

Zagrożenia w sieci oraz rozwiązania w zakresie zapewnienia bezpiecznych warunków korzystania z internetu

Nadużywanie internetu

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.

Dzieci i nastolatki, które mają problem z kontrolowaniem czasu online, często prezentują całe spektrum niepokojących objawów, np.: pogorszenie wyników w nauce, chroniczne zmęczenie, nagłe zmiany nastrojów, zachowania lękowe, depresyjne. Bywa też, że tych młodych ludzi wyróżnia zachowanie typowe dla osób uzależnionych od jakiegoś nałogu. Wiele nastolatków ujawnia symptomy dysfunkcyjnego korzystania z cyberprzestrzeni: 83,2 proc. uczniów deklaruje, że zdarzyło im się przebywać w sieci dłużej, niż planowali. Natomiast 29,8 proc. młodych ludzi twierdzi, że przedkładało korzystanie z sieci ponad obowiązki szkolne.

Pamiętaj!

- Ustal czas przeznaczony na aktywności w internecie. Obserwuj dziecko i zwróć szczególną uwagę na niepokojące zachowania (np. nadmierną agresję, odizolowanie, nadwrażliwość, utratę zainteresowania innymi aktywnościami).
- Rozmawiaj z dzieckiem. Zasygnalizuj mu, że się o nie martwisz, spróbuj wytłumaczyć swoje obawy.
- Spróbuj dowiedzieć się, co jest powodem uzależnienia twojego dziecka od internetu, a także w jakich sytuacjach korzysta ono intensywniej z sieci.

Niebezpieczne treści

Dzieci korzystające z internetu mogą uzyskiwać dostęp do niebezpiecznych treści takich jak pornografia lub materiały przesycane przemocą i nienawiścią. W opinii samych dzieci jest to najpowszechniejsze i najbardziej dotkliwe zagrożenie. Ich zdaniem głównym źródłem internetowych zagrożeń są przede wszystkim serwisy wideo, w których pojawiają się treści pornograficzne i przemoc (Livingstone, Kirwil, Ponte, 2013).

Pamiętaj!

- Pamiętaj, że filtr kontroli rodzicielskiej pomaga ograniczyć kontakt dziecka z potencjalnie niebezpiecznymi dla niego stronami internetowymi, zawierającymi szkodliwe treści. Zwróć uwagę na to, że dzieci i młodzież rzadziej łączą się z internetem, korzystając z komputera stacjonarnego, a coraz częściej wykorzystują do tego celu urządzenia mobilne (np. smartfon, tablet, konsolę do gry).
- Pamiętaj, że żadne narzędzie nie zapewnia gwarancji ochrony dziecka przed zetknięciem się z ryzykownymi i szkodliwymi treściami. Dlatego tak ważne są umiejętność mądrej reakcji ze strony osoby dorosłej oraz udzielenie wsparcia. Zachęcaj dzieci do dzielenia się z tobą wszelkimi niepokojącymi sytuacjami, jakie je spotkały w sieci czy których były świadkami.
- Uczul dziecko na zagrożenia związane z korzystaniem z publicznych/ otwartych sieci Wi-Fi (hotspotów). Mogą one w nieograniczony sposób umożliwiać dostęp do szkodliwych treści i narażać

najmłodszych użytkowników sieci na wiele zagrożeń (np. na utratę danych i/lub nawiązanie niebezpiecznych kontaktów).

Zagrożenia dla prywatności

Problematyka prywatności to jeden z kluczowych elementów bezpieczeństwa w kontekście technologii cyfrowej. Funkcjonalności globalnej sieci poniekąd przyzwyczajają 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).

Pamiętaj!

- Jeśli zamieszczasz w sieci zdjęcia dziecka lub filmy z jego udziałem, zastanów się, czy żadna z tych treści nie będzie dla niego w przyszłości obciążeniem i nie przyniesie mu wstydu.
- Uświadamiaj dziecko na temat jego prawa do ochrony prywatności, a także obowiązku poszanowania prywatności innych osób.
- Pamiętaj o ograniczeniu wiekowym związanym z uczestnictwem najmłodszych internautów w mediach społecznościowych.
- Kiedy dziecko zakłada swój pierwszy profil w sieci, pomóż mu mądrze skorzystać z udostępnianych przez serwis ustawień prywatności.

Cyberprzemoc i inne formy agresji w sieci

Przemoc rówieśniczą w sieci określa się angielskim terminem cyberbullying. W języku polskim funkcjonuje także inne pojęcie odnoszące się do tego zjawiska – cyberprzemoc, czyli przemoc z użyciem technologii informacyjnych i komunikacyjnych (internetu i telefonów komórkowych). 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).

Pamiętaj!

- Rozmawiaj z dzieckiem na temat przemocy w sieci, hejtu i mowy nienawiści. Ustalcie wspólnie, w jaki sposób można reagować na te zjawiska. Zapewnij dziecko o swoim wsparciu, jeśli doświadczy takiej sytuacji.
- Jako rodzic/opiekun prawny nigdy nie bagatelizuj sytuacji, w której twoje dziecko jest ofiarą przemocy w sieci. Reaguj natychmiast i działaj we współpracy ze szkołą/placówką edukacyjną. Wspólnie zabezpieczcie dowody (np. wykonując zrzuty ekranów).

- Rozmawiaj z dzieckiem o tym, jak może reagować jako świadek cyberprzemocy. Poinformuj dziecko, w jaki sposób może pomóc ofierze agresji w sieci, jednocześnie nie narażając się samemu na przemoc.

Uwodzenie dzieci i młodzieży w internecie

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.

Pamiętaj!

- Porozmawiaj z dzieckiem o jego znajomych z internetu. Jeśli w gronie swoich znajomych ma osoby, których nie zna z życia realnego, warto, aby je usunęło lub ograniczyło dostęp do publikowanych przez siebie materiałów.
- Zaoferuj dziecku wsparcie i powiedz, żeby zawsze informowało Cię, jeśli jakaś obca osoba będzie poruszała tematy związane z seksualnością lub inne, które je zaniepokoją.
- Poinformuj dziecko o możliwości zgłoszenia takiej sytuacji policji.
- Bądź uważna (-y), nietypowe zmiany w zachowaniu dziecka mogą niekiedy świadczyć o tym, że jest w niebezpiecznej relacji.

Zagrożenia informacyjne

Dostęp do wartościowych i sprawdzonych informacji jest nieograniczony, trzeba jednak umieć i chcieć je wyłuskać z bezkresu bezwartościowych (często fałszywych) treści. Mimo łatwego dostępu do naukowej wiedzy nadal dużą popularnością cieszą się teorie spiskowe, które dzięki internetowi mogą osiągać większy niż kiedykolwiek zasięg. Fałszywe informacje (ang. fake news) stały się skuteczną bronią stosowaną w walce politycznej i nie tylko. Bardzo istotnym aspektem selekcjonowania informacji jest umiejętność rozpoznania przekazu reklamowego, który biorąc pod uwagę specyfikę nowych mediów czasami nie jest łatwo na pierwszy rzut oka zauważyć. Fake newsy to fałszywe informacje, które rozpowszechniane są w celu dezinformacji i manipulacji ludźmi.

Pamiętaj!

- Podstawą przeciwdziałania większości zagrożeniom informacyjnym jest nauczanie młodzieży krytycznego podchodzenia do informacji, nie tylko tych znalezionych w internecie.
- Korzystaj z wartościowych scenariuszy zajęć lub innych materiałów na temat umiejętności krytycznego myślenia i weryfikacji danych (SciFun, 2016).
- Naucz dziecko korzystać z narzędzi służących do weryfikacji informacji znalezionych w internecie, np. zdjęć (odwrotne wyszukiwanie przez Images.google.com lub TinEye.com).

Zagrożenia technologiczne

Nazwa „złośliwe oprogramowanie” – malware (od ang. malware stanowiącego połączenie słów malicious, złośliwe, i software, oprogramowanie) – oznacza różnego rodzaju szkodliwe programy/aplikacje i skrypty (fragmenty kodów) celowo działające na szkodę użytkownika systemu, przykładowo zmierzające do uszkodzenia systemu (Madej, Terlikowski, 2009).

Programy typu spyware pełnią funkcje szpiegowskie, pozyskując i przysyłając bez wiedzy użytkownika dane z jego systemu do twórców spyware. Groźną odmianą malware są ransomware. Programy tego typu blokują dostęp do plików użytkownika na urządzeniu, zwykle szyfrując je.

Pamiętaj!

- Zainstaluj program chroniący przed różnymi typami niechcianego oprogramowania (nie tylko wirusami) i ustaw jego regularne aktualizacje.
- Aktualizuj system i aplikacje – zwłaszcza przeglądarki internetowe.
- Nie otwieraj odruchowo łączy przesyłanych pocztą lub komunikatorami – najpierw sprawdź, kto i po co ci je wysyła, czy nie pochodzą od bota, czy ich adres prowadzi do godnej zaufania strony oraz czy plik nie zawiera niebezpiecznych niespodzianek.

Źródło: „Bezpieczeństwo dzieci i młodzieży online” Kompendium dla rodziców i profesjonalistów, Polskie Centrum Programu Safer Internet, Warszawa 2018