

BEZPIECZEŃSTWO DZIECI ONLINE

Kompendium dla rodziców uczniów

Szkoły Podstawowej nr 350 im. Armii Krajowej w Warszawie

Zmieniająca się rzeczywistość, rozwój technologii, przenikanie świata online i offline postawiły przed dorosłymi nowe wyzwanie – konieczność przygotowania dziecka do sprawnego i bezpiecznego korzystania z nowych mediów. W ten proces muszą być zaangażowani zarówno rodzice, jak i pedagodzy oraz przedstawiciele instytucji i służb odpowiedzialnych za rozwój, wychowanie i bezpieczeństwo dzieci.

Szanowny 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, zadбай o to, by wiedziało, że może się do ciebie zwrócić z problemami.

Nawet jeśli zadbałeś o zabezpieczenia 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. Kiedy udostępnić dziecku Internet, telefon, laptop, tablet?

- -Rozmawiaj z dzieckiem, mów mu o zagrożeniach, na które może natrafić w Internecie. Naucz je, jak może sobie poradzić, jeśli będzie miało kontakt ze szkodliwymi treściami lub nieprzyjemnym zachowaniem innego internauty. Zainteresowanie dorosłego daje dziecku poczucie bezpieczeństwa i wykształca dobre nawyki korzystania z sieci i sprzętu elektronicznego. -
- Bardzo duże znaczenie ma to, w jaki sposób sam posługujesz się Internetem i urządzeniami elektronicznymi. Jesteś dla swojego dziecka przykładem.
- Ustal z dzieckiem zasady korzystania z Internetu. Powiedz mu, czego od niego oczekujesz. Ważne, by zasady korzystania z komputera były adekwatne do wieku dziecka. -
- Stosuj programy filtrujące treści, zabezpieczenia w przeglądarkach i oprogramowanie kontroli rodzicielskiej. Pamiętaj również o odpowiednim zabezpieczeniu komputera przed złośliwym oprogramowaniem. -
- Korzystajcie wspólnie z komputera – zawsze dziecko razem z rodzicem. Komputer nie może niczego dziecku zastępować: nie może być nagrodą, uspokajac, być sposobem na nudę lub brak kontaktu z rodzicami. -
- Warto przeglądać strony, z których może korzystać dziecko i sprawdzać, w jakie miejsca w sieci prowadzą. -
- Nie traktuj sprzętu elektronicznego i Internetu jako jedyne sposbu spędzania wolnego czasu przez twoje dziecko. Pomyśl o innych zajęciach, również tych ruchowych, w które warto angażować dziecko. Zadбай, by miało znajomych i spotykało się z nimi w realnym świecie. -

- Rozmawiaj z dzieckiem o grach i stronach, z których korzysta. Wspólnie z nim odkrywaj możliwości nauki i zabawy, jakie oferuje Internet. Na bieżąco oceniaj, co jest dla dziecka dobre, a co nie. - Rozmawiaj o tym, co się dzieje online. Dziecko poznaje świat przez bezpośredni kontakt, towarzyszące temu słowa nadają mu znaczenie. Młodym ludziom często brakuje umiejętności oceny i selekcjonowania informacji znalezionych w sieci. Dzięki obecności rodziców i rozmowie z nimi dzieci mają możliwość uczenia się tego, co jest wiarygodne i sprawnego korzystania z zasobów online. -
- Naucz dziecko zasady ograniczonego zaufania do osób, które spotykają w sieci. Jeśli zgadzasz się na kontakty dziecka z osobami poznanymi w Internecie, monitoruj te znajomości. Reaguj na wszelkie podejrzaną sytuacje. Zapewnij dziecko, że w sytuacji zagrożenia zawsze może liczyć na twoją pomoc. -
- Jeśli jesteś świadkiem podejrzaną sytuacji, w której bierze udział twoje dziecko, rozmawiaj z nim, daj mu poczucie, że ma w tobie oparcie. Razem szukajcie najlepszego wyjścia. Nie zostawiaj dziecka sam na sam z jego problemami. Nawet tymi, które wydają ci się niepoważne, bo istnieją wyłącznie w Internetowym świecie. Pamiętaj, że to tylko dziecko – może mu brakować dystansu nawet do tak błahych spraw, jak natrętne wpisy Internetowego trolla. -
- Umieść komputer w ogólnodostępnym miejscu, by wiedzieć, co robi twoje dziecko w internecie. -
- Ustal czas, który wolno dziecku spędzić przy komputerze i konsekwentnie pilnuj przestrzegania tych ustaleń.

2. Bezpieczny adres, login i hasło

- Ani adres mailowy dziecka, ani login do usług sieciowych nie powinny ujawniać informacji na temat dziecka – nie mogą zawierać imienia, nazwiska, informacji o wieku lub roku urodzenia ani innych prywatnych danych, pozwalających na zidentyfikowanie dziecka. W Internecie dziecko powinno się posługiwać „nickiem”, czyli Internetowym pseudonimem. To pod nim będą widoczne efekty jego aktywności w sieci.
- Nawet najbardziej złożone hasło nie ochroni konta, jeśli jego użytkownik sam je zdradzi. Przekaż dziecku, że nie powinno hasła nigdzie notować, a przede wszystkim – nie powinno się nim dzielić ze swoimi znajomymi, nawet najbardziej zaufanymi, nawet w dowód przyjaźni.
- Naucz dziecko, by po zakończeniu korzystania z danego serwisu ZAWSZE się z niego wylogowywało i nie zaznaczało opcji zapamiętywania hasła przez przeglądarkę, przede wszystkim na ogólnodostępnych komputerach.

3. Serwisy społecznościowe

Jeżeli zgadzasz się na korzystanie przez dziecko z serwisów społecznościowych (popularne serwisy społecznościowe nie są przeznaczone dla najmłodszych dzieci, obowiązująca np. na Facebooku granica 13 lat) zawnazsu ustal z nim zasady bezpieczeństwa. -

- Profil dziecka nie może być profilem otwartym, dostępnym dla wszystkich. W niektórych serwisach jest to ustawienie domyślne. Zmiany można dokonać w zakładce „ustawienia prywatności”, należy wybrać jego widoczność tylko dla bliskich znajomych. -

- Ustal z dzieckiem, jakie informacje na swój temat może zamieścić na profilu. Nie należy publikować informacji ułatwiających zidentyfikowanie dziecka, w tym adresu domowego, nazwy i adresu szkoły. -
- Profil powinien być zabezpieczony silnym hasłem, przypomnij dziecku o konieczności trzymania go w tajemnicy, nawet przed najbliższymi znajomymi. Jego ujawnienie może oznaczać utratę przez twoje dziecko Internetowej tożsamości i próby podszywania się pod nie – na przykład publikowania złośliwych, wymierzonych w inne osoby wpisów. -
- Ostrzeż dziecko przed dodawaniem do grona znajomych osób, których nie zna osobiście. Nie powinno również wysyłać do takich osób zaproszeń do grona znajomych. -
- Porozmawiaj z dzieckiem o zdjęciach i filmach, które publikuje na profilu, powinno unikać zdjęć ośmieszających (siebie i innych), o charakterze erotycznym lub seksualnym, wszelkich, które mogą być wykorzystane przeciwko dziecku. Naucz dziecko korzystania z funkcji udostępniania zdjęć tylko konkretnym osobom. -
- Zwróć uwagę dziecka na zamieszczane przez nie komentarze lub statusy. Nie mogą być wulgarne, obrażające lub w inny sposób kogoś krzywdzące. -
- Nadmierne korzystanie z serwisów społecznościowych może prowadzić do uzależnienia. Ustal z dzieckiem limit czasu na korzystanie z portali tego typu. -
- Przekaż dziecku, że powinno ignorować i usuwać wszelkie Internetowe zaczepki, ataki lub złośliwości pod swoim adresem, a w przypadku, gdy się powtarzają – zgłosić je moderatorowi serwisu. Reagowanie na nie agresją prowadzi jedynie do ich eskalacji. -
- Przekonaj dziecko, że powinno cię informować o wszystkich niepokojących sytuacjach.

4. Blogi/wideoblogi

Blog, czyli serwis Internetowy zawierający przemyślenia, osobiste lub tematyczne, wpisy, samodzielnie przygotowane materiały wideo lub zdjęcia, to częsta forma ekspresji młodych internautów. Może być ciekawą formą prezentowania i rozwijania pasji dziecka. Tym bardziej trzeba zadbać o jego bezpieczeństwo.

- - Zapoznaj się z serwisem, na którym dziecko prowadzi lub planuje prowadzić blog, sprawdź, czy udostępnia on regulamin, informuje o polityce prywatności. -
- Porozmawiaj z dzieckiem o tym, jakie materiały może bezpiecznie publikować na blogu. Zwróć szczególną uwagę na prywatne zdjęcia i filmy. Z młodszym dzieckiem możesz się umówić, że każdorazowo będziesz akceptował materiały przed ich publikacją. -
- Zwróć uwagę dziecka, by nie podawało na blogu nazbyt prywatnych informacji dotyczących jego i bliskich osób (przede wszystkim danych osobowych). -
- Porozmawiaj z dzieckiem o szanowaniu praw autorskich związanych z materiałami, które decyduje się publikować online.

5. 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). -
- Jeśli nie wiesz, jak rozwiązać problem związany z cyberprzemocą, zwróć się do konsultantów Helpline.org.pl (tel. 800 100 100, www.helpline.org.pl)

6. Niebezpieczne kontakty

Dzieci samodzielnie korzystające z Internetu są narażone na kontakty z obcymi osobami, m.in. za pośrednictwem czatów, komunikatorów, poczty elektronicznej, serwisów społecznościowych. Nie wszyscy użytkownicy sieci mają uczciwe intencje – dziecko może paść ofiarą próby wyłudzenia danych osobowych, kradzieży lub stać się źródłem informacji o bliskich, co może ułatwić popełnienie przestępstwa przeciwko nim. Zagrożeniem są również osoby próbujące zainteresować je niebezpiecznymi treściami (np. pornografią), zachowaniami (np. obrót narkotykami) lub ideami (np. faszyzmem, sektami).

- Młodsze dzieci powinny mieć ograniczony dostęp do serwisów komunikacyjnych, korzystać z nich jedynie w obecności rodziców. -
- Uświadom dziecku, jakie możliwości manipulacji daje Internet i jakie intencje mogą mieć obce osoby próbujące nawiązać z nim kontakt. -
- Przekaż dziecku, żeby kontaktowało się online jedynie z osobami, które zna spoza sieci. W przypadku nowych znajomości ustal z dzieckiem, że cię o nich poinformuje. -
- Przestrzeż dziecko przed przyjmowaniem w serwisach społecznościowych zaproszeń do grona znajomych od osób nieznanym. -
- Zwróć uwagę dziecka, by w kontaktach online z nieznanymi nie przysyłało prywatnych informacji i materiałów (zdjęć, filmów). -
- Ustal z dzieckiem kategoryczny zakaz przysyłania w sieci materiałów o charakterze seksualnym. Wyjaśnij mu, jakie wiążą się z tym zagrożenia.
- Przypomnij dziecku, że w sytuacji niepewności lub zagrożenia ze strony kogokolwiek w sieci zawsze powinno się do ciebie zwrócić o pomoc.
- Zwróć uwagę dziecka na zagrożenia związane ze spotkaniami z osobami poznanymi w sieci. Już samo nawiązywanie przez osobę dorosłą w Internecie kontaktów z dzieckiem, których celem jest doprowadzenie do spotkania i wykorzystania seksualnego lub pozyskanie

od dziecka materiałów pornograficznych, jest przestępstwem. Zawsze, kiedy podejrzewasz, że twoje dziecko padło ofiarą uwodzenia, poinformuj o tym policję

7. Sexting i kamerki Internetowe

W przypadku sextingu (zjawiska polegającego na przesyłaniu osobistych zdjęć i filmów o charakterze seksualnym za pośrednictwem telefonu i Internetu), zdarza się, że intymne zdjęcia trafiają do sieci – czasami wbrew intencjom ich odbiorcy, czasami w formie zemsty lub szantażu. W każdym z tych przypadków – jeśli już zostaną rozpowszechnione – ich usunięcie może się okazać niemożliwe. Podobnym zagrożeniem wobec dzieci są serwisy Internetowe oferujące transmisję na żywo – dla pojedynczego odbiorcy lub wielu widzów. Część z nich specjalizuje się w pokazach erotycznych, część umożliwia zarabianie pieniędzy osobom występującym przed kamerą Internetową

- Naucz dziecko, żeby pod żadnym pozorem nie wysyłało ani nie publikowało w sieci zdjęć i filmów nago lub o charakterze seksualnym. Rozmawiaj z dzieckiem o seksualności i zagrożeniach związanych z upublicznianiem intymnych zdjęć.

8. 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 informacja o poziomie trudności czy wymaganych umiejętnościach).

9. 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.

10. 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.

11. 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.

12. Wiarygodność informacji

Naucz dziecko zasady ograniczonego zaufania do treści dostępnych online. Naucz je również weryfikowania rzetelności informacji dostępnych w Internecie.

- Pokaż dziecku, jak poszukiwać informacji w sieci. Naucz je metod zaawansowanego wyszukiwania.
- Naucz dziecko weryfikowania treści poprzez porównywanie informacji z różnych źródeł.
- Zwróć uwagę dziecka na fakt, że blogi i inne fora wymiany opinii prezentują subiektywne poglądy ich autorów i obarczone są wysokim ryzykiem nierzetelności.
- Pokaż dziecku sprawdzone serwisy, które uznajesz za wiarygodne.
- Zwróć uwagę dziecka na treści marketingowe, które mogą sprawiać wrażenie obiektywnych informacji.
- Przekonaj dziecko, by w sytuacji wątpliwości co do wiarygodności znalezionych w sieci treści zwróciło się do ciebie o pomoc.

13. Publikowanie zdjęć dzieci w sieci

Przed zamieszczeniem zdjęcia dziecka w Internecie zastanów się, czy nie będzie to dla niego w przyszłości źródłem wstydu i zakłopotania.

- Profil, na którym publikowane są materiały, ustaw jako zamknięty (nieдоступny dla osób nieznanym).
- Każdorazowo w „ustawieniach” oznaczaj dostępność zdjęcia jako np. widoczne tylko dla rodziny i najbliższych znajomych.
- Nie podpisuj zdjęć imieniem i nazwiskiem dziecka. Fascynacja portalami społecznościowymi powoduje, że rodzice zakładają swoim pociechom profile już w wieku niemowlęcym. To niezgodne z regulaminem większości tego typu serwisów, przede wszystkim jednak – to narażanie bezpieczeństwa dziecka i jego prywatności na niepotrzebne ryzyko.

14. Zdrowie

Nadmierne korzystanie z mediów elektronicznych przez dzieci i młodzież może mieć negatywny wpływ na ich zdrowie. Spędzanie godzin przed komputerem, w pozycji zaprzeczającej zasadom ergonomii i w złych warunkach oświetleniowych, może spowodować: skrzywienie kręgosłupa, zanik mięśni, zwyrodnienie stawów (np. zespół cieśni nadgarstka, będący efektem długotrwałego używania myszy), otyłość, choroby wzroku (np. zespół suchego oka, wynikający z mniejszej częstości mrugania przed ekranem komputera).

- Ustal z dzieckiem pory korzystania z komputera, maksymalny dzienny czas, jaki może spędzić przy komputerze i innych mediach, czas jednorazowej sesji. Zadbaj o dobrze zorganizowane stanowisko komputerowe dziecka:

15. Zdrowie a urządzenia mobilne

Co prawda, badania nie rozstrzygają jednoznacznie, czy korzystanie z telefonów komórkowych wpływa np. na zwiększoną zapadalność na choroby nowotworowe, warto jednak, szczególnie w przypadku dzieci, zwrócić uwagę na bezpieczeństwo ich użytkowania. Wydawane do tej pory zalecenia podkreślają, że dzieci i młodzież powinny korzystać z telefonów komórkowych z umiarem. Jeżeli zgadzasz się, by twoje małe dziecko używało własnego telefonu komórkowego, zadbaj, by korzystanie z niego było ograniczone do niezbędnego minimum, maksymalny czas przeznaczony na rozmowy należy ustalić również w przypadku starszych dzieci (np. 20-30 minut dziennie).

16. Bezpieczeństwo sprzętowe

Niezbędnym minimum pozwalającym na ochronę komputera przed złośliwym oprogramowaniem jest posiadanie w nim zaktualizowanego programu antywirusowego i zapory sieciowej oraz systematyczna instalacja wydawanych aktualizacji oprogramowania i systemu

- Jeśli z komputera korzysta dziecko (nawet, jeśli jest to jego własny komputer, a przede wszystkim – jeśli jest to komputer używany przez kilku domowników), warto rozważyć stworzenie dla niego osobnego konta użytkownika z ograniczonymi uprawnieniami. Nie będzie wówczas mogło np. samodzielnie instalować nowych programów, co zminimalizuje ryzyko zainfekowania komputera złośliwym oprogramowaniem.

Zainstalowanie nowego programu będzie wymagało hasła administratora, którym dysponować będzie rodzic.

- Ostrzeż dziecko, że obok wirusów zagrożeniem są również fałszywe alarmy lub żarty, np. rozsyłana na portalach społecznościowych informacja o konieczności usunięcia jednego z istotnych plików systemowych. Przekonaj dziecko, by nie „naprawiało” komputera bez twojej wiedzy i informowało cię o napotkanych problemach.

17. Kontrola rodzicielska

Programy ochrony rodzicielskiej dają możliwość utworzenia niezależnych profili dla różnych użytkowników – innego dla dziecka, innego dla osoby dorosłej. Panel administracyjny (pozwalający na zmianę ustawień) jest chroniony hasłem, dzięki czemu rodzic ma pewność, że dziecko korzysta tylko z przeznaczonego i ustawionego specjalnie dla niego profilu.

- Żaden filtr, żadne oprogramowanie kontroli rodzicielskiej nie zapewnia stuprocentowej skuteczności. Ich uruchomienie nie oznacza, że można zapomnieć o siedzącym przy komputerze dziecku. Żaden z systemów kontroli rodzicielskiej nie jest w stanie zastąpić uwagi rodzica.

18. 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 zazdrości 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.

19. Blokowanie dostępu

Dostęp do telefonu, smartfona lub tabletu można zabezpieczyć hasłem, gestem (wzorem) lub kodem PIN. Razem z dzieckiem sprawdź, jaki sposób blokowania jest dostępny w jego telefonie, dzięki czemu w razie pozostawienia urządzenia bez opieki bądź utraty kontroli nad nim niepowołane osoby będą miały utrudniony dostęp do jego zawartości. Pamiętaj, by hasło, symbol lub kod nie były zbyt oczywiste, zwróć również uwagę dziecka na fakt, że są to informacje bezwzględnie poufne i nie powinno się nimi dzielić z rówieśnikami.

20. Mikropłatności

Mikropłatności służą do dokonywania opłat za np. usługi online, doładowanie konta w grze, zakup pakietów Internetowych. Popularnymi formami mikropłatności są SMS-y o podwyższonej płatności oraz wirtualne portfele.

- Przy numerze zaczynającym się od cyfry 7, kolejna cyfra po niej jest informacją o koszcie SMS-a. Analogicznie, w przypadku numeru SMS-a zaczynającego się od cyfry 9 – dwie kolejne cyfry ujawnia cenę netto SMS-a.

21. 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.

22. Co telefon wie o swoim użytkowniku?

Smartfony powoli zaczynają zastępować komputery. Angażując urządzenia mobilne w każdy aspekt naszego życia, warto uświadomić sobie fakt, że przechowując nasze różnorodne, często poufne dane, stają się one źródłem informacji o nas. Nawet najprostszy telefon zawiera sporo informacji na nasz temat: spis kontaktów, rejestr rozmów, odebrane i wysłane SMS-y, zdjęcia. W bardziej zaawansowanych urządzeniach mogą to być np. pliki pobrane jako załączniki do poczty elektronicznej lub numery karty kredytowej zapisane w aplikacjach. Niebezpieczeństwo rodzić mogą również notatki zawierające PIN-y lub np. hasła do kont. Warto pamiętać, że zagrożeniem jest nie tylko utrata danych i problemy z ich odtworzeniem, ale przede wszystkim – dostęp do nich niepowołanych osób.

- Zwróć uwagę dziecka, by nie wykorzystywało w telefonie funkcji zapamiętywania hasła do serwisów i usług sieciowych – w przypadku przejęcia telefonu przez inną osobę będzie ona miała swobodny dostęp np. do konta pocztowego naszego dziecka.
- Dane są gromadzone w usługach Internetowych. Warto pamiętać, że jeśli coś w Internecie jest za darmo, to najprawdopodobniej my stajemy się towarem. Firmy Internetowe, udostępniając bezpłatnie szereg usług, wykorzystują informacje na temat użytkowników, np. przekazując je innym firmom w celach reklamowych. Dzięki temu np. wyszukiwanie stron

poświęconych danym technicznym tabletów skutkuje wyświetlaniem przez kilka kolejnych dni reklam tabletów na stronach informacyjnych. Warto również zdać sobie sprawę z tego, że wyniki wyszukiwania mogą nie być obiektywne i różnić się pomiędzy komputerami, ponieważ zostały dopasowane do naszych preferencji ustalonych na podstawie historii surfowania i plików cookies. To swego rodzaju bańka informacyjna, która uniemożliwia nam dostęp do pełnych zasobów Internetu.

23. Geotagowanie

Geotagowanie to inaczej umieszczanie informacji dotyczących lokalizacji danej osoby lub obiektu. Dzięki urządzeniom mobilnym wyposażonym w GPS oznaczanie pozycji może odbywać się automatycznie. Geotagowanie jest wykorzystywane np. przez portale społecznościowe, które informują nas, że znana nam osoba odwiedziła jakieś miejsce.

- Warto się zastanowić, czy chcemy, by informacja o tym, gdzie przebywa nasze dziecko, była dostępna w sieci. Śledzenie kolejnych lokalizacji dodanych w portalu społecznościowym łatwo pozwala ustalić miejsca, w których ono systematycznie bywa.
- Dodatkowym aspektem jest geotagowanie zdjęć (również wykonanych tabletem lub smartfonem). Jeśli korzystamy z tej opcji, w pliku zdjęcia zostaje zaszyta informacja określająca miejsce jego wykonania. W funkcję geotagowania zdjęć mogą być wyposażone również niektóre aparaty fotograficzne. O ile bardzo ułatwia to katalogowanie np. fotografii z podróży, o tyle w przypadku zdjęć rodzinnych może już być zagrożeniem – upubliczniając zdjęcia robione np. we własnym ogrodzie wraz ze współrzędnymi zapisanymi przez GPS, jasno określamy miejsce, w którym mieszkamy.

24. Wi-Fi w domu

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 zmieniał ustawień sieci bez twojej zgody oraz nie udostępniał nazwy i hasła do Wi-Fi osobom trzecim, np. kolegom.

25. Publiczne sieci Wi-Fi

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 korzystanie z 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 miniaturka kłódka).

- WyposaŹ 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 zapor sieciowa (firewall) oraz zaktualizowany program antywirusowy.
- Przekonaj dziecko, by wyłączyło 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.

26. Kopie zapasowe

Utrata danych zapisanych na urządzeniu mobilnym należącym do dziecka (zdjęć, plików muzycznych, ale i zawartości książki telefonicznej) może być bolesna, nawet jeśli mają one jedynie wartość sentymentalną. Upadek lub zalanie urządzenia wodą, uszkodzenie karty pamięci może oznaczać, że dostęp do danych zapisanych w urządzeniu będzie niemożliwy (lub – ze względu na koszty odzyskiwania danych – nieopłacalny).

- Większość producentów urządzeń mobilnych udostępnia swoim użytkownikom bezpłatne wirtualne dyski, służące m.in. do tworzenia kopii zapasowych zawartości telefonu i wszystkich indywidualnych ustawień. Kopia zapasowa może być również przydatna w przypadku zmiany telefonu na nowy – pozwoli przenieść zawartość starego urządzenia i większość jego ustawień.
- Zwróć uwagę dziecka na fakt, że zawartość jego konta w chmurze jest bezpieczna do momentu, dopóki nie udostępni innym osobom hasła.

27. Bluetooth

Bluetooth pozwala na bezprzewodową wymianę informacji z innymi urządzeniami na niewielkie odległości. Technologia ta może być wykorzystywana np. do podłączenia zestawu głośnomówiącego do telefonu, komunikację z zewnętrznym urządzeniem GPS. Jednocześnie systematycznie pojawiają się informacje na temat odkrywania nowych metod włamań za pośrednictwem Bluetootha, polegających np. na wydobywaniu zawartości urządzenia, a nawet generowaniu kosztownych połączeń. Przekaż dziecku, by nie akceptowało prób sparowania urządzenia z innym urządzeniem, jeśli go nie zna, a w przypadku natrętnego ich powtarzania – zamknęło łączność Bluetooth.

Źródło:

1. <https://www.edukacja.fdds.pl/> *Bezpieczeństwo dzieci i młodzieży w Internecie “Bezpiecznie Tu i Tam”. Kurs dla rodziców i profesjonalistów*
1. <https://www.edukacja.fdds.pl/> *Dziecko i media. Poradnik dla rodziców*