Magiczny Kraków

### Cyberbullying

2024-11-25

**Did you know that one in five girls has experienced cyberbullying? Let's identify it, respond to it, and prevent it. Cyberbullying is an increasingly common but relatively new form of abuse and is often downplayed or ignored. Cyberbullying is actions or threats, using information and communication technologies, most often computers and smartphones connected to the Internet, that cause (or are likely to cause) physical, sexual, psychological or economic harm or suffering. While there are times when cyberbullying is primarily understood as peer/youth abuse, it has no age restrictions – cyberbullying is also committed against adults, with this abuse also "being of" certain gender, age, sexual orientation, fitness level, and religion.**

# Identifying cyberbullying

Various forms of abuse using new technologies are described below. Knowledge of this subject is crucial. Sometimes people who are subject to such abuse do not know the words to describe their experience. Without descriptions and knowledge, it is also difficult to create legal, educational, awareness and other tools to prevent, respond to and prosecute perpetrators of this abuse.

## Some of the most common online forms of abuse include:

- methodical and persistent sending of offensive e-mails and messages (e.g., via instant messaging),
- sending threats,
- publishing intimate photos or videos,
- sending a person unwanted materials of a sexual nature,
- tracking a person in various ways (on the Internet - using tracking apps or in "real life"),
- Internet hate speech/inflammation of abuse, deep resentment or hatred against a person who belongs to a discriminated group (e.g., women).

**Specific forms of cyberbullying also include doxing, trolling, flaming, sexting, and grooming.**

E-mail, chat rooms, instant messaging, websites, blogs, social networks, newsgroups, SMS and MMS services, but also mobile applications (e.g., tracking) and electronic devices controlled remotely and connected to the Internet (e.g., cameras, microphones, etc.) are the tools mainly used for this abuse.

# React

Although the vast majority of people consider cyberbullying unacceptable and at the same time a serious threat, often - whether we experience it ourselves or witness it - we don't know what to do.

Magiczny Kraków

# If you face cyberbullying:

- seek support from a trusted person(s) - tell someone about what happened/happens, and together consider what to do next, whom to inform,
- you can report abuse to the Police or the Prosecution Service; **it is always the perpetrator who is to blame, never the person against whom someone has committed abuse**,
- you can call (anonymously) the helpline: 116 111 - the Dajemy Dzieciom Siłę Foundation or 24/7 116 123 - the Institute of Health Psychology “Blue Line” Domestic Abuse National Helpline ,
- demand the immediate removal of a video or photo taken against your will (the will of the victim/injured person) or the cessation of any other cyberbullying activity,
- block contact with unwanted people in instant messaging and e-mail,
- demand that the site administrator remove compromising materials from the network,
- document evidence of abuse (save text messages, communication history, take screenshots, etc.),
- if the abuse occurred at an institution: school, workplace, community center, etc. - demand that you be assured of your safety and that action be taken against the perpetrator.

# What to do when witnessing cyberbullying

- do not forward harmful materials you receive online,
- inform the person who is being attacked that you see what is happening and support them,
- inform some trusted (adult) person, organization or the Police about what you see, hear or read on the Internet, portals, groups,
- always support colleagues who are victims of cyberbullying, you or he/she can call 116 111 for support.

# Prevention

The more we know about abuse, including cyberbullying, the better situation we are in. The second principle is to break the silence, taboo and solidarity with those who have experienced abuse. Another principle is to develop in each community: in a group of friends, at school, at home - plans to prevent and respond to cyberbullying cases. We must also put pressure on the public institutions that are responsible for protecting us from abuse. Cyberbullying is not our private problem.

# How to keep safe on the Internet?

While the person facing abuse is never to blame, there are some things you can do to increase your safety:

- update your knowledge of cyberbullying and digital safety,
- keep your personal data private,

- give your online profiles a secure status (private),
- protect your passwords and usernames,
- be sensible about the photos and videos of yourself you post online and to whom you send them,
- try not to share cell phones with colleagues,
- try not to respond to online taunts,
- use security settings in your own profiles; consider whether a private profile is more suitable for you: turn off comments or enable hate speech filters in apps,
- learn how to report content on your favorite portals, and use this feature when you discover hateful posts, bullying, fake news or false profiles.

# How to use the Internet and phone in a way not harmful to others

- treat others with respect (no verbal abuse, insulting, threatening behavior, etc.),
- do not post materials (videos, photos, texts) on the Internet that can hurt someone,
- always ask for permission if you want to take a photo or film someone, especially if you want to publish these materials,
- do not send out photos, videos and texts via your cell phone that may cause someone distress or harm.

## Glossary of terms related to the Internet and cyberbullying:

- Bodyshaming
- Creepshot
- Cyberstalking
- Cyberbullying
- Cyberflashing
- Deadnaming
- Deepfake
- Doxing, doxxing
- Flaming
- Geolocation
- Grooming
- Hacking
- Happy slapping
- Hate speech on the Internet
- Stalkerware
- Orbiting
- Outing
- Retaliatory pornography
- Abuse using internet-connected devices

Magiczny Kraków

- Trolling
- Silencing
- Sexting
- Sexual extortion
- Swatting

## Bodyshaming

Bodyshaming involves commenting on and mocking the shape, size or appearance of someone’s body - this can be done online and outside the digital world.

## Creepshot

sexually explicit photos of people taken without their consent.

## Cyberstalking

includes methodical and persistent sending of offensive e-mails and messages (e.g., via instant messaging), sending threats, publishing intimate photos or videos, and following a person in various ways (online, or in “real life” - using tracking apps). The effect includes undermining the stalked person's sense of security.

## Cyberbullying

persistent intimidation, coercion, or harassment intended to cause serious emotional distress and/or fear of physical harm. Most victims of this type of abuse are young people and children from vulnerable groups. Cyberbullying can also include requesting sexual favors or providing unwanted offensive, humiliating, degrading or intimidating content, as well as threats and hate speech on social media.

## Cyberflashing

involves sending unwanted sexually explicit images via dating apps, messaging apps or SMS, as well as via Airdrop or Bluetooth.

## Deadnaming

an intentional act of using the forename or surname given to a transgender person on his or her birth certificate (which does not correspond to his or her gender) to shame, threaten, intimidate or bully.

## Deepfake

a video in which the original face/character has been (seamlessly) replaced with another face using

algorithms, and sound is manipulated to create the illusion of another person's actions and expressions.

## Doxing, doxxing

this type of abuse involves searching for, collecting and publicly sharing personal data (home address, photos, names of the victim and his or her relatives) and sensitive data (e.g., background, sexual orientation) without that person's consent. Doxing can have serious psychological consequences. Moreover, by allowing victims to be physically located, it can also precede physical abuse. Perpetrators obtain information by searching publicly available databases and social networks, but also use hacking and manipulation. Doxing can be used for harassment and financial, sexual and other types of extortion, or even to “track down” the victim in the real world.

## Flaming

is a form of aggressive and hostile online communication that always contains insults, resentment and hatred. Typographically, comments are usually written in capital letters and include exclamation points. This type of cyberbullying is used to provoke a reaction from another user/user. It is closely related to trolling and is not generally recognized as abuse in legislation or politics. Flaming can be openly misogynistic and often contains threats or fantasies of sexual abuse or incites sexual abuse

## Geolocation

a function of a device to determine its geographic location based on GPS signals or other forms of communication.

## Grooming

Forcing a person to disclose or share their own erotic or sexual material. Unlike direct extortion, this is a process in which the perpetrator, using manipulation, enters into a relationship with the victim in order to obtain sexual content, such as nude photos, intimate conversations or other online interactions. Grooming begins with making contact with victims, especially minors, to build a relationship of trust, in which perpetrators use fake profiles to impersonate someone else and facilitate false friendships that end in extortion.

## Hacking

a process of gaining access to a computer system or network in an illegal or undesirable manner.

## “Happy slapping” (filmed attack)

a filmed assault/attack (physical or sexual assault) on a victim for the purpose of recording the assault and posting it on the Internet. *Happy slapping* is a euphemism for assault and battery.

Magiczny Kraków

## Hate speech on the Internet

inciting abuse or hatred against a person who belongs to a discriminated group (such as women). Although hate speech is a broad term, usually associated with abuse against groups based on their ethnicity, religion or national origin, it also occurs against women. Gender-based hate speech includes sexualization, objectification and degrading comments about physical appearance, as well as threats of rape and physical violence, and encouraging other Internet users to engage in such abuse.

## Spyware, stalkerware

software, usually in the form of an application, downloaded to someone's phone or device and used to track the activities of that device. Spyware is considered stalkerware in the context of domestic abuse.

## Orbiting

the perpetrator does not respond to someone's messages or does not communicate directly, but continues to view their content online (liking, viewing stories, etc.).

## Outing

the practice of revealing someone's sexual orientation or gender identity without their consent, often in public.

## Retaliatory pornography

Publicly sharing sexual content with one or more people without their consent. Most of the people who are attacked in this way are women. Usually, such materials are distributed by an ex-partner/boyfriend of the girl/woman. The perpetrator obtains sexually explicit images or videos during the relationship, or hacks or steals them from the victim's computer, social media accounts or phone to share them online.

## Abuse using internet-connected devices

Devices such as smart doorbells, speakers, security cameras or other internet-connected devices that can be remotely controlled are used to harass and control the victim. Examples of this type of abuse include turning on or off switches (such as lights or heat in the victim's home), locking (depriving) another person in a place by controlling a smart security system, or using security cameras or personal electronic devices for recording.

## Trolling

is the intentional involvement of others to disrupt a discussion/event online. It involves publishing

material in large quantities that deviates from the topic of discussion or disrupting discussions by sending aggressive and misleading messages. Trolls may not know the victims. Sexist trolling includes gender-based insults, cruel language and rape and/or death threats made by an organized group to humiliate women, especially those who express their opinions.

## Silencing

in the digital sphere, this means preventing full participation and self-expression on the Internet of a person who remains silent due to fear of abuse and harassment, which ultimately results in exclusion from communities and public debates in which he or she would like to participate.

## Sexting

involves exchanging, sending or receiving sexually explicit messages, often including pictures or videos, via SMS or chat.

## Sexual extortion

also known as “sextortion,” involves using the threat of publishing sexual content (photos, videos, false content, sexual gossip) to intimidate, coerce or blackmail and then obtaining more sexual content or to obtain money.

## Swatting

the use of telephones, and often computer systems, to fool emergency services into sending law enforcement to a specific location based on a false report.