BEZPIECZEŃSTWO W SIECI: CYBERPRZEMOC

Opracowanie: mgr Krzysztof Biełooki

Internet daje niesamowite możliwości: można poznać świat, nowych ludzi, dowiedzieć się wszystkiego o wszystkim. Ale niesie za sobą także zagrożenia, zwłaszcza dla dzieci. Dlatego musimy je chronić. Niniejszy artykuł służy wskazaniu tych zagrożeń, wyjaśnieniu zagadnień prawnych i możliwości przeciwdziałania tym zagrożeniom przy użyciu specjalistycznego oprogramowania.

Z badania przeprowadzonego w ramach kampanii „Chroń dziecko w sieci” wynika, że już ponad 80 proc. dzieci w wieku przedszkolnym regularnie korzysta z sieci. Co piąte dziecko przyznaje, że zdarzyło mu się trafić w sieci na treści przeznaczone tylko dla dorosłych - głównie erotyczne i pornograficzne, ale także strony zawierające wulgaryzmy, czy brutalną przemoc. Aż 89 proc. młodych ludzi deklaruje, że trafiło na takie treści przypadkowo. Jak w badaniu wypadli rodzice? Świadomość tego, że dotarcie do nieodpowiednich treści może dotyczyć ich dzieci, deklaruje jedynie 8 proc. z nich. Zaledwie 38 proc. uznaje problem szkodliwych treści za znaczący. Co piąty rodzic nigdy nie rozmawiał ze swoimi dziećmi o bezpieczeństwie w sieci, a spośród tych, którzy to zrobili, tylko połowa poruszała temat treści. 53 proc. opiekunów deklaruje, że ustaliła ze swoimi dziećmi zasady korzystania z internetu. Problem polega na tym, że zazwyczaj dotyczą one jedynie limitu czasu. Tylko 13 proc. rodziców stosuje oprogramowanie filtrujące w komputerze lub laptopie, zaś wykorzystywanie go w tabelach i smartfonach używanych przez dzieci potwierdza jedynie kilka procent z nich. Tymczasem eksperci alarmują, że dla najmłodszych jak i starszych dzieci kontakt z pornografią, czy brutalną przemocą, jaką bez większego problemu można znaleźć w sieci, może być szokiem, z którym trudno jest im sobie poradzić. Dlatego niezwykle ważne jest, żeby z jednej strony chronić dzieci przed takimi sytuacjami, a z drugiej odpowiednio na nie reagować. Autorzy kampanii podpowiadają też, co zrobić, by chronić dzieci.

Formy cyberprzemocy:

- rejestrowanie i publikowanie wizerunku osób bez ich zgody może być przestępstwem! Wizerunek osoby podlega ochronie prawnej! Nie można rozpowszechniać wizerunku osoby bez jej zgody (jeżeli nie jest to osoba publiczna pełniąca określone funkcje). Dzieci i młodzież, którzy dla zabawy robią zdjęcia ośmieszające innych i publikują je w internecie, np. na portalach społecznościowych Facebook, Twitter, Instagram, narażeni są na konsekwencje karne. Sąd może zasądzić kary: kary finansowe na rzecz poszkodowanego, nadzór kuratorski, publiczne przeproszenie, itp. W szkole uczniowi grozi m.in. zawieszenie w prawach ucznia, apel i przeproszenie na forum szkoły, przeniesienie do innej szkoły.

– cyberstalking – zjawisko używania Internetu i innych mediów elektronicznych do nękania, definiowane jako cyberprzemoc popełniana przez stalkera.

Stalking – nazwa pochodzi z języka angielskiego i oznacz „pochody" lub „skradanie się". Stalking jest definiowany jako „złośliwe i powtarzające się nagabywanie, naprzykrzanie się czy prześladowanie zagrażające czyjemuś bezpieczeństwu". Jest często powiązany z czynami karalnymi, tj. obrazą i zniewagą, zniszczeniem mienia, przemocą domową. Osoba dopuszczająca się stalkingu nazywana jest stalkerem. Przykładowe zachowania definiowane jako stalking to śledzenie ofiary, osaczanie jej (np. poprzez ciągłe wizyty, telefony, smsy, pocztę elektroniczną, podarunki) i ciągłe, powtarzające się nagabywanie. Działania te są szczególnie niebezpieczne, gdy mogą przybrać formę przemocy fizycznej, zagrażającej życiu ofiary!
W polskim kodeksie karnym stalking zdefiniowany jest jako uporczywe nękanie powodujące uzasadnione okolicznościami poczucie zagrożenia lub istotne naruszenie prywatności. Od 6 czerwca 2011 r. stanowi przestępstwo, zagrożone karą pozbawienia wolności do 3 lat (art. 190a § 1 k.k.) lub – w przypadku doprowadzenia ofiary do próby samobójczej – do 10 lat.

Przykłady cyberstalkingu:
1) publikowanie i rozsyłanie ośmieszających zdjęć i filmów w internecie,
2) wysyłanie wulgarnych wiadomości, np. wulgaryzmy, obraźliwe memy, zdjęcia porno, itp.,
3) włamania na konta, np. społecznościowe, blogi,
4) kradzież tożsamości, czyli podszywanie się pod inną osobę i działanie na jej niekorzyść, np. fałszywe konto na Facebook-u,
5) wykorzystywanie internetu w celu uwiedzenia i wykorzystania seksualnego, także osób nieletnich, np. zmiana tożsamości w celu wykorzystania seksualnego nieletniego.

Samookaleczenia i sambójstwa

Blue Whale Challenge ze wspieraniem potrzebujących nie ma nic wspólnego. Media piszą o nim: „śmiertelna gra dla nastolatków", „gra, która zbiera śmiertelne żniwo", „polują na zagubionych nastolatków z Polski". Podjęcie go ma prowadzić do załamania nerwowego, a nawet samobójstwa. Ile jest w tych określeniach prawdy? Wszystko wskazuje na to, że gra pojawiła się w Rosji już kilka lat temu. Na portalu VKontakte (odpowiednik Facebooka) młodzi ludzie dzielili się między sobą tym wyzwaniem. Sprawę miały badać też rosyjskie służby. Podobno dotarły do osoby z zaburzeniami psychicznymi, która rzeczywiście doprowadziła kogoś do samobójstwa. Zresztą niebieskiemu wielorybowi przypisuje się już 130 ofiar śmiertelnych. Natomiast jak wygląda sytuacja naprawdę, nikt nie wie. W Polsce jeszcze kilka dni temu nikt nie słyszał o niebieskim wielorybie. Dziś jest to jedno z najczęściej wyszukiwanych przez młodych ludzi haseł. Z jednej strony wydaje się, że może to być legenda, która z prawdą nie ma nic wspólnego. Z drugiej strony, skoro wyzwanie pojawiło się w sieci, to zawsze jest ryzyko, że ktoś potraktuje je na poważnie i zacznie w nią grać. Dlatego nie powinniśmy bagatelizować tej sprawy.

Czytaj więcej: http://www.dziennikzachodni.pl/strona-kobiet/macierzynstwo/a/niebieski-wieloryb-szokujaca-gra-ktora-konczy-sie-samobojstwem-co-to-jest-blue-whale-challenge,11884232/

W Polsce są już przypadki samookaleczeń inspirowanych Białym Wielorybem.
Czytaj więcej:
http://www.dziennikzachodni.pl/wiadomosci/gliwice/a/niebieski-wieloryb-15latek-z-gliwic-sie-powaznie-okaleczyl-niebieski-wieloryb-wyzwania-zabojcze,11902776/

Child grooming

Tłum. z ang.: „uwodzenie dziecka” – działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później je seksualnie wykorzystać. Jest to także mechanizm używany, by nakłonić dziecko do prostytucji czy udziału w pornografii dziecięcej.

Potocznie poprzez child grooming rozumie się uwodzenie dzieci przez Internet.

Uwodzenie przez Internet najczęściej jest procesem, w którym stopniowo postępuje przywiązanie dziecka do pedofila. W konsekwencji pojawiają się trudności emocjonalne u dziecka, a jeśli dojdzie do wykorzystania seksualnego, także poczucie winy za to, co się stało.

Włączanie dziecka w aktywność seksualną jest postępowaniem nieadekwatnym w stosunku do poziomu jego rozwoju psychoseksualnego. Ofiara tego rodzaju oddziaływań zawsze potrzebuje pomocy terapeutycznej, by wrócić do normalnego funkcjonowania.

Etapy child groomingu.

Poznawanie przyszłej ofiary następuje stopniowo.

W pierwszej fazie dochodzi do oswojenia z rozmówcą, a poruszane treści są niewinne.

Potem dochodzi do budowania relacji z dzieckiem poprzez utwierdzanie go w przekonaniu, że ma do czynienia z osobą, która o nim pamięta, stawia się w roli przyjaciela, często odwołuje się do swoich, podobnych doświadczeń życiowych.

Po zdobyciu zaufania dziecka pedofil zaczyna sprawdzać, czy ktoś dorosły może się dowiedzieć o ich kontakcie, czy ktoś kontroluje małoletniego.

Dziecko wiąże się emocjonalnie z nieznajomym poznanym w Internecie, jest to czas wprowadzania do rozmów wątków seksualnych. Jeśli dzieje się to zbyt szybko czy wzbudza opór dziecka, pedofil przeprasza i deklaruje zrozumienie. Z racji silnego przywiązania dziecku trudno jest odmówić rozmówcy, gdy prosi on o zdjęcia, wprowadza w tajniki masturbacji czy nalega na spotkanie. Atmosfera tajemniczości utrudnia dziecku weryfikację, czy to, co się dzieje, jest normalne oraz ewentualne zwrócenie się o pomoc, jeśli poczuje się skrzywdzone.

Cechy dziecka predysponowanego do bycia ofiarą:

- deprywacja emocjonalna, brak silnych więzi w realnym życiu, zarówno z dorosłymi, jak i w grupie rówieśniczej
- odrzucenie przez inne dzieci
- ufność
- chęć bycia ważnym i zwrócenia na siebie uwagi

- trzymanie wszystkiego w tajemnicy
- niska samoocena
- naiwność, podatność na manipulację
- wychowywanie się w niepełnej rodzinie

Uprawianie seksu z osobą małoletnią, która nie ukończyła 15. roku życia jest w Polsce karalne na mocy przepisów Kodeksu Karnego:

Art. 200 KK

§ 1. Kto obcuje płciowo z małoletnim poniżej lat 15 lub dopuszcza się wobec takiej osoby innej czynności seksualnej lub doprowadza ją do poddania się takim czynnościom albo do ich wykonania,
podlega karze pozbawienia wolności od lat 2 do 12.

§ 2. Tej samej karze podlega, kto w celu zaspokojenia seksualnego prezentuje małoletniemu poniżej lat 15 wykonanie czynności seksualnej.

Art. 197 KK

§ 3. Jeżeli sprawca dopuszcza się zgwałcenia:
1) wspólnie z inną osobą,
2) wobec małoletniego poniżej lat 15,
3) wobec wstępnego, zstępnego, przysposobionego, przysposabiającego, brata lub siostry,
podlega karze pozbawienia wolności na czas nie krótszy od lat 3.

Art. dotyczący bezpośrednio child groomingu (wg nowelizacji):

Art. 200a KK.

§ 1. Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim,
podlega karze pozbawienia wolności do lat 3.

§ 2. Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

Art. 200b.
Kto publicznie propaguje lub pochwala zachowania o charakterze pedofilskim, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2

Nastolatki a portale randkowe

Portale randkowe zapewniają, że dzięki nim można znaleźć prawdziwą miłość, odszukać swoją „drugą połówkę", która istnieje gdzieś na świecie. Randki w internecie uprawiają nie tylko ludzie dorośli, odpowiedzialni, ale również nastolatki, które mogą nie mieć świadomości istniejących zagrożeń. (…)
Randkowanie w przestrzeni wirtualnej wydaje się całkowicie niewinne. Dwoje ludzi pisze do siebie, flirtuje, zwierza i buduje związek. Z czasem pragnie się spotkać i skonfrontować wyobrażenia z rzeczywistością. Czasem rzeczywiście serwisy randkowe owocują małżeństwami i założeniem rodziny. W Polsce działa około 80 portali randkowych, ale tylko 10 z nich rzeczywiście przyciąga do siebie użytkowników. Realnie korzysta z nich, według badań Megapanel przeprowadzonych przez PBI i Gemius w listopadzie 2014 roku, około 3,1 mln użytkowników, ale aż 10 mln osób miało kontakt z takimi portalami. (...)
Nie można jednak zapominać o tym, że internet stwarza warunki do tego, aby kreować swój wizerunek w zupełnie inny sposób, niż rzeczywiście ma to miejsce. W kwestionariuszach w serwisach randkowych wiele osób mija się z prawdą, a nawet podszywa pod inne osoby, mając nieprzyzwoite, a nawet przestępcze zamiary. (...)
Randkowicze kłamią odnośnie swojego wieku, wyglądu, zainteresowań, stanu posiadania czy cech osobowości. Przyciągają do siebie niczego nieświadome osoby i umawiają się z nimi. Jest to szczególnie niebezpieczne dla młodych, niepełnoletnich osób. (…)

W serwisach randkowych aktywnie działają pedofile, które liczą na zawiązanie znajomości z niepełnoletnimi. Nastolatki mogą wykazać się naiwnością i chętnie zwierzać się swoim wirtualnym przyjaciołom. Kiedy druga osoba pisze, jacy jesteśmy wyjątkowi i atrakcyjni, chętnie jej wierzymy i obdarzamy zaufaniem. Może się to jednak skończyć tragicznie. Ochrona rodzicielska powinna zadziałać tutaj w taki sposób, aby nastolatek nie podawał obcym, zupełnie nieznanym przez siebie w rzeczywistości osobom swój telefon komórkowy czy podawał adres, pod którym mieszka. Należy uświadomić dziecku, że po drugiej stronie ekranu komputerowego może siedzieć zupełnie inna osoba niż mu się wydaje.

Czytaj więcej:
https://www.calmean.com/pl/randki-w-internecie-poznaj-zagrozenia-dla-dzieci/
https://www.wprost.pl/technologie/10048384/Randki-w-sieci-i-powazne-zagrozenie-jakie-za-soba-niosa-Czym-jest-sextortion.html

Aspekty prawne w konteście cyberprzemocy

Warto rozmawiać z dziećmi i młodzieżą na temat nieopowiedzianych „zabaw" w internecie i ich konsekwencjach.
Dzieci mogą odpowiadać za swoje czyny już od 13 r. ż.!
Poniżej wymienione są przepisy z Kodeku Karnego:

Art. 212 KK

§ 1. Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną niemającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności,podlega grzywnie albo karze ograniczenia wolności.

§ 2. Jeżeli sprawca dopuszcza się czynu określonego w § 1 za pomocą środków masowego komunikowania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. W razie skazania za przestępstwo określone w§ 1 lub 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.

Art. 190 KK

§ 1. Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od roku do lat 10.

Art. 216KK

§ 1. Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła,podlega grzywnie albo karze ograniczenia wolności.

§ 2. Kto znieważa inną osobę za pomocą środków masowego komunikowania,podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 207 KK

§ 1. Kto znęca się fizycznie lub psychicznie nad osobą najbliższą lub nad inną osobą pozostającą w stałym lub przemijającym stosunku zależności od sprawcy, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 1a. Kto znęca się fizycznie lub psychicznie nad osobą nieporadną ze względu na jej wiek, stan psychiczny lub fizyczny, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Jeżeli czyn określony w§1 lub 1a połączony jest ze stosowaniem szczególnego okrucieństwa, sprawca podlega karze pozbawienia wolności od roku do lat 10.

§ 3. Jeżeli następstwem czynu określonego w §1–2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2do 12.

Art. 202 KK

§ 1. Kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 3. Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od lat 2 do 12.

§ 4. Kto utrwala treści pornograficzne z udziałem małoletniego, podlega karze pozbawienia wolności od roku do lat 10.

§ 4a. Kto przechowuje, posiada lub uzyskuje dostęp do treści pornograficznych z udziałem małoletniego, podlega karze pozbawienia wolności od 3miesięcy do lat 5.

§ 4b. Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 4c. Karze określonej w § 4b podlega, kto w celu zaspokojenia seksualnego uczestniczy w prezentacji treści pornograficznych z udziałem małoletniego.

§ 5. Sąd może orzec przepadek narzędzi lub innych przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstw określonych w § 1–4b, chociażby nie stanowiły własności sprawcy.

Jakie mogą być konsekwencje wobec dziecka lub nastolatka łamiącego powyższe przepisy?
Przykłady:

- nagana (np. na forum szkoły)
- obniżenie oceny z zachowania
- sądowy nadzór rodziców
- sądowy nadzór kuratora
- sądowe zobowiązanie do właściwego zachowania
- umieszczenie w młodzieżowym ośrodku wychowawczym
- umieszczenie w zakładzie poprawczym
- kary finansowe na rzecz poszkodowanego, stowarzyszeń, itp.

Przykład: Nastolatek zakłada fałszywe konto na portalu z sexrandkami podając dane rówieśniczki bez jej wiedzy w celu jej upokorzenia w lokalnym środowisku.
Konsekwencje: nadzór kuratora, zadośćuczynienie finansowe na rzecz poszkodowanej, pokrycie kosztów sądowych, apel w szkole zarządzony przez dyrektora szkoły z publiczną naganą i oficjalnymi przeprosinami.

Jak chronić dzieci przed treściami niepożądanymi w Internecie?

- Kod PIN
  Pierwszym i głównym zabezpieczeniem, od którego należy zacząć, jest ustalenie PIN-u do urządzenia – zapobiegnie to niekontrolowanemu korzystaniu przez dziecko z naszego tabletu lub smartfona. Dodatkowo w wyniku jego zgubienia utrudni to znalazcy uzyskanie do niego dostępu.
- Aplikacje kontroli rodzicielskiej
  Przed udostępnieniem dziecku urządzenia warto zadbać o jego odpowiednie, dodatkowe zabezpieczenie. W tym celu można skorzystać z dostępnych na rynku aplikacji kontroli rodzicielskiej dających w tym zakresie naprawdę wiele możliwości. Przykłady:
  Beniamin
  Wersja demonstracyjna interesującego programu do zaawansowanej i jednocześnie prostej w obsłudze kontroli rodzicielskiej. Aplikacja pozwala ograniczyć wyświetlanie materiałów dostępnych w internecie. Może blokować dostęp do stron WWW o niepożądanej treści, na przykład o tematyce erotycznej. Beniamin jest również w stanie ograniczyć funkcjonalności komputera, jak blokowanie uruchamiania komunikatorów internetowych lub na przykład ściąganie plików. Program do pobrania tutaj.
  Visual Porn Blocker Free
  Darmowe i łatwe w obsłudze narzędzie chroniące nasze dziecko przed dostępem do treści pornograficznych we wszystkich przeglądarkach internetowych. Dostęp do Visual Porn Blocker Free chroniony jest hasłem. Zaletą Visual Porn Blocker Free jest blokowanie stron pornograficznych na wszystkich kontach użytkowników utworzonych w systemie Windows. Do pobrania tutaj.
  Mini Monitoring
  Program służy do inwigilowania poczynań użytkowników komputera. Aplikacja zapisuje zrzuty ekranowe, pełną historię pracy, wszystkie nowo otwarte okna i odwiedzane strony internetowe. Producent przygotował dwie wersje Mini Monitoring – standardową, którą bez kłopotów można odinstalować z systemu, oraz ukrytą, której działanie jest trudne do dostrzeżenia i zablokowania. Do pobrania tutaj.
  Opiekun Dziecka w Internecie
  Polski program do kontroli rodzicielskiej - wyposażony w mechanizmy oceny treści stron WWW, dzięki któremu możemy zablokować strony o tematyce pornograficznej, przemocy, sekt i satanizmie oraz narkotyków. Aplikacja

posiada bazę stron internetowych, zawierającą ponad 780 tys. adresów URL i około 3500 blokowanych słów i zwrotów w 7 językach europejskich. Opiekun Dziecka w Internecie umożliwia ograniczenie ilości czasu, jaki dziecko może poświęcić na korzystanie z Internetu. Do pobrania tutaj.

Visikid

Darmowy (do celów niekomercyjnych) program do kontroli rodzicielskiej. Aplikacja w przeciwieństwie do konkurencyjnych rozwiązań nie blokuje i nie zakazuje, a uczy odpowiedzialności i przestrzegania reguł jakich nauczyliśmy nasze dziecko. Visikid dodatkowo zbiera informacje o odwiedzanych stronach internetowych oraz uruchamianych aplikacjach oraz mierzy czas spędzony przez naszą pociechę przed komputerem. Do pobrania tutaj.

Aplikacja Kids Place

Pierwszą całkowicie darmową aplikacją (do pobrania w sklepie Play), która umożliwia nadzór rodzicielski nad użytkowaniem naszych telefonów i tabletów wyposażonych w oprogramowanie Android, jest program studia Kiddoware pod nazwą Kids Place. Pełni on funkcję swoistego panelu administratora, w którym możemy zarządzać praktycznie każdą aplikacją oraz usługą – zarówno pobraną z serwisu Google Play, jak i dostępną w ramach pakietu systemowego Androida. Program ten umożliwia stworzenie „placu zabaw" dla naszych pociech. Poprzez wskazanie aplikacji, z których będą mogły korzystać, blokujemy im dostęp do programów i usług, których naszym zdaniem nie powinny używać, zabezpieczając tym samym nasze prywatne dane przed ich ingerencją. Konfigurację placu zabaw zaczynamy od ustawienia PIN-u, dzięki któremu przy każdym wyjściu z aplikacji lub próbie zmiany jej ustawień musimy podać nasz kod. Następnie przechodzimy do ustawienia aplikacji dozwolonych. Możemy wskazać, które z naszych aplikacji zainstalowanych na telefonie będą mogły być używane oraz które z nich będą mieć możliwość połączenia z Internetem. Aplikacja Kids Place umożliwia także częściowe ograniczenie funkcjonalności wybranych programów za pomocą timera, odmierzającego czas, po którego upłynięciu użytkowanie wskazanych usług staje się niemożliwe. W razie potrzeby, gdy np. z urządzenia korzystają dzieci w różnym wieku, możliwe jest również stworzenie kilku profili administratorów i zapisanie różnorodnych ustawień konfiguracyjnych. W efekcie otrzymujemy gotowe miejsce zabaw, w którym nasze pociechy mogą korzystać z dozwolonych przez nas aplikacji.

Kaspersky Safe Kids Free

Darmowy program przeznaczony do kontroli rodzicielskiej. Aplikacja umożliwia rodzicom ochronę swoich pociech przed niebezpiecznymi treściami znajdującymi się w różnych zakątkach internetu. W wersji bezpłatnej oprogramowania użytkownik ma możliwość zarządzania aktywnością internetową, korzystaniem z aplikacji

oraz urządzeń. Dzięki tym prostym funkcjom rodzic ma może ograniczyć dostęp do wielu nieodpowiednich według niego treści. W wersji premium natomiast producent pozwoli użytkownikowi na określanie lokalizacji, monitorowanie aktywności na portalu społecznościowym Facebook, monitorowanie połączeń telefonicznych i SMS'ów oraz wysyłanie różnego rodzaju alertów i powiadomień w czasie rzeczywistym. Program do pobrania na stronie producenta lub dystrybutora Kaspersky lub tutaj.

DNS Angel

Niewielkie narzędzie, pozwalające chronić nasze pociechy przed stronami internetowymi, które zawierają treści pornograficzne, wyłudzają poufne informacje lub zawierają inne szkodliwe komponenty.

Narzędzie jest bardzo proste, nie wymaga od użytkownika żadnej konfiguracji i zapewnia skuteczną oraz natychmiastową ochronę przed witrynami zawierającymi nieodpowiednie dla dzieci treści. Jego zasada działania jest banalna i ogranicza się do podmiany domyślnych adresów DNS w systemie Windows na takie, które ograniczają dostęp do szkodliwych stron WWW. Wśród dostępnych opcji znajdziemy serwery DNS znane z oprogramowania zabezpieczającego Norton, a także Open DNS Family i MetaCert DNS.

DNS Angel nie wymaga instalacji w systemie oraz gotowy jest do użycia tuż po uruchomieniu. Z jego pomocą szybko i wygodnie zmienimy konfigurację adresów DNS w Windowsie, a także w razie potrzeby przywrócimy domyślne ustawienia. Program do pobrania tutaj.

Aplikacja Norton Family Premier

Kolejną ciekawą, darmową oraz wartą polecenia aplikacją jest Norton Family Premier, która może być używana nie tylko w urządzeniach sterowanych przez Andorid, iOS, ale również dla Windowsa. Oto najciekawsze funkcjonalności, jakie oferuje nam ten produkt:

· nadzorowanie korzystania z Internetu – umożliwia dzieciom swobodne poznawanie Internetu, jednocześnie dostarczając rodzicom informacji o odwiedzanych przez nie stronach i zapewniając narzędzia blokujące dostęp do nieodpowiednich treści (Windows, Android, iOS),

· powiadomienia przez e-mail – dowiaduj się, gdy dzieci próbują odwiedzić blokowaną witrynę. Umożliwi to przeprowadzenie rozmowy o odpowiednich treściach dla naszych pociech (Windows, Android, iOS),

· żądanie dostępu – zachęcaj do otwartej dyskusji, pozwalając dzieciom na wysłanie powiadomienia z programu Norton Family, gdy chcą poprosić o dostęp do blokowanej strony lub wyjątek od reguły domu (Windows, Android, iOS),

· nadzorowanie lokalizacji – zachowuj świadomość tego, gdzie znajdują się Twoje dzieci, używając narzędzi,

które pozwalają monitorować lokalizację urządzeń z systemem Android lub iOS oraz wyświetlać 30-dniową historię wcześniejszych lokalizacji,
· kontrola wiadomości SMS – nadzoruj wysyłane przez dzieci wiadomości SMS i określaj ich dozwolonych adresatów (Android),
· raporty miesięczne/tygodniowe – otrzymuj do skrzynki odbiorczej szczegółowe raporty dotyczące działań dzieci w Internecie (Windows, Android, iOS).
Więcej pod tym adresem.

– Bezpieczny Facebook
Małoletni uważają, że jeśli nie ma cię w sieci czy na Facebooku – nie istniejesz. Mówi to wiele o znaczeniu tego serwisu w ich świecie. Mimo że konto można założyć po osiągnięciu określonego wieku, wielu młodych ludzi obchodzi obostrzenia, aby korzystać z pełnych jego możliwości. Serwis nie posiada wbudowanej funkcji kontroli rodzicielskiej. Jednak jeśli dopilnujemy, aby dziecko zakładając konto, podało prawdziwą datę urodzenia, będzie miało dostęp tylko do treści odpowiednich dla jego wieku. Inne będą blokowane automatycznie. Dodatkowo trzeba oczywiście odpowiednio ustawić opcję Polityki Bezpieczeństwa (profil: tylko znajomi). Należy także jasno ustalić, co dziecko będzie mogło udostępniać innym oraz kto będzie mógł komentować zamieszczane posty. Pozwala to chronić młodego człowieka przed niebezpieczeństwami czyhającymi w sieci.

Decydując się na kupno komputera i podłączeniu go do Internetu powinniśmy również zadbać o prawidłową edukację: swoją i dziecka. Na początek warto dobrze zapoznać się z nowym narzędziem i uświadomić dziecku, że wbrew pozorom nikt nie jest w Internecie anonimowy. Komputer, z którego łączymy się z Internetem, ma - mówiąc w sposób uproszczony - unikalny numer, po którym możemy zostać łatwo zidentyfikowani. Musimy z całym naciskiem uświadamiać to dzieciom, które często bez kontroli ściągają na swój komputer muzykę, filmy i inne materiały objęte prawami autorskimi. Jeśli tego nie zrobimy, nie zdziwmy się, gdy pewnego dnia zapuka do domu policja i oskarży o piractwo Internetowe.

Internet daje dostęp do komunikatorów, które często wykorzystywane są np. przez pedofilów. Dlatego powinniśmy wpoić dziecku podstawowe zasady bezpiecznego korzystania z różnego rodzaju czatów:
· pod żadnym pozorem nie podawać swojego imienia, nazwiska i adresu
· nie godzić się na spotkania z nowo poznanymi osobami w świecie rzeczywistym.

Częste rozmowy na temat zagrożeń powinny uświadomić dziecku, że przyjemne pogawędki mogą mieć czasem tragiczne skutki. Internet to bogactwo stron o treści erotycznej, wulgarnej i pełnych przemocy. Nie są one przeznaczone dla dzieci, ale nie znaczy to, że dzieci na nie wchodzą.

W takim razie co robić kiedy podejrzewamy iż dziecko w sposób niewłaściwy korzysta z Internetu? Z pomocą przychodzi nam szereg programów ograniczających dostęp do stron o treści pornograficznej, z przemocą i niewłaściwych dla rozwoju dziecka oraz ograniczających możliwości instalacji i zapisywania plików.

Pamiętajmy, że instalacja programów blokujących nie zastąpi rzeczowej i spokojnej rozmowy uświadamiającej dziecku korzyści, które płyną z korzystania z sieci WWW, ale i podkreślaniu zagrożeń. Powinniśmy też budować zaufanie do własnego dziecka i z zainteresowaniem śledzić jego poczynania przed ekranem komputera.

Zaleca się wykonanie pięciu prostych kroków:

1. Ustal z dzieckiem zasady korzystania z internetu.
2. Udostępniaj dziecku jedynie pozytywne i bezpieczne treści.
3. Rozmawiaj z dzieckiem o jego doświadczeniach w sieci.
4. konfiguruj ustawienia bezpieczeństwa w urządzeniu.
5. Zainstaluj program do kontroli rodzicielskiej.

Gdzie szukać pomocy?

- szkoła (psycholog, pedagog, wychowawcy, dyrekcja)
- https://dyzurnet.pl (zgłaszanie nadużyć w internecie online)
- http://www.cert.gov.pl/ (zgłaszanie nadużyć w internecie online)
- http://www.dzieckowsieci.pl/ (porady)
- Policja tel. 112
- Niebieska Karta (może założyć Dzielnicowy Rewiru w Policji)
- Kryzysowy Telefon Zaufania 116 123
- poradnie psychologiczne

Przydatne źródła:

- http://poradnik.ngo.pl/wiadomosc/993029.html
- https://socialpress.pl/2014/01/cyberstalking-co-trzeba-wiedziec-jak-sie-bronic/
- https://www.calmean.com/pl/randki-w-internecie-poznaj-zagrozenia-dla-dzieci/
- https://www.wprost.pl/technologie/10048384/Randki-w-sieci-i-powazne-zagrozenie-jakie-za-soba-niosa-Czym-jest-sextortion.html
- https://wtb.org.pl/niebezpieczne-technologie?gclid=CjwKCAiA9MTQBRAREiwAzmytw6EU_IPhXA4SHl1r9UzH8uH7qQ35Aud_fYtpsxkqEzrGKKLIJy_rgxoCMpEQAvD_BwE
- http://www.mjakmama24.pl/rodzice/dom-prawo-finanse/blokady-i-filtry-rodzicielskie,569_490.html
- http://www.expressilustrowany.pl/najwazniejsze/a/50-zadan-niebieski-wieloryb-niebieski-wieloryb-to-bardzo-grozna-gra,11897521/
- http://www.dzieckowsieci.pl/