Jak zapewnić dzieciom bezpieczeństwo w internecie?

Poradnik dla rodziców

cyfrowobezpieczni.pl
BEZPIECZNA SZKOŁA CYFROWA

Poradnik dla rodziców

"Jak zapewnić dzieciom bezpieczeństwo w Internecie"

został opracowany w ramach projektu Cyfrowobezpieczni.pl

Publikacja została opracowana przez Zespół Ekspertów Naukowej Akademickiej Sieci Komputerowej instytutu badawczego NASK

Skład zespołu: Marcin Bochenek, Zuzanna Polak, Krzysztof Silicki, Agnieszka Wrońska

Konsultacja merytoryczna : prof. APS dr hab. Maciej Tanaś

Więcej informacji na temat projektu:
CYFROWOBEZPIECZNI.pl - Bezpieczna Szkoła Cyfrowa,
na stronie www.cyfrowobezpieczni.pl

Projekt jest finansowany przez Ministerstwo Edukacji Narodowej w ramach zadania „Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia”

MINISTERSTWO EDUKACJI NARODOWEJ

Spis treści

Internet – szanse i zagrożenia	2
Internet - przegląd niebezpiecznych zjawisk	3
Cyberprzemoc	3
Niebezpieczne kontakty	6
Szkodliwe treści	7
Seksting i inne zachowania ryzykowne	9
Nadużywanie internetu	11
Gry komputerowe	13
Zagrożenia technologiczne dla bezpiecznego korzystania z internetu	14
Gdzie uzyskać pomoc i zgłaszać nielegalne treści?	17
Gdzie szukać pomocy?	17

Korzystanie przez dzieci i młodzież z internetu jest rzeczą naturalną. Badania wskazują, że samodzielna przygoda z siecią rozpoczyna się w wieku niespełna 10 lat, ale w rzeczywistości wejście w cyfrowy świat ma miejsce znacznie wcześniej. Nikogo już nie dziwi widok 3 - 4 letnich maluchów sprawnie operujących tabletami. Internet odgrywa ważną rolę w życiu młodych ludzi. Służy im do zabawy, nauki, komunikowania się. W przypadku gimnazjalistów i uczniów szkół ponadgimnazjalnych średni czas korzystania z sieci to aż 3 godziny i 40 minut. Przeważająca większość z nich deklaruje, iż sama poznaje wirtualny świat. Tylko dla nielicznych przewodnikami po sieci są rodzice. Aż 55,6 proc. nastolatków uważa, iż opiekunowie nie interesują się ich aktywnością w sieci. Prawie wszyscy młodzi ludzie korzystają z serwisów społecznościowych.

Internet to jedno z największych technicznych osiągnięć naszych czasów. Pozwala nam lepiej poznawać świat, łatwiej się komunikować, zdobywać wiedzę, dostarcza nam rozrywki, wreszcie dzięki niemu sprawniej załatwiamy codzienne sprawy. Oczywiście korzystanie z internetu niesie ze sobą także potencjalne zagrożenia. Część z nich to przeniesione do wirtualnego świata, znane nam już od dawna zjawiska, takie jak przemoc, oszustwa, czy szerzenie nienawiści. Możliwości techniczne internetu rodzą także nowe zagrożenia i zwielokrotniają siłę i zasięg tych już znanych (plotki, pomówienia).

W prezentowanym materiale chcemy przedstawić Państwu, na czym polegają zagrożenia, na które mogą być narażone Wasze dzieci. Piszemy o profilaktyce, a więc o tym jak unikać niebezpiecznych sytuacji i o reagowaniu, czyli o tym co robić, gdy musimy reagować na trudne i często niebezpieczne wydarzenia.

Nasze porady nie mają charakteru technicznego, a ich stosowanie nie wymaga specjalnego przygotowania. Wielu rodziców obawia się rozmów na temat internetu ze swoimi dziećmi sądząc, że nie są do tego należycie przygotowani. Pamiętajmy – podstawową rolą rodziców nie jest wprowadzanie młodych ludzi w techniczne aspekty korzystania sieci, a wychowywanie i zapewnienie im bezpieczeństwa. Nie bójmy przyznawać się do braku szczegółowej wiedzy na temat funkcjonowania poszczególnych programów czy aplikacji. Skupiajmy się na znaczeniu ich funkcjonowania dla rozwoju i bezpieczeństwa najmłodszych.

Podstawowym narzędziem wychowawczym jest oczywiście rozmowa dająca szansę zrozumienia oczekiwań, niepokojów, fascynacji i problemów dziecka, będąca także okazją do przedstawienia mu możliwości i niebezpieczeństw płynących z korzystania z sieci. Ważnym aspektem działania rodziców jest wprowadzanie zabezpieczeń do używanego przez dzieci sprzętu, tak by do najmłodszych nie trafiały niewłaściwie treści. Pamiętajmy jednak, że nie jesteśmy

w stanie wprowadzić takich barier na wszystkich urządzeniach, do których ma dostęp nasze dziecko. Smartfon, tablet koleżanki czy kolegi może nie być wyposażony w programy filtrujące. Stąd właśnie wynika tak istotna rola procesu wychowawczego. Budujmy zaufanie między nami a dziećmi. W sytuacji wątpliwej, niebezpiecznej, w momencie zaistnienia problemu, młody człowiek zwróci się właśnie do rodziców. Gdy takiego zaufania nie będzie, może popełnić błąd, nie szukać pomocy, albo szukać jej w niewłaściwym miejscu.

Zwracajmy uwagę na to, jak nasze dzieci rozumieją przekaz kierowany do nich za pośrednictwem internetu. Chodzi tu między innymi o odróżnianie prawdy od fałszu, rozpoznawanie manipulacji i treści reklamowych. Wskazujmy, iż nie zawsze opis świata przedstawiany w mediach odpowiada rzeczywistości, a reklama jest przede wszystkim zachętą do sprzedaży i pokazuje pozytywną stronę produktu czy usługi.

Jednym słowem - **stawiajmy na dobrą profilaktykę, czyli na rozmowę, wspólne poznawanie świata nowych technologii. Nie budujmy systemu zakazów. Bądźmy jednak przygotowani na rozwiązywanie trudnych problemów.**

Internet - przegląd niebezpiecznych zjawisk

Poniżej opisujemy najczęściej spotykane w sieci zagrożenia. Lista ta nie obejmuje wszystkich potencjalnie niebezpiecznych sytuacji, z którymi może spotkać się nasze dziecko. Co więcej, ciągle pojawiają się nowe zagrożenia, ryzykowne mody i trendy. Jeszcze kilka miesięcy nic nie wiedzieliśmy o wielu istniejących obecnie i groźnych zjawiskach. Stąd tak ważny jest dobry kontakt zarówno z dziećmi jak i z ich nauczycielami, oraz wszystkimi osobami, które towarzyszą dzieciom w codziennych aktywnościach.

Cyberprzemoc

Młodzi ludzie wykorzystują internet do nauki i rozrywki, komunikowania się z innymi, poszukiwania informacji potrzebnych w życiu codziennym. Jest narzędziem do tworzenia własnego wizerunku, ale bywa również wykorzystywany do działań agresywnych i nacechowanych przemocą, a mających na celu dyskredytowanie jednej czy wielu osób. **Szczególną formą agresji elektronicznej jest cyberprzemoc (z ang. *cyberbullying*) definiowana jako przemoc rówieśnicza z wykorzystaniem internetu i urządzeń mobilnych.**

Jeden na pięciu polskich nastolatków przyznaje, że padł ofiarą wysyłania gróźb, rozpowszechniania kompromitujących materiałów czy systematycznego izolowania i wykluczania (EU-NET-ADB, FDN 2013).

Jakie formy przemocy stosują najczęściej młodzi użytkownicy internetu?

- Przerabiają i publikują ośmieszające zdjęcia, filmy
- Upubliczniają sekrety ofiary
- Dystrybuują nieprawdziwe informacje lub krzywdzące opinie czy oceny
- Złośliwie komentują wpisy i zdjęcia
- Przechwytują profil lub pocztę i podszywając się pod ofiarę prowadzą w jej imieniu korespondencję
- Celowo ignorują aktywność ofiary w sieci.

Pamiętajmy, że cyberprzemoc ma specyficzne cechy, które sprawiają, że ofiara narażona jest na duży dyskomfort emocjonalny, doświadcza wielu ataków i przykrości, których konsekwencje mogą być bardzo poważne i utrzymywać się również po zakończeniu prześladowania.

Cyberprzemoc oznacza w praktyce długotrwałe nękanie ofiary. Jest ona narażona na ataki, niezależnie od miejsca pobytu czy pory dnia. Ośmieszające czy kompromitujące materiały rozpowszechniane są bardzo szybko i są ogólnodostępne. Co więcej, z uwagi na szybkość kopiowania i udostępniania trudno jest całkowicie usunąć je z sieci. Sprawca może być trudny do ustalenia, jednak mitem jest jego pełna anonimowość. Z uwagi na wymienione powyżej aspekty, rodzicom i opiekunom znacznie trudniej dostrzec i reagować na cyberprzemoc.

Cyberprzemoc

Cyberprzemoc może nosić znamiona różnych przestępstw. Najczęściej dochodzi do naruszeń: art. 190 kk – groźba karalna, art. 190a kk – uporczywe nękanie (stalking), podszywanie się, 191a kk – naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody, 212 kk – zniesławienie, 216 kk – zniewaga, 267 kk – bezprawne uzyskanie informacji, 268 kk – utrudnianie zapoznania się z informacją, 268a kk – niszczenie danych informatycznych, 269 kk – uszkodzenie danych informatycznych, 269a kk – zakłócanie systemu komputerowego, art. 287 kk – oszustwo komputerowe, art.107 kodeksu wykroczeń – dokuczenia lub złośliwe wprowadzanie w błąd.

Jak zapobiegać?

- **Rozmawiajmy** z dzieckiem zarówno o **zasadach bezpiecznego korzystania z internetu**, jak i o internetowym savoir vivre, czyli o kulturalnym zachowaniu użytkownika mediów elektronicznych
- **Rozmawiajmy** o potencjalnych **konsekwencjach** podejmowanych przez dziecko działań i zachowań

- **Pokazujmy i przypominajmy o możliwościach ochrony** np. zablokowaniu użytkownika, ograniczeniu kontaktu oraz możliwości tymczasowego wyłączenia komentarzy na portalu społecznościowym lub blokowaniu połączeń i sms-ów
- Zwróćmy uwagę na to, że **nawet z pozoru niewinny żart może eskalować falę cyberprzemocy**, której konsekwencji sprawca nie jest w stanie przewidzieć
- Informujmy w jaki sposób dziecko powinno zachować się w sytuacji, gdy ma do czynienia z brakiem kultury lub naruszeniem jego godności osobistej. **Zachęcajmy dziecko, by dzieliło się problemem z zaufaną osobą i zgłaszało opiekunom** bycie ofiarą cyberprzemocy, ale również jej świadkiem czy sprawcą
- **Zwróćmy uwagę ile czasu** dziecko korzysta z telefonu komórkowego, komputera i innych urządzeń z dostępem do internetu, **na jakich portalach** społecznościowych i forach się udziela i **jakiego rodzaju treści**, opinie i komentarze publikuje. Jednak zawsze pamiętajmy o poszanowaniu jego prywatności. Budujmy klimat wzajemnego zaufania
- **Obserwujmy zachowanie dziecka** - gdy staje się smutne, nerwowe lub przygnębione, otrzymuje smsy, na które reaguje płaczem, obniżonym nastrojem, mniej korzysta z sieci, zrezygnowało lub ograniczyło kontakty z rówieśnikami. Tego typu zachowanie może wskazywać, że znalazło się w sytuacji problemowej.

Jak reagować?

- **Podejmujmy interwencję** w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy
- **Zapewnijmy dziecku wsparcie** - przekonajmy, że niezależnie od wagi problemu, incydentu czy roli, w której się znalazło (ofiara, świadek, sprawca), poinformowanie rodzica jest bardzo dobrym rozwiązaniem
- **Doradźmy dziecku, by nie utrzymywało kontaktu ze sprawcą**, nie odpowiadało na zaczepki, maile, smsy oraz nie usuwało dowodów cyberprzemocy, tylko pokazało je rodzicom lub innej osobie dorosłej i opowiedziało o problemie
- **Wiadomości emailowe, zdjęcia, wiadomości sms lub nagrane na pocztę głosową, komentarze w serwisach i na blogach mogą być narzędziami cyberprzemocy.** Zadbajmy o to, by nie zostały one skasowane lub usunięte. Pozwoli to na łatwiejsze rozwiązanie sprawy i wyjaśnienie problemu
- **Korzystajmy z porad specjalistów** (pedagodzy w szkole, specjalistyczne poradnie, linie telefoniczne i punkty pomocowe).

Niebezpieczne kontakty

Obecnie prawie każdy serwis internetowy spełnia funkcje społecznościowe. Użytkownicy internetu w różnym wieku posiadają konta w portalach społecznościowych, angażują się w kontakty na forach, czatach związanych z hobby, włączają się w działania wielu różnych internetowych społeczności, również grając online. Pozwala to na poznawanie nowych osób, sprzyja rozwijaniu zainteresowań, służy rozrywce, a często także pomaga w nauce. Należy jednak pamiętać, że kontakty w sieci mogą nieść za sobą pewne ryzyko, szczególnie jeżeli wykorzystujemy internet do nawiązywania relacji z osobami nieznanymi bezpośrednio w realnym świecie. Problem nawiązywania potencjalnie niebezpiecznych kontaktów z nieznajomymi nie dotyka tylko młodych ludzi, ale to właśnie oni, ze względu na swój wiek i brak doświadczenia w radzeniu sobie z trudnymi sytuacjami, są szczególnie narażeni na negatywne konsekwencje takich relacji.

Niebezpieczne kontakty to relacje

- z osobą dorosłą o skłonnościach pedofilskich, której celem jest uwiedzenie dziecka
- mające na celu wciągnięcie dziecka/nastolatka do grupy o radykalnych poglądach, np. subkultur propagujących zachowania agresywnych, werbunek online do sekt, grup przestępczych
- ze społecznościami propagującymi niebezpieczne zachowania - np. samookaleczanie, restrykcyjną dietę czy stosowanie substancji psychoaktywnych
- z cyberprzestępcami zainteresowanymi pozyskiwaniem danych osobowych i innych poufnych informacji, wykorzystywanych później w celach przestępczych.

Pamiętajmy, że każde urządzenie z dostępem do internetu – łącznie z konsolą do gier – może być miejscem nawiązywania niebezpiecznych kontaktów!

Jak zapobiegać ?

- **Jak najwcześniej zapoznajmy dziecko z zasadami bezpiecznego korzystania z internetu,** takimi jak: bezpieczny nick, silne hasło, czy wylogowywanie się. Ustalmy z dzieckiem zasady komunikowania się w sieci, przede wszystkim nie podawania danych osobowych, nie odpowiadania na zaczepki nieznajomych, nieakceptowanie zaproszeń, prezentów w grach od osób nieznanych
- **Wprowadźmy zasadę, iż dziecko informuje nas o każdym kontakcie z osobą dotąd nieznaną**
- Oczywiście nie każdy kontakt z osobą nieznajomą będzie niebezpieczny. Starsze dzieci oraz nastolatki powinny mieć możliwość nawiązywania takich

znajomości za wiedzą rodzica. **Ustalmy z dzieckiem zasady spotykania się w świecie rzeczywistym z osobą poznaną przez internet**, zgodnie z którymi rodzic zawsze powinien wiedzieć o takim spotkaniu, powinno się ono odbyć w miejscu publicznym i w towarzystwie zaufanego przyjaciela lub większej grupy kolegów i koleżanek

- Ograniczmy młodszemu dziecku możliwość kontaktu z innymi użytkownikami poprzez m.in. blokadę funkcji społecznościowych, takich jak czat czy możliwość wpisywania komentarzy oraz zwróćmy uwagę na ustawienia prywatności (w tym widoczności) konta należącego do dziecka.

Jak reagować w przypadku, gdy dziecko nawiąże kontakt z kimś potencjalnie niebezpiecznym?

- **W przypadku próby uwiedzenia dziecka**, która w świetle polskiego prawa jest przestępstwem, **należy zgłosić się na policję z dowodami zajścia** np. wydrukami zapisów rozmów, smsów, maili, zrzutów ekranu itp. Należy zapewnić dziecku dostęp do profesjonalnej opieki psychologicznej. Pamiętajmy również, że dziecko jest ofiarą, dlatego nie obwiniajmy go o tę sytuację
- W przypadku każdego niebezpiecznego kontaktu, powinniśmy przede wszystkim skupić się na dziecku. **Niebezpieczne kontakty różnego rodzaju są często nawiązywane w przypadku, gdy dziecko przeżywa problemy emocjonalne lub rodzinne w świecie realnym**
- **Zaobserwowanie jakiegokolwiek szkodliwego dla zdrowia zachowania** (samookaleczenia, restrykcyjna dieta, używanie substancji psychoaktywnych) **powinno zwrócić naszą uwagę również na świat wirtualny**. Tego typu zachowania mogą łączyć się z przynależnością dziecka do jakiejś niebezpiecznej społeczności działającej w internecie. Tu również może przydać się pomoc psychologa.

Szkodliwe treści

Dorośli użytkownicy internetu korzystają z zasobów sieciowych inaczej niż dzieci. Do zamieszczonych tam materiałów podchodzą z większym dystansem, w sposób bardziej nieufny, nie zawsze wierzą we wszystkie publikowane informacje, a przede wszystkim lepiej radzą sobie w sytuacji, kiedy natrafią na szczególnie nieprzyjemne treści. Mimo tego i dla nas, dorosłych ocena prawdziwości treści bywa trudna.

Dzieci inaczej podchodzą do napotkanych materiałów. Są bardziej ufne, czasem wprost łatwowierne, nie potrafią w prosty sposób odróżnić kłamstwa od prawdy, nie czytają między wierszami, a przede wszystkim są niezwykle wrażliwe na przekaz wizualny w postaci zdjęć, grafik i filmów. Są zatem zdecydowanie

bardziej narażone na konsekwencje związane z kontaktem z tzw. treściami szkodliwymi. **Szkodliwe treści to takie materiały, które mogą wywoływać nieprzyjemne uczucia u odbiorców, promują niebezpieczne zachowania lub prezentują radykalne poglądy**.

Szkodliwe treści to materiały

pornograficzne, w tym tzw. „pornografia dziecięca", czyli materiały prezentujące seksualne wykorzystywanie dzieci	**Art. 200 §3 kk** **Art. 202 kk**
nawołujące do zachowań przeciwko zdrowiu i życiu, takich jak samookaleczenia, stosowania wyniszczających diet, promocja zażywania potencjalnie niebezpiecznych substancji lub pochwalające samobójstwa	
dyskryminacyjne, nawołujące do wrogości, a nawet aktów agresji wobec różnych grup społecznych lub jednostek	**Art. 257 kk**
nieprawdziwe informacje, nie poparte wiedzą naukową, która może wpływać na postrzeganie rzeczywistości.	

Niektóre z tych materiałów są nielegalne, np. pornografia z udziałem osób małoletnich czy nawoływanie do przemocy na tle rasowym, jednak większość z nich nie stanowi naruszenia prawa.

Co **dziesiąty** badany zobaczył w internecie coś, co wywołało w nim zaniepokojenie lub nieprzyjemne odczucia (EU Kids Online, 2011)

17% polskich 9-16-latków miało kontakt z treściami potencjalnie zagrażającymi ich rozwojowi społecznemu.

Jak zapobiegać?

- Komputer przeznaczony dla dziecka powinniśmy wyposażyć w **program filtrujący i/lub inne narzędzie kontroli rodzicielskiej**. Im młodsze dziecko, tym filtr powinien być szczelniejszy
- **Rozmawiajmy z dzieckiem o tym, co robi w internecie.** Ustalmy ze starszym dzieckiem zasady poruszania się w sieci – np. nie wchodzenia na „strony dla dorosłych", a przede wszystkim zgłaszania sytuacji, w których dziecko zobaczyło coś, co je szczególnie zaniepokoiło czy przestraszyło

- W pewnym wieku dziecko zaczyna interesować się sprawami ciała i seksu. Należy zadbać, aby internetowe treści pornograficzne nie stanowiły źródła wiedzy na ten temat
- Wyjaśniajmy dziecku (szczególnie nastolatkowi), że **informacje publikowane w internecie mogą być nieprawdziwe i przekłamane**, a także analizujmy wspólnie podejrzane treści.

Jak reagować?

- **Nauczmy dziecko reagować** na szkodliwe materiały, między innymi pokazując jak zgłaszać niebezpieczne treści do administratora serwisu
- Jeżeli dziecko szuka w sieci informacji na temat zachowań szkodliwych dla zdrowia może to oznaczać, że przeżywa problemy w świecie rzeczywistym. **Zwracajmy uwagę na nietypowe zachowania** – chudnięcie, pobudzenie lub osowiałość, a także na objawy świadczące o próbach samookaleczeń, np. osłanianie przedramion
- **Kontakt dziecka z pornografią, w tym „dziecięcą", może oznaczać, że jest ofiarą uwodzenia przez osobę o skłonnościach pedofilskich**. Prezentacja takich treści ma na celu oswojenie dziecka ze światem seksu i zachęcenie go do własnej aktywności. Im młodsze dziecko, tym kontakt z tego rodzaju treściami powinien być dla nas bardziej niepokojący. Gdy okaże się, że nasze dziecko nawiązało niebezpieczną relację, natychmiast zgłośmy sprawę na policję.

Seksting i inne zachowania ryzykowne

Zagrożenia bezpieczeństwa dziecka mogą mieć różne przyczyny: mogą m. in wynikać z zachowań samych Internautów, szczególnie eksperymentujących nastolatków. Młodzi ludzie podejmują zachowania ryzykowne z różnych powodów, czasami z ciekawości i chęci sprawdzenia reakcji rodziców i rówieśników, a czasami w związku z problemami osobistymi, których nie potrafią rozwiązać.

Jakie ryzykowne zachowania podejmują młodzi ludzie w internecie?

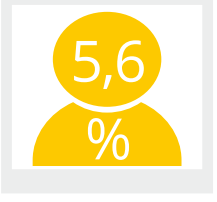
- **Seksting (w tym seksting kamerkowy)**

  To niebezpieczne zjawisko przesyłania treści (zdjęć, filmików) o charakterze erotycznym, głównie swoich nagich lub półnagich zdjęć, za pomocą internetu i telefonu komórkowego, popularne szczególnie wśród nastolatków. Seksting może również przyjmować formę seks-komunikacji na żywo, za pośrednictwem komunikatorów z wykorzystaniem kamerki

- **Poszukiwanie informacji na temat narkotyków i innych substancji psychoaktywnych lub aktywności szkodliwych dla zdrowia**
- **Podejmowanie niebezpiecznych kontaktów**
  (patrz rozdział „Niebezpieczne kontakty") Szczególnie groźne są relacje z nieznajomymi osobami dorosłymi, które mogą przejawiać skłonności pedofilskie i dążyć do zaangażowania dziecka w produkcję materiałów pornograficznych lub spotkanie w świecie rzeczywistym.
- **Hazard online**
- **Nadużywanie/patologiczne korzystanie z internetu**
- **Brak dbałości o swoją prywatność.**

Uwaga!

Materiały powstałe w procesie sekstingu mogą być wykorzystane w celu szantażu i wyłudzenia pieniędzy, pozyskania dalszych materiałów albo spotkania w świecie rzeczywistym. Takie zjawisko nazywa się *sextortion*.



5,6 procent nastolatków przyznaje, że zdarzyło im się wysłać swoje intymne zdjęcie osobie poznanej w internecie
(Nastolatki WSNP/RPD/NASK 2014)

W badaniach nad zachowaniami ryzykownymi w świecie realnym zauważono, że czynnikami chroniącym dziecko przed tego rodzaju postępowaniem jest m. in. posiadanie oparcia w rodzinie, zainteresowanie nauką szkolną, przynależność do pozytywnej grupy społecznej.

Jak zapobiegać?

- **Zapewnijmy dziecku potrzebne wsparcie,** a także pokażmy pozytywne przykłady aktywności i relacji w świecie online
- **Rozmawiajmy z dzieckiem o konsekwencjach zachowań ryzykownych**, w tym sekstingu. Badania pokazują, że prawie połowa nastolatków nie wie, że każdy czat kamerkowy można nagrać w celu późniejszego rozpowszechnienia. 13 proc. gimnazjalistów spotkało się z osobą dorosłą poznaną w internecie, i aż 20 proc. nie powiedziało o takim spotkaniu nikomu z bliskich, nawet rówieśnikom
- **Uczmy dziecko odmawiać** – może dzięki temu uniknąć poddania się presji rówieśniczej zachęcającej do podejmowania zachowań ryzykownych

- **Rozmawiajmy z dzieckiem o właściwym budowaniu swojego wizerunku w sieci**, przejrzyjmy wspólnie ustawienia prywatności konta na portalach społecznościowych i zastanówmy się jaki poziom ochrony prywatności zastosować.

Jak reagować?

- Jeżeli doszło do rozpowszechnienia materiałów sekstingowych, **reagujmy szybko oraz zapewnijmy dziecku wsparcie**, gdyż jest to dla niego niezwykle przykre i upokarzające doświadczenie. W przypadku, gdy dziecko jest niepełnoletnie, możemy mieć czynienia z przestępstwem polegającym na rozpowszechnianiu pornografii dziecięcej. Warto wówczas zgłosić sprawę policji
- **Zwróćmy się do administratorów serwisów czy dostawców usług** elektronicznych z prośbą o usunięcie treści. W niektórych przypadkach niezbędna może być pomoc wyspecjalizowanego zespołu reagującego
- Jeżeli dziecko uprawia hazard online, może szybko popaść w uzależnienie. Gdy zaobserwujemy niepokojące objawy, oceńmy sytuację i w razie potrzeby **zwróćmy się o radę do psychologa**
- **Każdy przypadek zachowania ryzykownego powinien wzbudzić naszą czujność**. Może się bowiem okazać, że dziecko podejmuje działania niosące ryzyko, ponieważ przeżywa poważne problemy natury psychologicznej.

Nadużywanie internetu

Różnorodność i atrakcyjność internetu powoduje, że młodzi ludzie chętnie i często korzystają z jego zasobów. Internet oferuje im możliwość rozwijania swoich zainteresowań, znalezienia rozmaitych informacji, komunikowania się i utrzymywania relacji towarzyskich. Prawie każdy nastolatek codziennie korzysta z internetu, a blisko połowa z nich dzięki posiadaniu urządzeń mobilnych, tj. smartfon, deklaruje stałą dostępność online.

86,2% loguje się do sieci codziennie

43,2% pozostaje online bez przerwy

Często rodzice inicjują pierwszy kontakt najmłodszych z urządzeniami mobilnymi i siecią, dając dzieciom rocznym i dwuletnim tablet lub smartfon. **Niemal co trzecie małe dziecko korzysta z urządzeń mobilnych codziennie lub prawie codziennie w celu zabawy, podczas jedzenia posiłków czy ułatwiania zasypiania.**

Atrakcyjność treści i aplikacji, z którymi użytkownicy stykają się w sieci, może powodować **utratę kontroli nad czasem i intensywnością korzystania z internetu, komputera, gier konsolowych lub gier komputerowych, czatów i portali społecznościowych i innych wirtualnych aktywności.** To z kolei wpływa na ograniczenie lub rezygnację z innych czynności dnia codziennego, a także prowadzić do zaniedbywania rodziny, obowiązków, nauki szkolnej czy hobby bądź unikania kontaktu z rówieśnikami.

Jak pokazują badania ok. **13 proc.** polskich nastolatków dysfunkcyjnie korzysta z sieci, tzn. nadużywa internetu lub jest zagrożonych jego nadużywaniem.

O niedosypianiu i zbyt małej liczbie godzin snu z powodu surfowania po sieci mówi prawie 20 proc. polskich nastolatków zaś ok. 30 proc. z nich odczuwa dyskomfort, kiedy nie ma dostępu do sieci.

? Jak rozpoznać że dziecko nieprawidłowo, dysfunkcyjnie korzysta z komputera/internetu/gier?

- **Czas, który dziecko spędza przy komputerze przewyższa czas poświęcany innym aktywnościom,** np. obowiązkom domowym i szkolnym, innym zainteresowaniom, kontaktom z rówieśnikami, a w skrajnych sytuacjach konkuruje z jedzeniem i spaniem

- **Pozbawienie czy ograniczenie możliwości skorzystania z komputera lub zagrania w grę powoduje u dziecka dyskomfort,** rozdrażnienie, złe samopoczucie, agresję oraz skłania go do kłamstw dotyczących czasu spędzanego w internecie – zaniżanie czasu lub oszukiwanie dotyczące sposobu wykorzystania sieci (wymówki typu: „odrabiam lekcje", „szukam materiałów do projektu")

- **Dziecko jest nadpobudliwe,** izoluje się, ma problemy ze snem, koncentracją, może przejawiać stany lękowe

- **Relacje i kontakty w świecie wirtualnym stają się dla dziecka ważniejsze od tych w świecie realnym,** a jego rozmowy i myśli często koncentrują się wokół gry (wyboru strategii, wyników, uczestników)

- **Prosi o zakup lub wydaje samodzielnie (w tym korzysta z mikropłatności) znaczne sumy** na nowe gry, akcesoria do gier lub wyposażenie postaci.

Jak zapobiegać?

- **Obserwujmy wirtualne nawyki i zainteresowania dzieci**, by rozmawiać z nim o aktywnościach podejmowanych w sieci i negatywnych konsekwencjach dla zdrowia fizycznego (choroby kręgosłupa, wzroku) oraz dla jego psychiki w sytuacji, gdy nadużywa internetu
- **Kontrolujmy czas, który poświęca na surfowanie** po sieci i/lub granie w gry. Wsparciem dla rodziców może być aplikacja pozwalająca na monitoring czasu i stron odwiedzanych przez dziecko
- **Dbajmy o to, żeby uczestniczyć w świecie dziecka/nastolatka** proponując i zachęcając do aktywności offline.

Jak reagować?

- W przypadku zaobserwowania niepokojących zachowań (patrz rozdział: Jak rozpoznać, że dziecko dysfunkcyjnie korzysta z komputera/internetu/gier?) **rozmawiajmy z dzieckiem, by zdiagnozować i nazwać problem**
- **Obserwujmy, w jakich sytuacjach dziecko ucieka w wirtualny świat**, ponieważ utrata kontroli nad używaniem internetu może być symptomem innych problemów emocjonalnych, społecznych lub rodzinnych
- **Ustalmy sposób i czas korzystania z internetu**, w tym gier (więcej o grach w następnym rozdziale), i konsekwentnie przestrzegajmy wyznaczonych reguł
- W sytuacjach, gdy niewłaściwe używanie nowych technologii wpływa na jakość życia i zagrożenie zdrowia (niedojadanie, niedosypianie, odrzucenie innych aktywności) **ograniczmy dostęp** wyjaśniając decyzję, obserwujmy zachowania i proponujmy inne aktywności offline
- **Korzystajmy z porad specjalistów** (pedagodzy w szkole, specjalistyczne poradnie, linie telefoniczne i punkty pomocowe).

Gry komputerowe

Gry komputerowe służą przede wszystkim rozrywce, ale mają również pozytywne aspekty – trenują niektóre umiejętności poznawcze, uczą współdziałania, a także pokazują, że każda decyzja ma swoje konsekwencje.

Może się jednak zdarzyć, że gra nieodpowiednio dobrana do wieku i wrażliwości dziecka będzie dla niego szkodliwa.

Gry na polskim rynku są oznaczone według systemu PEGI, co znacznie ułatwia decyzje zakupowe.

Symbole PEGI można znaleźć na opakowaniu. Wskazują one następujące kategorie wiekowe: 3, 7, 12, 16 i 18. Zostały one nadane przez specjalistów biorących pod uwagę zawartość gry oraz jej dostosowanie do poziomu rozwoju dziecka.

Co oznaczają symbole PEGI?

Kategorie wiekowe oznaczają dostosowanie treści gry do wieku dziecka. Nie dajmy się zwieść wrażeniu lub sugestiom, że jest to oznaczenie poziomu trudności, czy określenie liczby graczy. Kategoria „3" oznacza, że gra jest odpowiednia nawet dla najmłodszych, a kategoria „18" oznacza, że gra przeznaczona jest dla osób dorosłych, ponieważ zawiera treści o charakterze szkodliwym dla młodszego użytkownika.

Przy wyborze gry zapoznajmy się z jej klasyfikacją i zdecydujmy, czy dziecko jest gotowe na kontakt z takimi treściami.

Zagrożenia technologiczne dla bezpiecznego korzystania z internetu

Urządzenia elektroniczne, dzięki którym korzystamy z internetu, są podatne na rozmaite technologiczne zagrożenia.

Zagrożenia technologiczne to między innymi: **szkodliwe oprogramowanie** (np. *wirusy komputerowe, trojany bankowe, cryptoware*), ataki socjotechniczne (np. *phishing, czyli wykradanie danych w transakcjach on-line*), **wykradanie istotnych danych** (np. *dane osobowe, dane kart płatniczych*), **masowe przejmowanie komputerów** użytkowników i wykorzystywanie ich do szkodliwej działalności (*sieci BOTnet*) i inne.

Statystyki zagrożeń i incydentów publikowane na świecie i w Polsce świadczą, że mamy do czynienia z poważnym problemem. Według raportu CERT Polska za rok 2014, w polskim internecie każdej doby obserwuje się aktywność ponad 280 tysięcy zainfekowanych komputerów użytkowników.

Już od najmłodszych lat powinnyśmy wyrabiać nawyki bezpiecznego korzystania z nowoczesnych urządzeń mających dostęp do internetu.

Jak zapobiegać?

- **Sami stosujmy zasady bezpiecznego korzystania z sieci** i uczmy swoje dzieci właściwego postępowania
- **Włączmy opcję aktualizacji oprogramowania** we wszystkich urządzeniach (komputery, tablety, smartfony, konsole)
- Zadbajmy, aby były zainstalowane **programy antywirusowe**, a ich aktualizacje były włączone
- Pamiętajmy o zaporze firewall, która powinna być domyślnie uruchomiona w każdym systemie, który to oferuje (np. system Windows na komputerze czy też zapora na routerze w sieci domowej). **Zapora firewall** to "niewidzialna" ściana chroniąca nasz komputer. Jeśli mamy wątpliwości czy to zabezpieczenie działa w naszym komputerze zapytajmy specjalistę, nauczyciela informatyki
- Pamiętajmy o tworzeniu **kopii zapasowych** swoich danych (na zewnętrznych nośnikach danych lub w tzw. chmurze internetowej) .

Stosujmy podstawowe dobre nawyki bezpiecznego korzystania z sieci:

- **Nie otwierajmy załączników e-maili pochodzących z nieznanych źródeł**, ponieważ mogą zawierać wirusy bądź inne szkodliwe programy. Nie klikajmy na adresy internetowe zawarte w e-mailach pochodzących z nieznanych źródeł, ponieważ mogą prowadzić do zarażonych stron internetowych lub stron wyłudzających nasze prywatne dane
- Unikajmy połączeń ze stronami, które nie budzą zaufania, a w szczególności nie wpisujmy na takich stronach naszych identyfikatorów i haseł
- Na smartfonach i tabletach instalujmy aplikacje pochodzące z **zaufanych źródeł** (np. ze sklepów producentów systemów operacyjnych – Google/Android, Apple/IoS) – szkodliwe aplikacje z innych źródeł mogą np. wykradać listy kontaktów i inne dane, a także zawirusowywać urządzenia
- Przy podawaniu jakichkolwiek istotnych danych (w szczególności dotyczących np. naszych kart płatniczych) upewnijmy się czy połączenie jest szyfrowane (**zamknięta kłódeczka w pasku adresowym przeglądarki**), a strona należy do właściwego podmiotu (sprawdzić dane certyfikatu po kliknięciu w kłódeczkę)
- **Zmieniajmy hasła** do urządzeń, aplikacji i serwisów internetowych. Hasła powinny być odpowiednio długie i zawierać małe, duże litery, cyfry, a także znaki specjalnie, a jeśli to możliwe używajmy tzw. uwierzytelnień dwustopniowych (np. token czy sms w telefonie)
- **Nie dokonujmy ważnych operacji w internecie poprzez publiczne, otwarte sieci WiFi**, sieci w lokalach gastronomicznych, itp.

- Zwróćmy uwagę, że zagrożenia właściwe dla komunikacji **e-mail (wirusy, phishing) rozprzestrzeniają się także w portalach społecznościowych**, a nawet w internetowych grach komputerowych
- **Nie przekazujmy dziecku kart płatniczych czy danych tych kart**, a także identyfikatorów czy haseł w celu dokonania jakichkolwiek transakcji
- **Czytajmy regulaminy usług internetowych**, z których korzystamy
- Sprawdźmy **jakie usługi bezpieczeństwa oferuje operator**, który dostarcza nam internet. Coraz częściej, za niewielką opłatą możemy otrzymać pakiety usług, które pomogą nam dbać o bezpieczeństwo (antywirus, filtrowanie, monitorowanie).

Jak reagować?

- **Rozmawiajmy z dziećmi i młodzieżą o wszelkich niepokojących symptomach** czy zaobserwowanych zjawiskach, a także starajmy się odpowiednio zareagować
- Jeśli komputer przestaje sprawnie działać, jest wolny, zawiesza się nie zawsze oznacza to jakąś awarię. Sprawdźmy czy nie jest zawirusowany, upewnijmy się, że posiada działający **program antywirusowy** i ustalmy datę ostatniej aktualizacji, a następnie przeskanujmy programem antywirusowym całą zawartość urządzenia
- Jeśli padniemy ofiarą szkodliwego programu i mamy **zablokowany ekran żądający przesłania okupu za odblokowanie – nie wysyłajmy pieniędzy** (zwykle nawet zapłacenie okupu nie spowoduje, że odzyskamy dostęp do komputera), tylko odtwórzmy, korzystając z pomocy informatyka zawartość urządzenia z kopii zapasowej i zwróćmy uwagę, co mogło być przyczyną zdarzenia (np. brak aktualnego programu antywirusowego)
- **Jeśli padniemy ofiarą oszustw finansowych** przy korzystaniu z bankowości elektronicznej należy o tym **niezwłocznie powiadomić** nasz bank. Mamy szansę odzyskać swoje pieniądze jeśli stosowaliśmy się do zasad bezpieczeństwa rekomendowanych przez bank
- Jeśli padniemy ofiarą oszustwa w internecie możemy **zgłosić przestępstwo na policję** – wtedy nasze urządzenie komputerowe (jego zawartość) jest dowodem w sprawie i powinno być zabezpieczone do ewentualnej analizy
- Jeśli korzystamy z usług operatora internetu dbającego o bezpieczeństwo, w przypadku tego typu problemów **zwróćmy się o pomoc do odpowiedniego zespołu** zajmującego się nadużyciami (kontakt na stronie internetowej bądź w umowie)

Nie wpadajmy w panikę. Zwykle problem, z którym się zetknęliśmy, można rozwiązać. Jeśli nie znamy metody, którą należy się posłużyć skorzystajmy

z rad specjalisty. Nie starajmy się także udowodnić dziecku naszej kompetencji. Jeśli przyznamy się do naszego braku wiedzy czy umiejętności, będziemy budować wzajemne zaufanie.

Gdzie uzyskać pomoc i zgłaszać nielegalne treści?

Jeśli zachodzi podejrzenie, iż doszło do przestępstwa, powinniśmy zgłosić to policji. Rad i pomocy możemy szukać także w **istniejących zespołach reagujących** na zdarzenia w internecie, takich jak Dyżurnet.pl i CERT Polska oraz u swojego **operatora** internetu czy **administratora serwisu**. Pomocą może służyć nam także szkoła. Pamiętajmy o rozmowie z nauczycielem, wychowawcą i psychologiem szkolnym.

Nielegalne treści natomiast możesz zgłosić na policję, do administratora lub moderatora serwisu oraz do Zespołu Reagującego **Dyżurnet.pl** na **www.dyzurnet.pl**.

Gdzie szukać pomocy?

Zespoły i linie pomocowe dla dzieci i młodzieży oraz rodziców w sprawach dotyczących bezpieczeństwa dzieci, również w zakresie bezpieczeństwa w internecie, dostarczają wiedzy, wskazówek rozwiązania problemu oraz wsparcia psychologicznego.

Gdzie zgłaszać nielegalne treści?

- Policja
- Administratorzy / moderatorzy
- Zespół reagujący Dyżurnet.pl

Dyżurnet.pl przyjmuje anonimowe zgłoszenia za pomocą:

- formularza na stronie: www.dyzurnet.pl
- e-mail: dyzurnet@dyzurnet.pl
- infolinia: 801 615 005
- aplikacja mobilna dyzurnet.pl

telefony zaufania

800 12 12 12
Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka

800 100 100
telefon dla rodziców i nauczycieli w sprawie bezpieczeństwa dzieci

116 111
telefon zaufania dla dzieci i młodzieży

Internet to jedno z największych technicznych osiągnięć naszych czasów. Pozwala nam lepiej poznawać świat, łatwiej się komunikować, zdobywać wiedzę, dostarcza nam rozrywki, wreszcie dzięki niemu sprawniej załatwiamy codzienne sprawy.

Korzystanie przez dzieci i młodzież z internetu jest rzeczą naturalną. Badania wskazują, że samodzielna przygoda z siecią rozpoczyna się w wieku niespełna 10 lat, ale w rzeczywistości wejście w cyfrowy świat ma miejsce znacznie wcześniej. Nikogo już nie dziwi widok 3 - 4 letnich maluchów sprawnie operujących tabletami. Internet odgrywa ważną rolę w życiu młodych ludzi. Służy im do zabawy, nauki, komunikowania się. W przypadku gimnazjalistów i uczniów szkół ponadgimnazjalnych średni czas korzystania z sieci to aż 3 godziny i 40 minut. Przeważająca większość z nich deklaruje, iż sama poznaje wirtualny świat. Tylko dla nielicznych przewodnikami po sieci są rodzice.

Aż 55,6 proc. nastolatków uważa, iż opiekunowie nie interesują się ich aktywnością w sieci.

B:) cyfrowo bezpieczni.pl

kontakt@cyfrowobezpieczni.pl

Projekt jest finansowany przez Ministerstwo Edukacji Narodowej w ramach zadania „Poprawa kompetencji pracowników szkoły, uczniów i ich rodziców w zakresie bezpiecznego korzystania z cyberprzestrzeni oraz reagowania na zagrożenia”

MINISTERSTWO EDUKACJI NARODOWEJ