobom nieznajomym. Zdjęcia mogą być wykorzystane w nieodpowiedni sposób.

ROZMOWY
Z OBCYMI PRZEZ INTERNET

Informacje Rodzinne: Nie opowiadaj obcym o swojej rodzinie, jej strukturze czy planach wakacyjnych. To mogą być informacje, które narazić mogą ciebie lub twoją rodzinę na ryzyko.

Dane Szkolne: Unikaj ujawniania szczegółowych informacji o swojej szkole, nauczycielach czy kolegach. To może wpłynąć na twoje bezpieczeństwo w środowisku szkolnym.

Informacje Sensacyjne: Nie angażuj się w rozmowy o kontrowersyjnych czy wrażliwych tematach. Może to prowadzić do konfliktów lub ujawnienia prywatnych przekonań.

Sytuacje Niekomfortowe: Jeśli czujesz się niewygodnie w rozmowie, nie wahaj się zakończyć jej lub zablokować kontakt z daną osobą.

Fałszywy znajomy: Uważaj na osoby, które mogą próbować zdobyć twoje zaufanie poprzez kłamstwa czy manipulacje.

Informacje na temat rodziców : Unikaj informacji na temat zawodu, miejsca pracy czy też posiadanych przez dorosłych pieniędzy.

Pamiętaj, że zawsze warto być ostrożnym i świadomym, gdy rozmawiasz z obcymi w sieci. Zachowuj zdrowy dystans i nie ufaj zbyt łatwo. Twoje bezpieczeństwo jest najważniejsze!

SYGNAŁY, KTÓRE POWINNY CIE ZAALARMOWAĆ

Podczas rozmowy z obcymi w sieci istnieją pewne sygnały, które powinny wzbudzić twoją czujność

1. **Szybkie Przyjazne Relacje**: Jeśli osoba próbuje nawiązać głębokie i przyjazne relacje zbyt szybko, może to być próba manipulacji.

2. **Prośby o Osobiste Informacje:** Jeśli ktoś nagle pyta o twoje dane osobowe, finansowe lub inne poufne informacje, powinieneś być ostrożny.

3. **Brak Klarowności w Historii:** Jeśli historia osoby wydaje się niejasna, ma braki lub sprzeczności, być może ktoś próbuje ukryć swoją prawdziwą tożsamość.

4. **Nacisk na Spotkanie Osobiście:** Jeśli osoba nagle naciska na to, abyście się spotkali w rzeczywistości, być może warto zadać sobie pytanie, dlaczego tak bardzo na tym zależy.

5. **Prośby o Pieniądze lub Przysługi:** Jeśli ktoś prosi cię o pieniądze, podarunki lub przysługi po krótkiej rozmowie, to może być próba oszustwa.

6. **Prośby o Wysyłanie Zdjęć Prywatnych:** Jeśli osoba nagle chce, abyś wysyłał zdjęcia swoje lub swoich bliskich, to jest powód, aby być podejrzliwym.

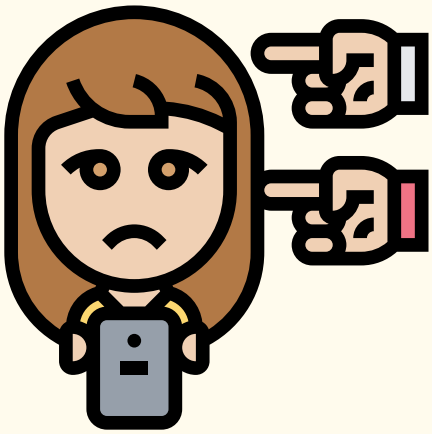
Język Agresji lub Niewłaściwego Zachowania: Jeśli ktoś zaczyna używać obraźliwego języka, grozi lub zachowuje się nieodpowiednio, to oznaka, że powinieneś przerwać rozmowę.

Próba Przekonania Cię do Czegoś: Jeśli ktoś wywiera presję lub ciągle próbuje przekonać cię do czegoś, być może ma ukryte motywy.

Nieodpowiednie Zadawanie Pytań: Jeśli pytania, które zadaje osoba, wydają ci się nieodpowiednie lub za osobiste, zachowuj ostrożność.

B**rak Konsystencji w Danych:** Jeśli osoba podaje się za kogoś, kto ma sprzeczne informacje o sobie na różnych platformach, to może być oszustwo.

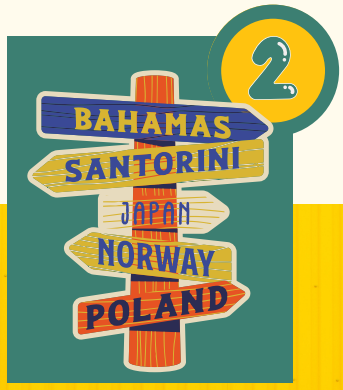
NIE MÓW NIKOMY: Jeśli rozmówca prosi Cię o ukrywanie rozmów między Wami, to jest powód, aby być podejrzliwym.



Czy Widzisz To, Co Ja?

Rozpoznawanie Prawdy w Świecie Wirtualnym

Zdjęcia mogą być modyfikowane przez filtry #1



Podawane informacj mogą być nie prawdziwe #2

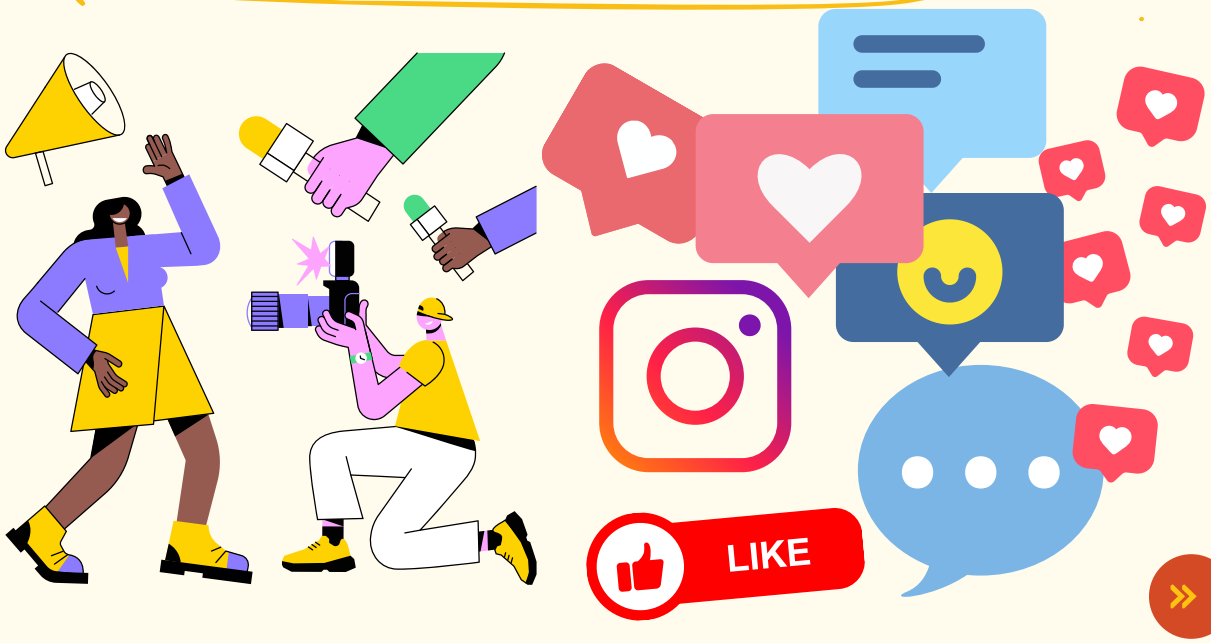
Sprawdzaj źródła #3

Wirtualny świat to miejsce pełne fascynujących historii, pięknych zdjęć i ciekawych informacji. Ale pamiętajcie, że nie wszystko, co widzicie w sieci, jest prawdziwe. To jak odkrywanie skarbów, ale trzeba zachować czujność, aby nie wpaść w pułapki fałszywych treści.

Jak Odróżnić Prawdę od Kłamstwa:

S**prawdzaj Źródła:** Zanim uwierzysz w coś, sprawdź, kto to napisał lub opublikował. Zaufane strony, serwisy informacyjne czy autorytety są bardziej wiarygodne.

Nie Daj Się Sloganom: Czasami widzisz krzykliwe nagłówki czy hasła, które chcą przyciągnąć uwagę. Zastanów się, czy to prawda, czy tylko chwyt reklamowy.



Poszukaj Weryfikacji: Jeśli jakaś informacja wydaje Ci się niewiarygodna, poszukaj innych źródeł, które potwierdzą lub zdementują to, co przeczytałeś.

Analizuj Zdjęcia: Fotografie mogą być manipulowane. Jeśli widzisz niesamowite zdjęcie, poszukaj, czy to nie jest montaż.

Budowanie Odporności Psychicznej:

Rozpoznawanie Fałszu: Ćwiczcie rozpoznawanie fałszywych informacji. To jak gra detektyw, w której musicie szukać dowodów.

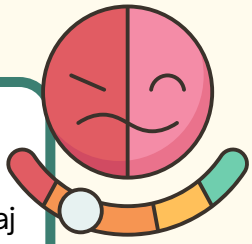
Krytyczne Myślenie: Zastanawiajcie się, czy to, co widzicie, ma sens. Czy brzmi logicznie czy raczej jest za dobre, by było prawdziwe?

Pytajcie o Opinie: Jeśli coś wam wydaje się podejrzane, pytajcie rodziców, nauczycieli czy dorosłych o ich zdanie.

Budowanie odporności psychicznej w świecie wirtualnym to jak trening super mocy. Im więcej ćwiczycie, tym lepiej radzicie sobie z różnymi informacjami. W ten sposób stajecie się mądrymi i odpowiedzialnymi odkrywcami w świecie pełnym informacji! 🌐🔍

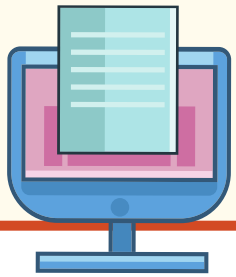
Jak Reagować na Cyberprzemoc
Twoja Mocna Odpowiedź

Cyberprzemoc to nieodpowiednie zachowanie lub agresja w internecie, która może sprawić, że czujesz się źle. Pamiętaj, że masz prawo do bezpiecznego i przyjemnego korzystania z sieci. Oto kilka kroków, jak reagować na cyberprzemoc:



Nie Reaguj Emocjonalnie

To, co osoba mówi w internecie, nie zawsze jest prawdziwe. Nie daj się ponieść emocjom i nie odpowiadaj agresją. Pozostaw spokój.



Zachowaj Dowody

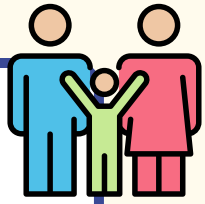
Jeśli jesteś ofiarą cyberprzemocy, zapisz lub zrób zrzut ekranu obraźliwych wiadomości czy komentarzy. To mogą być dowody w przyszłości.

Zablokuj osobę

Wiele platform internetowych pozwala na blokowanie użytkowników. Jeśli ktoś Cię obraża, zablokuj go, aby uniknąć dalszych kontaktów.

Skonsultuj Się

Porozmawiaj z rodzicami, opiekunami, nauczycielem lub inną osobą zaufaną. Opowiedz im o tym, co się dzieje - nie jesteś sam w tej sytuacji.



Rozmawiaj z Rodzicami

Jeśli jesteś dzieckiem lub młodzieżą, porozmawiaj z rodzicami lub opiekunami. Dziel się swoimi doświadczeniami i obawami.

Dbaj o Siebie

Zajmij się tym, co Cię uszczęśliwia. Czasem odpoczynek od internetu czy rozmowa z przyjacielem mogą pomóc Ci poczuć się lepiej.

Zrozumienie, Nie Jesteś Sam

Pamiętaj, że wiele osób doświadcza cyberprzemocy. Szukaj wsparcia w grupach online lub organizacjach, które pomagają ofiarom.

ZGŁOŚ!

1

Platformy Internetowe: Większość serwisów ma opcję zgłaszania nadużyć. Zgłoś przemoc lub nieodpowiednie treści.

2

Szkoła: Jeśli jesteś uczniem, poinformuj nauczyciela lub pedagoga, że doświadczasz cyberprzemocy.

3

Strażnicy Internetu: Jeśli ktoś grozi Ci przemocą lub próbuje Cię zastraszyć, zgłoś to odpowiednim służbom.

Pamiętaj, że Twoje bezpieczeństwo i dobre samopoczucie są najważniejsze. Nie bój się prosić o pomoc i walczyć o zdrowe, pozytywne doświadczenia w sieci. Niech Twoja reakcja będzie mocna i pełna odwagi!

SŁOWNICZEK ✦✦✦ POJĘĆ:

Bezpieczeństwo Cybernetyczne: Zespół działań, technologii i praktyk mających na celu ochronę systemów komputerowych i sieci przed atakami, hakerami oraz innymi zagrożeniami cyfrowymi.

Hasło: Sekretny ciąg znaków używany do uwierzytelniania użytkownika i zabezpieczania dostępu do konta lub danych.

Phishing: Oszustwo polegające na podszywaniu się pod wiarygodne źródło (np. bank), aby zdobyć poufne informacje od użytkownika, takie jak hasła czy numery kart kredytowych.

Malware: Skrót od "malicious software", oprogramowanie złośliwe. Obejmuje wirusy, trojany, robaki i inne szkodliwe programy komputerowe.

Firewall: System zabezpieczeń, który kontroluje ruch między siecią komputerową a internetem, blokując nieautoryzowane połączenia i zagrożenia.

Antywirus: Program komputerowy projektowany do wykrywania, blokowania i usuwania wirusów oraz innych złośliwych oprogramowań z komputera.

Bezpieczne Przeglądanie: Korzystanie z przeglądarki internetowej z włączoną funkcją blokowania niebezpiecznych witryn i oprogramowania.

Certyfikat SSL: Certyfikat zabezpieczający połączenie między przeglądarką a stroną internetową, zapewniający szyfrowanie danych i uwierzytelnianie.

Złośliwy Link: Link prowadzący do witryny lub strony, która zawiera złośliwe oprogramowanie lub próbuje wyłudzić dane.

Uwierzytelnianie Dwuetapowe: Dodatkowa warstwa bezpieczeństwa polegająca na wprowadzeniu dwóch różnych form uwierzytelniania, na przykład hasła i kodu SMS.

Dane Osobowe: Informacje identyfikujące konkretną osobę, takie jak imię, nazwisko, adres czy numer telefonu.

Zabezpieczenia Konta: Działania, takie jak mocne hasła, uwierzytelnianie dwuetapowe i regularna zmiana haseł, aby chronić konto przed nieautoryzowanym dostępem.

Skrót URL: Krótki link, który prowadzi do dłuższego adresu internetowego. Uważaj na skróty URL, które mogą prowadzić do podejrzanych stron.

Cookies: Małe pliki tekstowe przechowywane przez przeglądarkę, które przechowują informacje o twoich działaniach online. Mogą być wykorzystywane do śledzenia aktywności.

Ochrona Prywatności: Zbiór działań i praktyk, które chronią twoje dane osobowe i informacje przed nieuprawnionym dostępem, wykorzystaniem lub ujawnieniem..

Atak DDoS: Skrót od "Distributed Denial of Service". To atak, w którym hakerzy wykorzystują wiele urządzeń, aby przeciążyć stronę internetową lub usługę, uniemożliwiając dostęp użytkownikom.

Pamiętaj, że znajomość tych terminów może pomóc Ci lepiej zrozumieć i zachować bezpieczeństwo w internecie.

ZNAKI I SYMBOLE , KTÓRE POMOGĄ PAMIĘTAĆ O BEZPIECZEŃSTWIE W SIECI

Pamiętaj, że te symbole są nie tylko przypomnieniem o cyberbezpieczeństwie, ale również świetnymi narzędziami edukacyjnymi dla innych osób, które chcesz zaangażować w budowanie świadomości na ten temat. 🌐🔒

🔐 Zamek: To symbol oznaczający bezpieczne połączenie i zabezpieczenie danych, jak certyfikat SSL na stronach internetowych.	🛡️ Tarcza: Ten symbol symbolizuje ochronę i bezpieczeństwo, przypominając Ci, że warto chronić swoje dane w sieci.
🚫 Znak Zapytania w Trójkącie: To oznaczenie pojawia się często przy podejrzanych linkach czy niebezpiecznych plikach. To przypomnienie, aby być ostrożnym.	📅 Kalendarz z Zegarem: Przypomina, że warto regularnie zmieniać hasła i aktualizować oprogramowanie, aby zachować bezpieczeństwo.
⚠️ **Znak Ostrzeżenia:** Ten znak przypomina, że niektóre treści w sieci mogą być niebezpieczne. Bądź czujny i zwracaj uwagę na wszelkie sygnały ostrzegawcze.	📶 **Sygnał Wi-Fi:** Ten symbol przypomina, że łączysz się z internetem. Pamiętaj, aby korzystać tylko z bezpiecznych sieci Wi-Fi.
🔄 Strzałka Odświeżania: To przypomnienie, że warto odświeżać swoją wiedzę na temat cyberbezpieczeństwa i być na bieżąco z nowymi zagrożeniami.	🗑️ Kosz na Śmieci: Symbolizuje ważność usuwania starych i niepotrzebnych danych oraz plików, aby uniknąć przypadkowego dostępu do nich.
📝 Długopis i Papier: Przypomina, że warto pisać silne hasła i informacje uwierzytelniające na papierze, aby je pamiętać, ale trzymać w bezpiecznym miejscu.	🏆 Trofeum: Przypomina, że twoje bezpieczeństwo w sieci to osiągnięcie, które warto pielęgnować i dbać o nie.

Gdzie szukać pomocy?

800 100 100
TELEFON DLA RODZICÓW I NAUCZYCIELI

Linia czynna jest od poniedziałku do piątku w godzinach **12.00–15.00.**
Więcej informacji znajdziesz na stronie **https://800100100.pl/**

Bezpłatna i anonimowa pomoc telefoniczna i online dla rodziców i nauczycieli, którzy potrzebują wsparcia i informacji w zakresie przeciwdziałania przemocy, a także pomocy psychologicznej dzieciom przeżywającym kłopoty i trudności, takie jak: agresja i przemoc w szkole, cybeprzemoc i zagrożenia związane z nowymi technologiami, wykorzystanie seksualne, kontakt z substancjami psychoaktywnymi, depresja i obniżony nastrój, myśli samobójcze, zaburzenia odżywiania.

Pamiętaj, że nie jesteś sam w tej sytuacji. Szukanie pomocy to oznaka siły i odwagi. Ważne jest, abyś wiedział, że masz prawo do bezpiecznego i pozytywnego doświadczania internetu, a wsparcie jest dostępne, gdy go potrzebujesz

Oglądnij filmy przygotowane przez
Fundację FYLION o bezpieczeństwie
dzieci i młodzieży
w sieci na kanale Fundacji na YouTube

www.fylion.org

Projekt realizowany przy wsparciu finansowym
Województwa Małopolskiego.

FUNDACJA
FYLION

MAŁOPOLSKA

Fundacja FYLION
ul. Nawojowska 4/203
33-300 Nowy Sącz
e-mail: fylion@fylion.org
tel. 791 790 190