Plan zapewnienia bezpieczeństwa cyfrowego

oprac. Monika Markowska

Podstawowym elementem cyfrowego bezpieczeństwa w szkołach jest wiedza i świadomość **uczniów**, ale także **nauczycieli i rodziców** na temat możliwych zagrożeń i ryzyka związanego z korzystaniem z Internetu i nowoczesnych narzędzi cyfrowych.

Profilaktyka

- Upowszechnianie wśród dzieci i młodzieży wiedzy o bezpieczeństwie.
- Kształtowani właściwych postaw wobec zagrożeń.
- Aktywna profilaktyka powinna być prowadzona wobec i z udziałem wszystkich członków społeczności szkolnej - uczniów i ich rodziców oraz nauczycieli i innych pracowników placówki.

Netykieta – zasady dobrego zachowania w Internecie

- Nie flejmuj, czyli: nie obrażaj drugich.
- Nie staraj się na siłę zostać "pępkiem świata".
- Nie wysyłaj łańcuszków szczęścia i SPAM-u.
- Pamiętaj, że znajomi mają prawo do prywatności.
- Pamiętaj, że każdy może Cię znaleźć. Policja i mama również.
- Przestrzegaj prawa - adresy IP mogą być śledzone.
- Swoje opinie wyrażaj kulturalnie. Szanuj poglądy drugich.
- Sprawdzaj pisownię i podawaj źródła swoich informacji.
- Zwracaj uwagę prywatnie (nie w otwartym profilu przyjaciela!).

Przykłady zagrożeń

- Niebezpieczne treści.
- Hejt i fake news.
- Uzależnienie od Internetu.
- Phishing i spearphishing.
- Niebezpieczne kontakty w Sieci.
- Cyberprzemoc.

Niebezpieczne treści

- Takie, które mogą stanowić zagrożenie dla rozwoju dzieci. To nie tylko **pornografia** – to również treści **brutalne**, **obrzydliwe** czy promujące **niebezpieczne dla zdrowia zachowania**.

Hejt

- **Czyli mowa nienawiści** - to nieprzyjemne, obraźliwe wpisy pod filmami, zdjęciami czy postami.

- Co trzeci nastolatek spotkał się z mową nienawiści, a prawie 9% doświadczyło jej osobiście - wynika z badań **EU Kids online 2018**, prowadzonych pod kierownictwem prof. UAM Jacka Pyżalskiego w partnerstwie z Fundacją Orange. Mowa nienawiści i agresja stały się poważnym problemem.

Fake newsy

Fake newsy to nieprawdziwe informacje, które mogą mieć poważne konsekwencje i stają się plagą, a jej ofiarami padają zarówno dzieci, jak i dorośli.

Uzależnienie - podtypy

- **Uzależnienie od sieci** - przymus ciągłego śledzenia tego, co się dzieje w sieci.
- **Przeciążenie informacyjne** - gorączkowe przerzucanie informacji, udział w kilku listach dialogowych jednocześnie.
- **Uzależnienie od komputera** - przymus spędzania czasu z komputerem, nie ważne co się robi, ale komputer musi być włączony.
- **Erotomania internetowa** - nałogowe poszukiwanie materiałów pornograficznych i rozmowy o tematyce seksualnej w specjalnych chat-roomach).
- **Socjomania internetowa** - uzależnienie od kontaktów z ludźmi przez Internet z równoczesnym zanikiem kontaktów bezpośrednich.

Phishing i spearphishing

- Sytuacje, w której oszuści (hakerzy) wzbudzają nasze zaufanie po to, aby wyłudzić dane (np. hasło i login do facebooka) lub pieniądze, przesyłając maile czy sms-y.

- W **spearphishingu** hakerzy wysyłają informacje dostosowane do zainteresowań adresata.

Niebezpieczne kontakty w Sieci

- Uwodzenie dziecka (grooming).
- Wyłudzanie od dziecka materiałów z jego udziałem o charakterze seksualnym i erotycznym.
- Angażowanie w rozmowy o seksie.
- Wyłudzenie danych osobowych lub innych informacji w celach popełnienia przestępstwa przeciwko dziecku, rodzinie lub innym osobom.
- Nakłanianie dziecka do podejmowania zachowań zagrażających jego zdrowiu, a nawet życiu (np. zażywanie narkotyków, namawianie do samookaleczeń).

Cyberprzemoc

W przypadku dzieci i młodzieży **cyberprzemoc** to najczęściej przemoc rówieśnicza przy użyciu internetu i telefonów komórkowych. Jest to jedno z poważniejszych i bardziej powszechnych zagrożeń, z jakimi mogą mieć kontakt młodzi ludzie.

Formy cyberprzemocy

- Publikowanie ośmieszających filmów lub zdjęć.
- Publikowanie wulgarnych, prześmiewczych lub pełnych nienawiści i agresji komentarzy i wpisów.
- Włamania na konta serwisów społecznościowych.
- Nękanie telefonami i SMS-ami.
- Podszywanie się pod inne osoby.
- Wykluczanie ze społeczności internetowych.

Gdzie kryje się niebezpieczeństwo?

- Gry komputerowe.
- Czaty i komunikatory internetowe.
- Portale społecznościowe.

Jaką pomoc powinna zaoferować szkoła gdy dziecko stało się ofiarą przemocy

- **Poinformowanie rodziców** dziecka o problemie i okazanie im wsparcia i pomocy ze strony szkoły. W rozmowie z nimi pedagog lub wychowawca przedstawiają kroki, jakie zostały podjęte w celu wyjaśnienia zajścia oraz zapewnienia bezpieczeństwa poszkodowanemu uczniowi, a także, jeśli to wskazane, proponuje rodzicom i dziecku pomoc specjalisty (psychologa, pedagoga).

- **Wsparcie psychologiczne** (poradę, jak ma się zachować, aby zapewnić sobie poczucie bezpieczeństwa i nie doprowadzić do eskalacji prześladowania).
- Po zakończeniu interwencji należy **monitorować** sytuację ucznia sprawdzając, czy nie są wobec niego podejmowane dalsze działania przemocowe bądź odwetowe ze strony sprawcy.

Procedury bezpieczeństwa cyfrowego w szkołach

- Ministerstwo Edukacji Narodowej opublikowało zbiór rekomendacji i zaleceń dotyczących bezpieczeństwa w szkołach, którym istotną częścią są rekomendacje odnośnie procedur reagowania w przypadku zagrożenia bezpieczeństwa cyfrowego oraz procedury reagowania w szkole w przypadku wystąpienia incydentu zagrożenia.

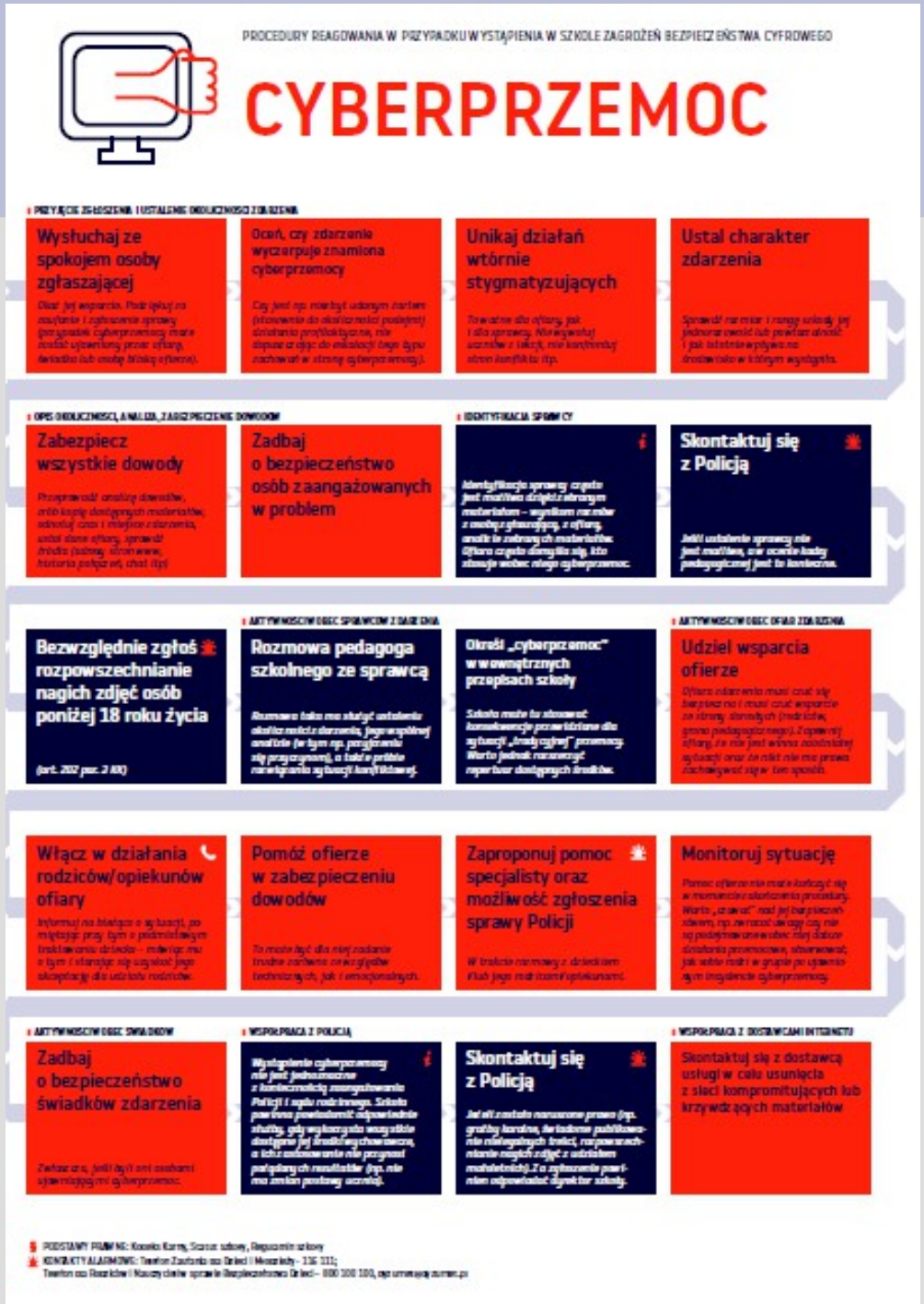
- Procedury_bezpieczenstwa_cyfrowego_w_szkole_rekomendacje

Procedury reagowania w przypadku wystąpienia w szkole zagrożeń bezpieczeństwa cyfrowego - infografiki

Źródło: Cyfrowobezpieczni.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>.

Przemoc, pornografia, sekty, popularyzacja faszyzmu, nawoływanie do samokaleczeń, werbunek do organizacji terrorystycznych, promowanie korzystania z narkotyków.

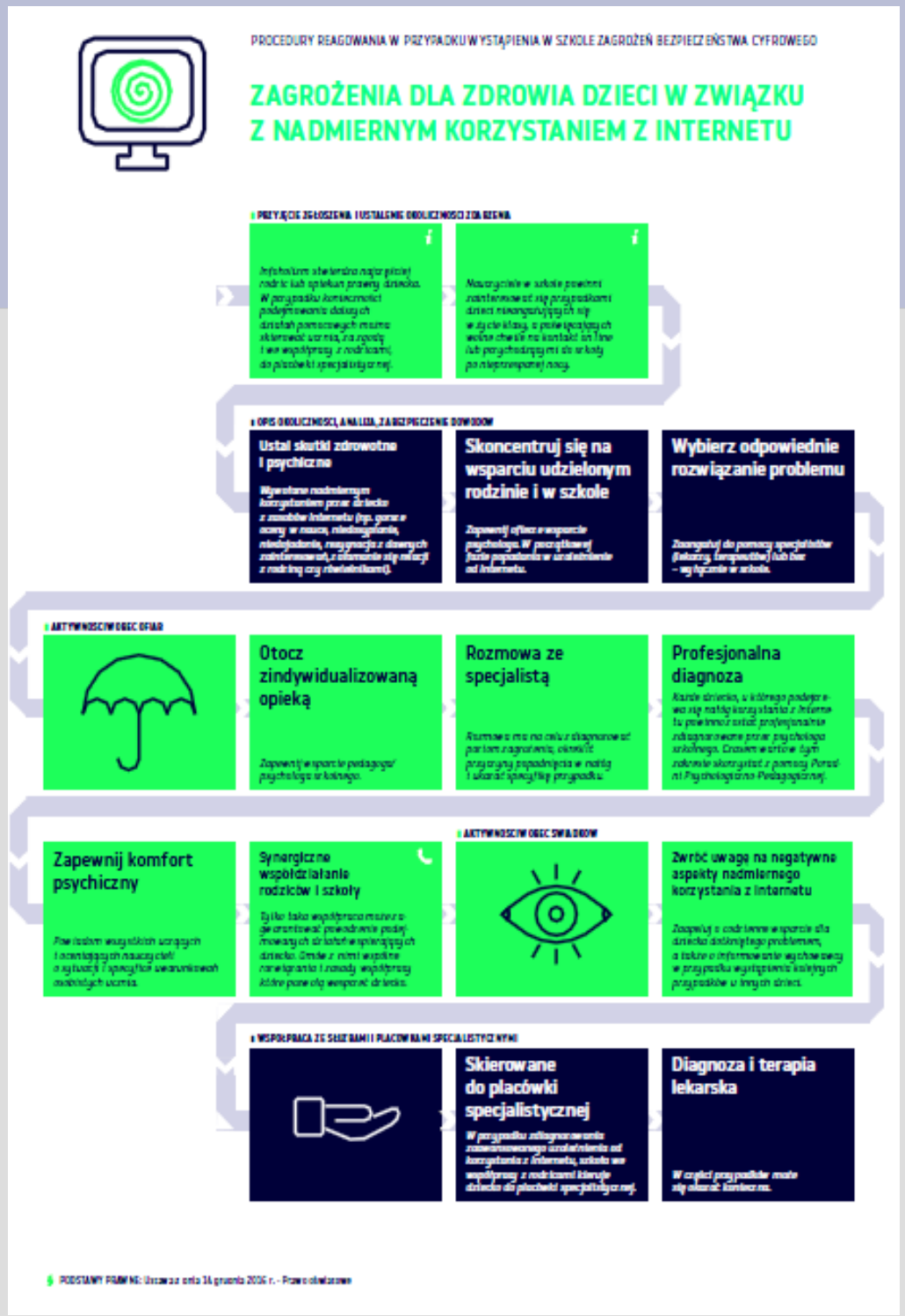
Nękanie, straszenie, szantażowanie z użyciem sieci, publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem sieci oraz podszywanie się w sieci pod kogoś wbrew jego woli.



Dotyczące nieodpowiedniego lub niezgodnego z prawem wykorzystania danych osobowych lub wizerunku dziecka i pracownika szkoły (przestępstwo).

Infoholizm (siecioholizm)

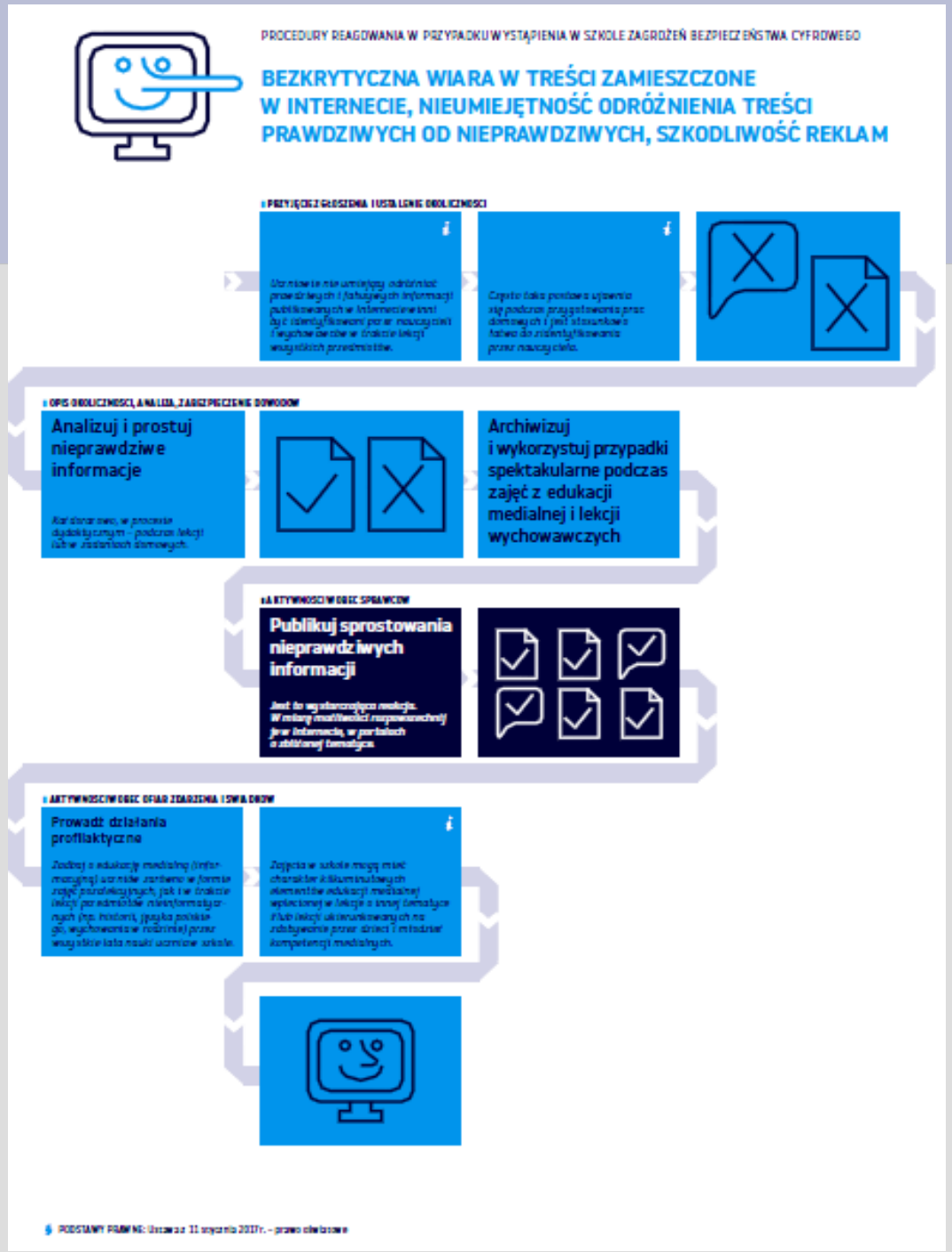
– nadmierne, obejmujące niekiedy niemal całą dobę korzystanie z zasobów Internetu i gier komputerowych (najczęściej sieciowych) i portali społecznościowych przez dzieci.



Zagrożenie obejmuje kontakty osób dorosłych z małoletnimi w celu zainicjowania znajomości prowadzących do wyłudzenia poufnych informacji, nawiązania kontaktów seksualnych, skłonienia dziecka do zachowań niebezpiecznych dla jego zdrowia i życia lub wyłudzenia własności (np. danych, pieniędzy, cennych przedmiotów rodzinnych).

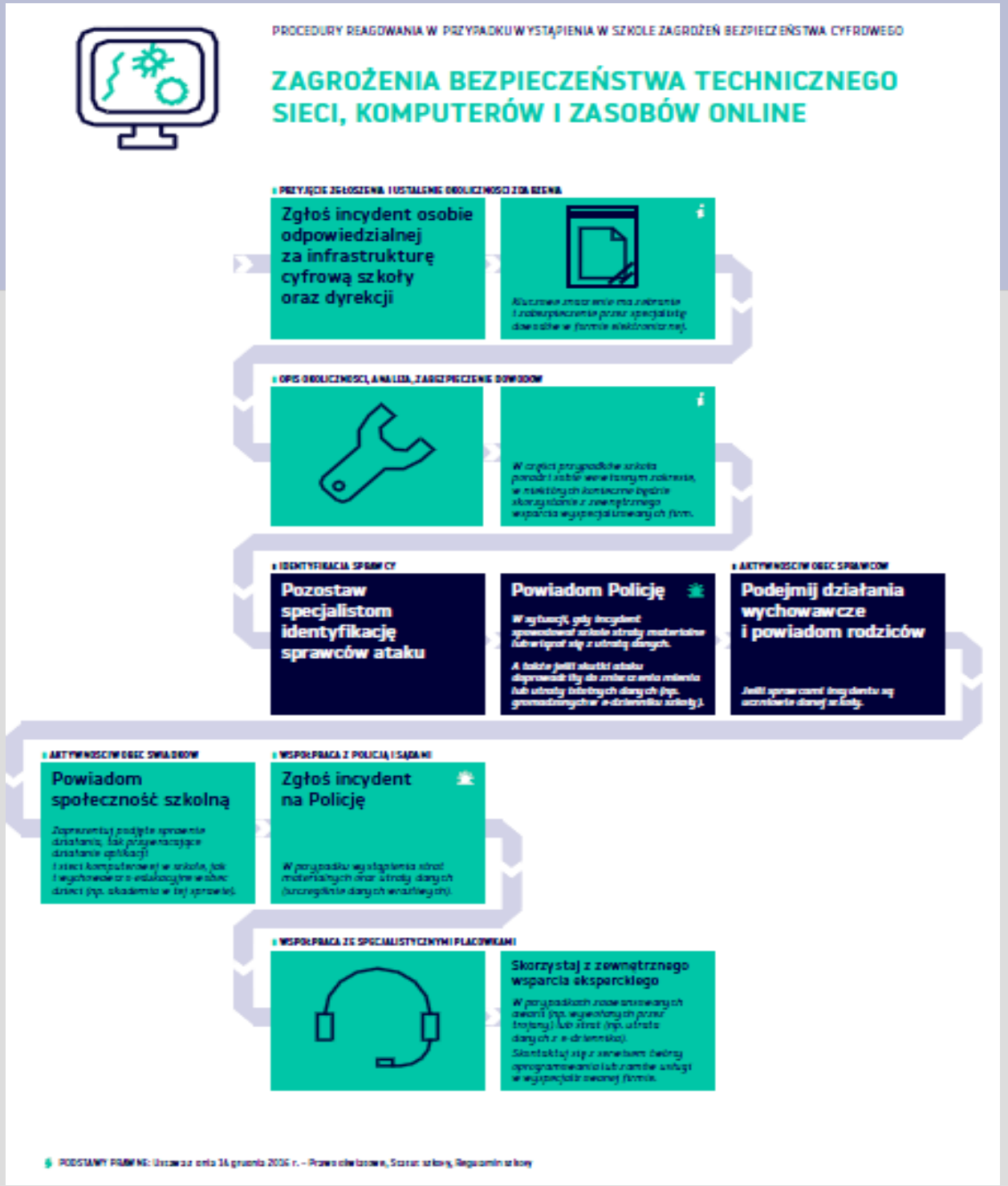
Prowokacyjne zachowania i aktywność seksualna jako źródło dochodu osób nieletnich - przesyłanie drogą elektroniczną lub publikowanie w portalach (społecznościowych) prywatnych treści, głównie zdjęć, o kontekście seksualnym, erotycznym i intymnym.

Nieumiejętność odróżnienia treści prawdziwych od nieprawdziwych, bezkrytyczne uznawanie za prawdę tez publikowanych w forach internetowych, kierowanie się informacjami zawartymi w reklamach.



Ryzyko poniesienia odpowiedzialności cywilnej lub karnej z tytułu naruszenia prawa autorskiego albo negatywnych skutków pochopnego spełnienia nieuzasadnionych roszczeń (tzw. copyright trolling).

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online.



Warto odwiedzić:

- **Dziecko w Sieci** - kampania „Chroń dziecko w Sieci” przestrzeganie przed konsekwencjami kontaktów dzieci w wieku przedszkolnym i wczesnoszkolnym ze szkodliwymi treściami w Internecie.

- **NASK** – państwowy instytut badawczy nadzorowany rzez Ministerstwo Cyfryzacji, prowadzi działalność związaną z bezpieczeństwem Internetu.

- **Saferinternet** – działania na rzecz bezpieczeństwa dzieci i młodzieży korzystających z Internetu i nowych technologii.

- **Fundacja Dajemy Dzieciom Siłę** - pomoc dla dzieci, które doświadczyły przemocy.

- **Dyżurnet.pl-** zgłaszanie nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

- **Telefon zaufania dla dzieci i młodzieży**

- **Telefon dla rodziców i nauczycieli**

- **Fundacja Orange** - działa na rzecz nowoczesnej edukacji.

- **Sieciaki** - portal edukacyjny
- **Necio.pl** - portal edukacyjny

Bibliografia:

- 116111.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://116111.pl/mlodziez>.
- Bezpiecznaszkola.men.gov.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://bezpiecznaszkola.men.gov.pl/bezpieczna-szkola-zagrozenia-i-zalecane-dzialania-profilaktyczne-w-zakresie-bezpieczenstwa-fizycznego-i-cyfrowego-uczniow/>.
- *Bezpieczna szkoła: zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów*, MEN, Warszawa 2017.
- Cyfrowobezpieczni.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: https://www.cyfrowobezpieczni.pl/procedury-bezpieczenstwa-cyfrowego-w-szkolach>.
- Dyzurnet.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://dyzurnet.pl/>.
- Fdds.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: https://fdds.pl/o-nas/>.
- Fundacja.orange.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://fundacja.orange.pl/>.
- Nask.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: <https://www.nask.pl/pl/dzialalnosc/projekty/safer-internet/3427,Safer-Internet.html>.
- *Rodzice Nastolatków 3.0: raport z ogólnopolskiego badania społecznego*, pod red. R. Lange, NASK, Warszawa 2019.
- Saferinternet.pl [online], [dostęp: 17 stycznia 2020]. Dostępny w Internecie: https://www.saferinternet.pl/>.
- *Standard bezpieczeństwa online placówek oświatowych,* pod red. J. Lizut, Fundacja Odkrywców Innowacji, Warszawa 2015.