BEZPIECZEŃSTWO DZIECKA W INTERNECIE

PORADNIK DLA RODZICÓW UCZNIÓW

SZKOŁY PODSTAWOWEJ NR 357

Szanowni Rodzice i Opiekunowie!

Internet - jego zasoby i możliwości komunikacyjne - to wielkie bogactwo, z którego korzysta na co dzień nowoczesna szkoła. Pozwala lepiej poznać świat, łatwiej się komunikować, zdobywać wiedzę, wreszcie dzięki niemu sprawniej załatwiamy codzienne sprawy. Oczywiście korzystanie z Internetu niesie ze sobą także potencjalne zagrożenia, a możliwości techniczne rodzą nowe zagrożenia i zwielokrotniają siłę tych już znanych (plotki, pomówienia).

Rodzicu - nie przeceniaj wiedzy swojego dziecka i jego umiejętności technicznych, a tym bardziej umiejętności dostrzeżenia niebezpiecznych sytuacji i poradzenia sobie z problemami. Jako dorosły jesteś odpowiedzialny za jego bezpieczeństwo w Internecie. Zadbaj o to, by wiedziało, że może się do Ciebie zwrócić z problemami. Nawet jeśli zabezpieczyłeś kwestie techniczne domowego komputera i poświęcasz swojemu dziecku uwagę w trakcie, kiedy używa Internetu, pamiętaj, że dostęp do sieci może mieć nie tylko w domu. Co więcej – by korzystać z Internetu, nie musi włączać domowego komputera. Warto więc wprowadzić ustawienia kontroli rodzicielskiej we wszystkich urządzeniach, do których dziecko ma dostęp.

1. USTAL Z DZIECKIEM ZASADY KORZYSTANIA Z INTERNETU

Skoro zgadzamy się na to, by dziecko miało dostęp do Internetu, musimy ustalić z nim zasady, które zapewnią mu bezpieczeństwo. To konieczne, by chronić je przed kontaktem z nieodpowiednimi treściami. Zasady muszą być dostosowane do wieku dziecka. Ważne, żeby nie poprzestać na jednorazowej rozmowie. **Do tematu zasad użytkowania Internetu i bezpieczeństwa w nim należy wracać, jeśli tylko pojawi się ku temu okazja w codziennej rozmowie.** Warto zachęcać dziecko do zadawania pytań, rozwiewać jego wątpliwości, tłumaczyć, dlaczego decydujemy się na pewne ograniczenia. Ważne, żeby dziecko miało świadomość, że dbamy o jego bezpieczeństwo. Dążmy do tego, by było przekonane o tym, że zawsze może zwrócić się do nas w sytuacjach dla siebie trudnych lub gdy będzie miało poczucie zagrożenia.

Warto zadbać o to, by dziecko korzystające z Internetu przestrzegało następujących zasad:

- Najmłodsze dzieci powinny korzystać jedynie z pozytywnych i bezpiecznych treści (strony, aplikacje, gry) wskazanych przez rodziców. Z czasem warto brać pod uwagę propozycje nowych treści spośród wskazywanych przez dzieci, każdorazowo je weryfikując. Po wprowadzeniu takiej zasady warto porozmawiać z dzieckiem na temat nieodpowiednich treści online. Trzeba zaznaczyć, że nie są to treści przeznaczone dla dzieci i że oczekujemy, iż dziecko nas poinformuje w razie kontaktu z nimi.
- **Czas korzystania z sieci powinien być ograniczony.** Zaleca się, by dzieci w wieku wczesnoszkolnym nie korzystały z urządzeń ekranowych dłużej niż dwie godziny dziennie. Dobrym pomysłem jest ustalenie dnia lub dni, np. weekendu, bez Internetu.
- **Dzieciom w wieku przedszkolnym należy towarzyszyć podczas korzystania z sieci.** Jeśli dzieci są starsze, warto jako rodzic możliwość wglądu w ekran komputera czy urządzenia mobilnego, z którego korzystają. Przy okazji warto zainteresować się aktywnościami dziecka online i nawiązać na ten temat rozmowę.
- **Najmłodsze dzieci nie powinny samodzielnie korzystać z wyszukiwarek, portali społecznościowych i innych serwisów dających nieograniczony dostęp do treści (zdjęć, filmów, tekstów).** Stopniowe wprowadzanie takich możliwości powinno odbywać się pod kontrolą rodziców i z uwzględnieniem ograniczeń wiekowych narzucanych przez serwisy. Warto takie sytuacje wykorzystać do edukacji dziecka w zakresie skutecznego i bezpiecznego poszukiwania treści, poszerzając jego wiedzę na temat nieodpowiednich treści. Najmłodsze dzieci nie powinny samodzielnie korzystać z komunikatorów czy portali

społecznościowych. Ewentualne kontakty online powinny być ograniczone do znajomych osób i odbywać się pod kontrolą rodziców. Zakaz ten należy poprzedzić rozmową na temat zagrożeń związanych z kontaktami z nieznajomymi.

- **Dzieci nie powinny publikować samodzielnie w sieci treści, szczególnie prywatnych informacji, filmów, zdjęć.** Taki zakaz powinien być połączony ze zwróceniem dziecku uwagi na zagrożenia związane z publikacją wizerunku i prywatnych informacji.
- **Należy umówić się z dzieckiem, ze za każdym razem kiedy trafi na nieodpowiednie treści lub cokolwiek innego je w sieci zaniepokoi, natychmiast nas o tym poinformuje**. Kiedy dziecko zgłasza kontakt z nieodpowiednimi treściami, warto rozpoznać, co się wydarzyło, pochwalić je za poinformowanie o takim zdarzeniu. Jeżeli dziecko jest zaniepokojone, trzeba wytłumaczyć mu sytuację, zastanowić się, jak zmniejszyć prawdopodobieństwo podobnych okoliczności w przyszłości.

2. UDOSTĘPNIAJ DZIECKU JEDYNIE POZYTYWNE I BEZPIECZNE TREŚCI

Kontakt z nieodpowiednimi treściami, jak pornografia, przemoc czy wulgarne materiały, może mieć szkodliwy wpływ na dziecko, podczas gdy odpowiednio dobrane treści i aktywności online mogą pozytywnie wpłynąć na jego rozwój społeczny, emocjonalny, moralny i poznawczy. Dlatego dobór stron internetowych, aplikacji czy gier staje się niezwykle ważnym zadaniem dla rodziców.

Warto przy tym zwrócić uwagę na kilka podstawowych kwestii:

- Należy udostępniać dzieciom treści z wiarygodnego źródła, stworzone z myślą o młodym odbiorcy.
- Udostępniane dzieciom treści powinny łączyć zabawę z edukacją i rozwojem – angażować je w aktywności plastyczne, muzyczne, rozwijać wyobraźnię, poszerzać wiedzę.
- W poszukiwaniu pozytywnych treści warto skorzystać z popularnych wyszukiwarek (np. Google) – wpisanie odpowiedniego hasła np. „aplikacje dla dzieci”, „strony dla dzieci” lub nazwy konkretnej gry czy aplikacji pozwoli zapoznać się z informacjami od dystrybutorów oraz opiniami innych internautów. Szukając aplikacji dziecięcych, warto skorzystać też z katalogu BeStApp prowadzonego przez Fundację Dajemy Dzieciom Siłę. Jest on dostępny jako aplikacja (dla systemu Android) oraz na stronie – www.fdds.pl/bestapp. Fundacja prowadzi także katalog dziecięcych stron internetowych BeSt dostępny pod adresem www.fdds.pl/best.

3. ROZMAWIAJ Z DZIECKIEM O JEGO DOŚWIADCZENIACH W SIECI

Dobry kontakt z dzieckiem, czas na rozmowę i zainteresowanie jego doświadczeniami są niezwykle ważne do rozwoju dziecka. Zapewniają mu poczucie bezpieczeństwa. Jeżeli w świecie dziecka pojawiają się urządzenia elektroniczne i Internet, to ważne, żeby również one były tematem rozmów z nim. Dzięki temu będziemy na bieżąco z doświadczeniami dziecka, poznamy jego preferencje, zobaczymy efekty jego aktywności online, damy mu szansę na pochwalenie się osiągnięciami (ważne, żeby je zauważać i doceniać). Rozmowa o doświadczeniach online będzie pomocna w zauważeniu niepokojących zdarzeń – również tych związanych z kontaktem z niebezpiecznymi treściami.

Jeżeli dowiemy się, że dziecko miało kontakt z pornografią czy scenami przemocy, nie wpadajmy w panikę. Ważne, żeby nie oceniać ani nie obwiniać dziecka za takie zdarzenia. Wyniki badań pokazują, że zdecydowana większość dzieci nie podzieliłaby się z rodzicami niepokojącymi zdarzeniami w sieci właśnie dlatego, że boją się oceny i konsekwencji (np. pozbawienia dostępu do Internetu). Ważne jest więc, żeby spokojnie ustalić okoliczności zdarzenia. Jeżeli kontakt z nieodpowiednimi treściami wprowadził dziecko w zakłopotanie, należy wytłumaczyć mu sytuację, w której się znalazło. Ważne, żeby nie pozostawiać pytań dziecka bez odpowiedzi. W przypadku scen filmowych czy fragmentów gier, które przestraszyły dziecko, należy wytłumaczyć mu, że to fikcja, że nikomu nie stała się krzywda. W przypadku kontaktu z erotyką i pornografią na miarę wieku dziecka należy wytłumaczyć mu, że materiały, które widziało, przeznaczone są dla dorosłych. Następnie należy się zastanowić, jak unikać podobnych sytuacji – zainstalować oprogramowanie filtrujące, wyeliminować szkodliwe gry, poinstruować dziecko, jakich aktywności w sieci unikać itd. Jeżeli dziecko opowiada o kontakcie ze szkodliwymi treściami poza domem – w szkole, domu rówieśników, należy porozmawiać o tej sytuacji z wychowawcą czy rodzicami kolegów dziecka. Należy tez być wyczulonym na sytuacje, w których ktoś prezentuje dziecku takie treści. **Pomocni w interwencji mogą być konsultanci bezpłatnej linii 800 100 100.**

4. CYBERPRZEMOC

- Przemoc w sieci często występuje równolegle z tradycyjną przemocą rówieśniczą, ale specyfika sieci (zasięg, możliwość pozornie anonimowego działania sprawcy) powoduje, że nawet błaha sytuacja może się stać dla dziecka bardzo poważnym doświadczeniem. Reaguj na przejawy cyberprzemocy i naucz dziecko, jak powinno na nie reagować. Nigdy nie bagatelizuj tego problemu. Cyberprzemoc może mieć dramatyczne skutki, zwłaszcza w sytuacji pozostawienia dziecka bez należytego wsparcia. Kategorycznie

przestrzeż je przed angażowaniem się w cyberprzemoc w roli sprawcy. Powiedz dziecku, że jeśli padnie ofiarą przemocy w sieci, powinno się natychmiast zwrócić do ciebie lub innej zaufanej osoby dorosłej (nauczyciel, pedagog szkolny).

- Przekonaj je, że nie powinno odpowiadać na cyberprzemoc przemocą, doprowadzi w ten sposób do jej eskalacji.
- Pokaż dziecku, jak może poinformować moderatora serwisu o nadużyciu (przycisk „Zgłoś nadużycie").
- Pokaż dziecku, jak zabezpieczyć dowody cyberprzemocy (zapisanie e-maili, zrzutów ekranu z agresywnymi komentarzami w serwisach społecznościowych, natrętnych SMS-ów)
- Przekaż dziecku, że jako świadek cyberprzemocy powinno reagować: udzielić wsparcia ofierze, poinformować o sytuacji osobę dorosłą.
- Przekonaj dziecko, że nigdy nie powinno popierać przemocy (np. poprzez udostępnienie krzywdzących materiałów, klikanie „Lubię to!" czy przyłączanie się do złośliwych komentarzy).

5. GRY

- Podstawą bezpieczeństwa młodych graczy jest dobór gier odpowiednich do wieku dziecka, ustalenie z nim zasad korzystania z gier oraz konsekwentne ich egzekwowanie. Reaguj, jeżeli zauważysz, że granie negatywnie wpływa na zachowanie dziecka. Zwróć uwagę na ewentualne symptomy uzależnienia
- Pamiętaj o Systemie PEGI. PEGI to ogólnoeuropejski system klasyfikacji gier (Pan-European Game Information, http://www.pegi.info/pl/) odnoszący się do wieku graczy, informujący o charakterze treści zawartych w grach komputerowych i wideo oraz aplikacjach. Klasyfikacja PEGI pomaga w podjęciu decyzji o zakupie gry dostosowanej do wieku gracza. Oznaczenia odnoszą się do treści zawartych w produkcie (nie jest to informacjach o poziomie trudności czy wymaganych umiejętnościach).

6. NADUŻYWANIE INTERNETU I TELEFONÓW

- Uzgodnij czas, jaki dziecko może poświęcić na korzystanie z mediów elektronicznych i porę dnia na to przeznaczoną. W przypadku dzieci w wieku wczesnoszkolnym i młodszych nie powinno to być więcej niż godzina dziennie.
- Naucz dziecko bezpieczeństwa. Ustal z dzieckiem, z jakich serwisów może korzystać, wybierzcie te, które są dostosowane do jego wieku. Skieruj jego uwagę na pozytywne zastosowania sieci.

- Zainteresuj dziecko formami aktywności niezwiązanymi z mediami elektronicznymi.
- Wykorzystaj oprogramowanie filtrujące i programy kontroli rodzicielskiej, pamiętaj jednak, że dzieci w wieku przedszkolnym i wczesnoszkolnym powinny korzystać z sieci pod okiem rodziców.

Jeśli podejrzewasz, że dziecko nadużywa Internetu lub mediów elektronicznych:

1. Nazwij problem. Porozmawiaj z dzieckiem, powiedz mu, co niepokojącego widzisz w jego zachowaniu.
2. Przyjrzyj się sytuacjom, w których dziecko ucieka w Internet lub sięga po elektroniczne gadżety. Wspólnie z dzieckiem poszukaj alternatywy, np. działań, które sprawiają mu równie dużo przyjemności lub w podobny sposób pomagają odreagować negatywne emocje.
3. Ustalcie harmonogram dnia, by zrównoważyć czas spędzany przez dziecko w sieci i poza nią.
4. Ustalcie zasady i etapy ograniczania korzystania z Internetu. Warto wraz z dzieckiem omówić stopniowe ograniczenie czasu przed monitorem.
5. Nagradzaj sukcesy w ograniczaniu czasu spędzanego w Internecie.
6. Jeśli dziecko korzysta z Internetu lub komputera w sposób, który zagraża jego zdrowiu i/lub życiu(np. zaniedbuje podstawowe potrzeby fizjologiczne), odłącz Internet, wyłącz komputer, ale wyjaśnij dziecku przyczyny tych ograniczeń. Dziecko poczuje się bezpieczniej, gdy będzie znało twoje intencje.

7. ZAKUPY W INTERNECIE

- Nie udostępniaj dziecku numeru swojej karty kredytowej. Sprawdź wiarygodność ewentualnej transakcji i sam wprowadź niezbędne dane. Sprawdź, czy dane karty nie zostały zapamiętane przez aplikację, dzięki której dokonałeś płatności
- Zdecydowana większość stron, na których dokonywane są płatności online, posługuje się protokołem szyfrującym przekazywane dane (HTTPS, znak kłódki w polu adresu). Brak tego bezpiecznego protokołu powinien wzbudzić podejrzenia co do rzetelności sprzedawcy.

8. NETYKIETA

W sieci, tak jak i poza nią, uczciwość i zasady kulturalnego zachowania obowiązują wszystkich. Zwróć na to uwagę swojego dziecka, bo poczucie anonimowości i brak bezpośredniego kontaktu z odbiorcą powodują, że dzieci łatwiej łamią te zasady w Internecie, niż w świecie rzeczywistym.

9. TELEFON I TABLET W SZKOLE

- Jeśli zgadzasz się na to, by dziecko zabierało do szkoły telefon, smartfon lub tablet, sprawdź, czy używanie tego typu urządzeń nie jest zabronione lub w jakiś sposób ograniczane przez regulamin szkoły. Drugą istotną kwestią jest ochrona prywatności – zarówno dziecka, jak i innych osób.
- Zwróć uwagę dziecka na fakt, że urządzenia te nie służą do zabawy w trakcie lekcji. Na czas zajęć telefon powinien być wyłączony lub wyciszony.
- Przypomnij dziecku, że korzystanie z takich urządzeń rządzi się również podstawowymi zasadami kultury i np. nie wolno filmować nikogo ani robić mu zdjęć, jeśli nie wyraża na to zgody.
- Porozmawiaj z dzieckiem o udostępnianiu telefonu innym osobom, w tym jego kolegom. Dostęp do urządzenia oznacza również dostęp do zawartych w nim informacji, którymi właściciel telefonu niekoniecznie chce się dzielić z innymi.
- Pamiętaj, że drogie urządzenie może być przedmiotem zawiści rówieśników dziecka. Rozważ, czy twoje dziecko rzeczywiście wykorzysta wszystkie funkcje najnowocześniejszego smartfona i czy posiadanie go nie narazi dziecka na nieprzyjemne sytuacje (np. Próby kradzieży) lub nie wpłynie negatywnie na jego relacje z rówieśnikami.

10. BLOKOWANIE USŁUG

- Dziecko (z powodu braku wiedzy, niedojrzałości społecznej) może nie być w stanie racjonalnie zarządzać wszystkimi funkcjami swojego urządzenia mobilnego. Dlatego zablokuj usługi, które nie są niezbędne dziecku, a mogą je narazić na dodatkowe koszty lub niebezpieczeństwo.

  Co można zablokować?

  Usługi o podwyższonej płatności. Blokada dotyczy określonych numerów o podwyższonej płatności, a także wiadomości SMS i MMS. Usługa jest bezpłatna u wszystkich operatorów. Blokadę można wprowadzić również w aplikacji kontroli rodzicielskiej. Alternatywą dla blokady jest ustanowienie limitu kosztów połączeń do określonych numerów, w tym numerów o podwyższonej płatności.
- Połączenia wychodzące do określonych numerów. Blokada dostępna u operatora lub poprzez zmianę ustawień telefonu.
- Połączenia przychodzące z konkretnych numerów, np. od osób, które nękają dziecko. Blokada dostępna jest z poziomu telefonu.

- Połączenia przychodzące z numerów zastrzeżonych (z ukrytą prezentacją numeru).
- Dostęp do stron ze szkodliwymi treściami. Blokadę dostępu do stron z treściami dla dorosłych możemy ustanowić za pomocą programów kontroli rodzicielskiej.

11. WI-FI W DOMU I MIEJSCACH PUBLICZNYCH

- Twoje dziecko może mieć wpływ na bezpieczeństwo i jakość działania domowej sieci bezprzewodowej.
- Zastanów się, czy przekazać mu dane pozwalające na dostęp do sieci Wi-Fi, czy też jedynie zapisać je w urządzeniach, z których dziecko korzysta. Jeżeli zdecydujesz się na pierwsze rozwiązanie, powiedz mu, by nie zmieniało ustawień sieci bez twojej zgody oraz nie udostępniało nazwy i hasła do Wi-Fi osobom trzecim, np. kolegom.
- Bezprzewodowy Internet udostępniany jest na terenie szkół, bibliotek, galerii handlowych i kawiarni, a coraz częściej nawet w parku lub na ulicy. Zazwyczaj sieci te są ogólnodostępne, a korzystaniez nich nie wymaga podawania hasła. Nie powinniśmy traktować ich jednak jako bezpiecznych – dużo łatwiej w nich o możliwość przechwycenia danych, przekierowania na strony ze szkodliwymi treściami bądź zainfekowania urządzenia wirusem.
- Zwróć uwagę dziecka, by używając ogólnodostępnego Wi-Fi, nie korzystało z serwisów wymagających logowania (poczta, serwisy społecznościowe) lub podawania danych osobowych. Jeśli się na to decyduje, to tylko w sytuacji, kiedy dane przekazywane są w postaci zaszyfrowanej (protokół HTTPS – informacja w oknie adresu przeglądarki, widoczna miniaturowa kłódka).
- Wyposaż urządzenie dziecka w filtry kontroli rodzicielskiej, dzięki którym będzie chronione przed szkodliwymi treściami, takimi jak np. pornografia. Pamiętaj jednak, że filtry nie dają stuprocentowego zabezpieczenia przed materiałami tego typu.
- Upewnij się, że w urządzeniu korzystającym z publicznej sieci, nawet tylko w celu przeglądania
  stron, jest włączona zapora sieciowa (firewall) oraz zaktualizowany program antywirusowy.
- Przekonaj dziecko, by wyłączało Wi-Fi w swoim telefonie, jeśli z niego nie korzysta i usuwało zapamiętane przez urządzenie sieci publiczne. Jeśli sieć taka została zapamiętana w danym urządzeniu, może się ono z nią połączyć, nawet bez wiedzy użytkownika. Dodatkową zaletą wyłączonego Wi-Fi jest dłuższy czas pracy bez ładowania baterii.

12. SKONFIGURUJ USTAWIENIA BEZPIECZEŃSTWA W URZĄDZENIU

Udostępniając dziecku urządzenie z dostępem do Internetu, należy odpowiednio skonfigurować ich system operacyjny. Jest to dosyć proste i powoduje znaczne ograniczenie dostępu do szkodliwych treści. W przypadku tabletów i smartfonów z systemem Android warto odpowiednio skonfigurować Google Play, przeglądarkę oraz aplikację serwisu YouTube. W nowszych wersjach systemu istnieje także możliwość stworzenia profilu ograniczonego, który będzie stanowił bezpieczną przestrzeń dla dziecka.

Właściciele urządzeń mobilnych z systemem iOS (iPad, iPhone) mogą ograniczyć dziecku dostęp do wybranych treści, korzystając z funkcji „Ograniczenia", która znajduje się w ustawieniach ogólnych. Określimy tam m.in. ograniczenie wiekowe dotyczące wyświetlanych filmów oraz używanych programów.

Zainstaluj program do kontroli rodzicielskiej

W celu poprawy bezpieczeństwa dzieci korzystających z Internetu warto zainstalować na urządzeniach, z których korzystają, oprogramowanie do kontroli rodzicielskiej. Programy tego typu dają możliwość filtrowania treści, kontrolowania czasu i aktywności dziecka online itp. Aplikacje tego typu na tablety i smartfony dostępne są w sklepach online właściwych dla danego systemu operacyjnego. Użytkownicy komputerów pobiorą takie programy z sieci lub kupią je w sklepie. Część programów i aplikacji kontroli rodzicielskiej udostępnianych jest gratis, za inne trzeba zapłacić. Zdarzają się również propozycje darmowych programów z płatnymi dodatkowymi funkcjonalnościami. Duża grupa programów działa na zasadzie abonamentu. Zazwyczaj w okresie próbnym można przetestować możliwości programu. Warto zwrócić uwagę, czy wybrany przez nas pakiet do kontroli rodzicielskiej umożliwia zabezpieczenie kilku urządzeń jednocześnie.

Źródła:

- https://www.edukacja.fdds.pl/ Bezpieczeństwo dzieci i młodzieży w Internecie "Bezpiecznie Tu i Tam". Kurs dla rodziców i profesjonalistów
- https://www.edukacja.fdds.pl/ Dziecko i media. Poradnik dla rodziców
- Poradnik dla Rodziców – www.cyfrowobezpieczni.pl