

**CYBER  
SPOT**



**Twój CYBERspot -  
wszystko co  
musisz wiedzieć**



**NASK**



**saferinternet.pl**



Dofinansowane przez  
Unię Europejską

# Wstęp

Hej! Żyjemy w czasach, w których internet jest wszechobecny i ma na nas wielki wpływ – od mediów społecznościowych po gry online, od nauki po zabawę. Ale z wielką mocą wiąże się wielka odpowiedzialność, prawda? Właśnie dlatego powstały CYBERspoty – specjalne zespoły w Twojej szkole, które pomogą Tobie i Twoim znajomym być bezpiecznym online. Brzmi ciekawie? A to dopiero początek!



## Czas na szybkie Q&A!

### 1. Co znajdziesz w tej broszurze?

Dowiesz się czym są CYBERspoty oraz poznasz kluczowe zagadnienia związane z bezpieczeństwem w internecie. Przygotuj się na praktyczne porady i konkretne wskazówki! Każdy rozdział poświęcony został innemu zagadnieniu z zakresu cyberbezpieczeństwa. Przy każdym temacie znajdziesz ponadto propozycje działań, które możesz podjąć w ramach aktywności CYBERspotu.

### 2. Czym są CYBERspoty?

CYBERspot to szkolny zespół do spraw cyfrowych. Jego celem będzie pomoc uczniom w Twojej szkole w tym, jak bezpiecznie korzystać z internetu i unikać zagrożeń. To Ty i Twój znajomi możecie być liderami tej zmiany!!

### 3. Dlaczego warto działać w CYBERspocie?

Świadomy użytkownik internetu to bezpieczny użytkownik: dowiesz się, jakie zagrożenia czyhają w sieci i jak sobie z nimi radzić.

Odpowiedzialne korzystanie z technologii: nauczysz się, jak korzystać z internetu w zdrowy i zrównoważony sposób.

Budowanie kompetencji liderkich: masz szansę stać się liderem w swojej szkole, ucząc się współpracy, komunikacji i umiejętności organizacji.

Wsparcie dla innych: pomożesz swoim rówieśnikom, kiedy napotkają problemy online. To doskonała okazja, żeby zrobić coś dobrego!



#### 4. Kto może dołączyć?

Do CYBERSpotów mogą dołączyć **uczniowie klas 7-8 szkół podstawowych oraz uczniowie ze szkół ponadpodstawowych**. Zespół CYBERSpotu w danej szkole może tworzyć od 2 do 6 osób. A wspierać Was będzie nauczyciel – koordynator, który pomoże Wam zorganizować aktywności i zadbać o to, żeby wszystko działało jak należy. Odbiorcami Waszych działań jest cała szkoła!

#### 5. Jaka jest Twoja rola w CYBERSpocie?

Twoim zadaniem jako CYBERlidera jest organizowanie i wspieranie w swojej szkole działań związanych z bezpieczeństwem w internecie. Na początek możesz rozwiesić plakaty informacyjne o CYBERSpocie w szkole. Możesz, wspólnie z swoim zespołem, organizować różne wydarzenia, akcje i kampanie, które zwiększać będą świadomość na temat cyberbezpieczeństwa. Każdy pomysł powinien się skonsultować z koordynatorem. Możesz także poprosić nas o poradę!

#### 6. Kto stoi za pomysłem CYBERSpotów?

CYBERSpoty to inicjatywa NASK w ramach Polskiego Centrum Programu Safer Internet (PCPSI), które od 2005 roku działa, by dzieci i młodzież mogły bezpiecznie korzystać z internetu. PCPSI tworzą dwie instytucje: NASK – Państwowy Instytut Badawczy i Fundacja Dajemy Dzieciom Siłę.

PCPSI realizuje trzy główne projekty:

- Saferinternet.pl: edukuje o zagrożeniach w sieci i uczy, jak bezpiecznie korzystać z internetu.
- Dyżurnet.pl: punkt kontaktowy, do którego można anonimowo zgłaszać nielegalne treści w internecie.
- Pomoc telefoniczna i online: telefony zaufania 116 111 dla dzieci i młodzieży oraz 800 100 100 dla rodziców i nauczycieli.

Dzięki CYBERSpotom, możesz wykorzystać te zasoby, by pomagać innym w bezpiecznym surfowaniu po sieci!

#### 7. Co zyskasz z udziału w CYBERSpocie?

- Zaświadczenie o udziale – oficjalny dokument, który potwierdzi Twoje zaangażowanie i będzie cennym dodatkiem do świadectwa lub CV.
- Szkolenia – uczestnictwo w profesjonalnych szkoleniach prowadzonych przez ekspertów NASK, podczas których rozwinięsz wiedzę na temat cyberbezpieczeństwa, komunikacji i pracy w zespole.
- Udział w projektach – możliwość udziału w prestiżowych projektach i działaniach, udział w panelach konsultacyjnych i konferencjach międzynarodowych.
- Kompetencje liderskie – zostaniesz liderem społeczności szkolnej, rozwijając swoje umiejętności przywódcze, organizacyjne i komunikacyjne.

Warto być aktywnym! Najbardziej zaangażowane drużyny otrzymają zaproszenie na stacjonarne wydarzenie w Warszawie.



# Kodeks CYBERlidera



**Działam w sposób etyczny.** Szanuję prywatność uczestników, promuję zdrową i konstruktywną komunikację oraz akceptuję różnorodność poglądów.



**Jestem gotów\_ pomagać innym.** Zawsze staram się spojrzeć na problemy z różnych perspektyw i wspierać innych.



**Kieruję uczniów do odpowiednich źródeł wsparcia.** Wskazuję, gdzie można uzyskać pomoc, jeśli jest to konieczne.



**Zachowuję poufność.** Nie ujawniam informacji, które mogą zidentyfikować osobę zgłaszającą problem. Informacje przekazuję wyłącznie Koordynatorowi, gdy jest to konieczne.



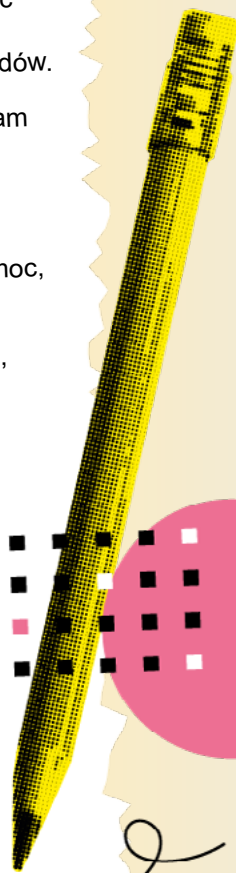
**Dbam o swoje bezpieczeństwo.** W razie niepokojącej sytuacji lub zagrożenia natychmiast informuję Koordynatora.



**Regularnie uczestniczę w szkoleniach.** Poszerzam swoją wiedzę na temat zagrożeń internetowych, korzystam z materiałów edukacyjnych.

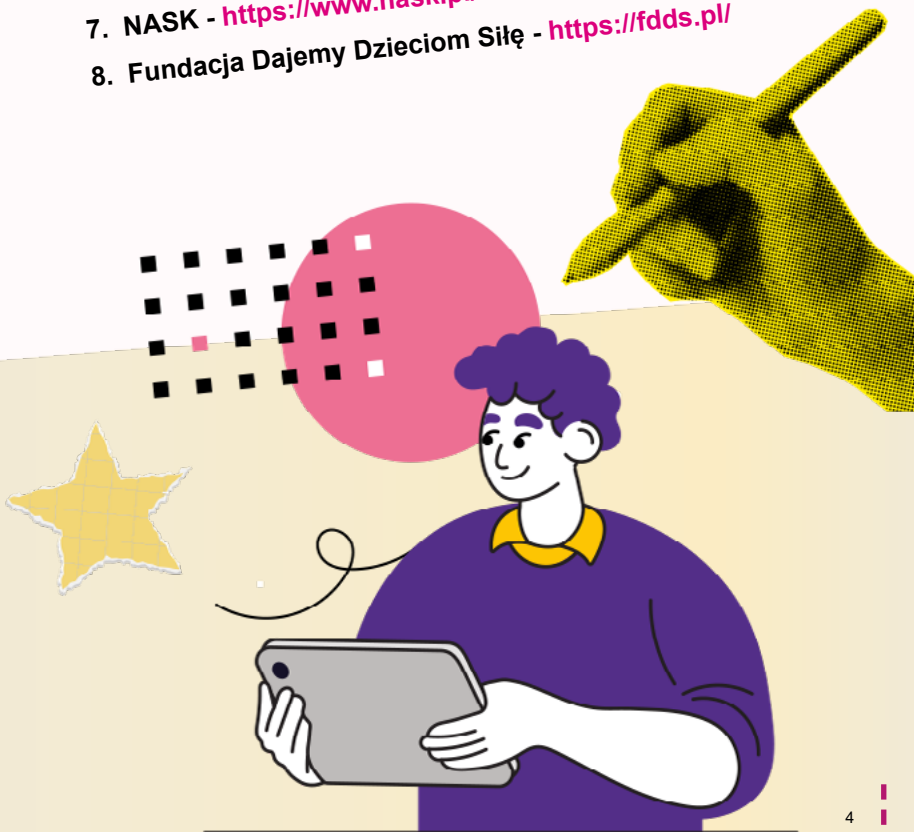


**Propaguję idee CYBERspotów.** Aktywnie promuję cyberbezpieczeństwo w swojej szkole, udostępniając materiały edukacyjne i aktywnie zachęcając do zaangażowania się w podejmowane działania.



# Sprawdź te strony!

1. Saferinternet - <https://www.saferinternet.pl/>
2. 116 111 - <https://116111.pl/>
3. Dyżurnet - <https://dyzurnet.pl/>
4. Cyberprofilaktyka - <https://cyberprofilaktyka.pl/>
5. Makeitclear - <https://makeitclear.edu.pl/>
6. CERT Polska - <https://cert.pl/>
7. NASK - <https://www.nask.pl/>
8. Fundacja Dajemy Dzieciom Siłę - <https://fdds.pl/>



# Rozdział 1: Cyfrowy dobrostan

Czy zastanawiał się kiedyś, ile czasu spędzasz online i jak wpływa to na Twoje samopoczucie?



## Słowniczek



### Cyfrowy dobrostan –

stan, w którym balans między czasem w sieci a poza nią jest zachowany. Kluczowa dla osiągnięcia równowagi jest umiejętność kontrolowania ilości i jakości czasu spędzanego z urządzeniami.



### Cyfrowy detoks –

świadoma przerwa od ekranów, której celem jest regeneracja umysłu i odzyskanie spokoju.



### FOMO (ang. Fear of Missing Out) –

strach, że omija nas coś ważnego, gdy nie jesteśmy online.



### Doomscrolling –

poświęcanie nadmiernej uwagi na przeglądanie negatywnych i niepokojących treści online (np. wiadomości o katastrofach lotniczych, kryzysach humanitarnych, chorobach czy konfliktach zbrojnych). Ten nawyk może zwiększać lęk i stres oraz negatywnie wpływać na nasze samopoczucie.



### Phubbing –

ignorowanie innych osób na rzecz korzystania z telefonu.



### Multiscreening –

potrzeba korzystania z kilku ekranów na raz. Objawia się np. równoczesnym przeglądaniem portali społecznościowych na telefonie i oglądaniem serialu na laptopie. Łatwo wtedy o dekoncentrację i przemęczenie.



### Binge watching –

oglądanie wielu odcinków serialu lub programu jeden po drugim bez przerw lub z krótkimi przerwami.

# Czy wiesz, że...?



Nastolatki spędzają w internecie średnio 5 godzin i 36 minut dziennie. W dni wolne ten czas wydłuża się do 6 godzin i 16 minut! Blisko 6,8% nastolatków jest online ponad 12 godzin dziennie, zaś niemal co dziesiąty młody internauta przebywa w sieci w godzinach nocnych (22:00–01:00). (NASK, 2023)

Sprawdź, ile czasu Ty spędzasz przed ekranami! Znajdź statystyki na swoich urządzeniach. Czy uważasz to za produktywny czas? A może chcesz coś zmienić?

## Dopamina – Twój mózgowy „like”!

Kiedy przewijasz Instagram, oglądasz kolejne filmy na TikToku, czy sprawdzasz Snapchat, Twój mózg produkuje dopaminę, zwaną także hormonem szczęścia. To neuroprzekaźnik odpowiedzialny za uczucie zadowolenia i nagrody. Aplikacje, których codziennie używasz są tak projektowane, by maksymalnie stymulować wydzielanie dopaminy i sprawiać, że będziesz chciał spędzać w nich coraz więcej czasu.



## Niekończące się treści

Feed na Instagramie czy Facebooku możesz przewijać niemal bez końca. Brzmi znajomo? Dawniej aplikacje informowały użytkowników, że nie ma już więcej nowych treści. Teraz jednak, nawet po zobaczeniu wszystkich aktualizacji od znajomych, serwisy proponują „nowe” treści, które mogą Cię zainteresować – rolki, memy, reklamy. Bardzo łatwo stracić wówczas poczucie czasu i spędzić godziny na scrollowaniu, prawda?



## Jak to działa?

Platformy społecznościowe używają algorytmów, które na bieżąco analizują co lubisz, w co klikasz, czemu poświęcasz najwięcej uwagi. Dzięki temu mogą proponować Ci treści, które najprawdopodobniej przyciągną Twoją uwagę. To trochę jak gra, która nie ma końca i ciągle oferuje nowe poziomy, wyzwania, nagrody. Ma to swoje dobre i złe strony. Załóżmy, że jesteś fanem wyczynowej jazdy na rowerze, chcesz więc oglądać filmiki, związane z rowerami, sportowcami, wyposażeniem rowerowym, a nie na przykład amatorskim gotowaniem koreańskich potraw. Algorytm dba o to, by zapewnić Ci dostęp do interesujących treści, ale powoduje także, że możesz spędzić w mediach społecznościowych więcej czasu niż planowałeś.

# Dowiedz się więcej!

Aby zrozumieć, jaki jest związek między dopaminą a naszymi aktywnościami online, obejrzyj film „DOPAMINA” przygotowany przez Fundację Dajemy Dzieciom Siłę.



Czy panujesz nad tym, jak i kiedy korzystasz z internetu?

## Pytania kontrolne

1. Czy rezygnujesz z ważnych obowiązków, żeby spędzić więcej czasu online? **TAK/NIE**
2. Czy korzystasz z internetu, by poprawić sobie humor? **TAK/NIE**
3. Czy potrzebujesz coraz więcej czasu online, żeby czuć satysfakcję? **TAK/NIE**
4. Czy szukasz nowych form rozrywki online, gdy te, które wcześniej lubiłeś, już Cię nie cieszą? **TAK/NIE**
5. Czy czujesz irytację, gdy nie możesz korzystać z internetu? **TAK/NIE**
6. Czy twoje samopoczucie pogarsza się, gdy musisz ograniczyć czas spędzany online? **TAK/NIE**
7. Czy kłócisz się z rodziną o czas spędzany w internecie? **TAK/NIE**
8. Czy zaniedbujesz obowiązki szkolne, żeby spędzać więcej czasu online? **TAK/NIE**
9. Czy próbowałeś ograniczyć korzystanie z internetu, ale wracasz do starych nawyków? **TAK/NIE**
10. Czy mimo świadomości negatywnych skutków nie potrafisz ograniczyć czasu online? **TAK/NIE**

Na podstawie Griffiths (1996) i Young (1998).

Zastanów się, jak czujesz się ze swoimi odpowiedziami. Na ile pytań odpowiedziałeś twierdząco? Jeśli masz wrażenie, że bycie online zaczyna mieć negatywny wpływ na Twoje życie, porozmawiaj z kimś, komu ufasz. Może to być rodzic, nauczyciel, psycholog szkolny czy inna dorosła osoba, która może Ci pomóc. Możesz też porozmawiać ze swoim przyjacielem.



# 10 wskazówek dotyczących higieny cyfrowej



Zacznij od obserwacji. Przyjrzyj się, jak korzystasz z telefonu przez cały tydzień. Zastanów się, jak to wpływa na Twoją codzienność.



Porozmawiaj o cyfrowym stresie z przyjaciółmi i rodziną. Podziel się swoimi doświadczeniami i posłuchaj ich rad.



Zaplanuj cyfrowy detoks. Wybierz czas na inne aktywności, które lubisz, aby zrobić sobie przerwę od ekranów.



Wyłącz niepotrzebne powiadomienia z aplikacji. To pomoże Ci skupić się na rzeczach ważniejszych niż ciągłe dźwięki przychodzących alertów.



Zrób porządk w swoich kontaktach w mediach społecznościowych. Nie musisz być na bieżąco ze wszystkimi newsami. Obserwuj profile, które sprawiają, że czujesz się dobrze i które wnoszą wartościowe dla Ciebie informacje.



Dostosuj ustawienia prywatności na swoich profilach, aby lepiej chronić swoje dane.



Wyłącz autoodtwarzanie na platformach streamingowych, aby uniknąć binge-watching'u.



Sprawdź aplikację, która informuje o czasie spędzonym przed ekranem i zastanów się, co jeszcze możesz dostosować, aby lepiej dbać o swoją równowagę cyfrową. Możesz poszukać aplikacji o nazwie „Cyfrowy Dobrostan” lub sprawdzić to w ustawieniach telefonu, wyszukując hasło „Czas przed ekranem”



Ćwicz bycie „tu i teraz”. Może zaczniesz od prostych ćwiczeń oddechowych, które pomogą Ci skoncentrować się na chwili obecnej?



Pomagaj innym dbać o cyfrowy dobrostan. Dziel się swoimi doświadczeniami i technikami, które pomogą innym zadbać o zdrowe nawyki online.

# Przykładowe działania, które może zorganizować Twój CYBERspot



- **Dzień Bez Smartfona.** Zaproponuj w swojej klasie lub szkole spędzenie jednego dnia bez telefonów. To świetna okazja, aby zobaczyć jak obecność smartfonów (lub ich brak) wpływa na nasze interakcje, koncentrację i ogólne samopoczucie.
- **Warsztaty z higieny cyfrowej.** Zorganizuj warsztaty na temat zdrowych nawyków korzystania z technologii. Możesz zaprosić do nich zewnętrznych ekspertów lub przeprowadzić własną lekcję korzystając z naszych scenariuszy lekcji uczeń-uczniowi -> <https://www.spokojnamlodosc.pl/scenariusz/cyfrowy-dobrostan/>

## Sprawdź to!

- Scenariusz lekcji uczeń-uczniowi <https://www.spokojnamlodosc.pl/scenariusz/cyfrowy-dobrostan/>
- Film „Dopamina” – [https://www.youtube.com/watch?v=Am71yBIS\\_ZQ&t=5s](https://www.youtube.com/watch?v=Am71yBIS_ZQ&t=5s)
- Artykuł „Doomscrolling. 10 rad jak radzić sobie z natłokiem negatywnych informacji” [https://cyberprofilaktyka.pl/blog/1/doomscrolling-10-rad-jak-radzic-sobie-z-natlkiem-negatywnych-informacji\\_i31.html](https://cyberprofilaktyka.pl/blog/1/doomscrolling-10-rad-jak-radzic-sobie-z-natlkiem-negatywnych-informacji_i31.html)
- Artykuł „Cyfrowy dobrostan – jak osiągnąć równowagę i kształtować zdrowe nawyki” [https://cyberprofilaktyka.pl/blog/cyfrowy-dobrostan-jak-osiagnac-rownowage-i-ksztaltowac-zdrowe-nawyki\\_i30.html](https://cyberprofilaktyka.pl/blog/cyfrowy-dobrostan-jak-osiagnac-rownowage-i-ksztaltowac-zdrowe-nawyki_i30.html)
- Poradnik „Jak osiągnąć cyfrowy dobrostan” <https://cyberprofilaktyka.pl/publikacje/poradnik-cyfrowy-dobrostan.pdf>
- Raport z badań NASK „Nastolatki 3.0” <https://www.nask.pl/pl/aktualnosci/5316.Co-robia-nasze-dzieci-w-sieci-czyli-Raport-z-najnowszego-badania-NASK-Nastolatki.html>



## Literatura cytowana:

1. Griffiths, M. D. (1996). Behavioural addictions: An issue for everybody? *Journal of Workplace Learning*, 8(3), 19-25.
2. Lange, R. (Red.), Wrońska, A., Ładna, A., Kamiński, K., Błażej, M., Jankiewicz, A., & Roślaniec, K. (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów i rodziców*. Thinkstat NASK i OSE <https://www.nask.pl/pl/raporty/raporty/5315.Raport-quotNastolatki-30quot.html>
3. Young, K. S. (1998). Internet addiction: The emergence of a new clinical disorder. *CyberPsychology & Behavior*, 1(3), 237–244.

## Rozdział 2: Cyberprzemoc

Internet przynosi nam wiele korzyści, ale naraża także na niebezpieczeństwa. Jednym z nich jest cyberprzemoc. W tej części dowiesz się czym jest cyberprzemoc, co mówią o tym zjawisku badania, a także dlaczego powstaje, jak ją powstrzymać i gdzie szukać wsparcia.



### Słowniczek

#### Cyberprzemoc –

czyli agresywne zachowania i działania w sieci. Można także spotkać się cyberbulling, dręczenie, nękanie czy prześladowanie w internecie. Jej formy są zróżnicowane, np.: agresja słowna, upublicznianie upokarzających zdjęć i filmików, wykluczanie z grona znajomych online, szantaż. Jej sprawcy czują się zwykle bezkarni i mają pozorne poczucie anonimowości.

#### Hejt –

(ang. hate – *nienawidzić*), silna antypatia wobec kogoś lub czegoś, obrażanie, poniżanie czy wyśmiewanie innych. Komentarze o negatywnym charakterze są publikowane najczęściej na forach czy w mediach społecznościowych. Hejt jest jedną z form cyberprzemocy, a doświadczycy go może każdy, niezależnie od wieku, pozycji społecznej, popularności.

#### Świadek / obserwator cyberprzemocy –

to osoba, która obserwuje jakąś formę cyberprzemocy i może zachować się różnie, wobec tego zjawiska i osób z nim związanych. Jeśli świadek np. lajkuje przesmiewcze treści, udostępniania dalej upokarzające materiały, to przylacza się do sprawcy i wzmacnia jego działania, a tym samym potęguje ból ofiary jej poczucie osamotnienia, braku wsparcia w grupie, bycia przeciwko niej. Bierno przyglądanie się cyberprzemocy może również ją nasilić, ponieważ sprawca odbiera to jako ciche przyzwolenie na swoje działania. Świadek, który aktywnie wstawia się za ofiarą, zwiększa szansę na skuteczne wsparcie osoby doświadczającej i przerwanie cyberprzemocy.

#### Osoba doświadczająca cyberprzemocy –

to ktoś, kto stał się obiektem przemocy w internecie. Często przyjmuje bierną postawę wobec zjawiska, lub nie jest w stanie jednoznacznie stwierdzić, że doświadcza przemocy (zaprzeczenie, racjonalizacja). Osoby doświadczające mogą reagować: bezsilnością, lękiem, poczuciem zranienia, wstydem, osamotnieniem, utratą zaufania, bezradnością, gniewem itp. Zdarza się, że usprawiedliwiają zachowania osoby stosującej przemoc, aby przetrwać.

#### Hejter /sprawca cyberprzemocy –

osoba atakująca inne osoby w internecie, nie ma znaczenia stopień znajomości. Zarówno znajomy ze szkoły, jak i obcy użytkownik, może rozpocząć atak. Hejter w poczuciu anonimowości i bez głębszej refleksji inicjuje i realizuje swoje działania, gdyż jest żądny uwagi odbiorców.

#### Ważne!

Treści publikowane w internecie zawsze pozostawiają cyfrowy ślad – także te komentarze, które zostają szybko skasowane.

#### Happy slapping –

o tym zjawisku mówimy, gdy przypadkowa osoba zostaje zaatakowana nieoczekiwanie, a całe zajście jest nagrywane, najczęściej smartfonem. Cel twórcy to zasięgi i kliknięcia.

#### Wykluczenie –

nieoczywistą formą cyberprzemocy jest sytuacja, w której atakowana osoba jest nieświadoma, że stała się obiektem cyberprzemocy. Jest to możliwe, gdy utworzona zostaje grupa celowo bez tej osoby w składzie, a pominięcie jej ma na celu stworzenie przestrzeni do swobodnej obnowy itp.

Źródło: Poradnik „ABC cyberbezpieczeństwa”,  
NASK-PIB, 2022 r.

# Jak walczyć z cyberprzemocą?



Znasz już najważniejsze definicje związane z cyberprzemocą. Wiesz, że brak reakcji jedynie wzmacnia działania sprawcy i zwiększa cierpienie ofiary. Jako CYBERSpot nie jesteście jednak bezradni! Istnieją działania i narzędzia, które mogą Wam pomóc w walce z cyberprzemocą – zarówno wtedy, gdy dotyczy ona Was, jak i Waszych kolegów czy koleżanek.

## Najskuteczniejsze formy walki z cyberprzemocą to:

- zgłaszanie jej do administratorów portali społecznościowych, którzy mają w obowiązku usuwać materiały naruszające ich regulamin;
- zwrócenie się jawnie o pomoc do wychowawców, opiekunów/rodziców i innych zaufanych dorosłych, a także anonimowo np. za pomocą telefonu zaufania;
- próba przekonania sprawcy do zaprzestania krzywdzących, przemocowych działań i otwarty sprzeciw.

## Prawo



W przepisach prawnych nie funkcjonuje odrębne pojęcie cyberprzemocy, jednak poszczególne jej formy mogą stanowić czyn niedozwolony w świetle prawa karnego i cywilnego.

Część aktów agresji w internecie traktuje się w odniesieniu do Kodeksu karnego jako przestępstwa. Można do nich zaliczyć: znieważanie, zniesławienie, włamanie informatyczne, groźby, nękanie – stalking.



# Pamiętaj!



**Rozmawiajcie** na temat przemocy w sieci, hejtu i mowy nienawiści.

Jako CYBERSpot upewnijcie się czy w Waszej szkole istnieją spisane procedury działania w przypadku wykrycia cyberprzemocy. Jeśli tak, możecie zadbać o promocję tej procedury wśród innych uczniów. Jeśli nie, możecie zgłosić potrzebę wypracowania takiej procedury przez szkołę.



**Dzielcie się informacją** o możliwości skorzystania z bezpłatnych, anonimowych telefonów zaufania dla dzieci i młodzieży.



**Zgłaszajcie** do administratorów i do zespołu Dyżurnet.pl strony zawierające mowę nienawiści.

**Uwaga:** Jeśli zgłosi się do Was osoba, która jest świadkiem lub osobą doświadczającą cyberprzemocy pamiętajcie, żeby przekierować tę osobę do właściwego nauczyciela, psychologa lub pedagoga szkolnego.

## 116 111 – TELEFON ZAUFANIA DLA DZIECI I MŁODZIEŻY

Bezpłatny i anonimowy telefon dla dzieci i młodzieży prowadzony przez Fundację Dajemy Dzieciom Siłę. Telefon działa codziennie – 7 dni w tygodniu, 24 godziny na dobę. Dzieci i młodzież mogą także zarejestrować się na stronie internetowej i napisać wiadomość do konsultantów pełniących dyżur online. Więcej informacji na stronie <https://116111.pl/>.

## 800 12 12 12 – DZIECIĘCY TELEFON ZAUFANIA RZECZNIKA PRAW DZIECKA

Bezpłatna działająca całodobowo telefoniczna linia interwencyjna dla dzieci i młodzieży. Osoby dorosłe mogą zgłaszać problemy dzieci lub rażące zaniedbania względem nich. Telefon działa codziennie – 7 dni w tygodniu, 24 godziny na dobę. Więcej informacji na stronie <https://brpd.gov.pl/telefon-zaufania>.

## DYŻURNET.PL

Zespół ekspertów NASK, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Zgłoszenia o potencjalnie nielegalnych treściach można przekazywać za pomocą formularza, na adres e-mailowy. Szczegółowe informacje można znaleźć na stronie <https://dyzurnet.pl/>.

Niektóre serwisy posiadają rozbudowany system wsparcia dla użytkowników i zgłaszania nadużyć:

-  Centrum Pomocy Facebooka: Facebook – Centrum pomocy
-  Centrum Pomocy Google: Google – Pomoc
-  Centrum Pomocy YouTube: YouTube – Pomoc (google.com)
-  X (Twitter): Zasady X: bezpieczeństwo, prywatność, autentyczność – i wiele więcej
-  Instagram: Centrum pomocy Instagramu
-  Centrum Pomocy TikTok: TikTok Help Center

# Przykładowe działania, które może zorganizować Twój CYBERspot

Upowszechnianie w szkole działań CYBERspotu, w tym przeciw cyberprzemocy. To propozycja przeprowadzenia w szkole **dnia poświęconego cyberprofilaktyce**. Można wykorzystać różne dostępne w szkole możliwości: radiowęzeł, stoisko na przerwie, plakaty, zaproszenie gościa zewnętrznego itp. Warto poruszyć temat hejtu, czy przedstawić szkolną procedurę reagowania.

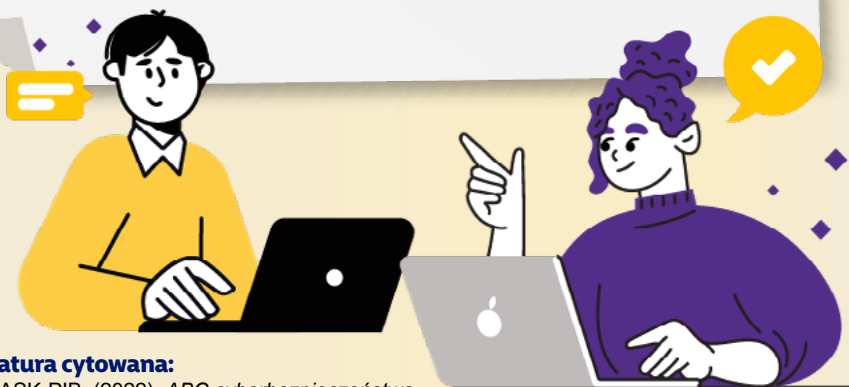
**Konkurs szkolny** na hasło przeciw cyberprzemocy, które pojawi się np. w gablocie, na stronie szkoły itp. Może być przeprowadzony w okolicy Międzynarodowego Dnia Przeciwdziałania Przemocy i Nękanii w Szkole w tym Cybernękaniu. Jest to stosunkowo nowe święto. Zostało ustanowione przez Konferencję Generalną UNESCO dopiero w 2019 r., obchodzone w pierwszy czwartek listopada.

Zorganizowanie z nauczycielem **profilaktycznej lekcji** nt. cyberprzemocy (można skorzystać z dostępnych scenariuszy – Cyberlekcje 3.0).

**Spotkanie z dyrektacją szkoły lub Radą Rodziców** na temat procedury cyberprzemocy w szkole. Możecie skonsultować procedurę, zebrać przemyślenia swoich rówieśników i zaprezentować je tym grupom. Ważne, aby to był dialog wszystkich zainteresowanych stron (dyrekcji, nauczycieli, rodziców, młodzieży).

## Sprawdź to!

- Artykuł: Trzy role, dwa trójkąty, jedno błędne koło - wielowymiarowe aspekty hejtu [https://cyberprofilaktyka.pl/blog/trzy-role-dwa-trojkaty-jedno-bledne-kolo---wielowymiarowe-aspekty-hejtu\\_i43.html](https://cyberprofilaktyka.pl/blog/trzy-role-dwa-trojkaty-jedno-bledne-kolo---wielowymiarowe-aspekty-hejtu_i43.html)
- Artykuł: Cyberprzemoc – czym jest i jak rozmawiać o niej z dzieckiem? [https://cyberprofilaktyka.pl/blog/cyberprzemoc--czym-jest-i-jak-rozmawiac-o-niej-z-dzieckiem\\_i27.html](https://cyberprofilaktyka.pl/blog/cyberprzemoc--czym-jest-i-jak-rozmawiac-o-niej-z-dzieckiem_i27.html)
- Filmik o cyberprzemocy dla klas 4-6: <https://www.youtube.com/watch?v=F5B5E9yAWYI>
- Filmik dla szkół ponadpodstawowych: #HejtOFF - Razem przeciwko hejtowi! <https://www.youtube.com/watch?v=fHIW32qJx2k>
- Filmik dla klas 7-8 i ponadpodstawowych: Program IMPACT - Lekcja 8 – Hejt <https://www.youtube.com/watch?v=w1dcGHx8VX0>
- Playlista filmików z kampani “Przerwij krąg przemocy”: [https://youtu.be/iDwR1hqLA\\_o?si=p2GVjh\\_bnAUBdksA](https://youtu.be/iDwR1hqLA_o?si=p2GVjh_bnAUBdksA)
- Materiały do Cyberlekcji 3.0: <https://www.gov.pl/web/baza-wiedzy/materiały-do-cyberlekcji-30>
- Projekt SELMA: <https://www.saferinternet.pl/materiały-edukacyjne/selma---pokonaj-hejt.html>
- Program IMPACT: <https://edukacja.fdds.pl/course/view.php?id=351>



### Literatura cytowana:

1. NASK-PIB. (2022). *ABC cyberbezpieczeństwa*.
2. NASK-PIB. (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów*.
3. Pyżalski, J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży*. Kraków: Impuls.
4. Walrave, M., & Heirman, W. (2009). Skutki cyberbullyingu – oskarżenie czy obrona technologii? *Dziecko krzywdzone. Teoria, badania, praktyka*, 8(1), 27–46.
5. UNICEF. (2023). Czym jest cyberbullying i jak go powstrzymać? Czym jest cyberbullying i jak go powstrzymać [unicef.pl]. Pobrano 29.10.2024 z <https://unicef.pl>

# Rozdział 3: Jak dbać o prywatność i wizerunek w internecie?



## Słowniczek

### Biały wywiad (OSINT) –

zbieranie i analiza informacji dostępnych publicznie, np. w mediach społecznościowych, na stronach internetowych, na forach czy w rejestrach publicznych, które cyberprzestępcy mogą wykorzystać do swoich działań.



### Cyfrowy ślad –

wszystkie ślady, które pozostawiamy w sieci, korzystając z różnych usług online, takich jak media społecznościowe, wyszukiwarki czy aplikacje. Cyfrowy ślady to zdjęcia, posty, komentarze czy każda inna aktywność w internecie.



### Ataki socjotechniczne –

Ataki socjotechniczne to metody, które polegają na manipulowaniu ludźmi w celu zdobycia ich prywatnych informacji, takich jak hasła czy dane osobowe. Oszuści często podszywają się pod zaufane osoby lub instytucje, aby wzbudzić zaufanie i nakłonić ofiarę do ujawnienia danych.

### Profilowanie –

proces analizowania danych osobowych oraz aktywności online w celu tworzenia profilu użytkownika, stosowany na przykład w reklamie spersonalizowanej.





# Czy wiesz, że...?



Zapewne, tak jak większość Polaków (94 proc. ankietowanych wg badania Serwisu ChronPESEL.pl i Krajowego Rejestru Długów), wiesz, że ochrona prywatności w sieci to poważna sprawa. Co ciekawe, bardziej ostrożne w tej kwestii są kobiety. Aż 25% ankietowanych zgodziłoby się udostępnić dane osobowe w zamian za dodatkowe korzyści, a 69 % młodych ludzi (18-24 lata) zdecydowałoby się udostępnić dane za darmowy produkt lub usługę. Czy na pewno taka okazja byłaby tego warta? Czy zdajesz sobie sprawę, że takie dane mogłyby ulec wyciekowi? Co mogą wtedy zrobić z nimi cyberprzestępcy?



## Jakie zagrożenia wiążą się z utratą prywatności w sieci?

Zapewne, tak jak większość Polaków (94 proc. ankietowanych wg badania Serwisu ChronPESEL.pl i Krajowego Rejestru Długów), wiesz, że ochrona prywatności w sieci to poważna sprawa. Co ciekawe, bardziej ostrożne w tej kwestii są kobiety. Aż 25% ankietowanych zgodziłoby się udostępnić dane osobowe w zamian za dodatkowe korzyści, a 69 % młodych ludzi (18-24 lata) zdecydowałoby się udostępnić dane za darmowy produkt lub usługę. Czy na pewno taka okazja byłaby tego warta? Czy zdajesz sobie sprawę, że takie dane mogłyby ulec wyciekowi? Co mogą wtedy zrobić z nimi cyberprzestępcy?

## Kradzież tożsamości



Gdy publikujesz swoje zdjęcia, lokalizację lub informacje o sobie, mogą one trafić w niepowołane ręce. Oszuści mogą stworzyć fałszywe profile, podszywać się pod Ciebie, a nawet korzystać z Twoich danych w celu zaciągnięcia pożyczki na Twoje nazwisko.

## Biały wywiad (OSINT) – jak cyberprzestępcy wykorzystują dostępne dane?

Platformy społecznościowe używają algorytmów, które na bieżąco analizują co lubisz, w co klikasz, czemu poświęcasz najwięcej uwagi. Dzięki temu mogą proponować Ci treści, które najprawdopodobniej przyciągną Twoją uwagę. To trochę jak gra, która nie ma końca i ciągle oferuje nowe poziomy, wyzwania, nagrody. Ma to swoje dobre i złe strony. Załóżmy, że jesteś fanem wyczynowej jazdy na rowerze, chcesz więc oglądać filmiki, związane z rowerami, sportowcami, wyposażeniem rowerowym, a nie na przykład amatorskim gotowaniem koreańskich potraw. Algorytm dba o to, by zapewnić Ci dostęp do interesujących treści, ale powoduje także, że możesz spędzić w mediach społecznościowych więcej czasu niż planowałeś.

## Deepfake

Technologia deepfake, która umożliwia tworzenie realistycznych, ale całkowicie fałszywych obrazów i nagrań wideo, może być również wykorzystana do manipulowania Twoim wizerunkiem. Wystarczy kilka zdjęć lub nagrań wideo z Twojego profilu, aby stworzyć fałszywe materiały, które mogą zaszkodzić Twojej reputacji. Uwaga na wysyłane głosówki – jeżeli cyberprzestępca włamie się na konto Twojego znajomego i znajdzie tam pliki głosowe, może je wykorzystać do stworzenia fałszywej wiadomości.

## Zastanów się również nad kwestią kreowania fałszywego wizerunku w sieci.



W mediach społecznościowych, wielu influencerów kreuje swój wizerunek, który często nie odzwierciedla tego, kim są naprawdę. Wyidealizowany wizerunek może wynikać z presji społecznej, chęci zaimponowania innym lub dostosowania się do popularnych trendów. Publikowanie idealizowanych zdjęć, podkolorowanych historii czy zmienionych faktów może prowadzić do tworzenia iluzji, która nie ma odzwierciedlenia w rzeczywistości. Takie działania niosą jednak za sobą pewne zagrożenia, szczególnie dla młodych ludzi.

U obserwatorów, szczególnie nastolatków, może to wywołać nierealistyczne oczekiwania wobec własnego wyglądu, co prowadzi do zaburzeń związanych z obrazem ciała, takich jak anoreksja czy bulimia, a także do ogólnego niezadowolenia z siebie.

Zdarza się, że influencerzy promują produkty lub usługi w zamian za wynagrodzenie. Jest to forma reklamy. Możemy przez to myśleć, że polecają dany produkt, bo go faktycznie cenią, a nie dlatego, że są za to opłacani. Zwracaj uwagę, na to czy w komunikacie pojawia się informacja o współpracy lub materiale sponsorowanym. Podejmuj swoje decyzje zakupowe w oparciu o różne źródła, a nie tylko przekaz ulubionego influencera.



Fałszywy wizerunek w sieci może być równie szkodliwy dla samych twórców. Utrzymywanie nieautentycznej wersji siebie, kreowanie idealnego życia i nieustanne porównywanie się z innymi może prowadzić do wypalenia, stresu, depresji i poczucia osamotnienia.



# Wskazówki, jak chronić swoją prywatność i wizerunek w sieci



**Sprawdź ustawienia prywatności w mediach społecznościowych** – upewnij się, że Twoje posty i zdjęcia są widoczne tylko dla wybranych osób.



**Zastanów się, zanim coś opublikujesz** – zawsze pytaj siebie, czy ta treść powinna być publiczna i jakie konsekwencje może mieć jej udostępnienie.



**Nie udostępniaj szczegółowych informacji osobowych** – unikaj publikowania takich danych jak adres, numer telefonu, a także informacji o Twoich bliskich.



**Korzystaj z pseudonimów w serwisach, które nie wymagają podawania prawdziwych danych** – nie musisz wszędzie używać swojego pełnego imienia i nazwiska.



**Dbaj o długie i silne hasła, oddzielne dla każdego konta** – hasło powinno zawierać co najmniej 14 znaków, może składać się z kilku losowych słów, ale nie powinno tworzyć znanego cytatu.



**Tam, gdzie to możliwe korzystaj z weryfikacji dwuetapowej** – zabezpieczaj konta dodatkową warstwą ochrony, jak weryfikacja dwuetapowa (2FA).



**Zgłaszaj nieprawidłowości** – jeśli zauważysz, że ktoś nielegalnie wykorzystuje Twoje dane lub wizerunek, zgłoś to administratorowi strony oraz odpowiednim służbom.



**Myśl krytycznie** – nie wszystko, co jest prezentowane w sieci jest prawdziwe! Zastanów się dwa razy, zanim uwierzysz w to, co widzisz i staraj się podchodzić krytycznie do treści online. Nie porównuj się do innych w sieci – pamiętaj, że media społecznościowe to często wyidealizowana wersja życia.

# Przykładowe działania, które może zorganizować Twój CYBERspot

**Warsztaty z ochrony wizerunku** Zorganizuj warsztaty w szkole, podczas których Twój koleś dowiedzą się, jakie zasady obowiązują w ochronie wizerunku oraz jakie są konsekwencje nieostrożnego udostępniania swoich danych w sieci. Skorzystaj z poradnika [\(Nie\)widzialne ślady online](#).

**Debata na temat prywatności online** Zorganizuj debatę na temat „Czy powinniśmy obawiać się śladu cyfrowego?”. Uczestnicy będą mogli przygotować argumenty za i przeciw, co zachęci ich do krytycznego myślenia o prywatności w sieci oraz konsekwencjach niewłaściwego korzystania z internetu.



## Wystawa „Rzeczywistość vs. Media społecznościowe”

Stwórz fizyczną lub wirtualną wystawę, na której pokazane będą porównania zdjęć „przed” i „po” obróbkę graficznej lub edytorskiej. Zaznacz, że niektórzy influencerzy publikują takie zdjęcia bez porównania.

## Sprawdź to!

- Poradnik dla nastolatków [\(Nie\)widzialne ślady online](#)
- Artykuł „Dwuetałowa weryfikacja - czemu warto ją włączyć i jak to zrobić” [https://cyberprofilaktyka.pl/blog/dwuetałowa-weryfikacja--czemu-warto-ja-wlaczyc-i-jak-to-zrobic\\_i45.html](https://cyberprofilaktyka.pl/blog/dwuetałowa-weryfikacja--czemu-warto-ja-wlaczyc-i-jak-to-zrobic_i45.html)
- Artykuł „Deepfake: jak sztuczna inteligencja może nas oszukiwać?” [https://cyberprofilaktyka.pl/blog/deepfake-jak-sztuczna-inteligencja-moze-nas-oszukiwac\\_i40.html](https://cyberprofilaktyka.pl/blog/deepfake-jak-sztuczna-inteligencja-moze-nas-oszukiwac_i40.html)
- Zalecenia CERT Polska <https://cert.pl/bezpieczne-hasla/>
- Biuletyn OUCH! CERTu <https://cert.pl/ouch/>

## Literatura cytowana:

1. Badanie na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych (UODO) pt. „Czy Polacy są gotowi udostępnić dane osobowe w zamian za dodatkowe korzyści?”, przeprowadzone w kwietniu 2024 r.



## Rozdział 4: Nie daj się dezinformacji!

Nastolatki spędzają w internecie średnio 5 godzin i 36 minut dziennie<sup>1</sup>. Ich stały kontakt z różnymi treściami w mediach społecznościowych zwiększa ryzyko kontaktu z dezinformacją. W tym rozdziale chcemy wyjaśnić Wam to zjawisko i zaproponować sposoby na obronę przed nim.



### Czym jest dezinformacja?

Dezinformacja to fałszywa bądź wprowadzająca w błąd treść, która jest celowo, intencjonalnie tworzona lub rozpowszechniana z zamiarem oszukania odbiorców bądź pozyskania określonych korzyści, np. ekonomicznych, politycznych, społecznych<sup>2</sup>. Może wyrządzić szkodę zarówno jednostkom, grupom, organizacjom, jak i krajom. Podsumowując - dezinformacja jest celowa, wprowadza odbiorców w błąd i ma przynieść konkretne korzyści.

### Czy wiesz że...?



Ponad 40% badanych twierdzi, że w internecie nie można odróżnić informacji prawdziwych od fałszywych. Jest to niepokojąca liczba, biorąc pod uwagę liczbę postów, które codziennie są wyświetlane przez młodych odbiorców.



Tylko około połowa nastolatków interesuje się wiarygodnością profili i autorów, których obserwują na portalach społecznościowych – wielu z nich nie sprawdza więc, kto i w jakim celu tworzy i udostępnia treści, które oglądają, czytają i komentują.



Dla co trzeciego nastolatka przekazywanie informacji przez wiele osób oraz liczne źródła medialne jednocześnie, to kryteria jej wiarygodności, przez co wzrasta ich podatność na kampanie dezinformacyjne.

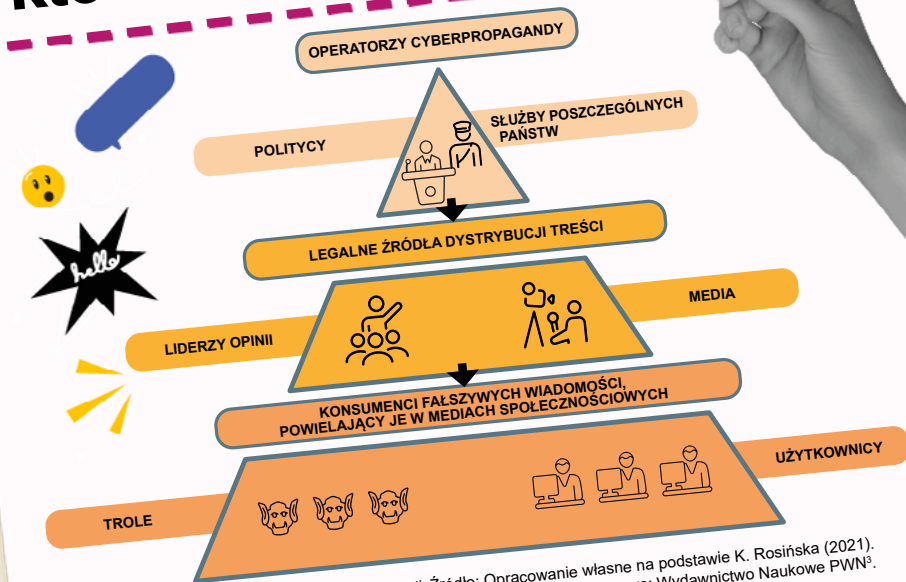


Tylko blisko 29% badanych obawia się dezinformacji, co może wskazywać na niską świadomość zagrożeń, jakie niesie dezinformacja i na konieczność intensyfikacji działań profilaktycznych w tym obszarze.

1. NASK-PIB (2023). Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów, <https://www.nask.pl/pl/aktualnosci/5316-Co-robia-nasze-dzieci-w-sieci-czyli-Raport-z-najnowszego-badania-NASK-Nastolatki.html>.

2. Kwiatkowska, A., Kosowska, Z., Oleszkiewicz, K., Adamczyk, S., Przemyska, P. (2023). Era (dez)informacji. Praktyczny poradnik dla kadry nauczycielskiej. NASK – Państwowy Instytut Badawczy.

# Kto nas dezinformuje?



Piramida kategorii twórców dezinformacji. Źródło: Opracowanie własne na podstawie K. Rosińska (2021). Fake news. Geneza, istota, przeciwdziałanie, Warszawa: Wydawnictwo Naukowe PWN<sup>3</sup>.

Dezinformować nas mogą zarówno konkretni ludzie, jak i całe instytucje, grupy czy organizacje. Wśród nich wymienić można m.in.:

- **Służby specjalne różnych krajów**, które mogą prowadzić operacje wywierania wpływu poprzez zakłócanie procesów politycznych i gospodarczych oraz próbę zaburzenia poczucia bezpieczeństwa. Wydawać by się mogło, że nie dotyczą nas takie działania, ale jest zupełnie odwrotnie. Pozornie niewinne, ale mające charakter dezinformacyjny, posty w mediach społecznościowych mogą być częścią szeroko zakrojonych kampanii dezinformacyjnych.
- **Polityków**, którzy mogą być źródłem dezinformacji poprzez np. posługiwanie się nierzetelnymi danymi lub wykorzystywanie nieprawdziwych informacji jako narzędzi wpływu politycznego.
- **Media** też mogą dezinformować poprzez publikowanie niesprawdzonych lub nie w pełni zweryfikowanych informacji.
- **Liderów opinii** jako osoby, które mają duży wpływ na poglądy, postawy i zachowania innych ludzi. W naszym przypadku są to najczęściej influencerzy. Nie jest tak, że każdy z nich wprowadza w błąd, ale warto zachować szczególną ostrożność. W niektórych przypadkach influencerzy rozprzestrzeniają nieprawdziwe przekazy nieintencjonalnie, ale mogą także tworzyć je świadomie, ukrywając własne motyw i interesy.
- **Trolle**, czyli użytkowników, którzy publikują złośliwe lub nieprawdziwe informacje. Mają oni na celu wywołać negatywne reakcje, zakłócić dyskusje lub manipulować opinią publiczną i społecznymi nastrojami.

3. Za: L. Gu, V. Kropotov, F. Yarochkin (2017). *The fake news machine: How propagandists abuse the Internet and manipulate the public*. [dostęp: 29.03.2024].



# Czy jesteście dezinformatorami?

Każdy użytkownik internetu może stać się źródłem dezinformacji – nawet w sposób niezamierzony. Czego więc unikać, by nie stać się narzędziem w rękach manipulatorów?



Nie wierz we wszystko od razu, lecz przeanalizuj intencje osoby lub grupy, która opublikowała dany post.



Nie udostępniaj niesprawdzonych informacji, żeby nie przyczyniać się do ich uwiarygodnienia.



Nie wchodź w interakcje z fałszywymi i szkodliwymi treściami, np. poprzez komentowanie lub zostawianie reakcji. W przeciwnym razie trafią one do większej liczby odbiorców.



## Kompetencje medialne w walce z dezinformacją

Pod pojęciem kompetencji medialnych kryje się zdolność do rozumienia, analizowania, oceny i tworzenia przekazów medialnych<sup>4</sup>. Jedną z kluczowych umiejętności w tym obszarze jest krytyczne myślenie, które objawia się poprzez:

- umiejętność odróżniania faktów od opinii;
- logiczne i obiektywne ocenianie informacji;
- analizę argumentów i dowodów.

## Jak weryfikować informacje?

- Widzisz emocjonalny nagłówek lub szokującą informację? Poszukaj informacji w innym źródle. Często wystarczy skorzystać z przeglądarki, by znaleźć artykuł portalu fact-checkingowego, który tłumaczy, że mamy do czynienia z nieprawdziwą treścią.
- Spotykasz się z zaskakującymi danymi? Przeczytaj więcej o samym badaniu, dowiedz się, co w tym obszarze mówią inni badacze.
- Influencer wypowiada się na ważne tematy np. zdrowotne? Sprawdź jakie ma doświadczenie i wiedzę dot. konkretnej sprawy. Odróżniaj fakty od opinii.
- Widzisz podejrzanе zdjęcia, filmy lub grafiki? W procesie weryfikacji obrazów przydatne mogą okazać się narzędzia, takie jak:



### Wyszukiwanie obrazem Google

Odwrócone wyszukiwanie pozwala odnaleźć źródła zdjęcia.



### FotoForensics

Narzędzia do wykrywania manipulacji cyfrowej przy zdjęciu.



### AlorNot

Serwis weryfikujący, czy obraz został wygenerowany przy pomocy AI.

NASK-PIB nie ponosi odpowiedzialności za skuteczność podanych narzędzi. Są one zarządzane przez zewnętrznych usługodawców.

4. G. Ptaszek (2014). *Pomiar indywidualnych kompetencji medialnych*. Pytania i problemy, „Kultura Popularna” 3 (41).

# Zasada 5Z. Czyli jak samodzielnie weryfikować informacje?

Umiejętność krytycznego myślenia jest kluczowa w procesie weryfikacji informacji. Z pomocą przychodzi także zasada 5xZ. Wskazuje ona na pięć prostych sposobów oceny wiarygodności treści:

1. **Z**weryfikuj, czy źródło informacji jest wiarygodne.  
Sprawdź, czy można zaufać osobie czy portalowi, który podał informację.
2. **Z**weryfikuj rzetelność i logikę przedstawionej sytuacji.  
Zastanów się, czy opisana sytuacja ma sens i czy przywołane wydarzenia brzmią prawdopodobnie. Co podpowiada Ci zdrowy rozsądek?
3. **Z**weryfikuj, czy tę samą informację potwierdza inne źródło.  
Spędź chwilę w internecie i przekonaj się, czy tę samą wiadomość podają inne strony, które budzą zaufanie.
4. **Z**weryfikuj, co jest opinią autora, a co faktem.  
Pamiętaj, że należy odróżniać fakty od opinii, by móc samodzielnie wyciągać wnioski i formułować własne zdanie.
5. **Z**głoś podejrzenie o rozpowszechnianiu dezinformacji.

Jeśli poprzednie punkty potwierdziły Twoje obawy o dezinformację, zgłoś ją w odpowiednim miejscu, np. do portali fact-checkingowych lub administratorów serwisów społecznościowych.



AI może być wsparciem, gdy umiejętnie korzystamy z możliwości, jakie oferuje. Możecie zorganizować konkurs dla uczniów, w którym ich zadaniem będzie zobrazowanie za pomocą plakatu niebezpieczeństw, jakie czyhają na dzieci i młodzież w internecie. Prace powinny zawierać element wygenerowany przez AI, ale także hasło edukacyjne. Jako CYBERSpot możecie zorganizować w szkole głosowanie na najlepsze propozycje, a plakaty rozwinąć na korytarzach. To dobry sposób, by rozwijać umiejętności graficzne i wykorzystać sztuczną inteligencję. Możecie zaproponować wykorzystanie bezpłatnego programu Canva canva.com do tworzenia prac konkursowych. Oferuje on także możliwość stworzenia grafik przy pomocy AI. Innym, darmowym programem, który może zostać wykorzystany do tego celu jest  Microsoft Copilot <https://copilot.microsoft.com/>.

Zaproszę uczniów do wzięcia udziału w quizie. Ich zadaniem będzie wskazać, czy grafika jest wykonana przez człowieka czy wygenerowana przez sztuczną inteligencję. Deepfake, a więc stworzone przy użyciu technik sztucznej inteligencji obrazy (ale także nagrania audio, wideo) są często wykorzystywane przez twórców dezinformacji do wprowadzania odbiorców w błąd, dlatego też warto ćwiczyć rozpoznawanie tego typu grafik. Nie musicie szukać przykładów takich obrazów, możecie skorzystać z gotowego rozwiązania Microsoftu - Quiz o AI - <https://www.realnotquiz.com/>.

Jeśli jako CYBERSpot chcielibyście przeprowadzić zajęcia na temat dezinformacji, możecie sięgnąć do poradnika Era (dez)informacji, który przygotował z NASK. Poza pigułką wiedzy w poradniku znajdziecie scenariusze zajęć, a także ciekawe ćwiczenia warsztatowe.

Podręcznik znajdziecie tutaj  
<https://cyberprofilaktyka.pl/publikacje/>





**Sprawdź to!**

- Kursy online dotyczące kompetencji medialnych: <https://makeitclear.edu.pl/kursy-dla-uczniow-w-wieku-14-17-lat.html?setlng=pl>
- Gra planszowa *Digital Braniacs*: <https://makeitclear.edu.pl/materialy-edukacyjne/graplanszowa-pl.html>



### Literatura cytowana:

1. Ptaszek, G. (2014). Pomiar indywidualnych kompetencji medialnych. Pytania i problemy. *Kultura Popularna*, 3(41), 6-17.
2. NASK-PIB. (2023). Nastolatki 3.0. *Raport z ogólnopolskiego badania uczniów*. [https://www.nask.pl/pl/aktualnosci/5316\\_Co-robia-nasze-dzieci-w-sieci-czyli-Raport-z-najnowszego-badania-NASK-Nastolatki.html](https://www.nask.pl/pl/aktualnosci/5316_Co-robia-nasze-dzieci-w-sieci-czyli-Raport-z-najnowszego-badania-NASK-Nastolatki.html)
3. Gu, L., Kropotov, V., & Yarochkin, F. (2017). *The fake news machine: How propagandists abuse the Internet and manipulate the public*. [https://documents.trendmicro.com/assets/white\\_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf](https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf)
4. Kwiatkowska, A., Kosowska, Z., Oleszkiewicz, K., Adamczyk, S., & Przemyska, P. (2023). *Era (dez)informacji. Praktyczny poradnik dla kadry nauczycielskiej*. NASK – Państwowy Instytut Badawczy.





## Rozdział 5: Jak nie dać się oszukać w internecie?

Czy zastanawiał się kiedyś, jak długie musi być nagranie, żeby posłużyło przestępcy jako próbka Twojego głosu do skopiowania?



### Słowniczek



**CERT Polska** – zespół działający w strukturach NASK – Państwowego Instytutu Badawczego, zajmujący się reagowaniem na zdarzenia naruszające bezpieczeństwo w sieci.



**Cyberhigiena** – zbiór porad, które pomagają w bezpiecznym korzystaniu z internetu i urządzeń.



**Deepfake** – technologia, która umożliwia tworzenie bardzo realistycznych, ale całkowicie fałszywych obrazów, filmów i nagrań dźwiękowych.



**Głosówka** – wiadomość głosowa nagrana z użyciem komunikatorów.



**Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.



**Phishing** – rodzaj oszustwa, w którym ktoś podszywa się pod zaufany podmiot lub osobę.



**Smishing** – rodzaj oszustwa polegający na wysłaniu fałszywych wiadomości tekstowych na czyjś telefon.



**Socjotechnika** – rodzaj manipulacji, mającej za zadanie oszukać Cię i zdobyć ważne informacje, np. dane osobowe, loginy i hasła, a nawet pieniądze.





# Czy wiesz, że...?



W zeszłym roku zespół CERT Polska zarejestrował ponad 80 tysięcy unikalnych incydentów<sup>5</sup>?! Co to oznacza? Po pierwsze to, że wpływa coraz więcej zgłoszeń, co jest bardzo dobrym znakiem tego, że obywatele wiedzą, gdzie mogą zgłosić niebezpieczną wiadomość lub próbę oszustwa. Po drugie – wzrasta liczba oszustów, więc przestępcy mogą próbować dotrzeć także do Ciebie.

## Socjotechnika

Kiedy korzystasz z telefonu, komputera czy tabletu może zdarzyć się, że ktoś będzie chciał się z Tobą skontaktować. Mowa tu nie o Twoich znajomych czy bliskich, tylko o ludziach wykorzystujących socjotechnikę, czyli rodzaj manipulacji, mającej za zadanie oszukać Cię i zdobyć ważne informacje, np. dane osobowe, loginy i hasła, a nawet pieniądze.

W jaki sposób to robią? Oszuści mogą do Ciebie dzwonić lub napisać podając się za osoby, które znasz lub osoby pełniące określone funkcje, takie jak policjant, pracownik banku czy operator sieci komórkowej. Mogą żądać natychmiastowej decyzji, ponieważ pod presją czasu łatwiej popełniamy błędy. Oszuści mogą też podszyć się pod Twojego znajomego i prosić o szybki przelew BLIK.

## Oszustwa z wykorzystaniem Twojego głosu

Zdarza Ci się nagrywać głosówki zamiast pisać długie wiadomości? To bardzo dobre rozwiązanie, kiedy chcesz szybko przekazać informację drugiej osobie. Musisz jednak pamiętać o jednym – nawet kilkusekundowe nagranie, jeśli wpadnie w ręce cyberprzestępców, może zostać wykorzystane do podrabiania Twojego głosu.

## Gdzie zgłaszać?

- Podejrzane wiadomości, uporczywe telefony czy wszelkie próby oszustwa należy zgłaszać. W ten sposób chronisz siebie i innych!
- Media społecznościowe czy inne strony www, posiadają na ogół **administrатора serwisu**. Warto pamiętać o możliwości skorzystania z tej pomocy.
- Nietypową wiadomość SMS warto od razu przekazać do **CERT Polska na numer 8080**, inne zgłoszenia związane z Twoim bezpieczeństwem internetowym można przesyłać poprzez stronę: [incydent.cert.pl](https://incydent.cert.pl).
- Oszustwa z wykorzystaniem Twoich danych czy kradzież pieniędzy należy kierować do odpowiednich instytucji, np. **policji**. Jeśli nie masz ukończonych 18 lat takiego zgłoszenia może dokonać Twój opiekun.

# 10 wskazówek dotyczących bezpieczeństwa w sieci



Nie podawaj prywatnych informacji o sobie i swoich bliskich.



Sprawdź tożsamość osoby, która się z Tobą kontaktuje.



Jeśli masz wątpliwości co do telefonu lub wiadomości – porozmawiaj o tym z rodzicami, opiekunami lub nauczycielem.



Nie podejmuj decyzji pod presją czasu czy czymś naciskiem.



Nie przekazuj danych, np. imienia i nazwiska, daty urodzenia, loginów i haseł.



Nie dokonuj przelewów ani nie udostępniaj kodów BLIK osobom, których nie znasz osobiście lub nie masz pewności co do ich tożsamości. Przed każdą transakcją upewnij się, że korzystasz ze sprawdzonego źródła, np. przy zakupach online zweryfikuj sprzedawcę np. czytając opinie na jego temat.



Nie klikaj w linki i nie otwieraj załączników z niesprawdzonego źródła.



Zweryfikuj grono znajomych i obserwujących w social mediach – sprawdź, kto ma dostęp do treści, jakie publikujesz na swoich profilach społecznościowych.



Zawsze sprawdzaj adres strony internetowej, na której się znajdujesz. Czasami przestępcy podszywają się pod stronę np. banku, zmieniając jedną literkę w nazwie strony internetowej.



Nie bój się pytać, jeśli czegoś nie wiesz lub nie rozumiesz, daj sobie czas na decyzję.

# Przykładowe działania, które może zorganizować Twój CYBERSpot

## Warsztaty z cyberhigieny

Zorganizuj warsztaty na temat bezpiecznego korzystania z urządzeń. Możesz zaprosić do nich zewnętrznych ekspertów.

## Dzień z impro-cyber-higieną

Zaproponuj w swojej klasie lub szkole dzień impro. Scenki na żywo z interakcją innych osób to świetna okazja, by zobaczyć, jak może rozwinąć się rozmowa z oszustem i jak się chronić w sieci.

## Dowiedz się więcej!

Aby zrozumieć, jakie zagrożenia mogą dotknąć również Ciebie zajrzyj na stronę: [bezpiecznymiesiac.pl](https://bezpiecznymiesiac.pl)

Znajdziesz tam wiele przydatnych informacji o zagrożeniach w sieci, jak i praktycznych porad, jak się chronić. Na przykład, przeczytasz do czego wykorzystywana jest sztuczna inteligencja i deepfake i znajdziesz sposoby rozpoznawania oszustw!

### Literatura cytowana:

1. Raport roczny z działalności CERT Polska 2023, [https://cert.pl/uploads/docs/Raport\\_CP\\_2023.pdf](https://cert.pl/uploads/docs/Raport_CP_2023.pdf)

# Rozdział 6: Grooming, sexting i udostępnianie materiałów intymnych bez zgody



## Słowniczek

### Consent –

(ang. zgoda) sytuacja, w której działania podejmowane są bez żadnej presji, szantażu oraz za (świadomą) zgodą i ze świadomością konsekwencji.



### Grooming –

(ang. uwodzenie) kontakty rozpoczynane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z osobą małoletnią, prowadzące do seksualnego wykorzystania.

### Nudesy –

potoczna nazwa nagich zdjęć.



### Sexting –

seksualnie nacechowany rodzaj elektronicznej komunikacji tekstowo-wizualnej, a więc takiej, podczas której wysyłane są zdjęcia lub filmy, przedstawiające nagość bądź czynność seksualną.



### Sextortion –

sytuacja, w której ktoś wymusza na Tobie zdjęcia, filmy lub kontakty intymne za pomocą szantażu.

### NCII –

z j. angielskiego *Non-Consensual Intimate Images* - a więc intymne zdjęcia i filmy (przedstawiające nagość lub osobę w trakcie czynności seksualnej), które zostały pozyskane lub/i rozpowszechnione bez zgody osoby, która jest na nich uwieczniona.

### Ghosting –

sytuacja, gdy ktoś nagle przestaje się z nami kontaktować – bez żadnego wyjaśnienia. Może dotyczyć znajomości online i offline. Przykład? Pisziesz z kimś, dobrze się dogadujecie, a nagle ta osoba przestaje odpisywać, ignoruje wiadomości i unika kontaktu.



## Kilka słów o Dyżurnecie

to zespół ekspertów NASK - Państwowego Instytutu Badawczego, działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z przemocą seksualną wobec osób małoletnich. Zgłoszenia o potencjalnie nielegalnych treściach można przekazać za pomocą anonimowego formularza na stronie [www.dyzurnet.pl](http://www.dyzurnet.pl) lub na adres mailowy [dyzurnet@dyzurnet.pl](mailto:dyzurnet@dyzurnet.pl).

Jeśli zgłoszona treść dotyczy: materiałów przedstawiających seksualne wykorzystywanie dzieci, twardej pornografii, rasizmu i ksenofobii, innych nielegalnych treści podejmowane są kroki, takie jak przekazanie informacji do policji, innych zespołów reagujących zrzeszonych w międzynarodowym stowarzyszeniu INHOPE. Specjaliści podejmują również działania wobec treści szkodliwych, które skierowane są przeciwko bezpieczeństwu dzieci.





To nawiązywanie kontaktu o charakterze seksualnym z niepełnoletnią osobą, często prowadzące do próby spotkania się „na żywo”. Zgodnie z polskim prawem, jeśli grooming dotyczy osoby poniżej 15. roku życia, to jest przestępstwem, a odpowiedzialność ponoszą sprawcy.

Grooming może przebiegać różnie. Oto najczęściej pojawiające się elementy, które powinny wzbudzić Twoją czujność, tzw. red flagi:

- ▶ Nieznana Ci osobiście osoba nawiązuje z Tobą kontakt za pośrednictwem internetu: serwisów społecznościowych, popularnych komunikatorów, chatów (także tak zwanych „chat ruletek”, polegających na losowym doborze rozmówców) czy gier online umożliwiających komunikację między graczami.
- ▶ Masz podejrzenie, że jest to osoba dorosła - może zaniżać swój wiek, może podawać się za Twojego rówieśnika lub nie ukrywać swojego prawdziwego wieku.
- ▶ Często, po nawiązaniu kontaktu, proponuje Ci kontynuować go na innych kanałach komunikacji (szczególnie takich, które umożliwiają przysyłanie zdjęć lub rozmowy wideo).
- ▶ Stara się z Tobą „zaprzyjaźnić”, podtrzymuje rozmowę, wyraża zainteresowanie – mimo, że dzieli Was różnica wieku i wcześniej w ogóle się nie znaliście. Może dużo komplementować, w szczególności Twój wygląd. Z czasem wprowadza do rozmów tematy intymne, nacechowane seksualnie.
- ▶ Może chcieć dawać Ci prezenty.
- ▶ Może przysyłać Ci swoje intymne zdjęcia oraz prosić o Twoje nudesy.
- ▶ Prosi o zachowanie Waszych rozmów w tajemnicy.
- ▶ Proponuje spotkanie – w realu lub online, na kamerkach.
- ▶ Zachowuje się bardzo nachalnie, prosi o przesłanie zdjęć lub spotkanie powtarza wielokrotnie i nie akceptuje odmowy. Z czasem może stać się agresywna, a nawet Ci grozić.



Jeżeli spotkał się z takimi zachowaniami, i czujesz, że przekraczają one w jakikolwiek sposób Twoje granice – zareaguj!

# Co możesz zrobić?



Przede wszystkim, **zablokuj taką osobę** – możesz ją odciąć jednym kliknięciem. Każdy serwis społecznościowy przewiduje taką opcję.



Nie czuj się zobowiązany do spełniania swoich wcześniejszych obietnic ani deklaracji złożonych tej osobie – na przykład wysłania zdjęć lub zachowania czegoś w tajemnicy. **Nie musisz robić czegoś, z czym czujesz się niekomfortowo**, tylko dlatego, że ktoś obcy o to bardzo usilnie prosi.



**Porozmawiaj z kimś zaufanym** – przyjaciółmi, koleżankami i kolegami ze szkoły. Być może okaże się, że Ty i Twój rówieśnik macie podobne doświadczenia i możecie liczyć na wzajemne wsparcie.



Warto również **zgłosić to komuś dorosłemu** – rodzicowi, nauczycielowi. Pomoże Ci ocenić ryzyko podobne doświadczenia i podjąć działania, które zapewnią Ci bezpieczeństwo.



**Rozważ zgłoszenie sprawy na Policję**. Jeżeli masz wątpliwości, skontaktuj się z nami na [dyzurnet.pl](https://dyzurnet.pl).



Jeżeli czujesz taką potrzebę, **poszukaj pomocy psychologicznej**. W Polsce działa wiele instytucji zapewniających darmową i anonimową pomoc dla osób małoletnich, oto niektóre z nich:

- Telefon zaufania dla dzieci i młodzieży: 116 111.
- Dziecięcy Telefon Zaufania Rzecznika Praw Dziecka: 800 12 12 12.
- Linia Pomocy [SEXED.PL](https://sexed.pl) – specjalna linia telefoniczna dla osób uwikłanych w przemoc w związkach i intymnych relacjach: 720 720 020.

# Sexting i upublicznianie intymnych materiałów

Sexting (nazwa powstała z połączenia angielskich słów „sex” i „texting”) to przesyłanie za pomocą internetu lub telefonu komórkowego swoich zdjęć, filmów bądź wiadomości o seksualnym charakterze.

Badania mówią, że nawet połowa nastolatków przynajmniej raz wysłała lub otrzymała materiały intymne<sup>6</sup>. **Jeden na sześciu chłopców przyznał, że takie zdjęcie później było dystrybuowane bez jego zgody. Taka sama sytuacja dotknęła jedną na pięć dziewczynek.**

Osoby poszkodowane rozpowszechnianiem materiałów intymnych często zgłaszają konsekwencje psychologiczne, takie jak stany lękowe, depresja, objawy stresu pourazowego. Doświadczają też poczucia utraty kontroli. Skutki są bardzo zbliżone do tych odczuwanych przez ofiary fizycznej napaści na tle seksualnym.

Groźba upublicznienia takich zdjęć często staje się podstawą do szantażu, czyli tzw. *sextortion* – gdy osoba po drugiej stronie żąda zapłaty lub kolejnych materiałów w zamian za nieudostępnianie tych, które już ma.

W ostatnim czasie można zaobserwować również niepokojący trend wykorzystywania sztucznej inteligencji do wytwarzania materiałów intymnych – często z użyciem wizerunku realnej osoby, tzw. *deep fakes lub deep nudes*. Ta technologia pozwala „zdjąć Twoje ubrania” na zdjęciu lub wkleić Twoją twarz na inną postać w taki sposób, że będzie to wyglądać bardzo realistycznie, w sposób trudny do odróżnienia od prawdziwych zdjęć. Za tworzenie i rozpowszechnianie takich zdjęć grożą sprawcy konsekwencje prawne, tak samo jak w przypadku zdjęć „prawdziwych”.

## Jak uniknąć upublicznienia intymnych materiałów?

- Najłatwiejsze rozwiązanie, to to oczywiste – nie rób i nie wysyłaj zdjęć, których nie chciałbyś widzieć krążących po internecie.
- Blokowanie osób naruszających Twoje granice to nie ghosting – to asertywność! Jeżeli czujesz się nieswojo w jakiejś konwersacji – zadbaj o siebie i po prostu ją zakończ. Nie musisz podawać powodu.
- Ustalaj własne granice i nie pozwól innym ich przekraczać, ale też szanuj granice innych – nie namawiaj nikogo do wysłania intymnych zdjęć.
- Bądź wsparciem – jeżeli otrzymasz intymne zdjęcie innej osoby – nie przysyłaj go dalej.



Powstały inicjatywy, które pomagają odnaleźć i usunąć takie treści w sposób anonimowy. Jest to serwis *Take it Down*, stworzony przez amerykańską organizację NCMEC, przeznaczony dla osób poniżej 18. roku życia. *Take it Down* współpracuje z największymi serwisami społecznościowymi. Serwis jest dostępny także w polskiej wersji językowej!

6. ECPAT, Badanie „Everything that is not a yes is a no” z 2021 roku, przeprowadzone na 13 tys. Respondentów w wieku 10-17 lat. [https://ecpat.se/wp-content/uploads/2020/12/ECPAT-Report-2021\\_Everything-that-is-not-a-yes-is-a-no.pdf](https://ecpat.se/wp-content/uploads/2020/12/ECPAT-Report-2021_Everything-that-is-not-a-yes-is-a-no.pdf)

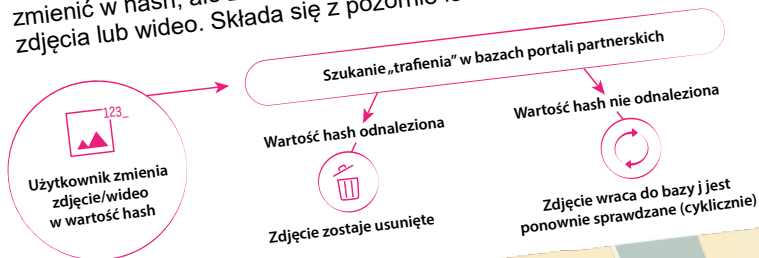
# Jak to działa?



**Użytkownik, który chce usunąć zdjęcie lub wideo**, które zostało udostępnione w sieci, na jednym z portali partnerskich, może w prosty sposób zamienić materiał wizualny znajdujący się na jego urządzeniu w wartość hash. Fizycznie, zdjęcie/wideo nie jest przysyłane do serwisu, pozostaje na urządzeniu zgłaszającego. Jedynie hash trafia do baz portali partnerskich i poszukiwane jest trafienie – w przypadku, gdy zostanie znalezione, zdjęcie lub film są usuwane.



**Hash** (inaczej funkcja skrótu) działa podobnie jak odcisk palca. Każde zdjęcie lub wideo ma swoją unikalną wartość hash, po której można je zidentyfikować. Plik można zmienić w hash, ale z wartości hash nie można odzyskać zdjęcia lub wideo. Składa się z pozornie losowych znaków.



## Sprawdź to!

- **Take it Down** – serwis umożliwiający usuwanie niechcianych zdjęć intymnych z portali społecznościowych, przeznaczony dla osób poniżej 18. roku życia. Więcej: <https://takeitdown.ncmec.org/pl/>.
- **Stop NCII** – serwis działający na tej samej zasadzie, co Take it Down, ale dla osób dorosłych. Więcej: <https://stopncii.org/>.
- **Nofiltr.org** – strona przygotowana przez amerykańską fundację Thorn. Misją Nofiltr jest zapewnienie młodym ludziom zasobów, które pozwolą im bezpiecznie poruszać się po internecie. Dzielą się prawdziwymi doświadczeniami i poradami dla młodzieży, korzystając z perspektywy młodych osób. Więcej: <https://nofiltr.org/>.
- **Kampania Stop Sextortion** – Kampania fundacji Thorn ma na celu zwiększenie świadomości na temat zjawiska sextortion, odczarowanie tego problemu i zachęcenie ludzi do szukania pomocy i wsparcia u swoich przyjaciół. Więcej: <https://www.youtube.com/watch?v=9yQ3fdt-tbUk>.



# Przykładowe działania w CYBERspocie



W ramach szkolnego projektu sprawdźcie, jak w popularnych komunikatorach i grach działają ustawienia prywatności – przygotujcie **broszurę lub plakat** informujący, jak działa blokowanie użytkowników i zgłaszanie nieodpowiednich treści.

Wyszukajcie w internecie różne **kampanie społeczne** dotyczące problemów groomingu, sextortion, sextingu. Przygotujcie swoją. Możecie wywiesić plakaty lub ulotki informacyjne.

Zorganizujcie **dyskusję grupową** na temat niepokojących rozmówców w sieci. Z jakimi zachowaniami kiedyś się spotkaliście? Jak na nie zareagowaliście? Przygotujcie plakat lub krótki filmik, na którym umieścicie to, co pomogłoby młodszym od Was osobom lepiej poradzić sobie z takimi sytuacjami w przyszłości. Pamiętajcie, by w tych dyskusjach uczestniczył psycholog szkolny lub inny ekspert.

Zorganizujcie **warsztaty** ze szkolnym lub zaproszonym z zewnątrz psychologiem, które pomogą Wam zrozumieć pojęcia consentu oraz pomogą wzmocnić Waszą asertywność.



**Autorzy:** Katarzyna Grabowska, Kamil Oleszkiewicz, Aleksandra Osuch, Zuzanna Polak, Anna Słupska, Natalia Wójcicka

**Redakcja merytoryczna i korekta językowa:** Aleksandra Ostaszewska, Julia Piechna, Anna Rywczyńska, Anna Słupska, Natalia Wójcicka

**Projekt okładki, opracowanie graficzne i skład:** Aneta Witecka

**Koordinacja:** Natalia Wójcicka

**Ilustracje na okładce i w publikacji:** © NASK-PIB, © AdobeStock

**Wydawca:** NASK – Państwowy Instytut Badawczy,  
ul. Kolska 12 01-045 Warszawa

**ISBN:** 978-83-68356-02-1

**Licencja:** Publikacja jest rozpowszechniana na zasadach licencji Creative Commons. Uznanie autorstwa – Użycie niekomercyjne (CC BY-NC) 4.0 Międzynarodowe.

**Finansowanie:** Publikacja jest współfinansowana ze środków Komisji Europejskiej w ramach programu Digital Europe.