**Temat: Bezpieczeństwo w sieci.**



**Warto zobaczyć :**

[**https://liblink.pl/zlkLLVtw1Z**](https://liblink.pl/zlkLLVtw1Z)**- dla dzieci,**[**https://liblink.pl/hYnYqEG0mY**](https://liblink.pl/hYnYqEG0mY)**- dla dzieci,**[**https://liblink.pl/Z1gsl4X17R**](https://liblink.pl/Z1gsl4X17R)**dla rodziców**

**Internet jest bardzo popularnym narzędziem komunikacji, nie tylko z powodu łatwej dostępności, ale również malejących kosztów ekonomicznych ponoszonych przez jego użytkowników. Na atrakcyjność sieci składają się też inne czynniki, np.: możliwość pozyskiwania aktualnych informacji, praktycznie nieograniczony dostęp do różnorodnych zasobów, możliwość komunikacji z internautami z całego świata, multimedialność. Dlatego też dzieci i młodzież, dorastając w otoczeniu nowoczesnych technologii, traktują i postrzegają korzystanie z internetu, a także znajdujących się w nim serwisów informacyjnych, edukacyjnych, społecznościowych i rozrywkowych, komunikatorów i rozmaitych aplikacji jako nieodłączny element ich codzienności domowej, szkolnej i środowiskowej. Podejmują one wiele rozmaitych aktywności w sieci, która w ich opinii jest „od zawsze” i która stanowi naturalne otoczenie, towarzyszące im w domu, szkole, przestrzeni publicznej. Przeważająca większość najmłodszych użytkowników sieci twierdzi, iż trudno im wyobrazić sobie codzienność bez internetu.**

 **Nastolatki wykazują się szczególnie intensywną aktywnością w internecie. Korzystanie z sieci stało się dla nich naturalnym elementem zachowania.**

**Jednak zbyt wczesne i niekontrolowane udostępnianie mediów elektronicznych najmłodszym dzieciom może doprowadzić do szeregu zaburzeń i mieć negatywny wpływ na ich rozwój. Intensywna obecność internetu nie tylko wśród dzieci, lecz także wśród rodziców wpływa negatywnie na relacje w rodzinie. To, co coraz częściej odciąga dorosłych od bycia w bliskim kontakcie z dzieckiem, to właśnie smartfony czy inne urządzenia ekranowe z dostępem do internetu.**

**Zagrożenie uzależnieniem od sieci, poza intensywnością dostępu, wzmacniane jest przez nagradzanie dzieci dostępem do urządzeń elektronicznych, zachęcanie nimi do jedzenia czy wykonywania innych codziennych czynności albo wykorzystywanie ich do uspakajania dziecka, szczególnie w sytuacjach jego silnych emocji. Tymczasem dzieci, przy uważnym i kochającym wsparciu i przewodnictwie rodziców, uczą się radzić sobie z emocjami, nazywać swoje potrzeby, rozmawiać i poszukiwać rozwiązań w sytuacjach, które są dla nich wyzwaniem, czy też wymyślać aktywności, które pomogą im opanować nudę.**

**Nieodpowiedzialne korzystanie z urządzeń elektronicznych może nieść wiele zagrożeń. Cyberprzemoc i agresja elektroniczna w internecie to zjawiska – pośrednio lub bezpośrednio – dotyczące większości polskiej młodzieży.**

**Do podstawowych form cyberprzemocy zalicza się: wyzywanie, nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie w internecie kompromitujących informacji, zdjęć, filmów, podszywanie się w cyberprzestrzeni pod kogoś wbrew jego woli, a także wykluczanie z grupy rówieśniczej online (np. poprzez usunięcie kogoś z grona znajomych na portalu społecznościowym).**

**Technologia cyfrowa sprawiła, że dzięki urządzeniom mobilnym każdy właściciel smartfonu może być stale zalogowany do sieci, mając nieograniczony dostęp do informacji i rozrywki. W sieci dyskutujemy, utrzymujemy relacje z bliższymi i dalszymi znajomymi, robimy zakupy, uczestniczymy w tele- i wideokonferencjach, wyrażamy siebie. Te często atrakcyjne i wartościowe możliwości spędzania czasu mogą jednak pochłaniać go zbyt wiele, sprawiając, że zamiast być dopełnieniem aktywności, zaczynają w naszym życiu dominować. Wielogodzinne angażowanie się w gry online, kompulsywne sprawdzanie mediów społecznościowych, wykorzystywanie każdej okoliczności na podłączenie się do publicznych sieci internetowych – to tylko wybrane przykłady nadmiernego korzystania z sieci.**

**Pamiętaj:**

**1.Ustal czas przeznaczony na aktywności w internecie.**

**2. Zwracaj uwagę na zachowania innych(np. nadmierną agresję]**

**3. Swoim zachowaniem w sieci wpływasz na zachowanie innych osób.**

**4. Zastanów się , zanim umieścisz swój materiał w internecie.**

 **Bądź dla nich przykładem!!!**

**Niebezpieczne treści w internecie to materiały, które mogą wywołać negatywne emocje u odbiorcy lub promują niebezpieczne zachowania . Zalicza się do nich przede wszystkim:**

**- treści pornograficzne dostępne bez żadnego ostrzeżenia, w tym materiały prezentujące seksualne wykorzystywanie dzieci;**

**-treści obrazujące przemoc, obrażenia fizyczne, deformacje ciała, np. zdjęcia lub filmy przedstawiające ofiary wypadków, okrucieństwo wobec zwierząt;**

**- treści nawołujące do samookaleczeń lub samobójstw, bądź zachowań szkodliwych dla zdrowia, np. ruch promujący anoreksję (pro-ana), zachęcanie do zażywania niebezpiecznych substancji, np. leków czy narkotyków;**

**- treści dyskryminacyjne, nawołujące do wrogości, a nawet nienawiści wobec różnych grup społecznych lub jednostek.**

**Oprócz treści niebezpiecznych isnieją również treści nielegalne.**

 **Mianem treści nielegalnych określa się materiały naruszające przepisy prawa. Nielegalne treści to wszelkie informacje, które nie są zgodne z prawem Unii Europejskiej lub prawem państwa członkowskiego. Są to:**

**- Treści terrorystyczne, czyli wszelkie materiały nawołujące do terroryzmu lub promujące terroryzm.**

**- Materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych,**

 **- Nielegalne nawoływanie do nienawiści, czyli publiczne zachęcanie do przemocy lub agresji skierowanej przeciwko określonej grupie osób/członkowi danej grupy, zdefiniowanych według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej.**

**Pamiętaj:**

**Internet jest przestrzenią komunikacyjną, którą wykorzystuje większość młodych osób, narażając się niekiedy na różne niebezpieczne sytuacje. Zdarza się, że w wyniku zawarcia znajomości w internecie dzieci stają się ofiarami sprawców, którzy dążą do tego, aby wykorzystać je seksualnie, zwerbować do grup przestępczych, sekt lub zachęcać do zachowań szkodliwych dla życia lub zdrowia.**

**Jeżeli znajdziesz się w takiej sytuacji poinformuj rodziców oraz policję o takiej sytuacji. Ponadto bądź uważna (-y).**

**Problematyka prywatności to jeden z kluczowych elementów bezpieczeństwa w kontekście technologii cyfrowej. Funkcjonalności globalnej sieci poniekąd przyzwyczają jej użytkowników do częstego dzielenia się informacjami, danymi osobowymi, których nie ujawnialiby w innych warunkach. Media społecznościowe preferują, aby ich członkowie podawali prawdziwe dane osobowe. Podobna sytuacja ma miejsce podczas korzystania z aplikacji, które wymagają szczegółowych danych do logowania. Warto też pamiętać o tym, że smartfony mogą być na stałe podpięte do kont bankowych, a wyszukiwarki zapisują obszerną historię aktywności internautów w sieci. Często zdarza się, że użytkownicy internetu automatycznie akceptują żądania witryn i usług sieciowych, zapominając, że mają prawo chronić swoje dane poprzez rezygnację z uciążliwych aplikacji (np. odwołujących się do różnych informacji zapisanych w urządzeniu, takich jak: kontakty, zdjęcia, hasła, a także pobierających, zdaniem ich właścicieli, zbyt wiele danych lub wymagających co chwilę skonfigurowania). Ustawienia prywatności znajdują się zarówno w konsolach do gier (urządzenia te w ostatnich latach były narażone na ataki ze strony cyberprzestępców), jak w smartfonach, gdzie eliminują przykładowo działanie usług lokalizacyjnych.**

**Pamiętaj:**

**1. Twórz silne hasła.
Silne hasło powinno składać się z małych i wielkich liter, a także cyfr i symboli. Pamiętaj, że hasło powinno zawierać nie mniej, niż 8 znaków. Im będzie ich więcej, tym oczywiście lepiej. Każdy kolejny znak to zwiększenie liczby kombinacji niezbędnych do jego złamania, a więc podniesienie poziomu bezpieczeństwa.**

**2. Pamiętaj, by hasła były różne do różnych kont i zarządzaj nimi
Używanie tego samego hasła do logowania się na wiele kont zmniejsza Twoje bezpieczeństwo. To tak, jakbyś za pomocą tego samego zamka zabezpieczył dom, samochód i biuro - jeśli ktoś uzyska dostęp do jednego z nich, wszystkie mogą zostać naruszone. Warto zatem tworzyć różne, silne hasła do różnych kont.

3. Aktualizuj oprogramowanie, nie odkładaj na później.
By chronić swoją aktywność online, zawsze uruchamiaj najnowszą wersję oprogramowania w przeglądarkach internetowych, systemach operacyjnych i aplikacjach na wszystkich urządzeniach. Niektóre usługi, w tym przeglądarka Chrome, będą się automatycznie aktualizować do najnowszej wersji. Inne mogą powiadamiać Cię, gdy nadejdzie czas aktualizacji. Nie warto tego odkładać.

4. Korzystaj z dwuetapowej weryfikacji.
Aby jeszcze skuteczniej zabezpieczyć swoje konta, skonfiguruj weryfikację dwuetapową, która, oprócz nazwy użytkownika i hasła do zalogowania się na Twoje konto, wymaga wykonania dodatkowego kroku - np. wpisania 6-cyfrowego kodu wygenerowanego przez aplikację Google Authenticator. Konfiguracja weryfikacji dwuetapowej znacznie zmniejszy szansę na uzyskanie nieautoryzowanego dostępu do konta.

5. Sprawdzaj czy korzystasz z szyfrowanego połączenia
Aby dowiedzieć się, czy można bezpiecznie otworzyć daną stronę, możesz sprawdzić informacje o jej zabezpieczeniach. Jeśli nie można wejść na stronę bezpiecznie lub z zachowaniem prywatności, Chrome wyświetla ostrzeżenie. Wystarczy otworzyć przeglądarkę i spojrzeć na symbol na lewo od adresu internetowego.**