

Bezpieczny Internet

Podstawowe zasady bezpieczeństwa - porady dla rodziców

1. Ustal z dzieckiem zasady korzystania z sieci adekwatne do jego wieku, takie jak: maksymalny czas spędzany w sieci, serwisy i strony internetowe, które może odwiedzać, sposoby reagowania na niebezpieczne sytuacje.

Możesz w tym celu posłużyć się „Umową o bezpiecznym korzystaniu z Internetu”, która jest dostępna w serwisie. By zwiększyć prawdopodobieństwo, że dziecko będzie przestrzegało zasad, nie narzucaj ich, ale uzgodnij je ze swoją pociechą – znajdźcie kompromis. Pamiętaj jednak o konsekwencji – robienie wyjątków, łamanie uzgodnień spowoduje, że dziecko nie będzie traktowało tych zasad poważnie.

2. Umieść komputer w powszechnie dostępnym miejscu w domu. Bądź obok swojego dziecka, kiedy surfuje po Internecie.

Nie musisz być policjantem, który sprawdza każdą ze stron, na które wchodzi Twoje dziecko. Nie pozwól jednak, by dziecko zamykało się sam na sam z komputerem w swoim pokoju. Jeśli komputer zostanie umieszczony tam, gdzie bywają wszyscy domownicy, jest mniejsze prawdopodobieństwo, że dziecko, zwłaszcza małe, trafi na treści nieprzeznaczone dla niego lub wejdzie w kontakt z niebezpieczną osobą. Twoje dziecko potrzebuje poczucia bezpieczeństwa, które możesz mu dać swoją obecnością i bliskością. Bądź z nim po to, by służyć mu radą i wskazać potencjalne zagrożenia.

3. Naucz dziecko zasady ograniczonego zaufania do osób i treści, na które trafia w sieci. Jeśli dopuszczasz możliwość kontaktów dziecka z osobami poznanymi w Internecie, kontroluj te znajomości. Reaguj na wszelkie podejrzane sytuacje! Zapewnij dziecko, że w sytuacji zagrożenia zawsze może liczyć na Twoją pomoc!

Jako rodzic jesteś odpowiedzialny zarówno za wprowadzenie swojego dziecka w świat realny, jak i wirtualny. Naucz je odróżniać wiarygodne źródła i fakty od wiadomości wyspanych z palca i informacyjnego szumu. Przekonaj je, że nie każda osoba spotkana w sieci jest tym, za kogo się podaje, a tym bardziej, że nie zawsze jest warta zaufania i otwartości. Naucz je, by samo nie rozpowszechniało fałszywych wiadomości, zwłaszcza dotyczących innych ludzi. Jeśli jesteś świadkiem podejrzanej sytuacji w której bierze udział Twoje dziecko – rozmawiaj z nim, daj mu poczucie, że ma w Tobie oparcie. Razem szukajcie najlepszego wyjścia z tej sytuacji. Nie zostawiaj dziecka sam na sam z jego problemami, nawet tymi, które wydają Ci się niepoważne, bo istniejące wyłącznie w internetowym świecie. To tylko dziecko – może mu brakować dystansu nawet do tak błahych spraw, jak natrętne wpisy internetowego trolla.

4. Naucz dziecko chronić prywatność. Jeżeli zgadzasz się na korzystanie przez dziecko z serwisów społecznościowych, pomóż mu stworzyć bezpieczny profil, maksymalnie chroniący jego prywatność.

Dzieci często są nazbyt łatwowierne. Nie potrafią przewidzieć konsekwencji, jakie mogą je spotkać chociażby dlatego, że ujawniły swój wiek. Internet jest polem działania pedofilów, a informacja o wieku dziecka jest dla nich ogromnym ułatwieniem. Podobnie niebezpieczne może być ujawnienie przez dziecko numeru telefonu lub adresu zamieszkania. Jeśli zgadzasz się, by dziecko angażowało się w znajomości zdobywane w serwisach społecznościowych, naucz je chronienia informacji na swój temat, ale i ograniczonego zaufania do osób, które – często natarczywie lub podstępnie – chcą się z nim zaprzyjaźnić. Nie znasz przecież ich intencji.

5. Przekonaj dziecko, by zawsze konsultowało z Tobą materiały, które publikuje w Internecie. Naucz je rozważli w takich sytuacjach.

Tak, jak w przypadku publikacji danych osobowych, dziecko nie zawsze jest w stanie realnie ocenić konsekwencje opublikowania w sieci jakichkolwiek materiałów. Internet nie zapomina – coś, co raz trafiło do sieci, dzięki możliwości wielokrotnego powielenia i umieszczenia na innych stronach, serwerach, serwisach, pozostaje praktycznie na zawsze. Dotyczy to zarówno zdjęć, filmów, jak i np. wpisów na internetowych forach. Bezmyślnie zamieszczone zdjęcie lub film będący dokumentacją głupiej zabawy mogą się zemścić w przyszłości, nawet tej odległej, bo dorosłej. Podobnie jest z materiałami, których założeniem jest obrażenie kogoś lub sprawienie mu przykrości. Umieszczenie ich w Internecie oznacza utratę kontroli nad nimi i ich rozpowszechnieniem, skutki ich publikacji mogą okazać się nieodwracalne.

6. Nie narażaj dziecka, publikując bezkrytycznie jego zdjęcia w sieci!

Również rodzice często zapominają o podstawowych zasadach bezpieczeństwa w Internecie, publikując na swoich stronach lub w serwisach społecznościowych zdjęcia swoich dzieci, nie zważając, że mogą one natychmiast trafić do kolekcji pedofila. Internet wciąż jest polem ich działań, a znalezione zdjęcia dzieci mogą jedynie ułatwić im wybór ofiary i dotarcie do niej. Bezkrytyczne zamieszczanie więc w Internecie ich zdjęć z wakacji – np. w stroju kąpielowym – to niepotrzebne wystawianie ich na ryzyko. Podobnie rzecz się ma ze zdjęciami niemowlaków – czy na pewno chcesz, by za kilkanaście lat przyszły szef Twojego dziecka widział je na zdjęciu z pieluchą?

7. Chronić komputer dziecka przed niewłaściwymi treściami. Upewnij się, że na komputerze Twojego dziecka działa zaktualizowany program antywirusowy i zaporę sieciową. Używaj filtru antyspamowego chroniącego program e-mailowy. Stosuj dostępne na rynku oprogramowanie filtrujące. Korzystaj z programów kontroli rodzicielskiej. Pamiętaj jednak, że żaden program nie jest w stanie zastąpić uwagi rodzica.

Naucz swoje dziecko, by samo dbało o swój komputer. Im mniej znajdzie się w nim wirusów, trojanów i innych śmieci, tym wygodniejsze i bezpieczniejsze będzie korzystanie z niego. Pozwoli to ograniczyć frustrację wynikającą z powolnego ładowania się, wieszania się stron lub wyskakujących okienek, czasami z treściami niebezpiecznymi dla dziecka. Zadaniem oprogramowania filtrującego jest uniemożliwienie dostępu do stron z potencjalnie niebezpiecznymi treściami. Nie chodzi wyłącznie o np. strony pornograficzne, ale i o te, które namawiają do agresji lub autoagresji (w tym samobójstw), propagujących nazizm lub anoreksję. Pokaż swojemu dziecku Katalog BeSt, a na pewno znajdzie tam zajmujące serwisy. Na pewno zainteresuje je również strona Sieciaków. Pamiętaj, że żaden program filtrujący nie zastąpi rozsądku dorosłej osoby. Nawet jeśli

komputer Twojego dziecka ma zainstalowane wszelkie dostępne programy do filtrowania treści, nie trać kontaktu ze swoim dzieckiem, nie zrzucaj odpowiedzialności za jego wychowanie na komputerową aplikację.

8. Upewnij się, że Twoje dziecko korzysta z gier adekwatnych do jego wieku, np. na podstawie oznaczeń PEGI.

PEGI (Pan European Game Information) to ogólnoeuropejski system klasyfikacji gier komputerowych. W interesie producenta jest zamieszczanie oznaczenia PEGI na opakowaniu gry – można je zobaczyć jeszcze zanim ją kupimy, klasyfikacja ta pozwala nam ocenić czy nasze dziecko już dojrzało do konkretnej gry. Opis kategorii jest dostępny na stronie PEGI . Dzięki temu można uniknąć pomyłek polegających na przykład na kupieniu kilkuletniemu dziecku gry ociekającej krwią lub pełnej wulgaryzmów. Nie daj się również zwieść prośbom swojego dziecka – oczywiście, że będzie Cię zapewniało, że w tę lub taką grę (którą PEGI przewiduje dla starszego dziecka) grają wszyscy jego koledzy. To Ty decydujesz do jakich gier lub treści będzie miało dostęp.

9. Sprawdź szkołę swojego dziecka. Upewnij się, że opracowała i wdrożyła system zapobiegania i reagowania na cyberprzemoc.

Cyberprzemoc rówieśnicza to nic innego, jak przemoc wśród rówieśników przeniesiona do Internetu. Może polegać na zmasowanych atakach na jedną osobę, których celem jest jej upokorzenie lub sprawienie przykrości. Równie dobrze może polegać na anonimowych atakach jednej osoby. O ile jednak tradycyjna przemoc rówieśnicza zazwyczaj jest dostrzegana przez nauczycieli, cyberprzemoc jest często niezauważana lub ignorowana. Sprawdź czy w szkole Twojego dziecka nauczyciele, szkolni psychologowie lub pedagodzy wiedzą jak reagować na przejawy cyberprzemocy, czy wiedzą jak rozwiązywać tego typu problemy, czy szkoła wypracowała system jej zapobiegania. Masz pełne prawo to wiedzieć.

10. Naucz dziecko szacunku dla innych internautów i przekonaj je, że nawet pozornie niewinne żarty potrafią bardzo krzywdzić.

Coś, co raz znajdzie się w Internecie prawdopodobnie już nigdy z niego nie zniknie. Jeśli zostanie powielone na innych stronach lub serwerach, prawdopodobnie nikt nie zdoła nigdy tego usunąć. Między innymi właśnie tego najbardziej obawiają się ofiary cyberprzemocy – faktu, że cały świat zobaczy niechciane zdjęcie lub dowie się o złośliwej plotce. Porozmawiaj z dzieckiem, pokaż mu, że niewinny lub nieprzemyślany żart powielony tysiące razy może krzywdzić. Pokaż mu, że nawet świadek agresji w Internecie, bezrefleksyjnie powielający wymierzony w kogoś materiał (choćby dlatego, że jest śmieszny) przyłącza się do grona agresorów. Zwróć uwagę dziecka, że również ono może stać się ofiarą czyjegoś nieprzemyślanego żartu. Pokaż mu, gdzie szukać wtedy pomocy w sieci, ale przede wszystkim – daj mu poczuć, że zawsze może na Ciebie liczyć.

Zajrzyj pod adres Helpline.org.pl i dowiedz się, na jaką pomoc możesz liczyć ze strony jego konsultantów. Poleć dziecku serwis edukacyjny www.sieciaki.pl. Dowiedz się więcej na temat zagrożeń na stronie www.dzieckowsieci.fdn.pl. W sytuacji, kiedy podejrzewasz, że Twoje dziecko padło ofiarą internetowego przestępcy lub nie wiesz, jak zareagować na jakąś sytuację dotyczącą Twojego dziecka, a związaną z Internetem, szukaj pomocy na stronie Helpline.org.pl lub pod numerem **800 100 100**.

Strony dla rodziców **rodzi**

<http://dziekowsieci.fdn.pl/podstawowe-informacje-dla-rodzicow?cat1=&cat2=961&cat3=1234>

<http://www.sieciaki.pl/dla-rodzicow-i-nauczycieli>