Jak chronić dziecko przed zagrożeniami w Internecie?

W tym miejscu dowiesz się w jaki sposób możesz chronić swoje dziecko przed zagrożeniami w Internecie. Dziecko, ktróre siedzi w domu przed komputerem tylko na pozór jest bezpieczne. Warto pamiętać, że krzywda wyrządzona mu w wirtualnym świecie, nie zniknie wraz z odłączeniem sieci lub zasilania tego popularnego sprzętu.

Żadne oprogramowanie filtrujące ani program antywirusowy nie wystarczy by zapewnić Twojemu dziecku bezpieczeństwo w Internecie. Dlatego zadbaj o swoje dziecko, rozmawiaj z nim, bądź obecny w jego życiu - również wirtualnym. Od najmłodszych lat kształtuj w nim właściwe nawyki pozwalające na konstruktywne korzystanie z potencjału Internetu. Zadbaj o swoją pociechę i naucz ją dbać o siebie. To najskuteczniejszy sposób by zapewnić dziecku bezpieczeństwo w Internecie.

1. Ustal z dzieckiem zasady korzystania z komputera adekwatne do jego wieku. Określ maksymalny czas jaki Twoje dziecko może spędzać w sieci, jakie serwisy i strony internetowe może odwiedzać, pokaż Mu sposoby reagowania na niebezpieczne sytuacje.

Możesz w tym celu posłużyć się „Umową o bezpiecznym korzystaniu z Internetu", która jest dostępna w serwisie dzieckowsieci.fdn.pl. 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.

Umieszczenie komputera tam, gdzie bywają wszyscy domownicy, zmniejsza ryzyko, że dziecko, zwłaszcza małe, trafi na treści nie przeznaczone dla niego lub wejdzie w kontakt z niebezpieczną osobą.

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!

Naucz swoje dziecko odróżniać wiarygodne źródła i fakty od 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. 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 profi, maksymalnie chroniący jego prywatność.

Dzieci nie potrafią przewidzieć konsekwencji, jakie mogą je spotkać kiedy ujawniają np tylko 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.

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

Tak, jak w przypadku publikacji danych osobowych, dziecko nie zawsze jest w stanie realnie ocenić konsekwencje opublikowania w sieci jakichkolwiek materiałów. Coś, co raz trafiło do Internetu, dzięki możliwości wielokrotnego powielenia i umieszczenia na innych stronach, serwerach, serwisach, pozostaje w nim praktycznie na zawsze. Dotyczy to zarówno zdjęć, filmów, jak i np. wpisów na internetowych forach. Nieprzemyślanie zamieszczone zdjęcie lub film będący dokumentacją wspólnej 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. Chroń komputer dziecka przed niewłaściwymi treściami. Upewnij się, że na komputerze Twojego dziecka działa zaktualizowany program antywirusowy i zapora sieciowa. 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 uniemożliwianie 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 równolatków 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 (chociażby 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.

Zobacz na jaką pomoc możesz liczyć ze strony konsultantów Helpline.org.pl. 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 10**

Zagrożenia bezpieczeństwa dzieci i młodzieży w Internecie

Internet to medium, które ma wiele pozytywnych zastosowań. Niestety niesie ze sobą równie dużo zagrożeń.

Młodzi internauci mogą być narażeni na:

cyberprzemoc- zjawisko wysyłania lub publikowania, przy użyciu nowych technologii (Internetu i telefonu komórkowego) materiałów (zdjęć, filmów, komentarzy, wiadomości itp.), które mają na celu wyrządzenie krzywdy drugiej osobie.

nieuprawniony dostęp - włamania do miejsc strzeżonych hasłem lub innym zabezpieczeniem (np. poczta email, konto na portalu społecznościowym itp.)

niebezpieczne kontakty- kontakty, które związane są z ryzykiem wystąpienia niebezpieczeństwa ze strony osób, z którymi młodzi użytkownicy Internetu rozmawiają lub korespondują.

uwodzenie w sieci (gooming) - to szczególna kategoria relacji tworzona w Internecie między osobami dorosłymi a dziećmi w celu ich uwiedzenia i wykorzystania seksualnego.

szkodliwe treści - treści pojawiające się w Internecie, które są nieadekwatne do wieku, wrażliwości i rozwoju dziecka (np. promujące przemoc, pornografię, zachęcające do ryzykownych zachowań itp.)

uzależnienie od Internetu - patologiczne używanie Internetu, które ma znaczący wpływ na pogorszenie funkcjonowania dziecka w sferze: fizycznej, psychicznej, interpersonalnej, społecznej, rodzinnej, ekonomicznej.

Więcej informacji na temat zagrożeń w sieci na stronie: www.dzieckowsieci.fdn.pl

Kontrola rodzicielska – granice prywatności dziecka i jego korzystania z Internetu

Zapytaj swoje dziecko, co robi w Internecie. Czym zajmuje się tam najczęściej? Nie wahaj się zadawać prostych pytań. To wiedza, którą może przekazać Ci Twoje dziecko - Internet to wynalazek ich czasów. Zapytaj, z kim rozmawia przez Internet. Poproś, aby pokazało Ci, w jaki sposób korzysta z Internetu. Powiedz, że chciałbyś wiedzieć, jakie informacje przekazuje swoim internetowym znajomym.

Powiedz, czego oczekujesz od dziecka w zakresie zasad bezpiecznego korzystania z Internetu. Korzystają z niego też osoby, które mają niewłaściwe intencje. Powiedz, zatem, czego, według Ciebie jako osoby dorosłej, nie wolno dziecku robić ze względu na jego i Wasze bezpieczeństwo. Pomóż mu zrozumieć, że nigdy nie powinno się podawać przez Internet osobistych danych (imienia i nazwiska, adresu, numeru telefonu) ani przesyłać lub publikować zdjęć, nagrań video. Wyjaśnij, że nie należy bez Twojej kontroli otwierać e-maili, odbierać wiadomości od osób nieznanych. Ty, jako osoba dorosła, możesz to robić. Zawartością takiego e-maila mogą być wirusy albo film lub zdjęcie o nieodpowiedniej dla dzieci treści.

Naucz swoje dzieci, że są ludzie, którzy kłamią, oszukują w Internecie i dlatego właśnie lepiej z nimi nie rozmawiać, ani nie odbierać od nich e-maili, wiadomości. Dzieci nie powinny spotykać się z osobami poznanymi w Internecie bez kontroli i wiedzy rodziców.

Poproś o zaufanie. Powiedz, że chcesz wiedzieć o tym, co je zaniepokoi w Internecie. Jeśli opowie Ci o tym, a Ty nie będziesz wiedział, co zrobić- zadzwoń lub napisz do Helpline. Razem zastanowimy się, co możemy zrobić. W Helplinie pracują ludzie, którzy są tam po to, by pomagać w trudnych sytuacjach.

Nie obwiniaj - w ten sposób nie rozwiążesz problemu, a dziecko straci odwagę, by opowiedzieć Ci o tym, co się stało. Pamiętaj, że dzieci często same obciążają się winą. Powiedz, jak ważne jest dla Ciebie to, by z Tobą rozmawiało. Doceń jego odwagę i zaufanie, jakim Cię obdarzyło. Powiedz swojemu dziecku, że zawsze może na Ciebie liczyć. Razem na pewno sobie poradzicie!

Najlepiej porozmawiać o zasadach, zanim zdecydujesz o podłączeniu komputera do Internetu. Jeśli jeszcze nie odbyliście takiej rozmowy, pamiętaj, że nigdy nie jest na to za późno. Co możesz zrobić, gdy twoje dziecko stało się ofiarą nadużycia w Internecie?

Dzieci i młodzież często czują się osamotnione i bezradne wobec krzywdzących zdarzeń w Sieci. Bardzo potrzebują wsparcia i reakcji dorosłych. Przeczytaj jakie kroki możesz podjąć, aby pomóc Twojemu dziecku w takiej sytuacji:

POROZMAWIAJ:

wysłuchaj - ważne jest, by dziecko mogło opowiedzieć o tym co się stało. Warto by dziecko dostało zapewnienie, że swoim doświadczeniem może podzielić się z rodzicami. Podkreśl , że to co je trapi jest dla Ciebie ważne (nawet jeśli z Twojej perspektywy problem wydaje się błahy lub łatwy do rozwiązania). Jeśli dziecko zdecydowało się opowiedzieć, to oznacza, że ma do Ciebie zaufanie i potrzebuje Twojej pomocy. W takiej sytuacji warto podkreślać, że może na Ciebie (lub Was - rodziców) liczyć; że razem znajdziecie dobre rozwiązanie.

nie oceniaj - dobrze by dziecko miało poczucie, że może opowiedzieć o tym co się stało i nie zostanie automatycznie obwinione, za to co się wydarzyło. Nie reaguj nerwowo. Spokojnie poproś dziecko o opowiedzenie o tym co miało miejsce. Sprawdź, co tak naprawdę się wydarzyło. Spróbuj zebrać jak najwięcej informacji. Postaraj się dowiedzieć kim jest sprawca cyberprzemocy - często dziecko nie wie kto to zrobił.

doceń fakt**,** że dziecko poinformowało Ciebie o problemie.

wspólnie zastanówcie się co jeszcze warto zrobić w tej sytuacji.

ZABEZPIECZ DOWODY.

W sytuacji gdy coś niebezpiecznego przydarzyło się w Internecie ważne jest jak najszybsze zebranie dowodów tego co się stało. Mogą one pomóc w ustaleniu tożsamości sprawcy i zapobiec jego dalszym działaniom. Są też cennym dowodem dla instytucji wymiaru sprawiedliwości i organów ścigania.

Dowodami, w zależności od tego co się wydarzyło, mogą być:

- wiadomości e-mailowe

- wiadomości sms i mms

- wpisy na stronach internetowych

- komentarze do zdjęć i treści umieszczane w serwisach społecznościowych, blogach, fotogaleriach

- treści rozmów prowadzonych przez komunikatory i czaty.

W zależności od charakteru zdarzenia i formy można stosować różne sposoby zabezpieczania dowodów:

Zachowywanie wiadomości. W przypadku rozmów telefonicznych i sms-ów, mms-ów trzeba zachować wiadomości i historię połączeń. Warto zachowywać wszelkie treści świadczące o wydarzeniu. W przypadku, gdy te treści są krzywdzące trzeba je jak najszybciej usunąć. Wcześniej jednak dobrze jest je zabezpieczyć.

Zabezpieczanie dowodów. Najlepszym zabezpieczeniem jest zrobienie zrzutu z ekranu - tzw. *screena*. Takiej jakby fotografii tego co aktualnie znajduje się na monitorze komputera. Aby go wykonać wystarczy nacisnąć klawisz *Print Screen*, pozornie nic się nie dzieje, następnie otworzyć program typu Paint lub Word i wybrać opcję: *wklej*. Taki dokument najlepiej zapisać na dysku komputera.

Archiwizowanie rozmów. Korzystając z czatów i komunikatorów warto uruchomić autoarchiwizację rozmów - funkcję automatycznie zapisującą rozmowy danego użytkownika. W ten sposób mamy dostęp do prowadzonych rozmów i wpisów. Łatwo również prześledzić historię wybranego kontaktu. W przypadku, gdy korzystamy z czatu czy komunikatora, który nie posiada takiej opcji, warto kopiować i zapisywać odbywane rozmowy w dowolnym edytorze tekstów. Ważne by zapisywany tekst był kompletny i zawierał również skopiowany link do strony na której się pojawił.

Wykonanie zrzutu animacji ekranu. Kolejnym sposobem na zachowanie obrazu, ale także animacji i ruchów wykonywanych na monitorze jest korzystanie z programów wykonujących zrzuty animacji.

Wydruk. Dowodem tego co się stało w Internecie może być również wydruk strony na której miało miejsce nieprzyjemne zdarzenie. Warto wtedy pamiętać o wydrukowaniu całej strony, wraz z paskiem tytułowym i adresem witryny. Dobrze jest też opisać wydruk - podając datę i godzinę wykonania.

SKONTAKTUJ SIĘ Z PROFESJONALISTAMI

Możesz potrzebować wsparcia i porady psychologa lub prawnika. Jeśli nie wiesz jak zareagować zachęcamy do kontaktu z Helpline.org.pl (nr tel.: 800 100 100). **Poszukaj** pomocy psychologicznej dla dziecka. Zdarza się, że dzieci bardzo skutecznie ukrywają trudności przeżywane w związku z tym co je spotkało. Warto wtedy porozmawiać z psychologiem.

Jeśli dziecko zetknęło się w Internecie z pornografią z udziałem małoletnich, koniecznie zgłoś to na stronie **www.dyzurnet.pl** - to hotline, który przyjmuje i reaguje na zgłoszenia, dotyczące występowania w Internecie **treści nielegalnych (pornografia dziecięca, treści rasistowskie i ksenofobiczne)**.

Jeśli podejrzewasz, że zostało złamane prawo, nie działaj na własną rękę, tylko jak najszybciej powiadom policję (tel.: 997 lub 112 albo **www.policja.pl**).

Jeśli sprawa wymaga przesłuchania dziecka, **domagaj się** możliwości skorzystania z tzw. **Niebieskiego Pokoju** (więcej informacji o procedurach związanych z udziałem dziecka w postępowaniu karnym można znaleźć na stronie programu Dziecko-Świadek Fundacji Dzieci Niczyje).

Jeśli stwierdzisz przypadek włamania lub próby włamania do komputera Twojego lub dziecka, jesteście nękani spamem przesyłanym za pośrednictwem polskich serwerów lub atakami hackerów, zgłoś to do zespołu Cert Polska po przez stronę **www.cert.pl .**

Warto podpisać z dzieckiem umowę, w której zawarte będą wspólnie ustalone zasady korzystania z Internetu, pomocne mogą okazać się proponowane przez serwis *Dziecko w sieci* wzory takich umów dostępne na stronie www.dzieckowsieci.fdn.pl

Pamiętaj o włączeniu właściwych filtrów rodzicielskich w ustawieniach wyszukiwarki, z której korzysta Twoje dziecko. Uchroni je to przed szkodliwymi treściami, które bezwiednie mogą pojawiać się w wynikach wyszukiwania.