

BEZPIECZEŃSTWO W SIECI

Poniżej przedstawiamy najczęściej spotykane zagrożenia w sieci, jej przejawy oraz informacje jak im zapobiegać.

NAZWA NIEBEZPIECZNEGO ZJAWISKA	PRZEJAWY	JAK ZAPOBIEGAĆ – PORADY DLA RODZICÓW
CYBERPRZEMOC	• przerabianie i publikowanie zdjęć, filmów • upublicznianie sekretów ofiary • upublicznianie nieprawdziwych informacji, krzywdzących opinii lub ocen • złośliwe komentowanie wpisów lub zdjęć • przechwytywanie poczty, podszywanie się pod ofiarę i prowadzenie w jej imieniu korespondencji • celowa ignorancja aktywności ofiary w internecie	• rozmawiamy z dzieckiem o zasadach bezpiecznego korzystania z internetu, o internetowym <i>savoir-vivre</i> • rozmawiamy z dzieckiem o potencjalnych konsekwencjach podejmowanych działań (cyberprzemoc może nosić znamiona przestępstwa. Najczęściej dochodzi do naruszeń art. 190 kk. - groźba karalna, art. 190a kk – uporczywe nękanie – stalking, art. 191a kk naruszenie intymności seksualnej, art. 212 kk – zniesławienie, art. 216 kk zniewaga itd.) • pokazujemy dzieciom możliwość ochrony poprzez, np. zablokowanie użytkownika, ograniczeniu kontaktu, bądź tymczasowym wyłączeniu komentarzu na portalach społecznościowych • zwróćmy uwagę, że z pozoru niewinny żart może nieść duże konsekwencje w przyszłości • zachęcajmy dziecko aby dzieliło się problemem z zaufaną osobą i zgłaszało opiekunom • zwróćmy uwagę ile czasu dziecko korzysta z telefonu, komputera bądź

		innych urządzeń z dostępem do internetu, z jakich aplikacji i portali społecznościowych korzysta, na jakich forach się wypowiada i jakiego rodzaju treści publikuje • obserwujemy zachowanie dziecka, gdy staje się smutne, nerwowe, ograniczyło kontakty z rówieśnikami. Takie zachowanie wskazuje, że znalazło się w sytuacji problemowej • podejmujemy interwencję w każdym przypadku ujawnienia cyberprzemocy • zapewnimy dziecku wsparcie, nawet jeśli okaże się sprawcą cyberprzemocy. Przekonajmy dziecko, że niezależnie od wagi problemu, incydentu i roli jakie pełni poinformowanie opiekuna jest bardzo dobrym rozwiązaniem • wszelkie dowody w postaci wiadomości smsowych, e-maili, screenów pozwoli na rozwiązanie sprawy i wyjaśnienie problemów • korzystaj z pomocy specjalistów (pedagog/psycholog, poradnie, linie telefoniczne i punkty pomocowe)
NIEBEZPIECZNE KONTAKTY	• nawiązywanie relacji z osobami nieznajomymi na forach, czatach związanych z hobby • włączanie się w działania wielu różnych grup społeczności również grając online!!!	• zapoznaj dziecko jak najszybciej z zasadami bezpiecznego korzystania z internetu: bezpieczny nick, silne hasło, wylogowywanie się • ustal z dzieckiem zasady komunikowania się w sieci, tj. nie podawania danych osobowych, nie odpowiadania na zaczepki nieznajomych, nieakceptowanie

		zaproszeń, prezentów w grach od osób nieznanych • wprowadź zasadę, że dziecko informuje nas o każdym kontakcie z osobą dotąd nieznaną • ustal z dzieckiem zasady spotykania się w świecie rzeczywistym z osobą poznaną przez internet
Jak reagować w przypadku, gdy dziecko nawiąże kontakt z kimś potencjalnie niebezpiecznym? • w przypadku 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 objąć dziecko pomocą psychologiczną a także nie obwiniać dziecka o zaistniałą sytuację • w przypadku każdego niebezpiecznego kontaktu, powinniśmy skupić się na dziecku, gdyż może ono przeżywać problemy emocjonalne lub rodzinne w świecie realnym • zaobserwowanie jakiegokolwiek szkodliwego dla zdrowia zachowania (samookaleczanie, restrykcyjna dieta, używanie substancji psychoaktywnych). Takie sytuacje mogą świadczyć o tym, że dziecko przynależy do jakiejś niebezpiecznej społeczności działającej w internecie		
SZKODLIWE TREŚCI	Szkodliwe treści to takie materiały, które mogą wywoływać nieprzyjemne uczucia u odbiorców, promują niebezpieczne zachowania lub prezentują radykalne poglądy, m.in.: • treści pornograficzne • samookaleczenia, nawołujące do restrykcyjnych diet, promowania zażywania substancji niebezpiecznych lub pochwalające samobójstwa	• komputer przeznaczony dla dziecka powinien być wyposażony w program filtrujący i/lub inne barierki kontroli rodzicielskiej. Im młodsze dziecko, tym filtr powinien być szczelniejszy • rozmawiajmy z dzieckiem o tym co robi w internecie, ustalmy z nim, np. nie wchodzenie na strony dla dorosłych, a przede wszystkim zgłaszanie sytuacji, w którym dziecko zobaczyło coś, co je szczególnie zaniepokoiło • wyjaśnijmy dziecku, że informacje publikowane w internecie mogą być nieprawdziwe i przekłamane a także analizujemy wspólnie podejrzaną treść

		• nauczmy reagować dziecko na szkodliwe materiały, m.in. jak zgłaszać niebezpieczne treści do administratora serwisu • zwracajmy uwagę na nietypowe zachowania dziecka, np. chudnięcie, pobudzenie, oswiałość bądź inne, np. osłanianie przedramion (samookaleczenia) • kontakt dziecka z pornografią, w tym „dziecięcą”, może oznaczać, że jest ofiarą uwodzenia przez osobę o skłonnościach pedofilskich
SEKSTING	• przesyłanie treści (zdjęć, filmów) o charakterze erotycznym, głównie swoich nagich lub półnagich zdjęć • seks-komunikacja na żywo, za pośrednictwem komunikatorów z wykorzystaniem kamerki	• zapewnijmy dziecku potrzebne wsparcie, a także pokażmy pozytywne przykłady aktywności i relacji w świecie online • rozmawiajmy z dzieckiem o konsekwencjach zachowań ryzykownych • uczmy dziecko odmawiać, może dzięki temu uniknąć poddania się presji rówieśniczej zachęcającej do podejmowania zachowań ryzykownych • rozmawiajmy z dzieckiem o właściwym budowaniu wizerunku w sieci, tj. przeżyjmy wspólne ustawienia prywatności konta w portalach społecznościowych i zastanówmy się jaki poziom prywatności zastosować • jeśli doszło do rozpowszechniania treści sekstingowych, reagujmy szybko oraz zapewnijmy dziecku wsparcie, gdyż jest to dla niego niezwykle upokarzające doświadczenie

		• zwróćmy się do administratorów serwisu z prośbą o usunięcie treści. W niektórych sytuacjach niezbędna będzie pomoc wyspecjalizowanego zespołu reagującego
UWAGA! Materiały powstałe w procesie sekstingu mogą być wykorzystywane w celu szantażu i wyłudzenia pieniędzy, pozyskania dalszych materiałów albo spotkania w świecie rzeczywistym. Takie zjawisko nosi nazwę <i>sextortion</i>.		
NADUŻYWANIE INTERNETU	• czas jaki dziecko spędza przy komputerze przewyższa czas poświęcony innym aktywnościom • pozbawienie czy ograniczenie możliwości skorzystania z komputera lub zagrania w grę powoduje u dziecka dyskomfort, rozdrażnienie, złe samopoczucie, agresję • dziecko jest nadpobudliwe, izoluje się, ma problemy z koncentracją, może przejawiać stany lękowe • relacje i kontakty w świecie wirtualnym stają się dla dziecka ważniejsze od tych w życiu rzeczywistym • dziecko prosi o zakup bądź wydaje samodzielnie pieniądze na zakup gier, akcesoriów	• obserwujmy wirtualne nawyki i zainteresowania dzieci, by rozmawiać z nim o aktywnościach podejmowanych w sieci i jego negatywnych konsekwencjach • kontrolujmy czas, który poświęca na surfowanie po sieci • dbajmy o to, żeby uczestniczyć w świecie dziecka/nastolatka proponując i zachęcając do aktywności offline • obserwujmy w jakich momentach dziecko ucieka w świat wirtualny, ponieważ utrata kontroli może wskazywać na problemy emocjonalne, społeczne czy rodzinne • ustal czas i warunki korzystania z internetu, w tym gier i konsekwencje pilnuj ustalonych granic • w sytuacjach pogarszania się zdrowia i samopoczucia dziecka, ogranicz dostęp, wyjaśniając decyzję, obserwujmy zachowania i proponujmy inne aktywności • korzystaj z porad specjalistów, pedagoga, psychologa, poradni, linii telefonicznych bądź punktów pomocowych

**ZAGROŻENIA
TECHNOLOGICZNE DLA
BEZPIECZNEGO
KORZYSTANIA Z INTERNETU**

- **szkodliwe oprogramowanie**, np. wirusy komputerowe, trojany bankowe, cryptoware
 - **ataki socjotechniczne**, np. phishing czyli wykradanie danych w transakcjach online
 - **wykradanie istotnych danych**, np. danych osobowych, z kart płatniczych
 - **masowe przejmowanie komputerów** użytkowników i wykorzystywanie ich do szkodliwej działalności, np. sieci BOTnet i inne
-
- sami stosujemy zasady bezpiecznego korzystania z sieci
 - włączmy opcję aktualizacji oprogramowania we wszystkich urządzeniach
 - zainstalujmy program antywirusowy oraz możliwość jego aktualizacji
 - pamiętajmy o zaporze **firewall**, która jest „niewidzialną ścianą” chroniącą nasz komputer
 - pamiętajmy o tworzeniu kopii zapasowych swoich danych
 - nie otwierajmy załączników e-mail pochodzących z nieznanych źródeł, ponieważ mogą zawierać wirusy bądź inne szkodliwe oprogramowanie
 - unikajmy połączeń ze stronami, które nie budzą zaufania, w szczególności nie wypisujemy na nich swoich danych, haseł, loginów
 - zmieniamy hasła, które powinny zawierać małe, duże cyfry i litery a także znaki specjalne
 - **nie dokonujemy ważnych operacji w internecie poprzez publiczne i otwarte sieci WI-FI**
 - **nie przekazujemy dziecku kart płatniczych czy danych z tych kart, identyfikatorów i kodów**
 - czytamy regulaminy usług internetowych z których korzystamy
 - sprawdzimy, jakie usługi bezpieczeństwa oferuje operator, który dostarcza nam usługi sieci internet

Zapraszamy na stronę MEN po więcej informacji

<https://bezpiecznaszkola.men.gov.pl/tematy/promujemy-bezpieczenstwo-w-sieci/materialy-5/>