

PRZEMOC W INTERNECIE
I INNE ZAGROŻENIA
W CYBERPRZESTRZENI

Magdalena Wilkowska

DEFINICJA CYBERPRZESTRZENI

- ▶ **Cyberprzestrzeń** (wg Wikipedii): (ang. *cyberspace*, hybryda będąca skrótem od *cybernetics space* 'przestrzeń cybernetyczna') – pojęcie początkowo używane w powieściach twórcy cyberpunku Williama Gibsona na określenie rzeczywistości wirtualnych, w których znajdowali się jego bohaterowie. Obecne znaczenie uległo zmianie i mianem tym określa się przede wszystkim *wirtualną przestrzeń*, w której komunikują się połączone siecią komputery lub inne media cyfrowe (na przykład telefonia komórkowa). Do łączenia komputerów służy najczęściej Internet. Tym samym jest to właściwie przestrzeń informatyczna, a nie cybernetyczna. Cyberprzestrzeń jest także określana jako nowego typu przestrzeń społeczna, w której spotykają się internauci.

PODZIAŁ UŻYTKOWNIKÓW INTERNETU

Mark Prensky w 2015r. podzielił użytkowników Internetu na dwie główne grupy:

- ▶ **CYFROWYCH TUBYLCÓW:** obecne pokolenie dzieci i młodzieży, wychowywane od początku w styczności ze światem wirtualnym.
- ▶ **CYFROWYCH IMIGRANTÓW:** pokolenie osób, dla których Internet nie jest czymś naturalnym, ponieważ wzrastali w czasach, kiedy wirtualny świat dopiero raczkował lub nie został jeszcze stworzony.
- ▶ Istnieje także trzecia grupa – **WYKLUCZENI CYFROWO**, do której należą seniorzy, stanowiący nadal w przewadze najmniej liczną grupę użytkowników Internetu oraz osoby wykluczone społecznie, np. poprzez sytuację finansowo-bytową lub zdrowotną.

STATYSTYKI

Dane z konferencji organizowanych przez NASK i współorganizujące instytucje (2014–2016)

- ▶ Kilka lat temu 98% dzieci i młodzieży korzystało z Internetu co najmniej raz na tydzień, 74% z nich logowało się codziennie (głównie za pomocą komputera stacjonarnego lub przenośnego).
- ▶ Obecnie mamy tendencję silnie wzrostową, gdzie zdecydowana większość korzysta z Internetu codziennie (86% nastolatków), najczęściej za pomocą urządzeń mobilnych (43%)¹
- ▶ 3,5 godziny na dobę – średni czas codziennego spędzania dzieci i młodzieży w świecie wirtualnym w Polsce.
- ▶ Z danych z raportu NASK (2015r) wiadomo, że w 2005r. Dyżurnet.pl przyjmował 40 zgłoszeń miesięcznie, natomiast obecnie liczba ta wzrosła do 1000 przypadków.
- ▶ 89,5% ogółu uczestników sieci deklarowało, że otrzymało kiedykolwiek propozycję sextingu,
- ▶ 12,3% powyższego problemu dotyczyło dzieci,

¹Lizut J., Wrońska A. (red.) "E-zagrożenia nowym wyzwaniem dla służb społecznych", Wyższa Szkoła Pedagogiczna, Warszawa 2014r.

STATYSTYKI

- ▶ 1% dzieci przyznało się w badaniach do skorzystania z propozycji sextingu,
- ▶ 38,4% dzieci deklaruje, iż spotkało się przynajmniej raz z osobą poznaną przez Internet.
- ▶ 5% rodziców wie, jakie zagrożenia czyhają w Internecie na ich potomstwo,
- ▶ 55% rodziców nie interesuje się powyższym tematem.
- ▶ 59% dzieci i młodzieży chroni swoją prywatność w sieci,
- ▶ 18% nie widzi potrzeby ochrony danych osobowych,
- ▶ 1,4% nie wie, jak chronić swoją prywatność w sieci,
- ▶ o 10% w ostatnich kilku latach wzrosła ilość wypadków na placach zabaw wśród dzieci w wieku do 5 lat – ma to związek z pojawieniem się smartfonów, z których korzystają rodzice lub opiekunowie podczas spędzania czasu z dzieckiem na placu zabaw.

STATYSTYKI

Z raportów NASK wynika, że obecnie znaczna część dzieci i młodzieży jest przekonana, że może pozostać w sieci anonimowa oraz bezkarna. Uświadomienie osobom nieletnim, że konsekwencją ich nielegalnych działań będzie zweryfikowanie ich tożsamości przez policję i wyciągnięcie wobec nich odpowiednich konsekwencji prawnych powoduje, że spada odsetek działań nacechowanych negatywnie. Obecnie zespoły reagowania Komendy Głównej Policji z łatwością potrafią określić źródła nielegalnych działań w sieci internetowej. Dlatego tak ważna jest odpowiednia prewencja, poprzez stosowną edukację nauczycieli, a następnie osób nieletnich oraz ich opiekunów prawnych.

Wiedza na temat zachowań w internecie

Wiedza na temat zasad zachowania w internecie	% odpowiedzi twierdzących
Dozwolone jest podawanie się w internecie za inną osobę (np. za kolegę).	91,4
Jeżeli pod informacją w internecie znajduje się nazwisko autora, oznacza to, że te informacje są prawdziwe i można im zaufać.	82,5
Ściągnięcie filmu „pirackiego” (nielegalne) z internetu jest mniejszym przestępstwem niż kradzież płyty z filmem w sklepie.	65,2
Gdy pod zdjęciem lub artykułem nie ma nazwiska autora, można ich dowolnie używać, np. zamieścić na blogu, na portalu społecznościowym lub w wypracowaniu szkolnym.	65,0
Informacje zamieszczone w Wikipedii są zawsze prawdziwe i można im zaufać.	61,7
W internecie jesteśmy zupełnie anonimowi, to znaczy możemy napisać coś bez podawania nazwiska i nikt nie dowie się, że to my.	57,2

Zródło: D. Kwiatkowska, M. Dąbrowski, *Dojrzałość technologiczna uczniów w świetle wyników badań ankietowych*, „E-mentor” 1(43), Wyd. SGH, Warszawa 2012, s.4-13.

SŁOWNICZEK NAJWAŻNIEJSZYCH POJĘĆ

- ▶ **INHOPE** - międzynarodowe stowarzyszenie, które zrzesza krajowe zespoły zajmujące się przeciwdziałaniem dystrybucji materiałów przedstawiających wykorzystywanie seksualne dzieci.
- ▶ **PROGRAM SAFER INTERNET** - uruchomiony w 1999r. program Komisji Europejskiej, którego głównym celem jest promowanie szeroko pojmowanego bezpiecznego korzystania z technologii informatycznej i Internetu przez dzieci i młodzież.
- ▶ **NASK** - Naukowa i Akademicka Sieć Komputerowa - instytut naukowo-badawczy, podlegający Ministerstwu Cyfryzacji, zajmujący się przede wszystkim opracowywaniem rozwiązań mających na celu zwiększenie bezpieczeństwa sieci teleinformatycznych i pozostałych systemów sieciowych. Ponadto prowadzi bazę narodowej domeny.pl i oferuje innowacyjne rozwiązania dla poszczególnych podmiotów. Jego częścią jest Akademia NASK, realizująca swoje działania, dotyczące bezpieczeństwa dzieci i młodzieży, poprzez dwa zespoły: Zespół Szkoleń i Projektów Społecznych oraz Zespół Dyżurnet.pl

SŁOWNICZEK NAJWAŻNIEJSZYCH POJĘĆ

- ▶ **Zespół Szkoleń i Projektów Społecznych NASK** – zajmuje się działalnością edukacyjną i popularyzatorską Instytutu, poprzez organizację szkoleń, corocznych i ogólnopolskich konferencji w temacie bezpieczeństwa w sieci, jest również kreatorem innowacyjnych projektów dotyczących rozwijania kompetencji dzieci i młodzieży z zakresu technologii informacyjnej.
- ▶ **CERT POLSKA (Computer Emergency Response Team)** – pierwszy powstały w Polsce w 1995r. zespół (działający w strukturach NASK), którego zadaniem jest reagowanie na incydenty w dziedzinie bezpieczeństwa sieci oraz bezpieczeństwa zagrożonych bezpośrednio wszystkich użytkowników Internetu. Od 1 lipca 2016r. CERT Polska stał się działem Narodowego Centrum Cyberbezpieczeństwa.
- ▶ **DYŻURNET.PL** – funkcjonuje od 2005r., jest komórką odpowiedzialną za przeciwdziałanie obecności w Internecie nielegalnych i szkodliwych treści. Zespół ten, jako priorytet stawia sobie interweniowanie wobec treści mających związek z seksualnym wykorzystywaniem dzieci i mową nienawiści. Treści te dotyczą także uwodzenia dzieci, dystrybucji materiałów, które przedstawiają seksualne wykorzystywanie dzieci i młodzieży oraz szeroko pojętej pedofilii.

SŁOWNICZEK NAJWAŻNIEJSZYCH POJĘĆ

- ▶ **NCC (Narodowe Centrum Cyberbezpieczeństwa lub NC Cyber** działające w strukturach NASK) – działa od 1 lipca 2016r. pod nadzorem Ministerstwa Cyfryzacji, funkcjonuje w systemie 24/7 przez cały rok, prowadzi działalność non-profit. Jego głównym zadaniem jest ochrona bezpieczeństwa cyberprzestrzeni RP (m.in. opracowywanie rządowych planów ochrony) oraz jej obywateli. Działa w czterech pionach: szkoleniowym, operacyjnym, analitycznym i badawczo-rozwojowym. W pionie operacyjnym za przyjmowanie zgłoszeń alertów dotyczących cyberprzestrzeni i reagowanie odpowiada CERT Polska (przemianowany obecnie na CERT Narodowy) równolegle wraz z włączoną w struktury NCC jednostką Dyżurnet.pl.
- ▶ **CERT.GOV.PL** – powstały w 2008r. Rządowy Zespół Reagowania na Incydenty Komputerowe, na mocy porozumienia MSWiA oraz ABW. Naczelnym jego celem jest ochrona jednostek organizacyjnych publicznej administracji RP, m.in. przed zagrożeniami w cyberprzestrzeni, informowanie o alertach i przeprowadzanie testów bezpieczeństwa.

SŁOWNICZEK NAJWAŻNIEJSZYCH POJĘĆ

- ▶ **FIRST** – międzynarodowe forum zrzeszające zespoły reagujące, typu CERT.
- ▶ **ZESPÓŁ ABUSE** – zespół zrzeszający różne instytucje i zespoły typu CERT, reagujące w Polsce.
- ▶ **POLSKIE CENTRUM PROGRAMU SAFER INTERNET (PCPSI)** – komórka stworzona przez NASK i Fundację Dajemy Dzieciom Siłę (dawniej Fundacja Dzieci Niczyje), w celu wdrażania kompleksowego programu Komisji Europejskiej dotyczącego bezpieczeństwa w Internecie osób małoletnich. Działania PCPSI są stale wspierane przez Komitet Konsultacyjny, w którego skład wchodzi wyznaczeni do współpracy przedstawiciele policji, instytucji rządowych, biznesu i środowiska akademickiego.

SŁOWNICZEK NAJWAŻNIEJSZYCH POJĘĆ

- ▶ **HOTLINE** – (zespół reagujący) punkt kontaktowy, którego zadaniem jest przyjmowanie zgłoszeń dotyczących przypuszczalnie nielegalnych treści umieszczonych w sieci internetowej.
- ▶ **DOMENA INTERNETOWA** – adres internetowy, np. <http://www.ppp1.waw.pl/>
- ▶ **PEGI – Pan European Game Information (Ogólnopolski System Klasyfikacji Gier, OSKG)**
Informuje o celu i zasadach danej gry oraz dla jakiej grupy wiekowej jest przeznaczona. System posługuje się ikonkami określającymi negatywne cechy danej gry.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ **CHILD GROOMING (uwodzenie dzieci w sieci)**

Uwodzenie nieletnich przez dorosłych za pomocą sieci. Jest to proces złożony, polegający na zdobyciu zaufania dziecka, w celu stopniowego zacieśniania relacji z przestępcą. Na pewnym etapie dochodzi szantaż, czy to emocjonalny, czy to z użyciem gróźb. Nowelizacja kk z 5.11.2009r. wprowadziła do katalogu przestępstw uwodzenie nieletnich także przez systemy telekomunikacyjne i teleinformatyczne.

▶ **CSAM (Child Sexual Abuse Materials)**

Materiały prezentujące wykorzystywanie seksualne dzieci/treści seksualne z wykorzystaniem osoby małoletniej. Zespół Dyżurnet.pl zwraca uwagę na nieścisłość odnośnie terminu "pornografia dziecięca" uważając go, jako niewłaściwy, ponieważ przyczynia się do zacierania różnic pomiędzy kinematografią pornograficzną traktowaną w aspekcie biznesu, a materiałami dokumentującymi wykorzystywanie seksualne dzieci, które w przeciwieństwie do pornografii są zabronione prawem.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ **CYBERPROSTYTUCJA (wirtualna prostytutka)**

Czerpanie korzyści materialnych wskutek udostępnianych przez Internet erotycznych materiałów z udziałem własnym osoby (zdjęcia, filmy). Może stanowić działalność zorganizowaną lub indywidualną, na przykład w formie serwisów umożliwiających połączenie sieciowe osoby oferującej tego typu usługi z klientem. Aktywność ta może mieć charakter dobrowolny lub wymuszony (stręczycielstwo). Materiały ukazujące nieletnich mogą być wykorzystywane przez osoby przejawiające skłonności pedofilskie.

▶ **CYBERPRZEMOC (CYBERBULLING)**

Zachowania nacechowane przemocą, z użyciem nowych technologii teleinformatycznych i telekomunikacyjnych. Może mieć formę: zastraszania, nękania, obrażania, upowszechniania kłamliwych czy upokarzających informacji, nierzadko może kwalifikować się jako zniesławienie.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ CYBERSTALKING

Nękanie innych osób za pomocą mediów elektronicznych i Internetu (jest to także podszywanie się pod daną osobę w celu jej ośmieszenia, wysyłanie pogróżek, oskarżeń, zamieszczanie komentarzy kompromitujących daną osobę).

▶ FLAMING

Celowe działanie, mające na celu zaognianie różnicy zdań pomiędzy dyskutującymi w serwisach społecznościowych czy w grupach dyskusyjnych.

▶ HAPPY SLAPPING

Umieszczanie w sieci filmów lub zdjęć osób w ośmieszających ich sytuacjach, bez zgody lub wbrew woli upokarzanych.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ KRADZIEŻ WŁASNOŚCI INTELEKTUALNEJ I PRAWA WŁASNOŚCI

Przywłaszczenie sobie cudzej własności i/lub praw do niej, poprzez nielegalne kopiowanie plików, filmów, muzyki, tekstów, zdjęć, szeroko pojętej twórczości, bez podania źródła czy autora, plagiat.

▶ MOWA NIENAWIŚCI (w której zawierają się takie negatywne zjawiska jak rasizm, ksenofobia)

Nawoływanie wobec danych osób czy grup społecznych, obrażanie lub pomawianie ich, na różnym tle, najczęściej religijnym, rasowym, etnicznym, światopoglądowym czy orientacji seksualnej, wyrażane najczęściej na forach portali społecznościowych lub w grupach dyskusyjnych.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ PHISHING (kradzież danych i tożsamości)

Kradzież danych osobowych w celu osiągnięcia korzyści majątkowych lub ośmieszenia, upokorzenia ofiary. Korzyści majątkowe mogą być związane z podjęciem pożyczek, kredytów lub dokonywaniem zakupów w sieci (za pomocą skradzionych danych kart płatniczych czy dostępu do kont bankowych). Natomiast kradzież tożsamości w celach upokorzenia ofiary może być wykorzystana do zakładania fałszywych kont na portalach społecznościowych.

▶ PRO-ANA (porcelanowe motyle)

Ana pochodzi od zwrotu anoreksja, jest to ruch propagujący styl życia mający na celu uzyskanie pozornie idealnego wizerunku, jaki tkwi w umyśle osoby dotkniętej anoreksją. Pro-ana stanowi ruch grup zamkniętych, zajmujących się promowaniem anoreksji pod płaszczyzną dążenia do perfekcji, propagujących tzw. "zdrowy styl życia", często posługują się symbolem motyli.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ SEXTING

Przesyłanie przy pomocy mediów elektronicznych swoich nagich zdjęć, najczęściej w prywatnych kontaktach, jednak istnieje tu ryzyko upublicznienia tych materiałów bez zgody osoby na nich widniejącej. Hasło przewodnie w kampanii edukacyjnej w Holandii – "Nie udostępniaj nigdzie tego, czego nie chciałbyś pokazać swojej babci", w Polsce prewencję prowadzono pod tytułem "Myślę, więc nie ślę", natomiast dla dzieci zaadaptowano na polskie warunki słowacką kreskówkę pt. „Bez kożuszka” z serii kresówek „Owce w sieci”, dotyczących bezpiecznego korzystania z Internetu.

▶ SEXTORTION

Forma szantażu, w której przestępca grozi ofierze udostępnieniem jej nagich zdjęć. Sprawca tego procederu nierzadko wchodzi nielegalnie w posiadanie zdjęć szantażowanej osoby, może być to także efektem działalności grup przestępczych, obezwładniających swoje ofiary pigułką gwałtu i wykonujących jej w następstwie tego kompromitujących zdjęć. Do procederu mogą być również wykorzystane zdjęcia pochodzące z uwodzenia dzieci w Internecie lub z sextingu.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ SPAM

Niepożądane wiadomości elektroniczne, dzielone na dwie zasadnicze grupy – mniej szkodliwą – wiadomości reklamowe i formę agresywną, zawierającą złośliwe oprogramowanie, którego celem jest kradzież naszych danych osobowych lub zawładnięcie zawartością naszych komputerów i urządzeń mobilnych. Spamy drugiej kategorii coraz częściej działają na bardzo wysublimowanych zasadach, np. mieszcząc się w wiadomościach łudząco podobnych do korespondencji powszechnie znanych firm czy instytucji, zawierających również ich skradzioną szatę graficzną strony internetowej i logo.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ TREŚCI NIELEGALNE.

Treści zakazane poprzez polskie prawo.

Cytowane za Dyżurnet.pl (<https://dyzurnet.pl/faq.html>):

"Za nielegalne treści w Internecie polskie prawo uważa:

- zachęcanie i namawianie małoletniego do podejmowania czynności seksualnych (art. 200a § 1 KK);
- propagowanie i pochwalanie zachowań o charakterze pedofilskim (art. 200b 2KK)
- uwodzenie małoletniego w Internecie (tzw. grooming) (art. 200a § 1);
- publiczne prezentowanie treści pornograficznych w taki sposób, że może to narzucić ich odbiór osobie, która sobie tego nie życzy (art. 202 § 1 KK);
- treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem (tzw. twarda pornografia) (art. 202 § 3 KK);
- treści pornograficzne przedstawiające wytworzony lub przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej (art. 202 § 4b KK);
- publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa lub nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (art. 256 KK);
- rozpowszechnianie i publiczne prezentowane treści, które mogą ułatwić popełnienie przestępstwa terrorystycznego (art. 205a KK);
- publiczne znieważanie grupy ludności albo poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości (art. 257 KK)."

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ TREŚCI SZKODLIWE.

Treści nieodpowiednie dla osób nieletnich oraz treści mogące promować niebezpieczne zachowania. Treści te mogą, ale nie muszą, być zabronione prawem obowiązującym w danym kraju. Są to np. materiały pornograficzne udostępniane bez ostrzeżenia (w tym treści zawierające seksualne wykorzystywanie dzieci), treści drastyczne (martwe lub okaleczone bądź zdeformowane osoby, mowa nienawiści, znęcanie się nad ludźmi lub zwierzętami), nawoływanie do samobójstw lub do działań wysoce szkodliwych dla zdrowia (np. ruch pro-ana, samookaleczanie się, niebezpieczne substancje psychoaktywne itd.).

▶ TROLLLOWANIE

Celowe i negatywnie nacechowane przeszkadzanie w dyskusji prowadzonej między internautami, na przykład na forach, w grupach dyskusyjnych, na czatach. Wiąże się ze złośliwą aktywnością, polegającą m.in. na komentowaniu dyskusji bez związku z tematem, obsesyjnym wytykaniem błędów ortograficznych, stosowaniem obraźliwych czy agresywnych sformułowań.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ TYPOSQUATTING

Celowe wykorzystywanie błędów we wpisanej przez użytkownika domenie internetowej w pasku adresowym lub w wyszukiwarce (błędy wynikające np. z przestawienia liter, pominięcia kropki czy myślnika itd.). Najczęściej wykorzystywane do podszywania się pod określone, popularne strony internetowe w celu zwiększenia liczby odsłon swojej strony (m.in. stron zarabiających na wyświetlaniu reklam, stron sklepów w sieci, zwiększających swoje przychody w skutek przypadkowych odsłon).

▶ CYBERSQUATTING

Proceder o identycznych zasadach działania jak typosquatting, ale towarzyszą mu działania zakazane prawnie lub działania złośliwe w stosunku do użytkownika wyszukującego dany adres internetowy. Poszukujący jest przekierowywany na nielegalne strony, za którymi nierzadko kryją się grupy przestępcze czerpiące korzyści z działalności łamiącej prawo, np. mającej zyski z seksualnego wykorzystywania dzieci.

NAJWAŻNIEJSZE ZAGROŻENIA ZWIĄZANE Z UŻYTKOWANIEM INTERNETU

▶ UZALEŻNIENIE OD INTERNETU I URZĄDZEŃ TELEKOMUNIKACYJNYCH

Określenie używane odnośnie osób spędzających zbyt wiele czasu w sieci, kosztem notorycznego zaniedbywania codziennych obowiązków, relacji rodzinnych, społecznych, czego efektem jest pogorszenie lub zaniechanie funkcjonowania na każdym z tych obszarów.

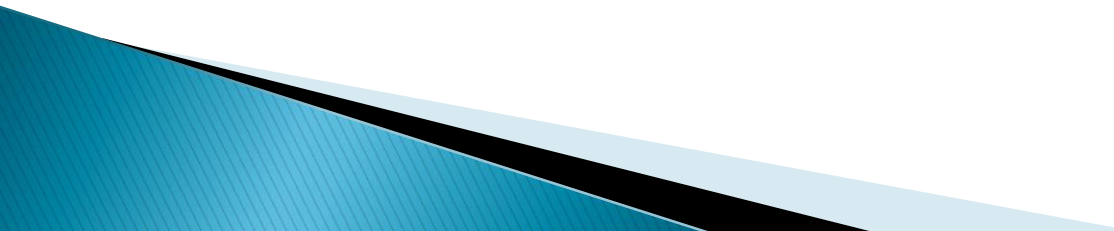
Może przyjmować formę fonoholizmu, infoholizmu, siecioholizmu, internetoholizmu, cybrzależności, uzależnienia od gier on-line. Odłączenie uzależnionego od Internetu skutkuje pojawieniem się u niego podobnych cech zachowania, typowych dla osób na odwyku.

PROCEDURA PRZEKAZYWANIA ZGŁOSZEŃ O TREŚCIACH SZKODLIWYCH LUB NIELEGALNYCH POMIĘDZY KOMÓRKAMI REAGUJĄCYMI

(na podstawie Dyżurnet.pl)

- ▶ 1. Przyjęcie nowego zgłoszenia do punktu kontaktowego (hotline).
- ▶ 2. Analiza przyjętego zgłoszenia i podjęcie odpowiednich kroków.
- ▶ 3. Ustalenie lokalizacji serwera:
 - jeśli materiał o nielegalnych treściach i/lub przedstawiający seksualne wykorzystywanie nieletnich znajduje się na polskim serwerze, następuje przekazanie go do Komendy Głównej Policji,
 - jeśli materiały znajdują się na serwerach poza granicami Polski i przedstawiają wykorzystywanie seksualne małoletnich, zostają przekazane przez zespół przyjmujący zgłoszenie do innego zespołu interwencyjnego, który jest zrzeszony w INHOPE i dalsze postępowanie odbywa się zgodnie z lokalnym prawem ustawowym,
 - jeśli materiały przedstawiające wykorzystywanie seksualne małoletnich znajdują się na serwerach poza granicami Polski i poza krajami zrzeszonymi w INHOPE, zostają przekazane do Komendy Głównej Policji w Polsce, odpowiedzialnej za skontaktowanie się z przedstawicielami policji z kraju, w którym znajduje się serwer z umieszczonymi na nim nielegalnymi lub szkodliwymi treściami.

PROCEDURA PRZEKAZYWANIA ZGŁOSZEŃ O TREŚCIACH SZKODLIWYCH LUB NIELEGALNYCH POMIĘDZY KOMÓRKAMI REAGUJĄCYMI (na podstawie dyżurnet.pl)

- ▶ 4. Przekazanie informacji: dostawcy lub właścicielowi portalu, administratorowi strony lub treści, moderatorowi serwisu – zabezpieczenie materiałów i ich usunięcie ze strony internetowej.
 - ▶ 5. Przekazanie zgłaszającemu informacji zwrotnej.
 - ▶ 6. Monitorowanie dostępności treści nielegalnych.
 - ▶ 7. Zamknięcie zgłoszenia.
- 

ZASADY OCHRONY RODZICIELSKIEJ DZIECI PRZED PRZEMOCĄ W INTERNECIE

(Na podstawie: <http://www.dzieckowsieci.pl/>)

- ▶ 1. Ustalenie z dzieckiem zasad korzystania z Internetu.
- ▶ 2. Udostępnianie dziecku wyłącznie bezpiecznych i pozytywnych treści.
- ▶ 3. Rozmawianie z dzieckiem o jego dotychczasowych doświadczeniach w korzystaniu z Internetu i o tym, na co powinno ono zawsze zwracać uwagę i jak reagować na zagrożenia.
- ▶ 4. Edukowanie dziecka poprzez rozmowę, filmiki, gry i publikacje dostosowane do jego wieku.
- ▶ 5. Skonfigurowanie ustawień zabezpieczeń we wszystkich urządzeniach, z jakich korzysta dziecko.
- ▶ 6. Zainstalowanie i stałe aktualizowanie programów kontroli rodzicielskiej (tzw. filtrów rodzinnych).

WSPARCIE DLA RODZICÓW I EDUKATORÓW

- ▶ **Fundacja Poza Schematami (ważne! – istnieje prywatna poradnia o identycznej nazwie, warto o tym pamiętać, by nie pomylić strony internetowej)**
www.fundacjapozaschematami.pl
- ▶ **Fundacja Dajemy Dzieciom Siłę (FDDS)**
fdds.pl
platforma e-learningowa: <https://www.edukacja.fdds.pl/>
- ▶ **Kampania „Dziecko w sieci” (NASK i FDDS)**
www.dzieckowsieci.pl/kampania
- ▶ **Dziecko w sieci – platforma e-learningowa**
<http://www.dzieckowsieci.pl/>
- ▶ **Akademia NASK**
akademia.nask.pl
- ▶ **Fundacja Studio Psychologii Zdrowia – projekt "Przedszkolak w sieci"**
studio-psychologii.pl/pl
- ▶ **„Cybernauci – kompleksowy projekt kształtowania bezpiecznych zachowań w sieci” – także dla szkół** <http://cybernauci.edu.pl/>

WSPARCIE DLA RODZICÓW I EDUKATORÓW

- ▶ **Polskie Centrum Programu Safe Internet**
www.saferinternet.pl/pl/
- ▶ **Fundacja Orange – Dziecko w sieci – platforma e-learningowa i kurs internetowy "Bezpiecznie Tu i Tam"**
fundacja.orange.pl/kurs/
- ▶ **PEGI (Ogólnopolski System Klasyfikacji Gier, OSKG)**
www.pegi.info/pl/index/id/362/#question_0
- ▶ **Edukacja Medialna – portal zawierający gotowe materiały dydaktyczne dla edukatorów, dotyczące bezpieczeństwa w sieci i ochrony wizerunku**
edukacjamedialna.edu.pl/
- ▶ **Centrum Bezpieczeństwa Rodzinnego Google – przewodnik dla rodzin, jak krok po kroku chronić swoje urządzenia teleinformatyczne:**
<https://www.google.com/intl/pl/safetycenter/>
- ▶ **Program Edukator.pl – Ogólnopolska Inicjatywa Edukacyjne KURSOR (platforma edukacyjna dotycząca bezpiecznego i świadomego korzystania z nowych technologii informacyjnych)**
<http://www.edukator.pl/O-programie,10242.html>
<http://www.edukator.pl/KURSOR,10241.html>

PUBLIKACJE DLA RODZICÓW I EDUKATORÓW

- ▶ **„Bezpieczeństwo dzieci on-line. Kompendium dla rodziców i profesjonalistów”**
http://www.saferinternet.pl/images/artykuly/projekty-edukacyjne/Kompendium_www.pdf
- ▶ **„Nadmierne korzystanie z komputera i Internetu przez dzieci i młodzież”**
http://www.saferinternet.pl/images/stories/pdf/nadmierne_korzystanie_z_internetu_przez_dzieci_i_mlodziuz.pdf
- ▶ **„Pomyśl, zanim kupisz. Zakup kontrolowany. Zanim kupisz dziecku komputer, tablet, telefon, laptop, konsolę, grę komputerową... pomyśl o jego bezpieczeństwie”**
https://it-szkola.edu.pl/upload/files/Broszura-Pomysl-Zanim-Kupisz-A5-v8-26-11-2015_ebibl.pdf
- ▶ **„Zostań znajomym swojego dziecka” cz. 1 i kolejne części (na YouTube)**
<https://www.youtube.com/watch?v=dptdxvV6hlc>
https://it-szkola.edu.pl/upload/files/broszura_ebibl.pdf
- ▶ **„Always on – zawsze w sieci. Materiały robocze do lekcji”**
docplayer.pl/26781438-Always-on-zawsze-w-sieci.html

PUBLIKACJE DLA RODZICÓW I EDUKATORÓW

- ▶ **Seria broszur „Zagrożenia w Internecie. Zapobieganie – reagowanie”**

https://it-szkola.edu.pl/upload/files/zapobieganie-reagowanie-cyberprzemoc_ebibl.pdf

https://it-szkola.edu.pl/upload/files/plakat_zagrozenia-w-internecie_ebibl.pdf

https://it-szkola.edu.pl/upload/files/cyberprzemoc_cz2_ebibl.pdf

https://it-szkola.edu.pl/upload/files/cyberprzemoc_seksting_ebibl.pdf

- ▶ **„Szkolne standardy bezpieczeństwa dzieci i młodzieży online”**

https://fundacja.orange.pl/files/user_files/user_upload/materialy_edu_dla_nauczycieli/Skolne_standardy_bezpieczenstwa/Skolne_standardy_bezpieczenstwa_online.pdf

- ▶ **„Bezpieczny Internet krok po kroku. Kurs nie tylko dla seniora”**

http://cafesenior.pl/wp-content/uploads/2014/03/bezpieczny_internet.pdf

- ▶ **„Bezpieczne media” – poradnik**

https://fundacja.orange.pl/files/user_files/user_upload/materialy_edu_dla_nauczycieli/Poradnik_Bezpieczne_media/Bezpieczne_media._Przewodnik_dla_rodzicow..pdf

PUBLIKACJE DLA RODZICÓW I EDUKATORÓW

- ▶ **„Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych”**
<https://cyberprzestrzen.wspkorczak.eu/pl/dokumenty/PRODUKT-FINALNY;102.html>
- ▶ **„E-zagrożenia nowym wyzwaniem dla służb społecznych”**
https://www.researchgate.net/profile/Lukasz_Tomczyk/publication/270157920_Pedagogiczno-techniczne_uwarunkowania_ochrony_wizerunku_w_sieci_Pedagogical_and_technical_conditions_of_protection_of_the_image_on_the_Internet/links/54a134bf0cf267bdb90196e0.pdf
- ▶ **„Kreatywna profilaktyka dla najmłodszych. Poradnik dla realizatorów zajęć”**
https://drive.google.com/file/d/0B48TV9MRUCY_YUVXZ0tkOHA2dWM/view
- ▶ **„Profilaktyka uzależnień behawioralnych wśród młodzieży gimnazjalnej”**
https://drive.google.com/file/d/0B48TV9MRUCY_RINldHNtQUJ5dE0/view
- ▶ **„Bezpieczna szkoła”**
<https://it-szkola.edu.pl/bezpieczenstwo>

PUBLIKACJE DLA RODZICÓW I EDUKATORÓW

- ▶ „Jak chronić dziecko przed nałogowymi zachowaniami”
https://drive.google.com/file/d/0B48TV9MRUCY_eHlINWxZUjJdE0/view
- ▶ „Owce w sieci” – e–podręcznik dla nauczyciela (scenariusze zajęć)
http://www.saferinternet.pl/images/artykuly/materialy/Owce/booklet%20pojedyncze%20ostrony%20_%20OWCE%20W%20SIECI%20125x122mm%20_%2008%20_%20do%20akceptu%20_%20OK.pdf
- ▶ „Bezpiecznie Tu i Tam” – materiały edukacyjne
https://fundacja.orange.pl/nasze-programy/bezpiecznie-tu-i-tam/?_ga=2.265285327.1162086074.1493855697-336399937.1493846899

Rodzice: <https://fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-rodzicow/>
Edukatorzy: <https://fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-nauczycieli-i-wolontariuszy/>
- ▶ „KURSOR – e–book dla nauczycieli”
http://pliki.edukator.pl/kursor_pliki/OIE_KURSOR_DLA_NAUCZYCIELI.pdf
- ▶ „Broszura „Zagrożenia internetowe. Wybrane zjawiska”
https://it-szkola.edu.pl/upload/files/Zagr-intern_ebibl.pdf

MATERIAŁY EDUKACYJNE DLA DZIECI I MŁODZIEŻY

- ▶ **Materiały do pobrania z Fundacji Orange**
<https://fundacja.orange.pl/strefa-wiedzy/materialy-edukacyjne-dla-dzieci-i-mlodziezy/>
- ▶ **Gra edukacyjna – "Bezpiecznie tu i tam,, Fundacji Orange**
format A4: http://biuroprasowe.orange.pl/wp-content/uploads/2017/03/Bezpiecznie-Tu-i-Tam_Orange_gra_A4.pdf
format A3: http://biuroprasowe.orange.pl/wp-content/uploads/2017/03/Bezpiecznie-Tu-i-Tam_Orange_-_gra_A3.pdf
- ▶ **"Przygody Plika i Foldera,,**
<http://akademia.nask.pl/projekt-38/o-nas.html>
- ▶ **"Plik i Folder – odkrywcy Internetu,,**
<http://akademia.nask.pl/projekt-38/o-nas.html>
<http://www.saferinternet.pl/pl/materialy-multimedialne/4238-plik-i-folder-odkrywcy-internetu>
- ▶ **Gra edukacyjna – „Rufus w opałach”**
<http://www.edukator.pl/Gra,10245.html>

MATERIAŁY EDUKACYJNE DLA DZIECI I MŁODZIEŻY

- ▶ **"Rysia i Tolek w krainie zdrowych nawyków,,**
https://drive.google.com/file/d/0B48TV9MRUCY_YXImZHBPUMWydIU/view
- ▶ **"Rysia i Tolek na Cyberzachodzie,,**
https://drive.google.com/file/d/0B48TV9MRUCY_OE5qbXRic09EZG8/view
- ▶ **"Miłość, a elektroniczna fascynacja,,**
https://drive.google.com/file/d/0B48TV9MRUCY_c0IpYIVsWUIJU Xc/view
- ▶ **"BHP użytkownika mediów elektronicznych,,**
https://drive.google.com/file/d/0B48TV9MRUCY_NFFzR1JkTTNnZkE/view

KURSY I PLATFORMY EDUKACYJNE DLA DZIECI I MŁODZIEŻY

Przedszkolaki:

- ▶ „Necio”
<http://www.necio.pl/>

Uczniowie:

- ▶ „Sieciaki”
<https://sieciaki.pl/>
- ▶ „Numanuma”
<http://www.numanuma.pl/>
- ▶ „Digitalyouth”
<http://www.digitalyouth.pl/>
- ▶ „W sieci ”
<http://www.wsieci.tv/>
- ▶ „Owce w sieci”
<http://pl.sheeplive.eu/>
- ▶ Fundacja Dajemy dzieciom Siłę – platforma e-learningowa dla dzieci i młodzieży
https://www.edu.fdds.pl/?option=com_szkolenia&optrs=2

INSTYTUCJE POMOCOWE I ZESPOŁY REAGOWANIA W POLSCE

- ▶ **Dyzurnet.pl** – punkt kontaktowy, tzw. hotline, gdzie można zgłaszać (anonimowo) przypadki występowania w sieci treści prawnie zabronionych
dyzurnet@dyzurnet.pl
801 615 005
- ▶ **cert@cert.pl** – punkt kontaktowy zespołu CERT
- ▶ **cyber-kgp@policja.gov.pl** – punkt kontaktowy drogą internetową Wydziału Wsparcia Zwalczenia Cyberprzestępczości Biura Służby Kryminalnej Komendy Głównej Policji
- ▶ **116 111** – telefon zaufania dzieci i młodzieży
www.116111.pl – formularz kontaktowy na stronie
- ▶ **800 100 100** – telefon dla rodziców i nauczycieli dotyczący bezpieczeństwa dzieci
pomoc@800100100.pl
- ▶ Poradnia "Dziecko w sieci" – Fundacji Dajemy Dzieciom Siłę, tel. **22 616 16 69**
- ▶ **Latarnicy.pl** – portal zrzeszający lokalnych animatorów i pomagający osobom powyżej 50 roku życia w stawianiu pierwszych kroków w Internecie, także w temacie bezpieczeństwa w sieci.

Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Kluczowym elementem pracy Akademii NASK jest dbanie o bezpieczeństwo młodych użytkowników Internetu, dlatego z myślą o nich opracowane zostały materiały edukacyjne na temat bezpieczeństwa w sieci. Treści te mają atrakcyjną formę i zostały przygotowane specjalnie pod kątem różnych grup wiekowych.”

Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Przygody Plika i Foldera w sieci – materiały przeznaczone dla klas I – III szkoły podstawowej, wprowadzające w wirtualny świat, uczące podstawowych zasad bezpiecznego korzystania z sieci. W skład **Przygód Plika i Foldera w sieci** wchodzi 6 krótkich filmów fabularnych i 5 odcinków w formie audiobooka. Powstał również zeszyt ćwiczeń dla dzieci – krzyżówki, łamigłówki i kolorowanki.”
- ▶ „**Plik i Folder – odkrywcy Internetu** – 4 krótkie filmy fabularne przygotowane dla dzieci z klas IV–VI szkoły podstawowej, przedstawiające problem nadmiernego korzystania z sieci, cyberprzemocy, uczące krytycznego podejścia do informacji znalezionych w Internecie oraz pokazujące możliwości, jakie dają nowe technologie w wyrażaniu siebie.”

www.plikifolder.pl

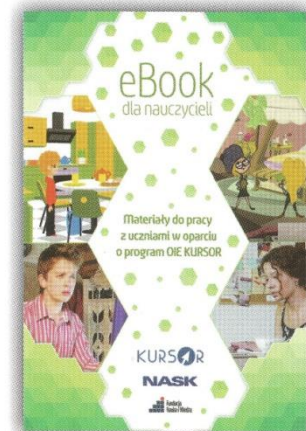


Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „**KURSOR** – zawiera materiały multimedialne przeznaczone dla uczniów starszych klas szkoły podstawowej oraz gimnazjum. Celem programu jest rozwijanie u nastolatków kluczowych kompetencji w zakresie bezpiecznego korzystania z nowych technologii. Pakiet materiałów zawiera między innymi 9 filmów animowanych. Bohaterowie kreskówek, żyjący w baśniowym świecie, w zabawny sposób przestrzegają przed niebezpieczeństwami on-line odczuwając ich skutki na własnej skórze. Krasnoludki wpadają w spiralę przemocy, Czerwony Kapturek poznaje w sieci niebezpiecznego znajomego, a siostry Kopciuszka wydają fortunę biorąc udział w telefonicznym konkursie. W ramach projektu powstała również gra edukacyjna **Rufus w opałach**, dzięki której uczniowie wcielając się w postać tytułowego Rufusa towarzyszą mu w jednym z wielu szkolnych dni i podejmują ważne decyzje, które mają wpływ na dalszą rozrywkę.”

www.kursos.edukator.pl

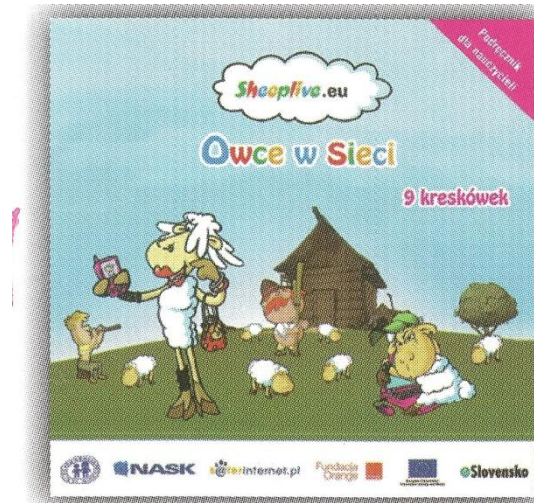


Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „**Owce w sieci** – to cykl animowanych bajek na temat najważniejszych zagrożeń sieciowych dla uczniów szkoły podstawowej. Twórcą filmów jest eSlovensco, słowacki projekt promujący bezpieczne zachowania w sieci. Bajki zostały zaadaptowane na polski grunt przez NASK oraz Fundację Dzieci Niczyje w ramach projektu Safer Internet.”

www.pl.sheeplive.eu



Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ **„Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów** – wśród publikacji mających na celu zapoznanie rodziców oraz profesjonalistów pracujących z dziećmi z problematyką bezpieczeństwa internetowego szczególnie zachęcamy do korzystania z kompendium, będącego wynikiem pracy ekspertów Akademii NASK oraz Fundacji Dzieci Niczyje prowadzących Polskie Centrum Safer Internet. Publikacja ta w kompleksowy sposób omawia cyfrowe wyzwania oraz zagrożenia, pozwala zaobserwować symptomy u młodych osób dotkniętych przemocą on-line bądź zmagających się z nadużywaniem sieci oraz daje praktyczne wskazówki, gdzie szukać pomocy i jakie procedury stosować w środowisku szkolnym.”

www.safeinternet.pl



Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Nadmierne korzystanie z komputera i Internetu przez dzieci i młodzież – zawiera artykuły dotyczące problemu uzależnienia od Internetu, opierające się na najnowszych badaniach oraz praktyce terapii uzależnień.”

www.safeinternet.pl



Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Seria broszur **Zagrożenia w Internecie. Zapobieganie – reagowanie** – broszury dedykowane nauczycielom, rodzicom i opiekunom, które prezentują w postaci plakatów podstawowe zasady bezpieczeństwa internetowego, zjawiska cyberprzemocy oraz sextingu, zagrożenia związane z nielegalnymi i szkodliwymi treściami oraz grami internetowymi i komputerowymi.”
- ▶ „Broszura **Zagrożenia internetowe. Wybrane zjawiska** – zawiera katalog definicji najważniejszych zagrożeń internetowych.”

www.dyzurnet.pl



Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Pomyśl, zanim kupisz – poradnik – zawiera porady dla dorosłych na temat tego, jak dokonać rozważnego zakupu sprzętu elektronicznego dla dzieci, a także opis zagrożeń internetowych, wskazówki jak uchronić przed nimi najmłodszych oraz gdzie się zwrócić o pomoc.”

www.zanimkupisz.safeinternet.pl



Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

- ▶ „Podaj dalej –Senior dla Kultury i Podaj dalej 2 – Senior dla Kultury – dwie publikacje poprojektowe, będące podsumowaniem działań projektu, jak również zawierające różne spojrzenie na problem wykluczenia cyfrowego seniorów w Polsce oraz barier w ich nauczaniu.”

Prezentacja wybranych publikacji i programów edukacyjnych

(Źródło: "Folder Akademii NASK", NASK, Warszawa 2015)

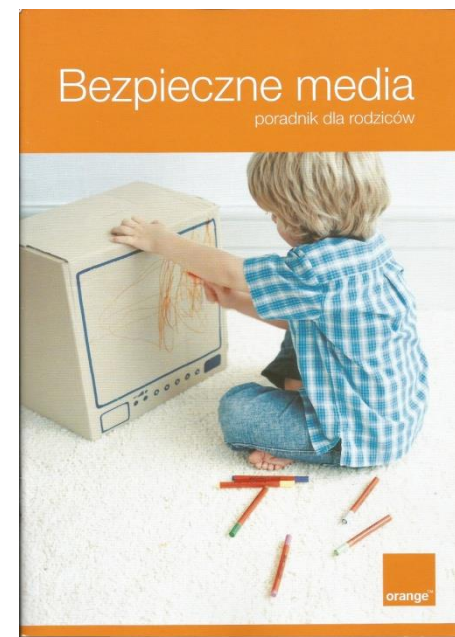
- ▶ Nowe odcinki **Zostań znajomym swojego dziecka** – nowa edycja projektu edukacyjnego (premiera na początku 2016 roku) składającego się z serii filmów oraz broszury edukacyjnej adresowanej do rodziców i opiekunów w celu zachęcania ich do aktywnego uczestniczenia w internetowym świecie dzieci. Projekt realizowany przez NASK w ramach projektu Safer Internet.

www.saferinternet.pl



Prezentacja wybranych publikacji i programów edukacyjnych

- ▶ **Bezpieczne media oraz Bezpiecznie Tu i Tam** – kompleksowy poradnik dla rodziców na temat bezpiecznego użytkowania mediów



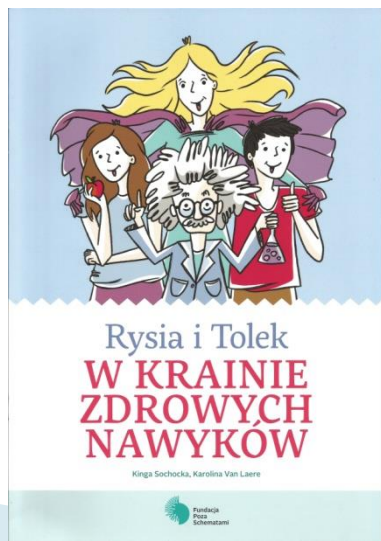
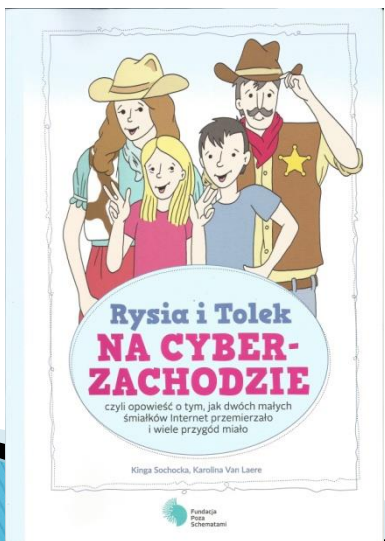
Prezentacja wybranych publikacji i programów edukacyjnych

- ▶ Poradniki dla edukatorów i rodziców na temat bezpiecznego użytkowania Internetu, wydane przez **Fundację Poza Schematami**



Prezentacja wybranych publikacji i programów edukacyjnych

- ▶ Poradniki dla dzieci i młodzieży na temat bezpiecznego użytkowania Internetu, wydane przez Fundację Poza Schematami



Bibliografia

- ▶ Lizut J., Wrońska A. (red.) "E-zagrożenia nowym wyzwaniem dla służb społecznych", Wyższa Szkoła Pedagogiczna, Warszawa 2014.
- ▶ Lizut J. (red.) "Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych", Wyższa Szkoła Pedagogiczna, Warszawa 2014.
- ▶ Polak Z., Różycka M., Marańda M., Szelań M. "Zagrożenia internetowe – wybrane zjawiska", NASK, Warszawa 2015.
- ▶ Van Laere K., Sochocka K., Biaduń-Korolczuk E. "BHP użytkownika mediów elektronicznych", Fundacja Poza Schematami, Warszawa 2015.
- ▶ Van Laere K., Sochocka K., Biaduń-Korolczuk E. "Miłość, a elektroniczna fascynacja", Fundacja Poza Schematami, Warszawa 2015.
- ▶ Wrzesień-Gandolfo A. "Bezpieczeństwo dzieci on-line. Kompendium dla rodziców i profesjonalistów", Polskie Centrum Programu Safer Internet, Wydanie III, Warszawa 2015.
- ▶ Akademia NASK (red.) "Folder Akademii NASK", NASK, Warszawa 2015.
- ▶ Kwiatkowska D., Dąbrowski M. "Dojrzałość technologiczna uczniów w świetle wyników badań ankietowych", E-mentor, 1(43), Wyd. SGH, Warszawa 2012.
- ▶ "Nadmierne korzystanie z komputera i Internetu przez dzieci i młodzież", Polskie Centrum Programu Safer Internet, Warszawa 2012.