dyżurnet.pl
NASK

Szantaż na tle seksualnym

wobec małoletnich w cyberprzestrzeni

NASK

Szantaż na tle seksualnym wobec małoletnich w cyberprzestrzeni

AUTORZY
Michał Marańda

REDAKCJA JĘZYKOWA
Marta Danowska-Kisiel, Tomasz Kulas, Michał Dąbrowski

OPRAWA GRAFICZNA
Agnieszka Makowska

Seria: internet – edukacja – bezpieczeństwo

Stan prawny na czerwiec 2025 r.

ISSN 2300-0074

---

dyżurnet.pl NASK saferinternet.pl Dofinansowane przez Unię Europejską

NASK PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Warszawa 2025

Spis treści

Szanowni Państwo,

jedne z najtrudniejszych zgłoszeń, jakie nadsyłane są do Dyżurnet.pl, dotyczą bezpośredniego zagrożenia poczucia bezpieczeństwa i są związane z szantażem na tle seksualnym. Szczególnie w przypadku osób małoletnich są to doświadczenia, które mogą zaważyć na całym ich przyszłym życiu.

Proces takiego szantażu przebiega z reguły dość szybko i bazuje na manipulacji dokonywanej przez sprawcę. Poszkodowanymi są nastolatki, ale też młodsze dzieci, które nie są świadome konsekwencji pewnych działań i łatwo podejmują rozmowę z nieznajomymi. Sprawca, po uzyskaniu intymnych materiałów, stawia osobę małoletnią w sytuacji, która jest ponad jej siły: grozi upublicznieniem zdjęć lub filmów, zmusza do przekazywania kolejnych intymnych materiałów albo przesyłania pieniędzy, których suma nigdy nie będzie dla sprawcy wystarczająca. Osoby pokrzywdzone często same przesyłają materiały intymne, kierując się fałszywym poczuciem bezpieczeństwa i zaufania do sprawcy – to właśnie ten mechanizm bywa wykorzystywany do późniejszego szantażu. Poczucie osamotnienia oraz wstyd dodatkowo utrudniają młodym poszkodowanym zwrócenie się o pomoc.

Co zrobić, by ograniczyć negatywne konsekwencje wynikające z szantażu na tle seksualnym? Jak przeciwdziałać temu zagrożeniu? Przede wszystkim musimy wiedzieć więcej i mieć świadomość

niebezpieczeństw, jakie wiążą się z podejmowaniem intymnych kontaktów w cyberprzestrzeni. Dotyczy to zarówno dzieci, młodzieży, ich bliskich i opiekunów, jak i profesjonalistów, którzy zajmują się bezpieczeństwem.

Dlatego w tej publikacji przedstawiamy nie tylko perspektywę międzynarodowych organizacji, prezentując wyniki przeprowadzonych przez nie badań, ale również analizujemy poziom omawianych zagrożeń w Polsce. Przywołujemy wyniki krajowych badań, które dotykały poruszonej w tym raporcie problematyki, jak i analizujemy zgłoszenia szantażu wobec małoletnich, które otrzymał w ostatnich latach Dyżurnet.pl.

Szantaż na tle seksualnym jest przestępstwem, dlatego zgłoszenie każdego takiego działania to kwestia absolutnie podstawowa. Równocześnie musimy też w każdy dostępny sposób minimalizować skutki tego typu przestępstw, jakie dotyczą osób pokrzywdzonych – w tym konsekwencje upublicznienia materiałów intymnych bez ich zgody. Tylko skoordynowane działania – obejmujące opiekunów, edukatorów, służby odpowiedzialne za egzekwowanie prawa oraz administratorów serwisów – mogą realnie powstrzymać dalsze krzywdzenie osob poszkodowanych i ograniczyć skalę rozprzestrzeniania się niechcianych treści.

Zapraszamy do lektury!
Zespół Dyżurnet.pl

Wstęp

Środowisko internetu od jego początków podlega nieustannej ewolucji pod względem zarówno kulturowym, jak i technologicznym. Sieć oferuje wiele możliwości i szans, jednocześnie narażając jej użytkowników na różnego rodzaju ryzyka i zagrożenia. Część z nich może być nowa, gdyż wiąże się z nową formą wymiany informacji w cyberprzestrzeni (np. Virtual Reality[1]). Część natomiast może być odmianą lub kumulacją znanych już wcześniej niebezpieczeństw. Największą ochroną powinni zostać objęci użytkownicy najmłodsi, którzy są narażeni na wszystkie zagrożenia, które dotyczą również dorosłych użytkowników, ale w ich przypadku trudniejsze jest wykrycie przestępstwa oraz ograniczenie jego skutków.

Jednym ze stosunkowo nowych, specyficznych dla cyfrowego środowiska zjawisk jest szantaż na tle seksualnym. Polega ono na nawiązaniu przez sprawcę kontaktu z wybranym użytkownikiem i skłonieniu go (często poprzez manipulację) do przekazania swoich intymnych treści lub uczestnictwa na żywo w wideotransmisji o seksualnym charakterze, która może zostać nagrana. Następnie sprawca grozi upublicznieniem pozyskanych materiałów, żądając albo przesłania nowych treści, albo przekazania środków finansowych. Jak pokazują badania i analizy, szantaż na tle seksualnym to wzrastające zagrożenie również wśród najmłodszych użytkowników.

1. Obraz sztucznej rzeczywistości stworzony przy wykorzystaniu technologii informatycznej. Polega na multimedialnym kreowaniu komputerowej wizji przedmiotów, przestrzeni i zdarzeń. Może on reprezentować zarówno elementy świata realnego (symulacje komputerowe), jak i zupełnie fikcyjnego (gry komputerowe science-fiction).

Zjawisko to może wiązać się z innymi wcześniej opisywanymi w literaturze zagrożeniami, takimi jak:

- uwodzenie osoby małoletniej (ang. *child grooming*),
- utrwalenie treści przedstawiającej seksualne wykorzystanie osoby małoletniej (ang. *Child Sexual Abuse Materials*, dalej: CSAM)[2],
- seksting, czyli udostępnianie stworzonych przez siebie materiałów o charakterze seksualnym[3],
- groźby, zastraszanie ze strony sprawcy,
- w przypadku spełnienia żądań sprawcy: przekazanie kolejnych treści CSAM lub korzyści materialnych,
- w przypadku ujawnienia treści CSAM przez sprawcę: wszelkie negatywne konsekwencje dla osoby poszkodowanej związane z upublicznieniem materiałów[4].

Powyższe zjawiska, jak pokazują np. sprawy zgłaszane do Dyżurnet.pl i analizowane przez zespół, przenikają się ze sobą i współwystępują. Pojawiły się nowe aspekty: chęć zdobycia korzyści materialnych, chęć zdobycia nowych materiałów przedstawiających seksualne wykorzystywanie dziecka, ale również groźby upublicznienia dotychczasowych materiałów – zdjęć, filmów i rozmów. Celem ataku sprawców stały się dzieci. Nieprzypadkowo – są łatwiejszym celem manipulacji.

2. Profesjonaliści zajmujący się zagadnieniem wykorzystywania seksualnego dzieci od dawna postulują zaprzestanie używania terminu „pornografia dziecięca" i jakiegokolwiek użycia terminu „pornografia" w kontekście dowodu przestępstwa, jakim jest zdjęcie lub wideo prezentujące seksualne wykorzystanie osoby małoletniej. Pornografia dotyczy treści przedstawiających seksualne zachowania osób dorosłych, w przypadku dzieci zachowania seksualne wobec nich są penalizowane praktycznie na całym świecie.
3. Termin pochodzący od połączenia słów *sex* oraz *texting* powstały w momencie upowszechnienia się komunikacji SMS. Obecnie nie jest ograniczony do wzajemnego przekazywania wiadomości tekstowych, ale również zdjęć czy treści wideo.
4. Więcej na ten temat w *Canadian Centre for Child Protection, Survivors' survey*, 2017. Również: A. Malec, *Skutki wykorzystania seksualnego dziecka*, 2006. https://dzieckokrzywdzone.fdds.pl/index.php/DK/article/download/240/170 (dostęp: 15.06.2023).

Jeden z pierwszych raportów na temat tego zjawiska opracowany został w roku 2016 przez amerykański *National Center for* Missing & *Exploited Children* (dalej: NCMEC)[5]. Pięciostronicowa publikacja *Trends identified in CyberTipline sextortion reports* bazowała na analizie zgłoszeń dotyczących szantażu seksualnego, przesłanych do działającego w ramach NCMEC zespołu CyberTipline od października 2013 roku. W raporcie została zdefiniowana istota zjawiska, scharakteryzowana motywacja oraz modus operandi sprawców szantażu na tle seksualnym. Autorzy podali również statystyki dotyczące wieku oraz podziału płciowego poszkodowanych dzieci. W publikacji przeanalizowane zostały też koszty emocjonalne, które ponoszą najmłodsi.

Do tej pory najpełniej omawianą problematykę ujęto w roku 2017 w raporcie *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*. Publikacja opracowana została przez działające w ramach Europejskiego Urzędu Policji (dalej: Europol)[6], Europejskie Centrum ds. Walki z Cyberprzestępczością (*EC3 European Cybercrime Centre*). Jednostka ta koordynuje transgraniczne działania organów ścigania przeciwko cyberprzestępczości oraz stanowi platformę ekspercką w tym zakresie.

W tym samym roku Europol zainaugurował kampanię prewencyjną „Say NO!" skierowaną do młodych użytkowników internetu. W jej ramach zrealizowano kilkuminutowy film przetłumaczony na wszystkie europejskie języki, opracowano broszury w formie krótkich obrazkowych opowieści oraz stworzono stronę z opisem zjawiska i radami, dotyczącymi tego, jak nie stać się jego ofiarą oraz sposobów radzenia sobie w sytuacji szantażu[7].

5. NCMEC to prywatna organizacja non-profit założona w 1984 roku przez Kongres Stanów Zjednoczonych. Jej celem jest poszukiwanie zaginionych dzieci oraz zapobieganie i zwalczanie ich wykorzystywania, również seksualnego. NCMEC prowadzi CyberTipline – zespół reagujący na zgłoszenia dotyczące różnych form seksualnego wykorzystywania dzieci w cyberprzestrzeni.
6. Europejski Urząd Policji (Europol) to Agencja Unii Europejskiej ds. Współpracy Organów Ścigania z siedzibą w Hadze.
7. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime (dostęp: 15.06.2023). Inicjatorką kampanii była podinsp. Katarzyna Staciwa, delegowana do pełnienia służby w EC3 w latach 2006–2018.

Według danych NCMEC[8], pierwsze zgłoszenia dotyczące szantażu na tle seksualnym odnotowano w roku 2013 i od tamtego czasu ich liczba nieustannie rośnie. Między rokiem 2019 a 2021 liczba zgłoszeń dotyczących szantażu na tle seksualnym zwiększyła się ponad dwukrotnie.

Globalna skala zjawiska jest dość trudna do oszacowania. NCMEC podaje liczbę ponad 260 tysięcy raportów dotyczących uwodzenia małoletnich poprzez internet, otrzymanych w latach 2016-2022, w czym zawiera się niesprecyzowana liczba zgłoszeń dotyczących wyłącznie szantażu na tle seksualnym[9].

Aktualne dane zamieszczone zostały w podrozdziale „Raporty NCMEC i Cybertip.ca".

8. *Trends identified in CyberTipline sextortion reports,* NCMEC 2016, s.1.
9. https://www.missingkids.org/netsmartz/topics/sextortion (dostęp: 15.06.2023).

Charakterystyka zjawiska szantażu na tle seksualnym w cyberprzestrzeni

Definicja i terminologia

Szantaż na tle seksualnym w cyberprzestrzeni jest rodzajem przestępstwa, w którym sprawca pozyskuje od innego użytkownika treści o charakterze seksualnym (za jego zgodą lub bez jego wiedzy i zgody), a następnie grozi ich ujawnieniem lub rozpowszechnieniem w celu wywarcia na nim presji lub uzyskania korzyści. Najczęściej szantażysta żąda od osoby poszkodowanej albo korzyści seksualnych (przekazania nowych treści lub bezpośredniego spotkania), albo korzyści finansowych. Zdarza się, że sprawca, ujawniając intymne treści poszkodowanej osoby, działa w celu dokonania na niej zemsty lub chce zbudować własną popularność. Są to jednak rzadsze przypadki.

Zjawisko bazuje na czterech kluczowych elementach (za Europol)[10]:

- **Treści** – wszelkie materiały (informacje, zdjęcia lub filmy), które osoba poszkodowana chce traktować jako intymne/prywatne.

10. *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*, Europol-EC3 2017, s.12.

- **Zagrożenie** – to, czemu osoba poszkodowana chciałaby zapobiec. W większości przypadków chodzi o ujawnienie intymnych materiałów.

- **Wartość** – to, czego sprawca żąda od osoby poszkodowanej.

- **Środowisko online** – powyższe trzy elementy występują razem w internetowej komunikacji.

W przypadku zjawiska szantażu na tle seksualnym nakierowanego na małoletnich ważna jest terminologia, mająca bezpośredni wpływ na interpretację sytuacji oraz odzwierciedlająca intencje regulatorów, badaczy i ekspertów. Niestaranne używanie języka i terminologii może prowadzić do powstawania niespójnych aktów prawnych i tym samym utrudniać skuteczne zapobieganie i reagowanie na przestępstwa skierowane przeciwko małoletnim[11].

Popularnym określeniem tego zjawiska, zapożyczonym z języka angielskiego, jest *sextortion*, powstałe z połączenia wyrazów *sex* (seks – aktywność płciowa między ludźmi) oraz *extortion* (wymuszenie)[12], używane zwłaszcza w Stanach Zjednoczonych. Termin ten jednak jest nieprecyzyjny, np. w roku 2008 użyty był przez Międzynarodowe Stowarzyszenie Kobiet-Sędziów jako określenie formy korupcji obejmującej wykorzystanie seksualne[13].

Europejscy eksperci (zarówno z Europolu, jak i Międzyagencyjnej Grupy Roboczej powołanej przez ECPAT w Luksemburgu) zwracają uwagę na fakt, że sformułowanie *sextortion* nie oddaje istoty problemu. Prócz tego, że Odnosi się do różnego typu zjawisk, a także nie oddaje w pełni perspektywy osoby poszkodowanej. Określenie to nie wskazuje, że czyn stanowi formę seksualnego wykorzystania i wiąże się z poważnymi konsekwencjami dla osoby poszkodowanej.

11. *Wytyczne dotyczące terminologii w dziedzinie ochrony dzieci przed wyzyskiwaniem seksualnym i wykorzystywaniem seksualnym*, ECPAT International/ ECPAT Luxembourg 2016, s. 13.
12. https://dictionary.cambridge.org (dostęp: 15.06.2023).
13. https://en.wikipedia.org/wiki/Sextortion (dostęp: 15.06.2023).

Według *Wytycznych dotyczących terminologii w dziedzinie ochrony dzieci przed wyzyskiwaniem seksualnym i wykorzystywaniem seksualnym*[14], sformułowanie *sextortion* nie wskazuje jednoznacznie, że chodzi o wyzyskiwanie seksualne dzieci i grozi trywializowaniem zjawiska. Autorzy zalecają, aby używać terminu *szantaż seksualny wobec dzieci*, który poprawnie opisuje rodzaj wymuszania (szantażu), podkreśla, że ma on charakter seksualny oraz że jest stosowany wobec dzieci.

Eksperci Europolu proponują inny niż *sextortion* termin, tzn. *online sexual coertion and extortion*, co można tłumaczyć jako „zjawisko seksualnego zmuszania i wymuszenia online", co również oddaje istotę przestępstwa.

Zgodnie z powyższymi wytycznymi, w języku polskim powinien być stosowany termin *szantaż na tle seksualnym wobec małoletnich w cyberprzestrzeni*. Termin ten najbardziej kompleksowo opisuje zjawisko, ponieważ:

1. Określenie „małoletni" obejmuje pełne spektrum osób do 18 roku życia, w tym poszczególne grupy, których rozumienie w codziennym języku może być odmienne, tzn. dzieci, nastolatki, młodzież.

2. Określenie „na tle seksualnym" ma na celu ukazanie, że treść seksualna pozyskana od poszkodowanego jest tłem szantażu. Sprawcy mogą dążyć do uzyskania korzyści o charakterze seksualnym, ale duża ich część zainteresowana jest wyłącznie korzyściami materialnymi.

3. „Cyberprzestrzeń" precyzuje miejsce zdarzenia stanowiące o wyjątkowości zjawiska. Ta publikacja poświęcona jest wyłącznie aktywnościom mającym miejsce w cyberprzestrzeni. Szantaż dokonywany poza tym środowiskiem może być tematem na oddzielną analizę.

14. Dokument opracowany przez Międzyagencyjną Grupę Roboczą powołaną przez ECPAT w Luksemburgu w 2016 r.

Miejsce występowania

Szantaż na tle seksualnym odbywa się najczęściej poprzez komunikatory w **serwisach społecznościowych** oraz **platformy umożliwiające rozmowy wideo**. Często to sprawca pierwszy kontaktuje się poprzez media społecznościowe, proponując następnie przejście na prywatne kanały w serwisach wideo lub wideokomunikatory.

Jeśli w danym kraju popularne są lokalne platformy internetowe, grupa sprawców i poszkodowanych ogranicza się głównie do ich użytkowników. W przypadku dokonania przestępstwa, miejscowe organy ściągania mogą we współpracy z administratorami względnie szybko próbować ustalić dane potencjalnego sprawcy.

W przypadku platform komunikacyjnych o globalnym zasięgu i międzynarodowej popularności liczba użytkowników będących potencjalnymi sprawcami i poszkodowanymi zdecydowanie rośnie. Stanowi to wyzwanie dla organów ścigania z różnych krajów.

Profil sprawcy

Sprawcą szantażu na tle seksualnym może być osoba znana dziecku ze świata realnego lub poznana podczas aktywności online. Motywacją jest tutaj chęć pozyskania materiałów intymnych, które sprawca zachowuje dla siebie lub wymienia z innymi.

Drugim typem sprawcy jest nieznajomy, należący do wyspecjalizowanej grupy przestępczej. Kierująca nim motywacja związana jest przede wszystkim z chęcią zdobycia środków finansowych, rzadziej są to same materiały seksualne i, co warto podkreślić, nie jest to motywacja osobista. Specjalizacja grupy przestępczej pozwala na wypracowanie technik manipulacyjnych oraz zminimalizowanie zaangażowania przy jednoczesnym zmaksymalizowaniu zysków. Grupy przestępcze pochodzą głównie z krajów Afryki Zachodniej (takich jak Nigeria i Wybrzeże Kości Słoniowej) lub krajów Azji Południowo-Wschodniej (takich jak Filipiny).

Europol rozróżnia dwa typy motywacji sprawców, możliwa jest też kombinacja obu grup[15].

Profil sprawców szantażu na tle seksualnym według Europolu

Motywacja seksualna	Motywacja finansowa
• Przeważnie mężczyzna • Działa samodzielnie, ale udostępnia lub wymienia pozyskane treści • Może działać zarówno na poziomie krajowym, jak i globalnym • Zna języki obce, co sprzyja podejmowaniu aktywności • Obiera za cel ofiary płci żeńskiej • Może znać ofiarę osobiście • **Główny cel:** uzyskanie materiałów seksualnych i/lub seksualnych korzyści offline	• Kobieta lub mężczyzna • Członek grupy przestępczej • Działa w zespołach zlokalizowanych w krajach rozwijających się (Filipiny, Wybrzeże Kości Słoniowej, Maroko) • Może działać zarówno na poziomie krajowym, jak i globalnym • Obiera za cel ofiary płci męskiej w krajach powiązanych językowo • Nie zna osobiście ofiary • **Główny cel:** zdobycie pieniędzy

Z badań NCMEC[16] wynika, że sprawcom szantażu wobec małoletnich chodziło głównie o pozyskanie kolejnych materiałów o charakterze seksualnym. Sprawcy oczekiwali przekazywania coraz większej liczby zdjęć lub filmów, w których osoba szantażowana będzie prezentowała coraz szersze spektrum seksualnych zachowań. **Zdarzała się eskalacja żądań polegająca na zmuszaniu poszkodowanych do angażowania kolejnych osób, takich jak rodzeństwo czy rówieśnicy**. Szantażowi tego typu znacznie częściej poddawane były dziewczynki niż chłopcy.

15. Europol, EC3 European Cybercrime Centre. *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*., 2017, s. 16-17.

16. *Trends*..., dz. cyt., s. 4.

Sprawcy motywowani seksualnie wysuwali też żądania bezpośredniego spotkania. W takim przypadku sprawcy zazwyczaj podawali się za osobę znajomą, np. byłego partnera. Natomiast gdy szantażysta zachowywał anonimowość, żądanie takie stanowiło manipulację i miało przekonać rozmówcę, że przesłanie zdjęć lub filmów będzie „mniejszym złem" niż bezpośrednie spotkanie. Żądania bezpośredniego spotkania w celach seksualnych kierowane były zarówno do dziewczynek, jak i do chłopców.

Drugim najczęściej występującym motywem sprawców było uzyskanie korzyści materialnych. W tym wariancie żądali przesłania pieniędzy za pośrednictwem systemu przekazów pieniężnych lub płatności online. Próbowali również uzyskać dane karty kredytowej albo bezpośrednio, albo prosząc osobę poszkodowaną o zarejestrowanie się na określonej stronie internetowej wymagającej od niej wprowadzenia tych informacji. Zdarzało się też, że sprawcy domagali się innych płatności lub towarów, takich jak waluta obowiązująca w grach online, telefony komórkowe czy ubrania.

Ten rodzaj szantażu motywowanego finansowo dotyczył głównie chłopców.

Pod koniec 2023 r. Federalne Biuro Śledcze[17] ze Stanów Zjednoczonych zwróciło uwagę na zwiększającą się liczbę przypadków szantażu na tle seksualnym, gdzie sprawca motywowany był finansowo[18].

Sprawcy pochodzili głównie z krajów Afryki Zachodniej lub krajów Azji Południowo-Wschodniej, a ich żądania dotyczyły przekazania przelewów finansowych, kart podarunkowych, a nawet kryptowalut.

17. Federalne Biuro Śledcze (ang. Federal Bureau of Investigation, FBI) – amerykańska agencja rządowa zajmująca się przestępstwami wykraczającymi poza granice danego stanu. Jest jedną ze służb specjalnych pilnujących bezpieczeństwa Stanów Zjednoczonych.

18. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion/financially-motivated-sextortion (dostęp 19.01.2024).

Profil osoby poszkodowanej

Szantażowi na tle seksualnym poddany może być każdy użytkownik cyberprzestrzeni, który wchodzi w kontakt z innym użytkownikiem. Poszkodowana osoba może znać rozmówcę osobiście, ale może zostać również wprowadzona w błąd, poddana perswazji lub zmuszona do przesłania materiałów o seksualnym charakterze. Dzieci i nastolatki, z uwagi na małe doświadczenie życiowe oraz wiedzę ogólną o świecie, nie dysponują takimi zasobami jak osoby dorosłe, a przez to mogą być łatwym celem dla wykorzystujących manipulacyjno-zastraszające techniki sprawców.

Jak prezentuje się rozkład wiekowy oraz podział z uwagi na płeć osób poddanych szantażowi na tle seksualnym? Według danych NCMEC[19]:

- 78% zgłoszeń dotyczyło dziewczynek, a 15% dotyczyło chłopców (w 7% zgłoszeń płci dziecka nie udało się ustalić);
- Wiek dzieci wahał się w przedziale od 8 do 17 lat ze średnią wieku 15 lat; jednak wiek dziewczynek częściej znajdował się na początku tej skali;
- Dziewczynki były szantażowane częściej w celu pozyskania od nich treści o charakterze seksualnym (84%) w porównaniu z chłopcami (53%);
- Chłopcy częściej szantażowani byli w celu pozyskania korzyści materialnych (32%) w porównaniu z dziewczynkami (2%).

Fazy szantażu na tle seksualnym wobec małoletnich

Proces szantażu na tle seksualnym, według dotychczasowych opracowań, może mieć następujący przebieg:

19. *Trends*..., dz. cyt., s. 1 i 4.

Faza przygotowawcza

Sprawcy wyszukują małoletnich rozmówców za pośrednictwem mediów społecznościowych, gier online, platform wideo (również z transmisjami na żywo) oraz aplikacji do przesyłania wiadomości.

Sprawca zazwyczaj posługuje się fałszywą tożsamością. Na swoim internetowym profilu zamieszcza zdjęcia osoby potencjalnie atrakcyjnej dla wybranego rozmówcy.

Może się zaprzyjaźniać również ze znajomymi potencjalnej ofiary i wchodzić w jej środowisko. Może udawać dalszego znajomego. Może też włamać się na konta osób znanych przyszłemu poszkodowanemu lub tworzyć fałszywe konta sprawiające wrażenie, że należą do znajomego.

Może tworzyć wiele kont i tożsamości, które otaczają potencjalną ofiarę.

Faza uzyskania materiałów

Sprawca nawiązuje kontakt.

Sprawca prosi małoletniego o przejście na platformę umożliwiającą prowadzenie rozmów wideo. Prosi o przesyłanie zdjęć i filmów o charakterze seksualnym i/lub namawia do wykonania czynności seksualnych w trakcie wideorozmowy. W niektórych przypadkach obiecuje wymianę intymnych treści lub wysyła takie treści jako pierwszy, aby zachęcić do zrobienia tego samego. Zdarza się, że aby uwiarygodnić przekaz, sprawca pokazuje wcześniej pozyskane wideo o charakterze seksualnym, pisząc w tym samym momencie, co osoba utrwalona na wideo. Dzięki temu odbiorca ma złudzenie przekazu odbywającego się w czasie rzeczywistym.

Sprawca może w zamian za przekazanie materiałów intymnych oferować gratyfikację w postaci pieniędzy, narkotyków, przedmiotów w grach internetowych.

Sprawca utrwala przekaz wideo lub uzyskane zdjęcia.

Faza szantażu

Sprawca ujawnia swoje żądania: w zależności od motywacji oczekuje przekazania kolejnych materiałów o charakterze seksualnym albo środków finansowych (zdecydowana większość sprawców robi to jeszcze tego samego dnia, w którym przechwycili intymne treści). Grozi przesłaniem materiału do bliskich, opublikowaniem go w internecie, zrobieniem krzywdy bliskim osobom.

Zdarza się, że sprawca wymusza, aby ofiara werbowała kolejne ofiary i wyłudzała intymne materiały.

Niespełnienie żądań sprawcy może skutkować ujawnieniem nagranego materiału, a zwłaszcza przekazaniem go członkom rodziny i znajomym poszkodowanej osoby albo/oraz udostępnieniem w jednym z serwisów pornograficznych.

Zdarza się, że sprawcy w celu wywołania silniejszej reakcji tworzą i przesyłają wytworzone materiały takie jak:

- fałszywy nagłówek wiadomości o aresztowaniu poszkodowanego,
- kolaż zawierający utrwalone treści seksualne wraz z informacjami identyfikującymi osobę poszkodowaną,
- roboczą wersję postu w mediach społecznościowych zawierającego utrwalone treści.

Sprawcy żądają płatności w przeróżnych formach: karty podarunkowe lub kody z takich kart, płatności mobilne, przelewy bankowe, przekazy pieniężne, kryptowaluty.

Sprawcy mogą rozpowszechniać treści niezależnie od spełnienia żądań przez osobę poszkodowaną.

Zdarza się, że rozmówca nie zgodzi się na przekazanie intymnych treści. W takiej sytuacji sprawca może wygenerować treść o charakterze seksualnym zawierającym twarz i postać pokrzywdzonego, a materiału użyć do szantażu.

Rozwój narzędzi do tworzenia i edycji multimediów, a także rosnąca popularność zastosowań sztucznej inteligencji, pozwalają na wysunięcie przypuszczenia, że szantaż oparty na wygenerowanych materiałach (tzw. *deepfake*[20]) będzie stosowany przez sprawców coraz częściej.

Bardzo ważnym aspektem zjawiska jest stosowana przez sprawców manipulacja. Może ona mieć formę „miękką", dzięki której przyszła osoba poszkodowana nabiera zaufania do rozmówcy, lub wręcz przeciwnie – formę „twardą" wzbudzającą poczucie zagrożenia lub poczucie winy.

Techniki manipulacji używane wobec pokrzywdzonego przez sprawców motywowanych seksualnie (wg NCMEC)[21]:

- Odwzajemnienie („Pokażę ci, jeśli ty mi pokażesz");
- Budowanie więzi poprzez nawiązywanie relacji przyjaźni lub relacji romantycznej;
- Fizyczna groźba zranienia lub napaści seksualnej na dziecko lub członków jego rodziny;
- Używanie wielu fałszywych tożsamości internetowych do kontaktu;
- Udawanie kogoś młodszego i/lub przedstawiciela płci przeciwnej;
- Uzyskiwanie dostępu do internetowego konta bez autoryzacji i kradzież zdjęć lub filmów o charakterze seksualnym;

20. *Deepfake* (zbitka wyrazowa od ang. *deep learning* „głębokie uczenie" oraz *fake* „fałszywy") – technika obróbki obrazu, polegająca na łączeniu obrazów twarzy ludzkich przy użyciu technik sztucznej inteligencji.
21. *Trends*..., dz. cyt., s. 3.

- Grożenie tworzeniem seksualnych zdjęć lub filmów przedstawiających dziecko przy użyciu narzędzi do edycji cyfrowej (*deepfake*);

- Grożenie samobójstwem, jeśli dziecko nie dostarczy treści seksualnych;

- Tworzenie fałszywego profilu dziecka (np. w mediach społecznościowych) i grożenie opublikowaniem treści seksualnych dziecka;

- Początkowo oferowanie dziecku czegoś, na przykład pieniędzy lub narkotyków, w zamian za zdjęcia/filmy o charakterze jednoznacznie seksualnym;

- Przedstawienie się jako pracownik agencji modelingowej w celu uzyskania zdjęć o seksualnym charakterze.

Podczas gdy większość tych taktyk manipulacji była stosowana w równym stopniu wobec chłopców i dziewczynek, w wykorzystywaniu niektórych metod pojawiały się znaczne różnice. Mówiąc dokładniej, gdy ofiarami byli chłopcy, sprawcy znacznie częściej podawali się za młodszych i/lub kobiety, oferowali wzajemność seksualną poprzez udostępnianie zdjęć lub transmisje na żywo, nagrywali nieświadome dziecko, a następnie grozili, że opublikują obrazy/filmy wideo, aby rodzina i przyjaciele mogli je zobaczyć. Natomiast gdy poszkodowanymi były dziewczynki, sprawcy znacznie częściej oferowali dobra materialne w celu uzyskania treści o charakterze seksualnym.

Techniki manipulacji używane wobec pokrzywdzonego przez sprawców motywowanych finansowo (wg FBI)[22]:

- Sprawcy zazwyczaj tworzą fałszywe profile wyglądające, jakby należały do nastoletnich dziewcząt.

22. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion/financially-motivated-sextortion (dostęp 19.01.2024).

- Mogą dodać do znajomych lub obserwowanych osoby znane przyszłemu poszkodowanemu.

- Mogą włamać się na konta osób znanych przyszłemu poszkodowanemu lub tworzyć fałszywe konta sprawiające wrażenie, że należą do znajomego.

  Konta te zazwyczaj mają niewielu obserwujących/znajomych i wyglądają na niedawno założone, co winno wzbudzić podejrzenie rozmówcy.

  Kluczowym elementem szantażu jest pozyskanie przez sprawcę od rozmówcy treści intymnych. Może to odbywać się poprzez manipulację lub bez wiedzy rozmówcy. Zdarza się jednak, że sprawca dysponuje takimi treściami jeszcze przed nawiązaniem bezpośredniego kontaktu.

Zdjęcia i filmy o charakterze seksualnym z udziałem małoletnich mogą być:

- tworzone przez najmłodszych samodzielnie na prośbę innej osoby;

- utworzone samodzielnie i wysłane do kogoś, kto o to nie prosił;

- wykorzystywane do wymuszania kolejnych materiałów od małoletniego, który wytworzył je wcześniej;

- redystrybuowane przez odbiorcę do rówieśników lub zamieszczane w internecie, skąd mogą być pobierane przez innych użytkowników.

Udostępnianie materiałów intymnych w środowisku rówieśniczym to innego typu problem niż przedstawiony wcześniej schemat związany z szantażem na tle seksualnym. Młodzież może uważać wymianę takich zdjęć czy filmów za normalną, podczas gdy rówieśnicy, którzy potem takie materiały rozpowszechnią, mogą nie być świadomi konsekwencji prawnych udostępniania prywatnego wizerunku innej osoby. Dlatego ważna jest edukacja, która jest kluczem do rozróżnienia przez młodych ludzi, co w komunikacji

online jest akceptowalne, a co zupełnie nie. Więcej na ten temat w podrozdziale „Badania Thorn na temat zjawiska samodzielnie wytwarzanych materiałów z kategorii CSAM – postawy i doświadczenia młodzieży w latach 2019–2021”.

Przyczyny i motywacje, czyli dlaczego dochodzi do szantażu na tle seksualnym wobec małoletnich

Z punktu widzenia sprawców metoda ta jest skuteczna ze względu na:

- względnie łatwe pozyskanie treści o charakterze seksualnym lub korzyści finansowych;
- bezproblemowe nawiązanie kontaktu poprzez kanały bezpośredniej komunikacji, szczególnie w mediach społecznościowych;
- możliwość ukrycia swej prawdziwej tożsamości, zarówno poprzez tworzenie fałszywych profili, przekazywanie zmanipulowanych treści foto/wideo, jak i używanie narzędzi do anonimizacji (proxy, sieć Tor);
- podatność nieświadomych użytkowników internetu, szczególnie dzieci, na manipulację.

Czynniki motywujące sprawców (według Europolu)[23]:

1. Zainteresowanie seksualne dziećmi, gdy celem wymuszonej wymiany jest zdobycie materiałów seksualnych (zdjęć lub filmów przedstawiających dziecko) lub wymuszenie bezpośredniego spotkania w celach seksualnych.

23. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of-children (dostęp: 15.06.2023).

2. Interes ekonomiczny, w którym celem jest czerpanie korzyści finansowych z wymuszenia.

3. Świadomość sprawcy, że ofiary mogą niechętnie zgłaszać się do organów ścigania lub szukać pomocy, ponieważ wstydzą się materiałów, które posiada sprawca, lub nie są świadome, że są ofiarami przestępstwa.
Możliwa jest również kombinacja wymienionych wyżej czynników nr 1 i 2.

Europol zwraca uwagę, że niezależnie od motywacji, cyberprzestrzeń sprzyja sprawcom w następujących obszarach[24]:

- anonimowość i możliwość stosowania technik manipulacyjnych;
- eliminacja barier geograficznych – możliwość otrzymania pożądanych zysków przez sprawcę niezależnie od lokalizacji;
- duża liczba potencjalnych ofiar;
- zarządzanie – w zakresie manipulacji i skłonienia rozmówcy do tworzenia materiałów seksualnych, zdjęć lub filmów, lub udziału w dostosowanych do potrzeb sprawcy transmisjach na żywo;
- obniżenie ryzyka – w zakresie ukrywania prawdziwej tożsamości;
- wzmocnienie zagrożenia wobec osoby poszkodowanej na skutek łatwej ewentualnej dystrybucji pozyskanych treści.

Wśród nastolatków seksting (udostępnianie stworzonych przez siebie materiałów o charakterze seksualnym) jest powszechną formą flirtowania i eksperymentowania. W przypadku sprawcy

24. *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*, Europol-EC3 2017, s.12.

będącego rówieśnikiem nastolatka, który jest ofiarą szantażu, motywacją mogą być korzyści społeczne, takie jak uwaga, popularność i afirmacja. Może to też wynikać z chęci zemsty na partnerze po zakończeniu związku[25]. Nieletni sprawcy mogą nie zdawać sobie sprawy, że łamią prawo.

Dlaczego użytkownicy wchodzą w obarczone ryzykiem internetowe interakcje o charakterze seksualnym?

Czynniki sprzyjające nawiązaniu intymnego kontaktu online:

- brak satysfakcjonujących relacji, szczególnie tych o charakterze intymnym,
- ciekawość,
- łatwość nawiązania kontaktu,
- możliwości uzyskania gratyfikacji seksualnej „tu i teraz”,
- „bezkosztowość” – w kontakt inwestowany jest tylko czas,
- (złudne) poczucie bezpieczeństwa w relacji niebezpośredniej.

25. Zjawisko to jest określane mianem *revenge porn*, co można przetłumaczyć jako „rozpowszechnianie treści pornograficznych umotywowane zemstą”. Polega na rozpowszechnianiu w internecie zdjęć lub filmów o charakterze seksualnym bez zgody osoby widocznej na zdjęciach. Sprawcą jest często były partner/partnerka, który uzyskuje zdjęcia lub filmy w trakcie poprzedniego związku i ma na celu publiczne zawstydzenie i upokorzenie ofiary w odwecie za zakończenie związku. Jednakże sprawcy niekoniecznie są partnerami lub byłymi partnerami, a motywem nie zawsze jest zemsta. Treści można również uzyskać, włamując się do komputera, kont w mediach społecznościowych lub smartfonu, a ich celem może być wyrządzenie szkód w życiu osoby poszkodowanej (np. utrata pracy lub w niektórych przypadkach spowodowanie samobójstwa) – za European Institute For Gender Equality.

https://eige.europa.eu/publications-resources/thesaurus/terms/1459?language_content_entity=en (dostęp: 14.10.2023).

Według Europolu małoletni mogą stać się ofiarami szantażu seksualnego ze względu na[26]:

- podatność na zagrożenia na poziomie relacyjnym (wyrażanie potrzeb lub młodzieńczo brzmiące nazwy profilu użytkownika) lub na poziomie technicznym (brak wiedzy na temat bezpieczeństwa online);
- brak kontroli lub słabą kontrolę rodzicielską;
- otwartość na nadmierne udostępnianie, w tym materiałów erotycznych stworzonych przez siebie;
- znaczną ilość czasu spędzanego online każdego dnia;
- częste korzystanie z sieci społecznościowych i innych środków komunikacji online, w szczególności za pośrednictwem urządzeń mobilnych;
- skłonność do zaprzyjaźniania się z nieznajomymi przez internet;
- swobodne podejście do seksualnych interakcji lub komunikacji online;
- brak wiedzy technicznej (konieczność stosowania silnych haseł, znajomość sposobów radzenia sobie z podejrzanymi linkami itp.)

26. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of-children (dostęp: 15.06.2023).

Spotkanie się z szantażem jest dla osób małoletnich szczególnie trudną sytuacją i zdarza się, że nikomu o niej nie mówią. Trudności z podzieleniem się tym wyjątkowo stresującym problemem wynikają z[27]:

- obawy przed spełnieniem groźby,
- poczucia winy i obaw, że otoczenie będzie je obwiniać o zaistniałą sytuację,
- obaw, że nikt nie uwierzy w prawdziwy przebieg wydarzeń,
- poczucia zdezorientowania i braku wiedzy, co zrobić,
- wrażenia osamotnienia i braku pomysłu, do kogo zwrócić się o pomoc,
- poczucia wstydu, szczególnie w przypadku chłopców.

27. https://www.missingkids.org/netsmartz/topics/sextortion (dostęp: 15.06.2023).

Szantaż na tle seksualnym wobec małoletnich w zgłoszeniach Dyżurnet.pl

Dyżurnet.pl to działający od 2005 r. w ramach NASK-PIB punkt kontaktowy do zgłaszania nielegalnych treści w internecie. Od roku 2018 główna działalność, polegająca na przyjmowaniu i analizie zgłoszeń dotyczących przypadków rozpowszechniania treści pornograficznych z udziałem małoletnich za pośrednictwem technologii informacyjno-komunikacyjnych, wpisana została do Ustawy o krajowym systemie cyberbezpieczeństwa[28].

Pierwsze zgłoszenia dotyczące szantażu na tle seksualnym zaczęły trafiać do Dyżurnet.pl w roku 2017 i z każdym następnym rokiem ich liczba rosła. Zdecydowana większość z nich dotyczyła osób pełnoletnich.

28. Art. 26 pkt.6 pdpkt.3) w Dz. U. 2018 poz. 1560, *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.*

Poniższa analiza dotyczy wyłącznie przypadków szantażu wobec osób małoletnich (w tym jedna osoba w wieku 18 lat), których ogółem było 36. Do końca roku 2021 takich przypadków było 15. Rok 2022 był jak do tej pory najliczniejszy pod względem otrzymanych zgłoszeń. Do Dyżurnet.pl napłynęło wtedy 13 przypadków szantażu na tle seksualnym. W roku 2023 nadeszło osiem zgłoszeń.

Notka metodologiczna:

Zgłoszenia od pokrzywdzonych, ich rodziców oraz świadków przekazywane były do Zespołu Dyżurnet.pl różnymi sposobami:

- poprzez e-mail: dyzurnet@dyzurnet.pl
- poprzez formularz na stronie www.dyzurnet.pl
- przez działający w NASK-PIB zespół CERT Polska, do którego trafiło pierwotne zgłoszenie.

Treść pisemnych zgłoszeń analizowana była według następujących kategorii:

1. Osoba dokonująca zgłoszenia

2. Perspektywa osoby pokrzywdzonej
   - płeć,
   - wiek w momencie zgłoszenia,
   - wiek w momencie utrwalenia intymnej treści,
   - konsekwencje emocjonalne.

3. Perspektywa sprawcy
   - płeć,
   - użycie fałszywej tożsamości,
   - lokalizacja,
   - miejsce nawiązania kontaktu,
   - metoda pozyskania intymnych materiałów,
   - żądania,

- charakter groźby w przypadku niespełnienia żądania,
- realizacja groźby.

Zgłoszenia analizowane były głównie na podstawie pierwotnej treści zgłoszenia. W kilku przypadkach zgłaszający nadesłali dodatkowe informacje w odpowiedzi na prośbę analityka Dyżurnet.pl. Nie było jednak ustalonego skryptu zapytań do zgłaszającego ani formularza z wymaganymi informacjami, które miał podać zgłaszający. Nadrzędnym celem zespołu Dyżurnet.pl było udzielenie szybkiej odpowiedzi z poradą, jak postępować w trudnej dla osoby poszkodowanej sytuacji.

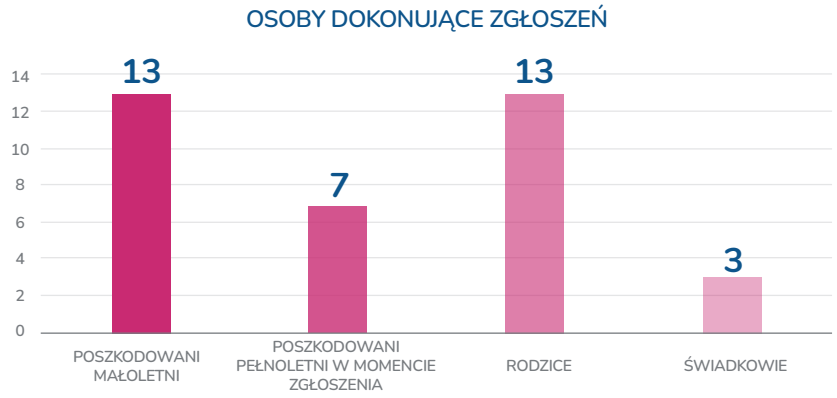
W dalszej części opisane są poszczególne elementy analizowanych zgłoszeń.

Osoba dokonująca zgłoszenia

W 20 przypadkach (56% ogólnej liczby) zgłoszenie przesłała osoba pokrzywdzona, jednak siedem z nich było już w tym momencie pełnoletnich (pięć kobiet, dwóch mężczyzn). Osiem zgłoszeń nadesłanych zostało bezpośrednio przez osoby niepełnoletnie, w wieku 14–17 lat (pięć dziewczynek, trzech chłopców). W czterech przypadkach nie można było ustalić wieku pokrzywdzonego małoletniego. Wiek można było oszacować jedynie na podstawie kategorii formularza, przez który zostało przesłane zgłoszenie (treści pornograficzne z udziałem małoletniego). Dotyczyło to trzech dziewczynek i jednego chłopca.

Rodzice byli osobami zgłaszającymi w trzynastu przypadkach (36% ogólnej liczby), choć tylko w jednym podpisali się wspólnie. Zdecydowanie częściej zgłaszają matki (osiem przypadków) niż ojcowie (dwa przypadki). W dwóch przypadkach ustalenie płci rodzica nie było możliwe na podstawie tekstu zgłoszenia.

Trzykrotnie przypadki szantażu na tle seksualnym (9% ogólnej liczby) zgłosili świadkowie, w dwóch przypadkach dotyczyło to płci męskiej, w trzecim nie było wystarczających danych w zgłoszeniu, by określić płeć świadka.



Rys. 1. Osoby dokonujące zgłoszeń

Wnioski: małoletni są skłonni zgłaszać się bezpośrednio, kiedy są w wieku powyżej 14 lat. Częściej czynią to dziewczynki.

W przypadku młodszych nastolatków (najmłodszy pokrzywdzony miał 10 lat) zgłoszenia dokonują rodzice, głównie matki.

Świadkowie relatywnie rzadko zgłaszają zaobserwowane przypadki szantażu na tle seksualnym.

Perspektywa osoby pokrzywdzonej

Płeć

12 przypadków dotyczyło chłopców, natomiast dziewczynki były pokrzywdzonymi w 25 przypadkach, bowiem jedno zgłoszenie dotyczyło dwóch dziewczynek.

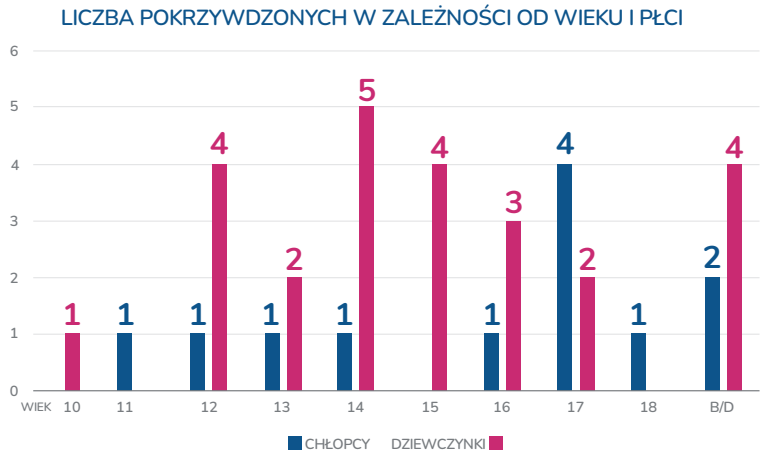
Wiek w momencie zgłoszenia

Zgłoszenia dotyczyły osób małoletnich, ale w momencie zgłaszania niektóre z nich były już pełnoletnie. Taka sytuacja dotyczyła siedmiu

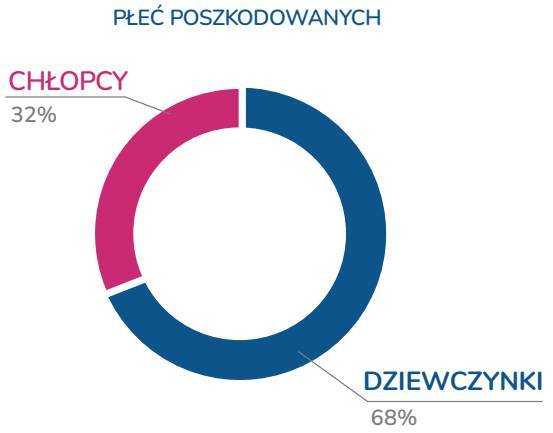
osób i w momencie zgłoszenia ich wiek wahał się od 18 do 22 lat (pięć kobiet, dwóch mężczyzn). Pozostali poszkodowani znajdowali się zakresie wiekowym 10–18 lat.

Wiek w momencie utrwalenia intymnej treści

Szczegółowy rozkład osób poszkodowanych w zależności od wieku i płci prezentuje rys. 2.



Rys. 2. Liczba pokrzywdzonych w zależności od wieku i płci



Rys. 3. Płeć poszkodowanych

Wnioski: Najliczniejszą grupę pokrzywdzonych stanowią dziewczynki – są to aż 25 przypadki (w tym jeden, gdzie szantażowane były dwie dziewczynki). Sprawy dotyczące chłopców stanowiły 12 przypadków.

Najbardziej dotknięta szantażem była grupa w wieku 12–16 lat, choć zgłoszone było także i dziecko 10-letnie. Również dziewczynki w tej grupie stanowiły zdecydowaną większość.

Lokalizacja

W zgłoszonych sprawach brak było informacji o przebywaniu czasowym lub stałym osób poszkodowanych poza granicami kraju. Domniemywać można, że osoby pokrzywdzone pochodziły wyłącznie z Polski.

Konsekwencje emocjonalne

W ośmiu przypadkach zgłoszeń (23% ogólnej liczby) zgłaszający wskazywali problemy natury emocjonalnej w związku z sytuacją. W pięciu dotyczyło to bezpośrednio osoby poszkodowanej, która zgłosiła sprawę, a w trzech – rodziców poszkodowanych małoletnich.

Sześć przypadków dotyczyło dziewczynek, dwa przypadki – chłopców.

Niezależnie od płci, poszkodowani i ich rodzice mówią o lęku, strachu, bezradności.

Poniżej fragmenty zgłoszeń (pisownia oryginalna):

Nie chcę by błąd mojej młodości zniszczył mi życie.

Córka ma 12 lat i naprawdę pierwszy raz ja zobaczyłam tak przestraszoną (...) Naprawdę się przestraszyłam i chcę uchronić swoje oraz inne dzieci od takich osób.

Nie wiem teraz co robić, cały czas się martwię żeby nie poszło to w internet bo najzwyczajniej jestem już wtedy skończony,

nie rozmawiałem o tym z rodzicami bo wstydzę się tego i to mocno. Nie wiem jakie kroki mam postąpić z tym niby jak na razie nie mogę odszukać w internecie żeby było to wstawione, no ale nie wiem martwię i to bardzo.

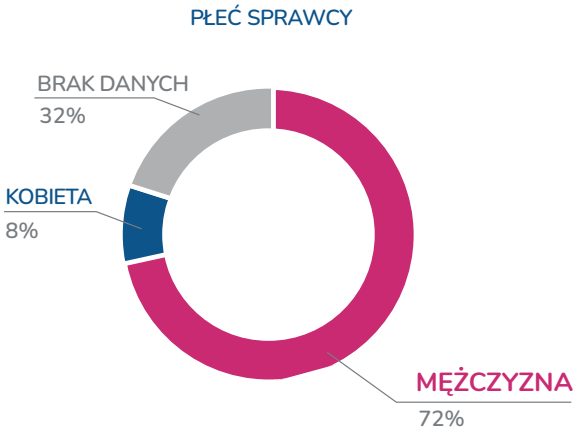
Nie wiem co mam robić, jestem gotowy nawet się zabić!

Córka ma myśli samobójcze. Nie wiem jak tego człowieka powstrzymać. Córka usunęła konta, jest przerażona.

Perspektywa sprawcy

Płeć

W 26 przypadkach sprawcą był mężczyzna, w trzech kobieta. W siedmiu przypadkach nie udało ustalić się płci szantażysty na podstawie tekstu zgłoszenia.



Rys. 4. Płeć sprawcy

Użycie fałszywej tożsamości

W dziesięciu przypadkach sprawca, podejmując kontakt z potencjalną ofiarą, używał fałszywych tożsamości:

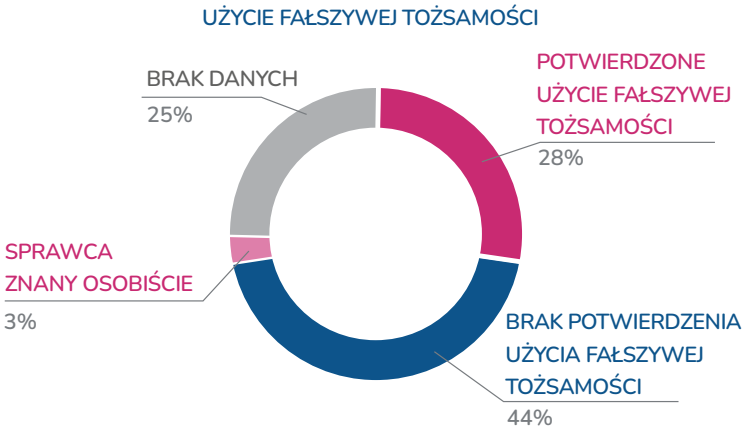
- Dwa przypadki dotyczyły zarówno sprawcy mężczyzny, jak i sprawcy kobiety, którzy występowali pod różnymi tożsamościami internetowymi (ale bez podawania fałszywej płci);
- Dwóch sprawców przedstawiało się jako 16-letnie dziewczynki;
- Dwóch szantażystów udawało młodych chłopców;
- Trzech sprawców przedstawiło się jako dorosła kobieta;
- Jeden podszywał się pod dziecko.

Poszkodowani wspominali w zgłoszeniu o fałszywej tożsamości, gdyż w tych przypadkach sprawca wysuwając żądania używał innej tożsamości niż tej, za pomocą której nawiązał kontakt.

W 16 przypadkach poszkodowani nie zaobserwowali symptomów użycia przez sprawcę fałszywej tożsamości.

W jednym przypadku sprawca był osobiście znany poszkodowanej (były partner).

W dziewięciu przypadkach nie udało się pozyskać bliższych informacji na ten temat.



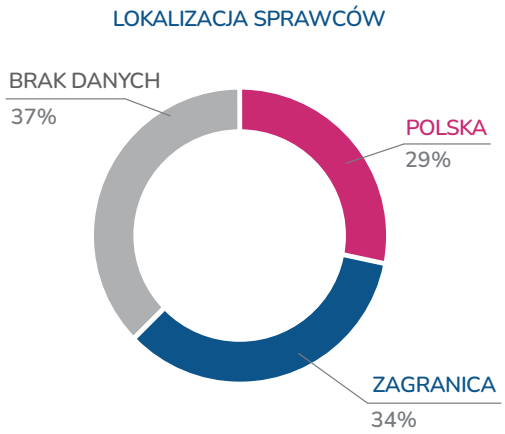
Rys. 5. Użycie przez sprawcę fałszywej tożsamości

Wnioski: Ofiary w przeważającej liczbie przypadków poznały szantażystę w internecie i nie spotkały wcześniej tej osoby offline. W większości przypadków (44%) poszkodowani nie stwierdzili, by sprawca używał fałszywej tożsamości, co nie oznacza, że jego profil pokrywał się z prawdziwymi danymi. Taka sytuacja miała miejsce tylko w jednym przypadku, kiedy sprawca i poszkodowany znali się osobiście.

Lokalizacja

12 sprawców pochodziło spoza Polski (dziesięciu mężczyzn, dwie kobiety). Dziesięciu sprawców pochodziło z Polski (dziewięciu mężczyzn, jedna kobieta).

W 13 przypadkach nie udało się pozyskać bliższych informacji na temat lokalizacji sprawców.



Rys. 6. Lokalizacja sprawców

Wnioski: Sprawcy pochodzili zarówno spoza granic Polski, jak i z kraju. Komunikacja z szantażystami z zagranicy odbywała się zarówno w języku angielskim, jak i w języku polskim; sprawca używa wtedy translatora.

Miejsce nawiązania kontaktu

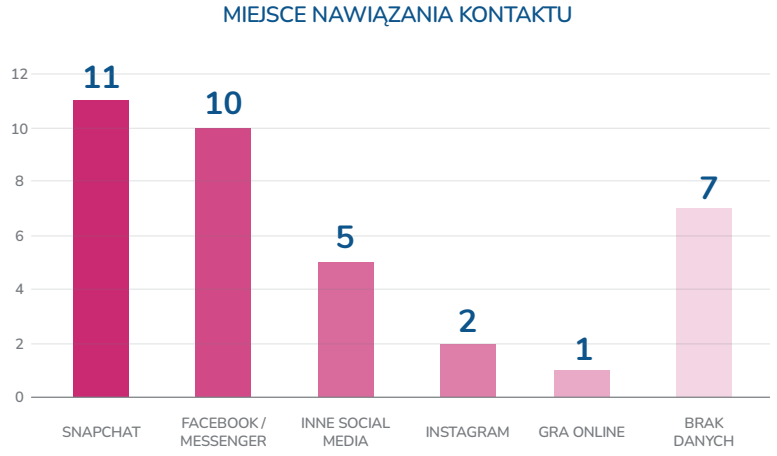
Kontakt sprawcy z osobą poszkodowaną najczęściej był inicjowany na komunikatorze Snapchat, którego dotyczyło 11 przypadków.

W dziesięciu przypadkach kontaktowano się na serwisie społecznościowym Facebook i powiązanym z nim komunikatorze Messenger.

Serwisu Instagram dotyczyły dwa przypadki.

Pojedyncze przypadki obejmowały takie serwisy społecznościowe i komunikatory, jak: Czateria, WhatsApp, Omegle, Discord, Interpals.

W jednym przypadku znajomość została zawarta podczas gry online.



Rys. 7. Miejsce nawiązania przez sprawcę kontaktu

Wnioski: Większość zgłoszonych przypadków szantażu na tle seksualnym polegała na nawiązaniu kontaktu przez sprawcę za pomocą komunikatorów internetowych lub serwisów społecznościowych, a następnie pozyskaniu od rozmówcy intymnych treści.

Metoda pozyskania intymnych materiałów

W 16 przypadkach osoba pokrzywdzona zgodziła się na sugestię rozmówcy i samodzielnie przesłała mu intymne treści. Co interesujące, w jednym przypadku intymne treści pochodziły z internetu i nie przedstawiały poszkodowanej osoby, w przeciwieństwie do pozostałych trzynastu spraw.

Sześć przypadków dotyczyło sytuacji, gdy osoba poszkodowana nie zdawała sobie sprawy, że jest nagrywana w trakcie intymnych czynności.

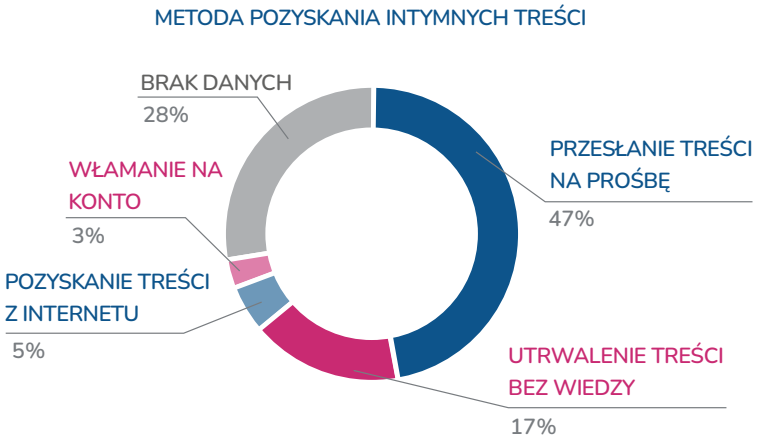
Jeden przypadek dotyczył włamania na konta serwisów społecznościowych i pozyskania stamtąd intymnych treści osoby pokrzywdzonej. Był też pojedynczy przypadek przesłania intymnych treści do rzekomej agencji fotomodelingu, skąd trafiły do serwisu w anonimowej sieci Tor[29] i stamtąd uzyskał je szantażysta.

Kolejny przypadek dotyczył transmisji samodzielnie przeprowadzanych na żywo w serwisie pornograficznym, gdzie były utrwalane bez wiedzy osoby poszkodowanej. Następnie zamieszczane były na stronach pornograficznych, skąd pozyskał je szantażysta.

Jeden przypadek to szantaż nie bazujący na pozyskanych intymnych materiałach, ale na zainfekowaniu, a następnie zablokowaniu komputera pokrzywdzonego.

W dziesięciu przypadkach brak było informacji, jak doszło do przechwycenia intymnych treści.

29. Tor (za wikipedia.org) – wirtualna sieć komputerowa implementująca trasowanie cebulowe drugiej generacji. Sieć zapobiega analizie ruchu sieciowego i w konsekwencji zapewnia użytkownikom prawie anonimowy dostęp do zasobów internetu. Tor może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych.



Rys. 8. Metoda pozyskania przez sprawcę intymnych treści

Wnioski: Zdecydowana większość przypadków (64% ogólnej liczby) opierała się na decyzji osoby małoletniej, aby albo wykonać samodzielnie intymne zdjęcie lub nagranie i następnie przesłać je dalej, albo uczestniczyć w transmisji na żywo, podczas której podejmowana była aktywność seksualna.

Żądania

W 16 przypadkach sprawca żądał od pokrzywdzonej osoby utrwalenia i przekazania nowych intymnych treści. W kwestii podziału płci sprawców i pokrzywdzonych wyglądało to następująco:

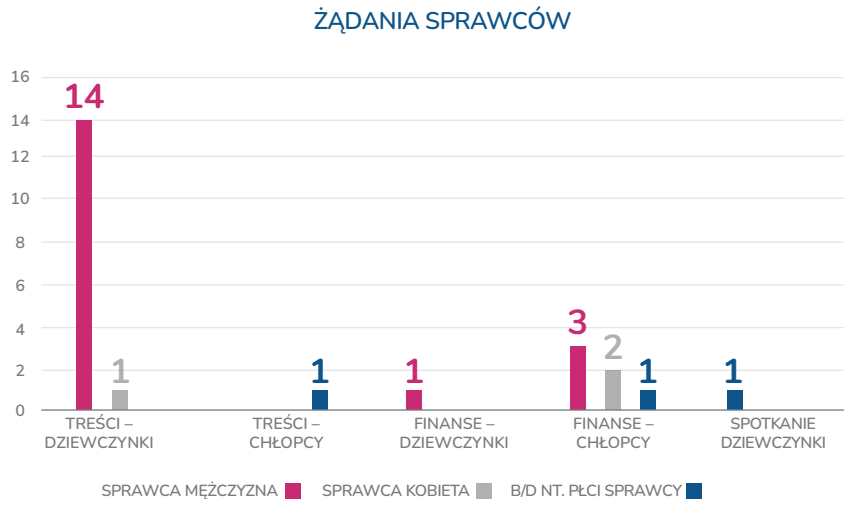
- W 14 przypadkach sprawca mężczyzna nakłaniał poszkodowaną dziewczynkę do przysłania nowych treści;
- W jednym przypadku sprawczyni (kobieta) domagała się od 14-letniej dziewczynki kolejnych materiałów;
- Jeden przypadek wiązał się z nakłanianiem do wysłania intymnego zdjęcia 11-letniego chłopca, którego urządzenie zostało zablokowane po kliknięciu na link wysłany przez sprawcę/sprawczynię.

- Pojedynczy przypadek dotyczył żądania sprawcy mężczyzny bezpośredniego spotkania w celu seksualnym, wystosowanego wobec 12-letniej dziewczynki;

Siedem przypadków stanowiło szantaż na tle finansowym. Sześć z nich dotyczyło chłopców, którzy szantażowani byli przez kobietę (dwa przypadki), przez mężczyznę (trzy przypadki) i w jednym przypadku przez osobę, której płci na podstawie tekstu zgłoszenia nie udało się ustalić.

Jeden przypadek szantażu na tle finansowym dotyczył dziewczynki szantażowanej przez mężczyznę.

W 12 przypadkach nie udało się ustalić charakteru żądań sprawcy na podstawie tekstu zgłoszenia.



Rys. 9. Żądania sprawców w zależności od płci

Wnioski: Zdecydowana większość zgłoszeń szantażu była związana z przekazaniem przez osobę poszkodowaną (dziewczynkę) nowych intymnych treści, co świadczy o seksualnym charakterze podjętej przez sprawcę (zazwyczaj mężczyznę) aktywności.

Siedem przypadków szantażu obejmowało uzyskanie korzyści finansowej przez sprawcę i dotyczyły one głównie chłopców.

Charakter groźby w przypadku niespełnienia żądania

W 11 przypadkach sprawca groził poszkodowanemu przekazaniem intymnych treści lub informacji o nich jego znajomym. Trzy przypadki obejmowały groźbę przekazania zdjęć czy filmów członkom rodziny. W 11 przypadkach sprawca groził, że w przypadku niespełnienia żądań materiały trafią do internetu.

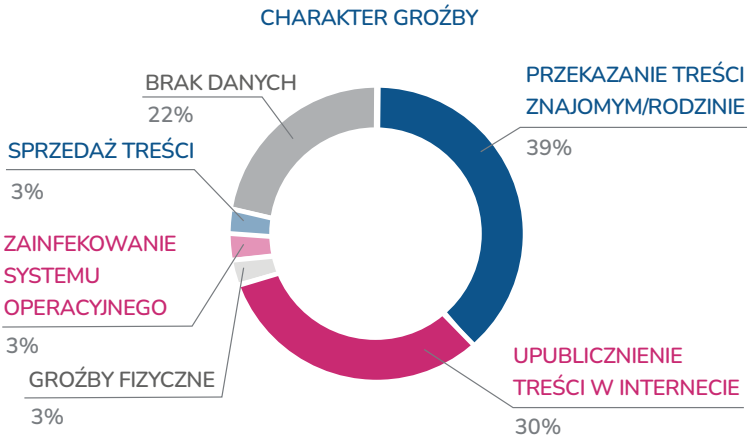
W jednym przypadku sprawca dodatkowo groził sprzedażą intymnego zapisu. Dotyczyło to treści opublikowanych w sieci Tor.

Jeden przypadek, prócz pogróżek upublicznienia treści w internecie, wiązał się z groźbami wystosowanymi wobec rodziny pokrzywdzonej. Było to o tyle poważne, że sprawczyni twierdziła, iż zna adres zamieszkania ofiary.

W kolejnym przypadku szantaż nie wystąpił. 15-letnia dziewczyna zorientowała się w trakcie intymnego kontaktu poprzez Snapchat, że rozmówca utrwala treści bez jej zgody. Zwróciła się z tym do ojca, który przesłał zgłoszenie do Dyżurnet.pl, pytając o dalsze postępowanie w takiej sytuacji.

Jeden przypadek polegał na zainfekowaniu systemu operacyjnego poszkodowanego chłopca poprzez przekazanie linku ze szkodliwym oprogramowaniem. W zamian za naprawę systemu sprawca żądał przesłania nagiego zdjęcia chłopca.

W ośmiu przypadkach nie udało uzyskać się informacji o charakterze groźby.



Rys. 10. Charakter groźby

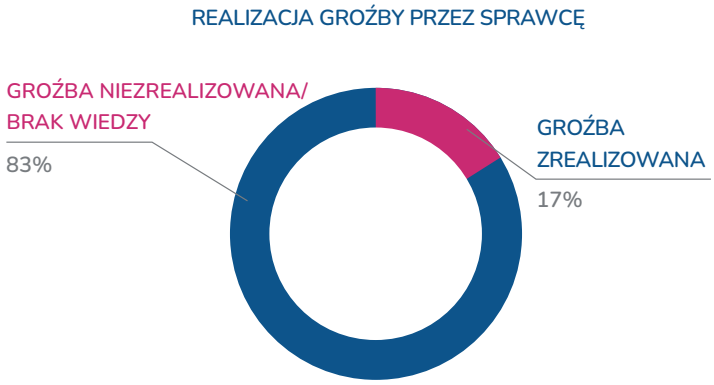
Wnioski: W przeważającej większości (69% ogólnej liczby) groźby sprawcy były związane z przekazaniem intymnych treści przedstawiających osobę poszkodowaną jej znajomym, rodzinie lub z ich publikacją w internecie.

Realizacja groźby

W sześciu przypadkach sprawca już zrealizował swoją groźbę i przekazał treści znajomym (dwie sytuacje) lub opublikował je w internecie (cztery przypadki). Publikacja nastąpiła w takich serwisach jak Snapchat, Twitter oraz VK (VKontakte).

Sprawca w jednym przypadku zaczął rozsyłać wiadomości poprzez Instagram do znajomych poszkodowanej z zapytaniem, czy chcą uzyskać jej intymne treści.

Niestandardowy był jeden z niedawno zgłoszonych przypadków szantażu. 11-letni chłopiec poznał na platformie gier online rzekomego rówieśnika, od którego otrzymał link. Po kliknięciu linku system operacyjny urządzenia został zablokowany, a rozmówca zażądał przesłania nagiego zdjęcia. Po jego otrzymaniu miał odblokować system. To niestandardowy modus operandi sprawcy. Może być zapowiedzią szerszego wykorzystywania tej metody w przyszłości.



Rys. 11. Realizacja groźby przez sprawcę

Wnioski: W większości przypadków (29 przypadków – 83% ogólnej liczby) sprawca nie zrealizował swojej groźby lub poszkodowany nie miał wiedzy o jej ewentualnym spełnieniu. Wynikać to może z faktu, że większość zgłoszeń szantażu zostało wysłanych do Dyżurnet.pl zaraz po sformułowaniu groźby

Podsumowanie

Na podstawie przeanalizowanych zgłoszeń można założyć, że przebieg szantażu na tle seksualnym w cyberprzestrzeni zazwyczaj wygląda następująco:

1. Małoletnia osoba, zazwyczaj dziewczynka w wieku 12–16 lat, otrzymuje poprzez serwis społecznościowy lub komunikator wiadomość od nieznajomego;

2. Nieznajoma osoba może używać fałszywej tożsamości, zatem może wyglądać na rówieśnika lub rówieśniczkę i pochodzić zarówno z kraju, jak i z zagranicy;

3. W trakcie rozmowy poruszone zostają tematy o charakterze intymnym, rozmówca nalega na przesłanie treści o takim charakterze, ewentualnie proponuje wideorozmowę;

4. Małoletni zgadza się na podzielenie się intymnymi treściami albo treści te są utrwalane bez jego wiedzy podczas wideorozmowy;

5. Wkrótce po pozyskaniu intymnych treści sprawca może już pod inną tożsamością zażądać przesłania kolejnych tego typu materiałów lub przekazania pieniędzy;

6. W przypadku niespełnienia żądań sprawca grozi przekazaniem intymnych treści znajomym, rodzinie lub ich opublikowaniem w internecie;

7. W wyniku zaistniałej sytuacji osoba poszkodowana odczuwa lęk, strach i bezradność. Może zgodzić się na żądania sprawcy i przekazać mu nowe intymne treści lub pieniądze;

8. Osoba poszkodowana wskutek ciągłych żądań sprawcy decyduje się poszukać pomocy – czy to u rodziców, czy też na zewnątrz, np. zwracając się o poradę do zespołu Dyżurnet.pl.

Najnowsze badania zjawiska szantażu na tle seksualnym i zjawisk pokrewnych

W tym rozdziale zamieszczono przegląd najnowszych badań dotyczących zjawiska szantażu na tle seksualnym. W pierwszej części rozdziału zaprezentowane zostały badania ogólnoświatowe. Druga część obrazuje polską perspektywę badawczą. Badania różniły się pod kątem metodologicznym i ilościowym; opisane zostały w kolejności chronologicznej.

Świat

Badania Thorn na temat zjawiska samodzielnie wytwarzanych materiałów z kategorii CSAM – postawy i doświadczenia młodzieży w latach 2019–2022

Thorn to międzynarodowa organizacja, która działa na rzecz zwalczania seksualnego wykorzystywania dzieci w internecie. Organizacja została założona w roku 2009 przez amerykańskich aktorów Demi

Moore i Ashtona Kutchera. Od 2019 roku Thorn przeprowadza coroczne badanie grupy tysiąca małoletnich w wieku 9–17 lat, które ma na celu określenie charakterystyki zjawiska samodzielnego wytwarzania treści o charakterze seksualnym. Badanie obejmuje udostępnianie intymnych zdjęć rówieśników, również bez zgody osób na nich utrwalonych.

W raportach z badań używany jest termin *self-generated child sexual abuse material*, SG-CSAM. Można to przetłumaczyć jako „samodzielnie wytwarzane materiały z kategorii CSAM (przedstawiające wykorzystywanie seksualne dziecka)".

Termin SG-CSAM oznacza:

Wyraźnie seksualne obrazy dziecka, które prawdopodobnie zostały zrobione przez uwidocznione na nich dziecko. Obrazy te mogą wynikać zarówno z doświadczeń za obopólną zgodą, jak i pod przymusem. Dzieci często określają doświadczenia za obopólną zgodą jako seksting lub dzielenie się nagością.

W ciągu trzech lat gromadzenia danych niektóre kwestie, na które pierwotnie zwrócono uwagę w 2019 r., pozostały niezmienne, ale w tym czasie pojawiły się też nowe zagrożenia.

Pierwsze badanie z roku 2019 pokazało, że[30]:

- Tworzenie i udostępnianie intymnych treści jest coraz bardziej powszechne, a wiele dzieci postrzega seksting jako coś normalnego wśród rówieśników.

- Odczucia małoletnich zależą od tego, czy się zgadzają na przesłanie intymnych treści, czy też są przymuszani. Szkody wynikające z początkowej zgody mogą gwałtownie wzrosnąć, gdy intymne treści zostaną udostępnione dalej.

30. *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences*, Thorn 2020, s. 3.

- Reakcje otoczenia na szukanie pomocy przez dzieci w tej sprawie często wahają się od bierności po obwinianie; pogłębia to szkody wynikające z negatywnych doświadczeń w internecie i jeszcze bardziej izoluje dzieci, które znalazły się w tej sytuacji.

Kolejne badanie obejmowało pierwszy rok pandemii COVID-19 i związany z tym lockdown oraz jego wpływ na badane zjawisko.

Odpowiedzi ujawniły, że dzieci praktycznie w równym stopniu były podzielone w postrzeganiu wpływu COVID-19 na doświadczenia SG-CSAM wśród ich rówieśników. Połowa twierdziła, że ich zdaniem pandemia nie miała wpływu na częstotliwość wysyłania lub udostępniania przez ich rówieśników SG-CSAM lub na wyciek intymnych zdjęć. Druga połowa uważała, że COVID rzeczywiście miał wpływ na doświadczenia ich rówieśników w ramach SG-CSAM, jednak badani prezentowali różne opinie co do kierunku tego wpływu. Podział i w tym wypadku był równy – 25% twierdziło, że częstotliwość kontaktu ich rówieśników z SG-CSAM podczas pandemii wzrosła, kolejne 25%, że spadła.

Raport z roku 2022 zawierał następujące ustalenia i wnioski[31]:

Od 2019 roku obserwuje się stały wzrost liczby małoletnich, którzy przyznają się do udostępniania samodzielnie wytworzonych treści o charakterze seksualnym. W 2021 r., podobnie jak w 2020 r., w przybliżeniu jedna na sześć osób małoletnich zgłosiła, że dzieli się takimi treściami. Obejmuje to jednego na siedmiu małoletnich w wieku 9–12 lat i jednego na pięciu w wieku 13–17 lat.

Odsetek małoletnich deklarujących, że zobaczyli intymne treści przedstawiające rówieśnika udostępnione bez jego zgody, pozostaje na względnie stabilnym poziomie 20%. Jednak postrzeganie, że jest to „normalne i akceptowalne" zachowanie, rośnie z roku na rok. W 2021 roku jeden na sześciu małoletnich przyznał, że wierzy, że

31. *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2021*, Thorn 2022, s. 4.

jego przyjaciele przynajmniej czasami udostępniają intymne treści przedstawiające rówieśników bez ich zgody.

Chłopcy nadal stanowią grupę zwiększonego ryzyka. Konsekwentnie deklarują większe prawdopodobieństwo ponownego udostępniania treści innych osób i sądzą, że takie udostępnianie jest legalne. W porównaniu z 2019 r. liczba młodszych chłopców (w wieku 9–12 lat) twierdzących, że udostępniali własne treści, wzrosła ponad dwukrotnie, podczas gdy przekazywanie takiej deklaracji wśród starszych chłopców (w wieku 13–17 lat) prawie się potroiło.

W listopadzie 2023 r. ukazało się najnowsze opracowanie Thorn zawierające dane z badań z roku 2022. Najważniejsze wnioski dotyczą[32]:

- **Normy w związkach się zmieniają:** aż 69% młodych osób, które udostępniły swój własny SG-CSAM, zrobiło to w ramach romantycznych związków offline, przy czym dziewczęta częściej niż chłopcy twierdzą, że wymiana nastąpiła w ramach związku.

- **Platformy używane do interakcji seksualnych w internecie są różnorodne:** platformy, na których większość małoletnich zgłosiła interakcję seksualną, to Snapchat, Facebook, Instagram, Messenger, TikTok i X (Twitter). Platformami o najwyższym wskaźniku tych interakcji wśród młodych użytkowników były Omegle, Telegram, Kik, Facebook i X (Twitter).

- **Chłopcy w dalszym ciągu są narażeni na zwiększone ryzyko, zwłaszcza związane z rozpowszechnianiem treści bez zgody osób na nich przedstawionych:** chłopcy nieco częściej (+8%) niż dziewczęta deklarują, że udostępnili własne nagie zdjęcia, a ponad 1,5 raza częściej niż dziewczęta zgłaszają, że przesłali dalej czyjeś zdjęcia.

- **Coraz więcej młodych ludzi szuka pomocy:** co budujące, małoletni częściej szukają wsparcia offline po doświadczeniu interakcji

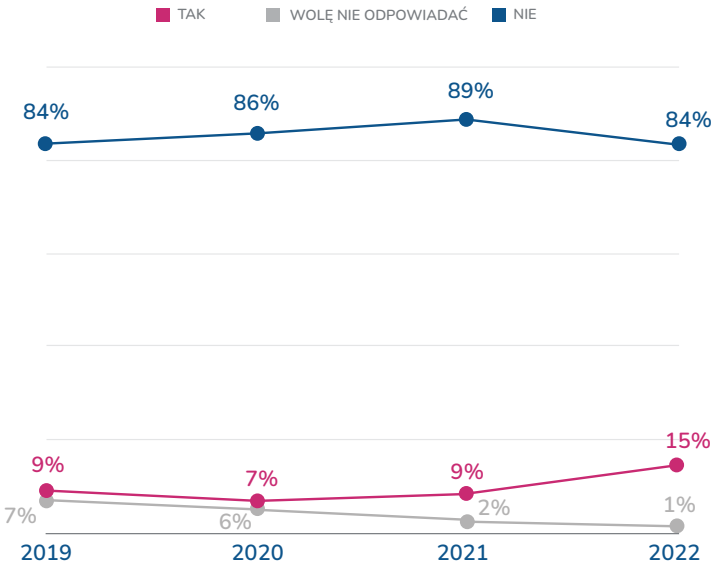
32. https://www.thorn.org/blog/decoding-youth-behavior/ (dostęp: 23.11.2023).

seksualnych w internecie. W 2022 r. liczba osób szukających wsparcia offline wzrosła o 12 procent w porównaniu z rokiem poprzednim.

Aktualne badanie zwraca uwagę na zmieniające się normy wśród młodych ludzi, podkreślając rosnącą normalizację udostępniania treści seksualnych. Dyrektor generalna Thorn, Julie Cordua, uznała, że ustalenia te świadczą o konieczności prowadzenia otwartego dialogu między rodzicami, opiekunami a dziećmi:

Najnowsze dane pokazują, że dzielenie się nagimi zdjęciami przez małoletnich, i to zarówno swoimi, jak i rówieśników, jest coraz bardziej normalne. Zwrócenie uwagi na te zachowania świadczy o potrzebie rozpoczęcia przez rodziców i opiekunów dialogu z dziećmi na temat potencjalnych zagrożeń i niebezpieczeństw związanych z udostępnianiem tego typu treści – a także na temat zgody, tak samo jak w przypadku eksploracji seksualnej offline. Umożliwiając bardziej produktywne i otwarte rozmowy na trudne, a czasem niewygodne tematy, możemy poprawić bezpieczeństwo dzieci w internecie na całym świecie.

Zrozumienie tych zachowań i spostrzeżeń jest niezbędne, bo może pomóc w zapobieganiu szkodliwej redystrybucji SG-CSAM.



Rys. 12. Doświadczenia w udostępnianiu SG-CSAM bez zgody, z podziałem na lata. Czy kiedykolwiek udostępniłeś(-aś) w internecie zdjęcie lub film o charakterze seksualnym bez zgody przedstawionej tam osoby?[33]

Raporty NCMEC i Cybertip.ca

W aktualnej informacji na temat zjawiska amerykański **NCMEC** zauważa jego znaczącą ewolucję, bo zmienił się rodzaj żądań sprawców szantażu seksualnego wobec dzieci. O ile w analizie z roku 2016 głównym motywem przestępców było uzyskanie kolejnych treści o charakterze seksualnym, o tyle w początkach roku 2022 aż 79% sprawców żądało pieniędzy. Cały rok 2022 zamknięty został liczbą przeszło 10 tys. zgłoszeń szantażu finansowego na tle seksualnym. Do końca lipca roku 2023 było to już prawie 13 tys. przypadków.

33. *Youth Perspectives on Online Safety, 2022: an Annual Report of Youth Attitudes and Experiences Findings from 2022 qualitative and quantitative research among 9-17-year-olds*, Thorn 2023, s. 27.

W 2022 r. cała kategoria *Online enticement* (w której zawiera się szantaż na tle seksualnym) objęła 80 524 zgłoszeń, co stanowi wzrost o 82% rok do roku. W poprzednich latach sprawcy wykorzystywania seksualnego częściej szantażowali dziewczynki w celu uzyskania dodatkowych treści o charakterze seksualnym. W 2022 r. zaobserwowano duży wzrost liczby chłopców szantażowanych w celu uzyskania korzyści finansowych. Niestety, kilka z tych przypadków miało tragiczny finał, kiedy szantażowane dzieci odebrały sobie życie[34].

Kanadyjski **Cybertip.ca**[35] podaje dane za okres lipiec 2022 r. – styczeń 2023 r. W tym czasie otrzymał ponad 1700 zgłoszeń, spośród których 91% poszkodowanych stanowili chłopcy. Przestępcy od chłopców żądają pieniędzy, od dziewczynek więcej treści seksualnych. Żądania zapłaty często pochodzą od zorganizowanych, międzynarodowych grup przestępczych.

W 79% przypadków szantaż miał miejsce na Instagramie lub Snapchacie, gdzie Instagram stanowi miejsce nawiązania kontaktu, który potem przenosi się na Snapchat.

Najnowszy raport NCMEC za rok 2023 mówi o liczbie prawie 187 tysięcy zgłoszeń dotyczących Online enticement (w tej kategorii zawiera się szantaż na tle seksualnym). W przeciągu lat 2021–2023 to wzrost o przeszło 300%. NCMEC zauważa ciągły wzrost liczby przypadków w których sprawcy agresywnie szantażują dzieci w celu uzyskania korzyści finansowych.[36]

34. https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata (dostęp: 17.11.2023).

35. Cybertip.ca to działająca od 2002 r. oficjalna kanadyjska infolinia służąca do zgłaszania przypadków wykorzystywania seksualnego dzieci w internecie. Funkcjonuje w ramach Kanadyjskiego Centrum Ochrony Dzieci, we współpracy z lokalnymi organami ścigania i Królewską Kanadyjską Policją Konną, której Krajowe Centrum Koordynacji ds. Wykorzystywania Dzieci koordynuje i wspiera krajowe dochodzenia w sprawie wykorzystywania seksualnego dzieci.

36. https://www.missingkids.org/content/dam/missingkids/pdfs/2023-ncmec-our-impact.pdf (dostęp 23.04.2024 r.)

Badanie WeProtect / Economist Impact dot. narażenia dzieci na krzywdy seksualne w sieci

WeProtect Global Alliance to połączenie dwóch inicjatyw, działające w tej formie od roku 2020:

1. Globalnego sojuszu przeciwko wykorzystywaniu seksualnemu dzieci w internecie Komisji Europejskiej i Departamentu Sprawiedliwości Stanów Zjednoczonych;oraz

2. WePROTECT, ustanowionego przez rząd Wielkiej Brytanii jako globalna, wielostronna odpowiedź na potrzebę zwalczania wykorzystywania seksualnego dzieci w internecie.

WeProtect Global Alliance zrzesza rządy, sektor prywatny, społeczeństwo obywatelskie i organizacje międzyrządowe w celu opracowania zasad i rozwiązań chroniących dzieci przed wykorzystywaniem seksualnym i nadużyciami w internecie.

Badanie *Szacunki dotyczące narażenia dzieci na krzywdy seksualne w sieci i ich czynniki ryzyka. Badanie doświadczeń z dzieciństwa 18-latków w czterech krajach europejskich* zostało przeprowadzone przez Economist Impact pod egidą WeProtect w okresie od lutego do marca 2023 r. Objęło ono doświadczenia 2 tys. 18-latków z czterech krajów europejskich (Francji, Niemiec, Holandii i Polski), którzy mieli regularny dostęp do internetu jako dzieci, aby zrozumieć ich doświadczenia i narażenie na krzywdy seksualne online w dzieciństwie. Pojęcie to obejmuje zestaw szkodliwych zachowań uznawanych za czynniki ryzyka dla potencjalnego lub rzeczywistego wykorzystywania seksualnego dzieci online. W Polsce badanie objęło 500 respondentów.

Wyróżniono cztery główne ryzykowne zachowania (wyniki dla Polski):

1. Badani otrzymali przed ukończeniem 18. roku życia treści o charakterze jednoznacznie seksualnym od osoby dorosłej, którą znają, lub kogoś, kogo nie znają.

   Wynik: 57% badanych w Polsce zgodziło się z powyższym stwierdzeniem.

2. Osoba dorosła, którą znali, lub ktoś, kogo nie znali, poprosił(-a) ich o zachowanie w tajemnicy części ich interakcji online o charakterze jednoznacznie seksualnym.

   Wynik: 30% badanych w Polsce potwierdziło powyższe twierdzenie.

3. Udostępnione zostały zdjęcia ankietowanych osób o charakterze jednoznacznie seksualnym bez ich zgody (przez rówieśnika, znajomą osobę dorosłą lub nieznajomego).

   Wynik: 21% badanych w Polsce zadeklarowało, że w ich przypadku tak było.

4. Zostali poproszeni o zrobienie czegoś o charakterze seksualnym online (tzn. byli nakłaniani do czynności seksualnej lub pokazania intymnych części ciała), z czym czuli się niekomfortowo lub czego nie chcieli zrobić.

   Wynik: 51% badanych w Polsce zgodziło się z powyższym stwierdzeniem.

   W kontekście zjawiska szantażu na tle seksualnym szczególnie istotne są dwie ostatnie deklaracje. O ile końcowe pytanie nie odpowiada na kwestię, jaki odsetek badanych zgodził się na czynność seksualną mimo dyskomfortu, to w pytaniu poprzednim mamy konkretne dane. Aż 21% badanych potwierdziło, że ich intymne zdjęcia zostały udostępnione innym bez ich zgody.

Interesująco wypada sprawa świadomości zagrożeń, która jest relatywnie wysoka, przynajmniej w deklaracjach respondentów. Postawiono twierdzenie:

Kiedy miałem(-am) mniej niż 18 lat, byłem(-am) w stanie zidentyfikować wiadomość lub treść, która była potencjalnie powiązana z niebezpiecznym lub szkodliwym źródłem.

Zgodziło się z nim aż 72% polskich badanych.

Wygląda to znacznie lepiej niż w przypadku deklarowanego wsparcia ze strony dorosłych. Tak prezentują się wyniki procentowe pozytywnej odpowiedzi badanych na poniższe twierdzenia:

Zanim ukończyłem(-am) 18 lat, odpowiedzialna osoba dorosła rozmawiała ze mną o bezpieczeństwie w internecie związanym z seksem (np. o tym, jak radzić sobie z osobami, które kontaktują się w celu omówienia lub udostępnienia/żądania informacji lub zdjęć o charakterze seksualnym) – zgoda 54% badanych;

Kiedy miałem(-am) mniej niż 18 lat, odpowiedzialna osoba dorosła dobrze wiedziała, co robię online – zgoda 47% badanych;

Kiedy miałem(-am) mniej niż 18 lat, miałem(-am) zaufaną osobę dorosłą, do której mogłem(-am) się zwrócić, jeśli otrzymałem(-am) wiadomość lub zobaczyłem(-am) treść, która była potencjalnie powiązana z niebezpiecznym lub szkodliwym źródłem – zgoda 62% badanych.

Fakt, że tylko połowa młodych respondentów zgodziła się z deklaracjami o świadomości internetowych zagrożeń wśród osób dorosłych oraz ich wiedzy o aktywności dziecka w internecie, wskazuje na zdecydowanie niewystarczające zaangażowanie dorosłych w kwestię ochrony dzieci online.

Jak prezentują się wyniki polskich respondentów na tle pozostałych państw europejskich (Francji, Niemiec i Holandii)?

Wyniki polskich respondentów są zbliżone do wyników innych europejskich państw. Jest jednak pewna różnica, bardzo istotna z perspektywy kwestii szantażu na tle seksualnym.

W Polsce 21% ankietowanych wskazuje na udostępnienie swoich własnych zdjęć o charakterze jednoznacznie seksualnym bez ich zgody. Natomiast w innych krajach takich deklaracji pojawia się dużo więcej: we Francji jest to 27%, w Niemczech – 41%, a w Holandii – 43%[37].

Badanie Snap Inc. przedstawicieli „pokolenia Z" i narażenia ich na metody wykorzystywane w szantażu na tle seksualnym

W czerwcu 2023 r. opublikowano badania wykonane przez Snap Inc., właściciela m.in. platformy Snapchat. Badanie przeprowadzone zostało na grupie przeszło 6 tys. przedstawicieli tzw. „pokolenia Z" – nastolatków i tzw. młodych dorosłych z Australii, Francji, Niemiec, Indii, Wielkiej Brytanii i Stanów Zjednoczonych. „Pokolenie Z" obejmuje osoby urodzone po roku 1995. Są to pierwsi ludzie dorastający w mocno zdigitalizowanym społeczeństwie.

Aż 65% respondentów stwierdziło, że oni lub ich znajomi padli ofiarą oszustwa internetowego typu *catfishing* lub ich konta zostały zhakowane przez przestępców, którzy ukradli treści o charakterze intymnym. Dotyczyło to wszystkich używanych platform i urządzeń, nie tylko Snapchata.

Catfishing ma miejsce, gdy przestępcy udają kogoś, kim nie są, aby nakłonić ofiarę do udostępnienia danych osobowych lub treści o charakterze seksualnym. Tymczasem hakowanie zazwyczaj polega na uzyskaniu przez przestępcę nieautoryzowanego dostępu do urządzeń elektronicznych ofiary lub kont w mediach społecznościowych w celu kradzieży intymnych zdjęć lub innych informacji osobistych.

37. *Estimates of childhood exposure to online sexual harms and their risk factors. A study of childhood experiences of 18-year-olds in four European countries.* WeProtect Global Alliance and Economist Impact 2023.

W obu schematach pozyskane treści były wykorzystywane do szantażowania młodych ludzi, a sprawcy żądali pieniędzy, kart podarunkowych, większej ilości materiałów o charakterze seksualnym w zamian za nieudostępnianie tych materiałów rodzinie i znajomym.

Ponad połowa (51%) respondentów zadeklarowała, że oni sami lub ich znajomi byli celem lub ofiarą catfishingu, a 47% tych przypadków dotyczyło respondentów bezpośrednio w ciągu ostatnich trzech miesięcy.

Z kolei 47% respondentów stwierdziło, że ich urządzenia lub konta w mediach społecznościowych zostały zhakowane, przy czym 39% takich przypadków miało miejsce w ostatnim kwartale.

71% respondentów ankiety, którzy wymienili *catfishing* jako metodę oszustwa, proszonych było przede wszystkim o udostępnienie intymnych zdjęć lub danych osobowych.

Na takie udostępnienie zgodziło się 44% badanych. Co udostępnili? Prawie jedna trzecia (30%) stwierdziła, że ujawniła dane osobowe, podobny odsetek (31%) udostępnił intymne zdjęcia.

Jedna czwarta podała pewne prywatne informacje odnoszące się do znajomych lub rodziny.

W przypadkach włamań 57% respondentów podało, że im (lub znajomemu) ukradziono dane.

38% stwierdziło, że sprawcy ukradli dane osobowe, a w 18% – intymne zdjęcia.

Po przejęciu treści lub informacji zaczynają się groźby i szantaż. Według respondentów sprawcy żądali korzyści materialnych, takich jak pieniądze czy karty podarunkowe. Przestępcy chcieli również kontaktu osobistego lub nawiązania stosunków seksualnych. Respondenci wskazywali również na żądania dodatkowych zdjęć i filmów o charakterze seksualnym oraz dostępu do danych osobowych i do kont internetowych.

Co interesujące, przy obydwu metodach pozyskiwania wrażliwych danych odsetek badanych poddanych szantażowi był podobny – 26% (*catfishing*) i 25% (*hacking*). W obu grupach 24% ogółu respondentów podjęło działania, aby zaradzić tej sytuacji, co stanowi zdecydowaną większość osób poddanych szantażowi.

Szukanie pomocy

Ogółem w badaniu 56% respondentów zadeklarowało, że oni lub ich przyjaciele szukali pomocy po tym, jak grożono im ujawnieniem danych przyjacielowi, rodzicowi lub innej zaufanej osobie dorosłej. Niewiele ponad połowa ankietowanych (51%) stwierdziła, że zgłosiła incydent na platformie, do hotline/helpline lub do organów ścigania. 38% zablokowało sprawcę, a mniejszy odsetek podjął inne działania, w tym aktualizację zabezpieczeń konta (30%) lub zamknięcie konta (26%).

W przypadku osób, których urządzenia lub konta zostały zhakowane, najpopularniejszym działaniem sieciowym było zgłaszanie tego faktu (57%), czy to na platformę (32%), do *hotline/helpline* (25%), czy też do organów ścigania (23%). Ponadto ponad połowa (55%) szukała pomocy u innych osób, w tym przyjaciół, rodziców i innych zaufanych dorosłych.

Kwestia płci:

W badaniu odsetek osób poddanych szantażowi wyniósł odpowiednio:

- 56% mężczyźni/chłopcy
- 44% kobiety/dziewczęta

Autorzy badania zwracają uwagę, że szczególnie chłopcy i młodzi mężczyźni nie powinni przez sytuację szantażu przechodzić sami. Podzielenie się informacją z bliskimi oraz zgłoszenie sprawy odpowiednim podmiotom przynosi im odczuwalną ulgę[38].

38. W komentarzu autorzy badania z Snap Inc. zawarli następujące stwierdzenie: *„Naszym nadrzędnym celem – jako platformy, branży i wielostronnego konsorcjum zajmującego się zagrożeniami i szkodami w internecie – powinno być rozwiązanie tych problemów, zanim jeszcze się pojawią, z naciskiem na zapobieganie poprzez podnoszenie świadomości, edukację i międzysektorową współpracę."*

Polska

Badanie NASK-PIB „Nie na pokaz”. Analiza wyników badania dotyczącego treści intymnych publikowanych przez młodzież[39].

Badanie jakościowe zostało przeprowadzone we wrześniu 2021 r. na zlecenie Zespołu Dyżurnet.pl (NASK-PIB) przez SW Research. Została w nim wykorzystana jakościowa technika indywidualnych wywiadów pogłębionych (IDI) o charakterze retrospektywnym.

Przeprowadzono 37 indywidualnych wywiadów przy użyciu platformy Zoom. W badaniu wzięły udział osoby w dwóch grupach wiekowych: 18–21 lat (28 respondentów) oraz 22–24 lata (9 respondentów). Łącznie przebadano 15 mężczyzn i 22 kobiety.

Główne wnioski z badania:

1. **Kontakt w sieci z materiałami o charakterze intymnym** jest zjawiskiem powszechnym i dotyczy ogromnej części internautów, w tym także dzieci (12–14 lat).

2. **Wyciek materiałów *self-generated sexual content*** został przez badane osoby uznany za jedną z najtrudniejszych sytuacji, w jakiej może znaleźć się ktoś wysyłający tego typu zdjęcia lub filmy.

3. **Presja na wysłanie materiałów *self-generated sexual content*** jest powszechnym problemem. Można wyróżnić trzy jej odmiany. Pierwszym rodzajem jest naleganie partnera (w większości płci męskiej) na przesłanie „nudesów”. Drugą formą jest presja rówieśnicza, polegająca na ogólnym przekonaniu nastolatków w środowisku szkolnym, że przesyłanie materiałów intymnych jest czymś powszechnym i że w określonych sytuacjach (np. związek) wręcz

39. *Nie na pokaz. Analiza wyników badania dotyczącego treści intymnych publikowanych przez młodzież*, NASK Dyżurnet.pl 2022.

wskazanym. Trzecią formą presji jest miękki, ale bardzo odczuwalny rodzaj kodu kulturowego, opartego na kulcie ciała i atrakcyjności zewnętrznej. Badani zauważali, że ten ostatni rodzaj presji obecny jest głównie w internecie.

4. W przypadku dzieci i nastolatków niegotowych na kontakt z tego typu materiałami – może to skutkować **nieprzyjemnymi lub, w skrajnych przypadkach, nieodwracalnymi skutkami w sferze psychiki i zachowań osób poszkodowanych** (odrzucenia/zamrożenia sfery seksualnej w przyszłości lub zbyt wczesnego, nagłego rozbudzenia tej sfery, prowadzącego do uzależnienia od seksu oraz innych zaburzeń na tym tle).

5. Osoby badane wielokrotnie wskazywały, że w wyniku tak powszechnego i masowego kontaktu z materiałami o charakterze pornograficznym z czasem **następuje zobojętnienie, przebodźcowanie tym tematem.**

6. Według badanych **obojętność może być również formą wyparcia** trudnych do przeżywania uczuć związanych z kontaktem z tego typu treściami, w szczególności gdy był on nagły, niespodziewany i niechciany albo nastąpił w bardzo młodym wieku.

7. Badani wskazywali na **dwa rodzaje materiałów o charakterze intymnym,** rozróżniane pod względem chęci ich otrzymania. Pierwszy stanowią materiały, których odbiorca nie chce otrzymać. Były one ocenione negatywnie prawie przez wszystkich badanych. Drugi rodzaj stanowią materiały wysyłane za obopólną zgodą (np. w związku). Ten rodzaj zdjęć i filmów o charakterze intymnym został przez większość badanych osób oceniony pozytywnie.

8. Większość badanych stwierdziła, że w przypadku trudnych sytuacji, związanych z materiałami *self-generated sexual content*, takich jak wyciek zdjęć lub filmów, presja rówieśnicza, zawiedzenie się na kimś lub otrzymanie treści o charakterze seksualnym, których nie chcieli otrzymać, **nie zwróciliby się o wsparcie do rodziców ani do szkoły** z powodu strachu, że zostaną ukarani, obwinieni lub niezrozumiani.

9. Ankietowani jednogłośnie twierdzili, że **wsparcie, jakiego oczekiwaliby w takiej sytuacji, powinno opierać się na empatii, zrozumieniu ich sytuacji i budowaniu w nich poczucia bezpieczeństwa.** Nie powinno z kolei opierać się na moralizowaniu, stygmatyzowaniu, ocenianiu i wypominaniu błędów. Wsparciu takiemu nie powinna też towarzyszyć atmosfera strachu lub wstydu.

10. W wypowiedziach osób badanych widoczna była **niepokojąco niska świadomość zasad dotyczących bezpieczeństwa w cyberprzestrzeni.** Niektóre osoby świadomie ignorowały znane im zasady bezpiecznego korzystania z internetu.

Badanie NASK-PIB „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców”[40]

Badanie zrealizowane między październikiem 2022 r. a listopadem metodą CAWI (ang. Computer-Assisted Web Interview – wspomagany komputerowo wywiad przy pomocy strony WWW) na populacji 4984 uczniów (7 i 8 klasa szkoły podstawowej oraz 1 i 2 klasa szkoły ponadpodstawowej). W badaniu wzięło też udział 1255 rodziców i opiekunów prawnych.

Jednym z kilkudziesięciu tematów dotyczących różnych aspektów korzystania z cyberprzestrzeni był seksting.

Na pytanie „Czy zdarzyło Ci się otrzymać czyjeś nagie lub półnagie zdjęcie za pośrednictwem internetu i telefonu komórkowego lub smartfona?” pozytywnie odpowiedziało 32,7% nastolatków przy czym różnica procentowa pomiędzy dziewczynkami a chłopcami otrzymującymi takie treści wynosi zaledwie 2%.

Wraz z wiekiem popularność sekstingu rośnie. W szkole średniej już co drugi nastolatek potwierdza, że otrzymał treści z czyimś nagim wizerunkiem.

40. https://www.nask.pl/pl/raporty/raporty/4295,RAPORT-Z-BADAN-NASTOLATKI-30-2021.html (dostęp 25.01.2024).

Rodzice nie mają wiedzy na temat zjawiska. Jedynie 5,6% rodziców deklaruje, że ich dzieci otrzymały nagie zdjęcia za pośrednictwem internetu, a z deklaracji nastolatków wynika, że co trzeci z nich otrzymał takie treści.

Drugim pytaniem było „Czy zdarzyło Ci się wysłać swoje nagie lub półnagie zdjęcie za pośrednictwem internetu i telefonu komórkowego lub smartfona?"

Pozytywnej odpowiedzi udzieliło 5,6% badanych nastolatków. Warto przytoczyć wartość z badania, które dotyczyło roku 2020 – wtedy uzyskano 2,2% potwierdzającej odpowiedzi.

Nie ma różnic w zachowaniach sekstingowych pomiędzy dziewczętami a chłopcami – podobny odsetek z nich deklaruje przesyłanie intymnych treści.

Zjawisko występuje częściej w starszych klasach szkół ponadpodstawowych i w większych miastach. Uczniowie szkół średnich trzykrotnie częściej niż ich młodsi koledzy i koleżanki przesyłają materiały sekstingowe. Nastolatki z dużych miast blisko dwukrotnie częściej deklarują przesyłanie takich treści niż ich rówieśnicy z obszarów wiejskich czy miejscowości do 20 tysięcy mieszkańców.

Zaledwie 1% rodziców jest świadomy takiej aktywności ich nastoletnich dzieci.

FDDS: Diagnoza przemocy wobec dzieci w Polsce 2023[41]

Badanie dotyczące wiktymizacji młodych osób jest przeprowadzane cyklicznie co 5 lat przez Fundację Dajemy Dzieciom Siłę (FDDS)[42] od roku 2013. Najnowszą edycję badania kwestionariuszowego zrealizowano w kwietniu i maju 2023 r. na ogólnopolskiej reprezentatywnej próbie warstwowo-losowej nastolatków w wieku 11–17 lat.

Pośród wielu form przemocy doświadczanej przez nastolatków autorzy badania wyselekcjonowali grupę zachowań o nazwie „wykorzystywanie seksualne bez kontaktu fizycznego" a wśród nich tzw. „niechciany seksting".

Zjawisko to badane było pytaniem „Czy kiedykolwiek ktoś bez Twojej zgody udostępnił Twoje zdjęcia lub film przedstawiający Cię nago lub prawie nago?"

Spośród próby 1403 nastolatków w wieku 13–17 lat, pozytywnie odpowiedziało 3% z nich, z czego 1% potwierdziło, że sytuacja miała miejsce w ciągu ostatniego roku.

Respondenci pokrzywdzeni niechcianym sekstingiem nie różnili się między sobą statystycznie pod względem uwzględnianych cech demograficznych takich jak płeć oraz miejsce zamieszkania. Jedynym różnicującym czynnikiem był wiek – w grupie 14–17 lat było to 4% pozytywnych odpowiedzi, w grupie młodszej 13–14 lat było to 2%.

41. https://fdds.pl/_Resources/Persistent/0/e/3/9/0e397c8f31d01856cd8d4a9430e56eade6648565/Diagnoza%20przemocy%20wobec%20dzieci%20w%20Polsce%202023%20FDDS.pdf (dostęp 25.01.2024).

42. Fundacja Dajemy Dzieciom Siłę (FDDS) (do 2016: Fundacja Dzieci Niczyje FDN) – największa w Polsce organizacja pozarządowa, która chroni dzieci przed krzywdzeniem i pomaga tym, które doświadczyły przemocy psychicznej, fizycznej i wykorzystywania seksualnego. Wspiera rodziców oraz opiekunów w rozwijaniu kompetencji rodzicielskich i wychowawczych. Organizuje szkolenia, seminaria i konferencje dla profesjonalistów na temat profilaktyki wykorzystywania dzieci i ochrony ich przed krzywdzeniem. Prowadzi anonimowy, bezpłatny i ogólnopolski telefon zaufania dla dzieci i młodzieży. Tworzy sieć Centrów Pomocy Dzieciom, które oferują pomoc psychologiczną, prawną oraz medyczną dzieciom pokrzywdzonym przestępstwem i ich rodzinom. Oferta pomocowa jest bezpłatna.

Szantaż na tle seksualnym jako metoda wyłudzeń typu scam

Scam (dosłowne tłumaczenie: oszustwo) jest typem masowo wysyłanej wiadomości drogą e-mailową (tzw. automatyczny, wielokrotny *autoresponder*) lub za pomocą komunikatorów internetowych. Jej celem jest zazwyczaj próba wyłudzenia pieniędzy od osób, które w wyniku wprowadzenia w błąd odpowiedzą na otrzymaną wiadomość.

Nie jest to zatem klasyczny szantaż, który wymaga od sprawcy nawiązania kontaktu z konkretną osobą. Zamiast tego sprawca wysyła bardzo dużą liczbę wiadomości do wielu osób. Celem tego zabiegu jest znalezienie osób, które przejmą się otrzymaną wiadomością i wyślą żądaną kwotę lub skontaktują się ze sprawcą z własnej inicjatywy.

Od roku 2018 do Dyżurnet.pl zaczęły docierać zgłoszenia dotyczące rzekomego pozyskania przez nadawcę korespondencji treści intymnych adresata. Odbyć się to miało poprzez instalację na komputerze adresata złośliwego oprogramowania, które nagrywać go miało w trakcie przeglądania stron pornograficznych. Oprogramowanie to miało też przejmować listę kontaktów z programu pocztowego i mediów społecznościowych.

W zamian za nieujawnienie intymnych treści osobom z listy kontaktów nadawca żądał wpłaty na portfel kryptowalut. Całość tej korespondencji uwiarygadniana była prawdziwym hasłem stosowanym przez adresata, a które nadawca pozyskał w ramach jednego z wielu wycieków danych do logowania. Korespondencja ta wysyłana była w sposób masowy do użytkowników, których hasła zostały ujawnione wskutek wycieku danych.

Początkowo e-maile wysyłane były w języku angielskim. Nasilenie tego zjawiska nastąpiło wiosną 2019 r., tym razem korespondencja była wysyłana do losowych użytkowników już bez podania ich prawdziwego hasła, za to w języku polskim. W roku 2023 Dyżurnet.pl obserował co najmniej trzy kampanie wyłudzeń.

Wiadomości typu *sextortion scam* od lat mają tę samą strukturę i ten sam przekaz. Podajemy przykład ostatniej (pisownia oryginalna):

Witaj zboczeńcu, Pragnę poinformować Cię o sytuacji, która może okazać się dla Ciebie nieprzyjemna. Możesz jednak na tym zyskać, jeśli będziesz postępować mądrze.

Słyszałeś o Pegasusie? Jest to program szpiegujący, który instaluje się na komputerach i smartfonach. Umożliwia hakerom monitorowanie aktywności właścicieli danych urządzeń. Zapewnia dostęp do kamery internetowej, komunikatorów, e-maili, zapisów rozmów itp. Działa dobrze na systemach Android, iOS i Windows. Chyba już zrozumiałeś, do czego zmierzam.

Minęło kilka miesięcy, odkąd zainstalowałem go na wszystkich Twoich urządzeniach, ponieważ nie byłeś zbyt wybredny w kwestii linków, które klikałes podczas przeglądania Internetu. W tym okresie poznałem wszystkie aspekty Twojego życia prywatnego, ale jeden jest dla mnie szczególnie ważny.

Nagrałem wiele filmów, na których masturbujesz się przy bardzo kontrowersyjnych filmach porno. Biorąc pod uwagę, że ogladasz tylko jeden typ filmów, mogę stwierdzić, że niezły z Ciebie zboczeniec. Wątpię, czy chciałbyś, aby Twoi przyjaciele,

rodzina i współpracownicy o tym wiedzieli. Mogę uczynić te nagrania publicznymi przy pomocy kilku kliknięć.

Każdy numer w Twojej książce kontaktowej nagle otrzyma te filmy – w WhatsApp, na Telegramie, na Skype, na e-mail – dosłownie wszędzie. To będzie tsunami, które zmiecie wszystko na swojej drodze, a przede wszystkim zniszczy Twoje dotychczasowe życie. Nie myśl o sobie jak o niewinnej ofierze.

Nikt nie wie, dokąd może zaprowadzić Twoja perwersja w przyszłości, więc potraktuj to jako rodzaj zasłużonej kary, która ma Cię powstrzymać. Lepiej późno niż wcale. Jestem kimś w rodzaju Boga, który widzi wszystko. Jednak nie panikuj. Jak wiemy, Bóg jest miłosierny i przebaczający – ja też. Ale moja łaska nie jest darmowa.

Przelej 1190 EUR na mój portfel bitcoin:
1E8J2XdCho2NmK7AFdvbQa45hShKG2TfBM

Gdy otrzymam potwierdzenie transakcji, trwale usunę wszystkie filmy, które Cię narażają, odinstaluję Pegasusa ze wszystkich Twoich urządzeń i zniknę z Twojego życia. Możesz być pewien – moją korzyścią są tylko pieniądze. Inaczej nie pisałbym do Ciebie, ale w sekundę, bez słowa, zniszczyłbym Ci życie.

Otrzymam powiadomienie, gdy otworzysz mój e-mail i od tego momentu masz dokładnie 48 godzin na przesłanie pieniędzy. Jeśli kryptowaluty to dla Ciebie niezbadana woda, nie martw się, to bardzo proste. Po prostu wpisz w Google „wymiana kryptowalut", a wtedy nie będzie to trudniejsze niż kupowanie bezużytecznych rzeczy na Amazon.

Natomiast zdecydowanie radzę Ci zrobić, co nastepuje: Nie odpowiadaj na tego e-maila. Wysłałem to z tymczasowego e-maila, więc nie można mnie namierzyć)Nie kontaktuj się z policją. Mam dostęp do wszystkich twoich urządzeń i jak tylko dowiem się, że pobiegłeś na policję, filmy zostaną opublikowane. Nie próbuj resetować ani niszczyć swoich urządzeń. Jak wspomniałem powyżej: monitoruję

całą Twoją aktywność, więc albo zgadzasz się na moje zasady, albo filmy zostaną opublikowane.

Pamiętaj też, że kryptowaluty są anonimowe, zatem nie ma możliwości zidentyfikowania mnie na podstawie podanego adresu. Powodzenia, mój zboczony przyjacielu. Mam nadzieję, że to ostatni raz, kiedy się kontaktujemy. I przyjacielska rada: od teraz zwracaj większą uwagę na swoje bezpieczeństwo w Internecie.

W przypadku, gdy tego typu wiadomości zawierają prawdziwe hasło stosowane przez adresata, warto sprawdzić, czy rzeczywiście nastąpił wyciek danych. Można to bezpłatnie zweryfikować na stronie, podając jedynie swój adres e-mail: https://haveibeenpwned.com/

W przypadku potwierdzenia wycieku koniecznie należy zmienić dotychczasowe hasło, a otrzymaną korespondencję usunąć.

W pozostałych przypadkach otrzymaną korespondencję trzeba usunąć.

W obydwu przypadkach o próbie wyłudzenia poinformować należy działający w ramach NASK-PIB zespół CERT Polska zajmujący się bezpieczeństwem teleinformatycznym w Polsce: https://incydent.cert.pl/

Aspekty prawne zjawiska

W Polsce szantaż na tle seksualnym nie jest ujęty bezpośrednio w przepisach kodeksu karnego. W zależności od sytuacji sprawę można zgłosić za pośrednictwem podmiotu przyjmującego zgłoszenia z tego zakresu lub bezpośrednio na policję.

W przypadku, kiedy poszkodowanym jest małoletni poniżej 15. roku życia, obowiązuje:

Art. 200a.
§ 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.

W sytuacji, gdy małoletniemu poniżej 15. roku życia prezentowane były treści pornograficzne, ma zastosowanie:

Art. 200.
§ 3. Kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter albo rozpowszechnia treści pornograficzne w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi, podlega karze pozbawienia wolności do lat 3.

W sytuacji, kiedy małoletni poniżej 18. roku życia przekazał utrwalone treści pornograficzne lub sprawca twierdzi, że jest w ich posiadaniu, obowiązuje:

Art. 202.
§ 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 3 miesięcy do lat 5.

Przestępstwa te ścigane są z urzędu.

Sprawę można zgłosić do zespołu Dyżurnet.pl działającego w ramach NASK-PIB na adres e-mail: dyzurnet@dyzurnet.pl

W korespondencji należy załączyć zapis rozmowy ze sprawcą.

W pozostałych przypadkach szantażu na tle seksualnym sprawy należy zgłaszać bezpośrednio policji jako przestępstwa z następujących artykułów, w przypadku których przestępstwa **ścigane są na wniosek pokrzywdzonego:**

Art. 190.
§ 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. Ściganie następuje na wniosek pokrzywdzonego.

Art. 191.
§ 1. Kto stosuje przemoc wobec osoby lub groźbę bezprawną w celu zmuszenia innej osoby do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3.

Art. 191a.
§ 1. Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Ściganie następuje na wniosek pokrzywdzonego.

Rekomendacje dla młodego użytkownika internetu

Sygnały ostrzegawcze w kontakcie online[43]:

- Coś się nie zgadza. Profil rozmówcy online nie pasuje do tego, co widzisz i słyszysz, kiedy z nim rozmawiasz lub czatujesz.
- To dzieje się zbyt szybko. Rozmówcy niemal od razu wyrażają wobec ciebie silne emocje i szybko proponują przejście na bardziej prywatny kanał, sugerując rozebranie się lub seks podczas rozmowy wideo.
- Mają wymówki. Mówią, że ich kamera internetowa nie działa, a zamiast tego wysyłają nagie zdjęcie, które rzekomo ich przedstawia.
- Wywierają presję. Ciągle proszą cię o prezentowanie zachowań seksualnych i wysyłanie nagich zdjęć, na których widoczna jest twoja twarz.

43. https://www.esafety.gov.au/key-topics/image-based-abuse/deal-with-sextortion (dostęp: 15.06.2023).

Mechanizmy raportowania i wsparcia dla poszkodowanych

Dobre praktyki i rekomendacje

Tryb postępowania dla małoletniej osoby poszkodowanej:

1. **Zakończ kontakt z osobą, która cię szantażuje.**
   Nie wysyłaj pieniędzy ani materiałów! Zablokuj szantażystę na portalach społecznościowych oraz w komunikatorach, za pomocą których rozmawialiście, ale nie usuwaj historii rozmów.

2. **Porozmawiaj o sytuacji z rodzicem, opiekunem lub zaufaną osobą dorosłą.**

3. **Zadbaj o ustawienia prywatności na portalach społecznościowych:**
   - ogranicz widoczność informacji o sobie oraz o swoich znajomych,
   - nie udostępniaj publicznie listy znajomych,
   - zablokuj otrzymywanie wiadomości od osób, których nie znasz.

4. Pokaż tę publikację zaufanej osobie dorosłej, żeby dowiedziała się, jakie kroki należy dalej wykonać.

5. Jeśli nie masz możliwości skontaktowania się z rodzicem, opiekunem lub inną zaufaną osobą dorosłą, **zadzwoń na telefon zaufania dla dzieci i młodzieży prowadzony przez:**

   Fundację Dajemy Dzieciom Siłę
   116 111 (https://116111.pl/)

   lub **telefon zaufania Rzecznika Praw Dziecka**
   800 12 12 12 albo czat na www.brpd.gov.pl

Tryb postępowania dla rodzica lub opiekuna małoletniej osoby poszkodowanej:

1. **Porozmawiaj z dzieckiem.**

2. **Wykonaj poniższe kroki, jeśli wcześniej nie zrobiło ich dziecko:**
   - Zablokuj szantażystę na portalach społecznościowych oraz w komunikatorach.

- Ogranicz widoczność profili dziecka lub nawet zlikwiduj tymczasowo profile na portalach społecznościowych.

3. **Zabezpiecz dowody dla organów ścigania** (zrzuty ekranu konwersacji oraz jak najwięcej informacji o profilu sprawcy mogących pomóc w jego identyfikacji).

4. **Zgłoś sprawę na policję** (dokładne informacje, jak to zrobić, znajdziesz w rozdziale poniżej).

5. Jeśli do szantażu doszło na portalach społecznościowych, **zgłoś** incydent **do administracji tych serwisów.**

6. Istnieje specjalna platforma stworzona przez amerykańską organizację **National Center for Missing & Exploited Children**, która umożliwia szybkie i bezpłatne zgłoszenie prywatnych zdjęć lub filmów publikowanych w sieci bez zgody.

7. W razie potrzeby, skorzystaj z telefonu zaufania Fundacji Dajemy Dzieciom Siłę służącego pomocą dorosłym w kwestii bezpieczeństwa dzieci: 800100100 lub na stronie www.800100100.pl

Zgłoszenie sprawy na policję

Szantaż na tle seksualnym osoby małoletniej jest przestępstwem ściganym z urzędu. Dlatego, gdy doszło do takiej sytuacji, sprawę należy zgłosić bezzwłocznie na policję.

UWAGA!
Przed dokonaniem zgłoszenia warto:

- zanotować wszystkie ważne informacje dotyczące zdarzenia, np.: co, kiedy i gdzie się wydarzyło, kto uczestniczył w zdarzeniu w roli sprawcy i ofiary, jak doszło do popełnienia potencjalnego przestępstwa,
- zabrać ze sobą dowody przestępstwa,
- zabrać ze sobą dokument potwierdzający tożsamość.

Jak zgłosić sprawę na policję?

Ustnie:

W każdej jednostce policji i prokuratury w Polsce funkcjonariusz ma obowiązek przyjąć takie zgłoszenie. Zgodnie z polskim prawem zgłoszenie musi zakończyć się spisaniem protokołu, który powinien zostać podpisany przez zgłaszającego. Jest to istotne, ponieważ jedynie protokół z przesłuchania podpisany przez osobę składającą zeznania stanowi podstawę prawną do wszczęcia przez policję postępowania.

Pisemnie:

Do każdej jednostki policji i prokuratury w Polsce zgłoszenie można także wysłać e-mailem, pocztą lub faksem.

Dokument powinien zawierać:

- dane o zgłaszającym (imię, nazwisko, adres),
- dane adresata (posterunku, komendy, komórki policji),
- możliwie przejrzysty opis sprawy, z uwzględnieniem posiadanych informacji o sprawcy oraz dat i godzin zdarzeń,
- własnoręczny podpis.

Do pisma należy dołączyć posiadany materiał dowodowy. W przypadku pisemnego zgłoszenia funkcjonariusz prowadzący

postępowanie może wezwać zgłaszającego/świadka do złożenia zeznań.

Anonimowo:
Ta forma zgłoszenia zainicjuje czynności policji, jednak w takim przypadku nie będą udzielane informacje o dalszym toku postępowania.

WAŻNE:

W trosce o bezpieczeństwo psychiczne dziecka należy zredukować do minimum liczbę jego przesłuchań oraz czynników stresowych. Zgłoszenia można dokonać bez udziału dziecka w najbliższej jednostce policji.

W przypadku zgłoszenia przestępstwa, w którym pokrzywdzony jest małoletni, przesłuchanie takie przeprowadza sąd na posiedzeniu z udziałem biegłego psychologa w tzw. „przyjaznym pokoju przesłuchań".

W jaki sposób usunąć swoje materiały intymne z internetu?

W sytuacji, gdy intymne materiały już trafiły do internetu, można je samodzielnie zgłosić do usunięcia poprzez wyspecjalizowane serwisy. W tym celu potrzebna jest kopia zdjęcia lub filmu, ale nie ma konieczności ich bezpośredniego przesyłania. Zamiast tego utworzony zostanie cyfrowy „odcisk palca" pliku (hash).

Wsparcie psychologiczne dla osób poszkodowanych oferowane jest głównie w formie platform i telefonów zaufania świadczących doraźną pomoc:

1. **Dla dzieci i młodzieży:**

   Numer telefonu 116 111 i strona https://116111.pl/ – telefon zaufania dla dzieci i młodzieży prowadzony przez Fundację Dajemy Dzieciom Siłę

2. **Dla dorosłych:**

   https://116sos.pl/ – platforma dla osób potrzebujących wsparcia w kryzysie emocjonalnym, psychologicznym czy prawnym prowadzona przez Instytut Psychologii Zdrowia Polskiego Towarzystwa Psychologicznego i NASK-PIB.

   https://centrumwsparcia.pl/ – centrum wsparcia dla osób dorosłych w kryzysie psychicznym prowadzone przez Fundację ITAKA-Centrum Poszukiwań Ludzi Zaginionych.

Profilaktyka i zapobieganie szantażowi na tle seksualnym wobec małoletnich

Szantaż na tle seksualnym to złożone zjawisko wymagające działań na różnych poziomach i w wielu dziedzinach. Europol zwraca uwagę na potrzebę działań w następujących obszarach[44]:

1. Kwestie techniczne

- Wytyczne dla branży IT
- Oprogramowanie zapobiegawcze
- Regulaminy oparte o zasady bezpiecznego internetu

2. Kwestie badawcze

- Porównanie krajowych legislacji
- Badania na temat sprawców przestępstw o charakterze seksualnym online

44. *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*, Europol-EC3 2017, s. 20.

- Badania porównawcze na temat różnic w zachowaniach online i offline

- Ocena krajowych strategii zapobiegania seksualnemu wykorzystywaniu online

- Uwzględnienie ważnego znaczenia profilaktyki

3. Kwestie działań organów ścigania

- Strony internetowe do zgłaszania przestępstw związanych z wykorzystywaniem seksualnym online

- Porady i ostrzeżenia policji zamieszczane w mediach

4. Kwestie edukacji i uświadamiania

- Porady dla rodziców i dzieci dotyczące bezpiecznych zachowań w internecie.

  Szantaż na tle seksualnym jest zagrożeniem, które może być powiązane z sekstingiem (kiedy intymne treści przesłane bliskiej osobie trafiają w niepowołane ręce), a czasem groomingiem (kiedy celem sprawcy jest pozyskanie tego rodzaju materiału od ofiary). Profilaktyka powinna zatem w dużej mierze opierać się na podobnych zasadach, co profilaktyka pozostałych zagrożeń. Tutaj szczególnie ważne jest zapewnienie dziecku bezpiecznej przestrzeni do zgłoszenia sytuacji szantażu.

Działania zapobiegawcze proponowane przez ekspertów zespołu Dyżurnet.pl:

1. Buduj relację z dzieckiem

Relacja oparta na zrozumieniu, szacunku, wzajemnej komunikacji i bliskości jest kluczowa. Jeżeli dziecko wytwarza materiały intymne, nie należy go oceniać, oskarżać lub też reagować złością, bo nigdy nie

możemy mieć pewności, na ile działało świadomie, a na ile zostało do tego zmuszone. Często młode osoby dzielą się takimi materiałami w wyniku manipulacji lub presji rówieśniczej.

Podejmowanie przez osoby młode działań ryzykownych jest etapem dorastania, które często pozwala im poznać siebie, nabyć życiowego doświadczenia i umiejętności radzenia sobie z konsekwencjami oraz zrozumieć zasady społeczne. Jeżeli dojdzie do takiej sytuacji, należy rozmawiać oraz próbować zrozumieć punkt widzenia młodej osoby, pokazywać możliwe wyjścia z sytuacji oraz konsekwencje działań.

2. Ustal z dzieckiem jasne reguły nawiązywania znajomości online

Młody człowiek musi być świadomy, że jakiekolwiek próby namawiania go do wytworzenia materiałów o charakterze seksualnym lub uczestnictwa w wideorozmowie o takim charakterze, wykraczają poza ramy zwykłej internetowej znajomości i należy je zgłosić osobie dorosłej. Wspólnie ustalcie zasady prywatności oraz dostosujcie ustawienia profili z serwisach internetowych.

3. Rozmawiaj z dzieckiem na temat potencjalnych zagrożeń w sieci

Szantaż na tle seksualnym w Polsce nadal nie jest odpowiednio nagłośnionym zagrożeniem, tak więc dziecko może nie być tego świadome. Ważne jest przedstawienie przebiegu takiego szantażu i pokazanie, że sprawca może oczekiwać różnych rzeczy.

4. Ucz swoje dziecko zasad ograniczonego zaufania wobec internetowych znajomości

Tak samo jak w przypadku przeciwdziałania groomingowi (uwodzeniu), ważne jest, aby dzieci zdawały sobie sprawę, że nie wszyscy mówią prawdę w internecie i mogą podawać się za kogoś zupełnie innego. Chociaż może się wydawać, że tylko najmłodsze dzieci nie mają tej świadomości, bardzo istotne jest zwrócenie na to uwagi także nastolatkom, łatwo poddającym się wpływowi tzw. influencerów. Starsze dzieci warto uświadamiać o różnych sposobach manipulacji, jakim mogą być poddawane.

5. Ucz swoje dziecko asertywności

Jak wykazały badania Europolu, ofiarami szantażu na tle seksualnym częściej zostają osoby łatwo ulegające wpływom. Od najmłodszych lat warto wzmacniać w dzieciach poczucie własnej wartości i budować umiejętność stawiania granic. Dziecko powinno umieć odmawiać zachowań, na które nie ma ochoty, szczególnie w przypadku próśb o wysłanie zdjęć o intymnym charakterze. W sytuacjach, kiedy czuje się do czegoś podobnego zmuszane lub jeżeli do takiej sytuacji już doszło, powinno mieć możliwość zwrócenia się do bliskiej osoby dorosłej, która wesprze je emocjonalnie i pomoże w rozwiązaniu problemu.

6. Poszerzaj swoją wiedzę na temat cyberbezpieczeństwa (również w kwestiach technologicznych) i przekazuj ją dziecku

Czasem intymne treści nie muszą być wysyłane do innych użytkowników lub publikowane w internecie, aby stały się narzędziem w rękach przestępcy. Może dojść do sytuacji wykradzenia ich z komputera osobistego, smartfonu czy dysku w chmurze. Warto mieć to na uwadze i pamiętać o aktualizacji oprogramowania antywirusowego, zabezpieczaniu wrażliwych danych hasłem oraz stosowaniu zabezpieczeń dostępu na smartfonach – zarówno jeżeli chodzi o sprzęt używany przez wielu domowników, jak i osobiste urządzenia dzieci.

7. Korzystaj z aplikacji do kontroli rodzicielskiej

Aplikacje kontroli rodzicielskiej mogą być pomocne, ale nie powinny stanowić jedynej ochrony przed zagrożeniami online. Aplikacje tego typu mogą ograniczyć możliwość kontaktu młodych użytkowników z treściami nielegalnymi lub szkodliwymi, w tym z materiałami pornograficznymi. Warto wspomnieć, że wiele tego typu narzędzi przesyła ostrzeżenia do rodzica i blokuje treści, jeśli dziecko chce przesłać lub ma otrzymać materiały pornograficzne. Aplikacje dają również możliwość kontroli czasu korzystania z internetu, blokowania konkretnych fraz, umożliwiają wgląd do tego, z kim dziecko się kontaktuje.

Więcej informacji dotyczących ryzykownych zachowań seksualnych oraz metod zaradczych i profilaktyki znajdziesz w innych naszych publikacjach:

- Metawersum. Zagrożenia, szanse, wyzwania. NASK-PIB Dyżurnet.pl, Warszawa 2023

- Nie na pokaz. Analiza wyników badania dotyczącego treści intymnych publikowanych przez młodzież. NASK-PIB Dyżurnet.pl, Warszawa 2022

- Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki. NASK-PIB Dyżurnet.pl, Warszawa 2019

Publikacje te dostępne są na naszej stronie internetowej:
https://dyzurnet.pl/publikacje

Bibliografia

1. *Estimates of childhood exposure to online sexual harms and their risk factors. A study of childhood experiences of 18-year-olds in four European countries*. WeProtect Global Alliance and Economist Impact 2023.

2. *Nie na pokaz. Analiza wyników badania dotyczącego treści intymnych publikowanych przez młodzież*. NASK Dyżurnet.pl, Warszawa 2022.

3. *Nowe formy przestępczości przeciwko dzieciom. Seksualne zmuszanie i wymuszenie online*. Staciwa K. w (red) E. W. Pływaczewski, D. Dajnowicz-Piesiecka, E. Jurgielewicz-Delegacz. Badania kryminologiczne a praktyka. Perspektywa krajowa i międzynarodowa. Wolters Kluwer Polska Sp. z o.o., Warszawa 2021.

4. *Online sexual coercion and extortion as a form of crime affecting children. Law Enforcement perspective*. Europol, EC3 European Cybercrime Centre, Holandia 2017.

5. *Ryzykowne zachowania seksualne i seksualizacja młodych użytkowników internetu. Zarys problematyki*. NASK Dyżurnet.pl, Warszawa 2019.

6. *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences*, Thorn 2020.

7. *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020*, Thorn 2021.

8. *Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2021*, Thorn 2022.

9. *Trends identified in CyberTipline sextortion reports*, National Center for Missing & Exploited Children 2016.

10. *Youth Perspectives on Online Safety, 2022: an Annual Report of Youth Attitudes and Experiences Findings from 2022 qualitative and quantitative research among 9-17-year-olds*, Thorn 2023.

11. *Wytyczne dotyczące terminologii w dziedzinie ochrony dzieci przed wyzyskiwaniem seksualnym i wykorzystywaniem seksualnym*, ECPAT International / ECPAT Luxembourg 2016.

12. Strona internetowa Cybertip.ca, 2023: https://www.cybertip.ca/en/online-harms/sextortion/

13. Strona internetowa eSafety Commissioner, 2023: https://www.esafety.gov.au/key-topics/image-based-abuse/deal-with-sextortion

14. Strona internetowa Europol, 2023: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of-children
oraz
https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

15. Strona internetowa FBI, 2023: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion/sextortion
oraz
https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion/financially-motivated-sextortion

16. Strona internetowa NCMEC, 2023: https://www.missingkids.org/theissues/sextortion
oraz
https://www.missingkids.org/netsmartz/topics/sextortion

17. Strona internetowa THORN, 2023: https://www.thorn.org/sextortion/

18. Strona internetowa WeProtect Global Alliance, 2023: https://www.weprotect.org/blog/two-thirds-of-gen-z-targeted--for-online-sextortion-new-snap-research/

NASK

NASK jest Państwowym Instytutem Badawczym nadzorowanym przez Ministra Cyfryzacji.

Cyberbezpieczeństwo i ochrona użytkowników oraz działania związane z zapewnieniem bezpieczeństwa są kluczowym polem aktywności NASK. Reagowaniem na zdarzenia naruszające bezpieczeństwo sieci i przyjmowaniem zgłoszeń o naruszeniach zajmuje się zespół CERT Polska (www.cert.pl) oraz Dyżurnet.pl. Zgodnie z Ustawą o Krajowym Systemie Cyberbezpieczeństwa NASK-PIB został wskazany na poziomie krajowym jako jeden z trzech Zespołów Reagowania na Incydenty Komputerowe tzw. CSIRT, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy internetu.

NASK współtworzy również zaplecze analityczne oraz badawczo-rozwojowe dla Krajowego Systemu Cyberbezpieczeństwa, prowadzi działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Działalność naukowo-badawcza NASK ma również wymiar wdrożeniowy i prorynkowy. W naszym instytucie badacze komercyjny problem ujmują w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, ale również innowacyjnych. Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako

wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie, analiza, przetwarzanie i transfer danych, a także złożone systemy sieciowe, w tym systemy IoT oraz mobilne sieci ad hoc. Obecnie rozwijany jest w badaniach obszar sztucznej inteligencji. Istotne miejsce zajmują badania dotyczące biometrycznych metod weryfikacji tożsamości w bezpieczeństwie usług. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki. NASK prowadzi także rejestr nazw w domenie .pl (www.dns.pl).

NASK

Państwowy Instytut Badawczy

ul. Kolska 12

01-045 Warszawa

Recepcja

+48 22 380 82 00

+48 22 380 82 01

Sekretariat

+48 22 380 82 04

+48 22 380 82 01