

# WETO! European Youth Against Digital Bullying



# VETO! European Youth Against Digital Bullying (2022-1-PL01-KA220-YOU-000086175)









Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

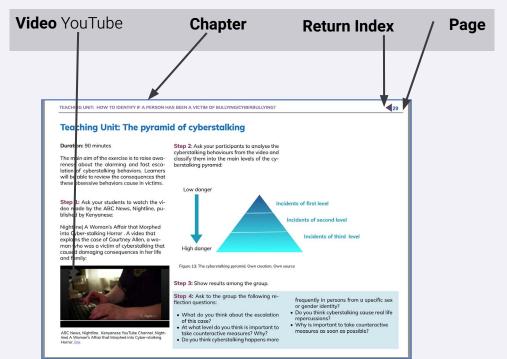


# How to use this Book



This is an interactive book, click, enjoy and discover









### **WETO! European Youth Against Digital Bullying**

#### Introduction

- Who is this guide for?
- How to use this guide
- Why a gender approach to cyberbullying?

### What is cyberbullying?

- Differences between bullying in the physical and digital environment.
- Teaching Unit: How to identify if a person has been a victim of bullying/cyberbullying?
- Cyberbullying typology
- Denigration or Dissing
- Teaching Unit: The art of gossips
- Masquerading, Catfishing, Phishing, Digital identity theft
- Disclosure of information (Doxing and Outing)
- Teaching Unit: The outing case of Channing Smith
- Exclusion
- Cyberstalking
- Teaching Unit: The pyramid of cyberstalking
- Electronic insults: Flaming and trolling
- Happy slapping
- Teaching Unit: The erosion of empathy and respect
- Sextortion or Online Sexual Coercion
- Teaching Unit: The case of Ashley Reynolds

### **Cyberbullying roles**

- Bully
- Teaching Unit: Test: Am I a bully?
- Victim and Vulnerable groups
- Bystanders
- Teaching Unit: Step on or stand for

### **Conditions for cyberbullying**

- Image: Digital identity and personal branding
- Digital narcissism and social digital voyeurism
- Self-esteem
- Teaching Unit: Celebration of being myself
- Impulsivity and Recklessness
- Gender roles/identity
- Peer-pressure
- Resilience
- Privacy
- Empathy. Teaching Unit: Walking on my shoes

### **Environments where cyberbullying takes place**

- Primary interactions
- Couple. Teaching Unit: True partner VS toxic partner
- Social
- Teaching Unit: Stereotypes and cyberbullying
- Cyber-bullying means. Teaching Unit: Cyberbullying public and private means

### Consequences of cyberbullying

- Legal
- Personal. Low self-esteem
- Mental health consequences
- Teaching Unit: The Feeling Wheel
- Physical consequences
- Self-harm
- Social

### Critical thinking to counteract cyberbullying: an integrated response

- What to do if you are a victim of cyberbullying?
- As a youth worker, what to do if your learner notifies a cyberbullying incident?
- What to do if you are a bystander?
- Advices for protecting from cyberbullying
- The THINK Tool for a healthy online communication
- Teaching Unit: The tree of the healthy digital environment
- Teaching Unit: The rainbow of hearts
- Teaching Unit: Roll the dice!
- Teaching Unit: The anti-cyberbullying T-shirt movement

#### References



## Introduction

### Who is this guide for?

Now-a-days youngsters are immersed in online interactions in which some years ago were unimaginable. For youngsters and digital natives is very common to develop many of their daily activities online: as academic or professional tasks, communication, entertainment, gaming, and so on. The constant exposure to digital media in youth communities has raised cyberbullying, becoming a serious issue that affects youngsters wellbeing. However, not only youngsters are involved in cyberbullying incidents, but also this phenomenon can affect other people from other ages.

This interactive book offers knowledge, advices, techniques and tools to help young people and youth workers recognize and address the difficulties presented by cyberbullying. It provides methods and tools to help them understand the complexity of cyberbullying, which will be helpful for:

- Assisting young learners who are victims of cyberbullying.
- Training young learners in cyberbullying as a mechanism for prevention and counteraction.
- Raising awareness in youngsters about the negative consequences of cyberbullying incidents.

 Enhancing skills to provide safe environments and boost good digital practices within the interaction of youngsters.

This edition is also for young people, serving as a digital compass to fight against cyberbullying. Besides, they will acquire confidence in how to stop these incidents and support their peers.

Throughout the text, it is expected to promote a culture of respect, empathy and responsible digital citizenship, by helping readers understand the many types of cyberbullying and the negative impacts they cause. It is expected to create a more secure and encouraging online community where everyone can interact with resilience and confidence. This book will serve as a source of inspiration, empowerment, and education.



### How to use this guide

This book will facilitate you to study at your own rythm, whether you are a young person figuring out the complexities of the digital world or a youth worker dedicated to helping the next generation. Each person's learning path is different; therefore this reading offers a self-paced learning environment that enables you learn efficiently and develop a deeper comprehension of the subtleties associated with cyberbullying.

Statistics are detailed so youth workers and youngsters become aware of the magnitude and gravity of cyberbullying. Through these figures, they will understand the necessity of tackling this issue and collaborating together to build safer online places.

Teaching units are provided for youth workers to work with their groups. Furthermore, most of the activities included in these units can be done by any reader on their own. This will allow that a group of learners or individual readers benefit from these activities.

Reflection questions are included to promote awareness and critical thinking. This introspection method will encourage young people and youth workers to explore the complexities of cyberbullying and their main actors. They will also serve as a way to navigate in the readers' minds and hearts. Furthermore.

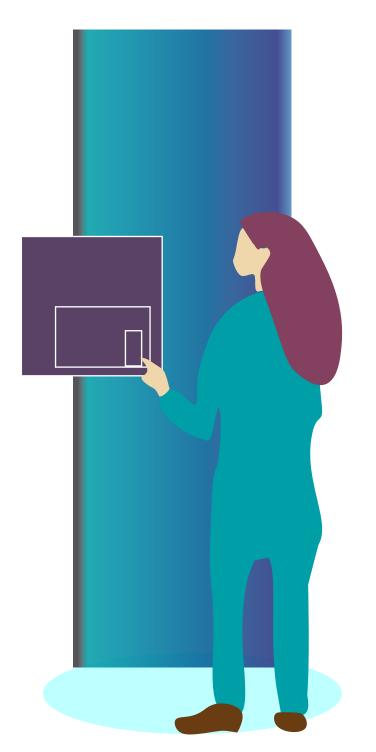
research activities are intended to strengthen critical thinking and analysis capacities.

Readers will know some difficulties that real people encountered online, through study cases. These examples act as teaching aids, shedding light on the dynamics of cyberbull-ying and encouraging, in turn, empathy.

### Why a gender approach to cyberbullying?

Readers will keep in mind how cyberbullying affects people differently depending on their gender, sexual orientation or sexual expression. The book offers comprehensive details to shed what are the unique obstacles, susceptibilities, and experiences associated with gender in the digital world. It provides ideas for comprehending the interconnectedness of the types of cyberbullying that affect individuals based on gender.

Lastly, we encourage everyone who uses this guide to start advocating for change. Share your expertise with others to increase awareness of cyberbullying and its effects. In this way, you will contribute to having a safer and more compassionate online world. Let's fight together against cyberbullying.



# What is cyberbullying?

To understand the concept of cyberbullying, first it is necessary to comprehend the definition of bullying. According to the American Psychological Association Dictionary of Psychology, bullying is "a persistent threatening and aggressive physical behavior or verbal abuse directed toward other people, especially those who are younger, smaller, weaker, or in some other situation of relative disadvantage".

<u>UNICEF</u> defines cyberbullying as "is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted."

The growth of the interactions and activities in the digital world has taken the society by surprise. Most of us were not prepared for this fast transition, in terms of appropriate behaviors. Neither governments, nor policy makers were prepared in terms of rules and policies for the digital world. This fast transition and the lack of preparation have created a social and legal void, where important threats have arisen; cyberbullying is a clear example. Cyberbullying has been constantly present in children's, youngsters' and adults' lives, since there were no moral guidelines or firm regulations to prevent and address it.



### Differences between bullying in the physical and digital environment

Some incidents of bullying can be very similar in the online world (cyberbullying). However some important considerations when comparing bullying in physical and digital environments are:

#### **Indirect Interaction**

Physical Environment: The interaction of bullying is direct. The incident between the bully and the victim is in most of times face to face. Bullies may act aggressively, either verbally or physically, when the victim is around.

**Digital Environment:** Cyberbullying may happen indirectly in the digital world through online means. Victims can be perpetrated by persons they know or complete strangers. Cyberbullying can be done via text messaging, social media, or other digital platforms that do not require direct face-to-face interaction.

### **Anonymity**

**Physical Environment:** In traditional bulying, there is minimal anonymity and the victim usually knows who the attacker is. It is usually easy to identify the bully.

**Digital Environment:** Despite that not all bullies are anonymous, a higher level of anonymity is involved in cyberbullying. The use of fictitious accounts or internet pseudonyms by perpetrators makes it difficult for victims to identify their harassers.

Being anonymous is one of the disadvantages in cyberbullying because for the bully is easier to start and escalate the incidents, as they feel protected behind their anonymous identity.

#### **Pervasiveness**

**Physical Environment:** Bullying in the traditional sense is restricted to certain physical settings, such as companies, schools, or communities. The effect is limited to those specific environments.

**Digital Environment:** Cyberbullying is not limited by geographical limitations. When people have access to digital devices and the internet, it may happen anywhere and at any time, which has a more widespread effect on the lives of the victims.

### **Ubiquity**

**Physical Environment:** Bullying in the past was more isolated and might not have occurred as frequently. It usually occurs at particular times or under particular circumstances.

**Digital Environment:** Because digital gadgets offer continual connectivity, cyberbullying is pervasive. Bullying may occur around-the-clock for victims, and many find it more difficult to leave since the internet world is constantly available.



## Teaching Unit: How to identify if a person has been a victim of bullying/cyberbullying?

**Duration:** 3 hours

In many cases, children and youngsters who are victims of bullying and cyberbull-ying do not report it, for different reasons such as:

- Fear of repercussions from bullies.
- Fear they become more vulnerable.
- Fear of being judged.
- Think they will not have sufficient support; feeling helpless.
- Getting punishments.
- Think people will laugh about them.
- Shame.
- Need to handle the situation by themselves.
- Do not want to continue "spreading the message". This means telling others what is being said about them.
- Etc.

Bullying and cyberbullying can leave devastating consequences in the victims' lives that we will review in-depth in the chapter "Consequences of Cyberbullying". Therefore, as a youth worker, parent or youngster, it is very important to identify the signs indicating when an individual is a victim of cyberbullying and bullying.

### **Teaching Exercise:**

**Step 1:** The following list includes different signs for identifying if a person has become victim. Provide the list to your learners and ask them to analyse each of the signs and classify them into 3 groups:

**Group 1:** Signs for cyberbullying and bull-ying

Group 2: Signs for cyberbullying

Group 3: Signs for bullying

### **List of signs:**

- Loneliness
- Constant avoidance of mentioning their regular online activities/interactions.
- The youngster/child loses interest in people and things.
- Loss of friends.
- The youngster/child reacts emotionally to what they see on their device by laughing, becoming angry or being unhappy.
- The youngster's/child's social media profiles are deleted or replaced.
- Constant headaches.
- Eating disorders.

- Unexplained injuries.
- Constant stomachaches.
- Low self-esteem.
- Talking about suicide.
- Lack of concentration.
- Avoiding going to work, school, social situations, etc.
- Destroyed or lost belongings.
- When other people are around, the youngster/child hides their screen.
- Self-harming.
- Depression.
- Sleeping disorders and nightmares.
- Being unhappy in specific environments, such as school, work, leisure activities, etc.
- Poor performance at school/work.
- Anxiety.
- Sudden increase or decrease in the usage of digital devices.

### Step 2: Share with the group the results:

Some examples of signals of bullying and cyberbullying are:

- Loneliness.
- Depression.
- Low self-esteem.
- Anxiety.
- Constant headaches.
- Constant stomachaches.
- Being nervous after having an online interaction (reading a message, etc.)
- Eating disorders.
- Poor performance at school/work.
- Avoiding going to work, school, social situations, etc.
- · Loss of friends.
- Self-harming.
- Talking about suicide.
- Unexplained injuries.
- Sleeping disorders and nightmares.
- Lack of concentration.

#### Additional signs of cyberbullying are:

- The youngster's/child's social media profiles are deleted or replaced.
- Being nervous after having an online interaction (reading a message, etc.)
- A youngster/child reacts emotionally to what they see on their device by laughing, becoming angry or being unhappy.
- Sudden increase or decrease in the usage of digital devices.
- When other people are around, the youngster/child hides their screen.
- Constant avoidance of mentioning their regular online activities/interactions.
- The youngster/child loses interest in people and things.

#### Additional signs of bullying are:

- Being unhappy in specific environments, such as school, work, leisure activities, etc.
- Destroyed or lost belongings.

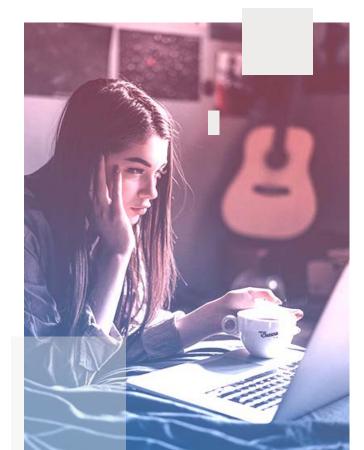
**Step 3:** After analyzing the results, ask the group to think on more signs for each of the groups. Provide some time and then ask them to share their answers.

**Step 4:** After making the final list, make some reflections by asking your learners:

- Are you able to identify if someone is being a victim?
- Do you know somebody who might be suffered cyberbullying or bullying?

- Have you been a victim? If yes, do you think you had some of this signs?
- Mention to the group some of the reasons victims do not report it. Then, ask, if you were a victim, did you look for help?
  - -If yes, what happened?
  - -If no, why?

**Step 5:** Ask the group to make a poster for each of the groups and paste it in your facilities. Also, ask your learners to take pictures of the posters and upload them in their social media.



### **Cyberbullying typology**

#### Harassment

The Cambridge Dictionary defines harassment as an "illegal behaviour towards a person that causes mental or emotional suffering, which includes repeated unwanted contacts without a reasonable purpose, insults, threats, touching, or offensive language"

According to the Study "Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada, Concepts and Recommendations", the author, Randy McCall mentions that online harassment can be manifested in a direct and indirect way towards the victim:

#### Online direct harassment

It is when the victim receives directly, to their online accounts (social media, email, Whatsapp, etc.), messages that are intimidating, embarrassing, disrespectful, aggressive, etc.

#### Online indirect harassment

When the victim is attacked in other media different than their personal accounts (social media groups, forums, websites, etc.). For example:

- Publish fake posts under the victim's name
- Starting a website to rate the physical aspects of the victim
- Subscribing the victim to app accounts

or services, without their permission.

• etc.

#### **Online threats**

Online threats refer to any kind of intimidating or hostile communication, statements or messages sent over digital means, with the goal of injuring, frightening or coercing the target. Online threats are divided into:

#### **Explicit threats**

These are threats for harming the victim, such as physical threats, property damage threats, or other activities that can cause emotional distress. Explicit threats are clearly directed to the victim, for example:

- Watch your back because I will beat you"
- "If you do not send me more pictures, I will block your computer"
- "If you do not send me the money, I will erase your account"

• etc.

### Implied threats

The intention of causing damages to the victim is the same as the explicit threat. However implied threats are communicated by clues, insinuations, indirect language, etc. The victim should have to infer the danger from the implied message, for example:

- "People like you should be beaten"
- "If I were you, I would stop"
- etc.

In both cases, victims should contact the police if the threat is putting their lives at risk.

In the course of this chapter you will see how online threats can be manifested in different types of cyberbullying, especially in phishing, digital identity theft, doxing, outing, cyberstalking and sextortion.



### **Denigration or Dissing**

Denigration or dissing can be defined into the following actions:

- To deny the importance of an individual.
- To attack a victim's reputation.
- To underestimate with others the good value of a person.

The attacker spreads false, cruel or hurtful information about the victim, through digital means. Denigration occurs in several ways, such as:

Character assassination: is the act of making untrue or defamatory comments about a person's morality, personality, or other attributes, in an effort to damage their reputation.

Spreading False Information: Some cyberbullies have the ability to spread false information about their victims, making their friends or other people think things about their behavior, personal lives, or opinions that are not true.

**Public Humiliation:** This consists in humiliating the victim, usually by publishing pictures, videos, or comments in an embarrassing or compromised way.

Creating Defamatory Content: The perpetrators design websites, social media profi-

les, and other online content with the purpose of criticize their victim.

Impersonation: The attackers create fake social media profiles; create fake websites; subscribe to groups or forums and publish inaccurate or harmful information under the victim's identity. This can cause major repercussions for the victim.

**Deface profiles:** Perpetrators can attack the victims' social media profiles through the comments section, posting on their profiles, etc. affecting their reputation.

**Denigration through words:** Denigration can be directed towards an individual or a specific group. Sometimes, without the intention of hurting someone, we can be using vocabulary that underestimates the value of a group. For example:

Figure 1: Denigration through words. Facebook screenshot.

ue agosto - Guiza, Egipto - 🌝

•••

When we as Black peoples use some words, we are subliminally endorsing the denigration of Black people. Even the word denigration, if you know the origin of it, you will stop using it. It originates from the N word.

Don't say Blackmail. Say malign Don't use blacklist. Use delist Reject Blackmarket. Instead use parallel market Instead of 'paint him black', say spoil his reputation

Constant use of these words inadvertently paint an image of Blackness as negative, especially when they are contrasted with words that project Whiteness as positive, such as whitewash, stainless or spotless white, or pure white. Stop calling people 'black devils'. It is scripting your mentality to hate yourself and your fellow blacks. Especially when the mainstream media has turned Christ from an police skin Semite to a blond haired and blue eyed Caucasian. You see the guy behind me (the Sphinx)? He was a Black man, and nobody in his right mind builds a statue for the devil. Project blackness positively!

#RenosNuggets

## Teaching Unit: The art of gossips

**Duration:** 90 minutes

The aim of this activity is to explore and gain a deep understanding of how gossips can cause denigration on persons, affecting their reputation.

**Step 1:** Divide your learners into pairs. Avoid that these pairs are formed by close friends; try to establish pairs of learners who do not have a constant interaction.

**Step 2:** Give 10 minutes to the pairs to present themselves. Each person should tell to their peers 3 true statements about themselves.

**Step 3:** Ask each person to go to the front and present their peer. This person should share the 3 true statements and present 1 extra false statement about the other. The false statement should have to be realistic; avoid telling false statements that are very easy to identify "my peer went to the moon", "my peer speaks all the languages from the world". etc.

**Step 4:** Ask to the rest of the group to vote to determine which of the statements (1, 2, 3 or 4) is false.

**Step 5:** Unveil the false statement and compare the votes.

**Step 6:** Do the same process to each of your learners.

**Step 7:** Ask them the following reflection questions:

- Were you able to identify all of your peers' false statements?
- Were false statements easier to identify on close friends than on people you do not know very well?
- How can false statements lead to changing a person's life?
- Why do you think that other people can believe in gossips?
- How can gossips easily be distributed?
- Which types of gossips do you normally encounter in the digital world?
- In which media do you find gossips more often?
- How will you react in the future when you hear a gossip?

This activity is important as participants will have the chance to examine real-life examples of gossips coming from their peers. Participants will learn that a gossip can play an important role, especially in the digital world:

- Gossips can influence public opinion.
- If the gossip is good, it will be fast distributed.
- Gossips can be connected to broader societal issues.
- Gossips can affect a person's image and well-being.
- Etc..



### Masquerading, Catfishing, Phishing, Digital identity theft

Masquerading is when the bully creates a fake social profile, email, or account to bother a person via online. The victim is contacted through one of these ways, which appearance looks as it is coming from someone else.

Masquerading is the first step for committing other types of cyberbullying:

### **Catfishing**

The Cambridge Dictionary defines catfish as "someone who pretends on social media to be someone different, in order to trick or attract other people."

In most of times, catfishing involves a masquerading profile, where a person pretends to be in love with the victim and have an online relationship in order to obtain money, gifts, etc.

### The most common signs to suspect that we can be victims of catfishing are:

- The fake lover wants to move forward the relationship very fast.
- Fake lovers make a thousand excuses for not meeting in person.

- At first, they pretend and show that they have a nice life, without financial problems. All of a sudden, fake lovers have a conflictive situation (i.e. health problems, accidents, etc.) and ask for financial support.
- Their stories about themselves and family may have contradictions and lack of coherence.
- Lack of track about their personal profiles.
- The fake lover asks to make the relationship more special, making in to keep it as a secret.
- Avoiding having video conferences, or showing their face.
- etc.

The term catfishing became popular in youth communities after the release of the "Catfish" TV show, produced by MTV, where Nev Schulman and Max Joseph help real people to verify the genuineness of their lover's identities and find the person behind the mask.

The MTV channel provides a 24-hour pass where you can have access to some of the Catfish episodes for free. The episodes demonstrate how scammers operate and the consequences that catfishing has on real victims. If you are interested, you can access to the pass here: <a href="https://www.mtv.com/episodes">https://www.mtv.com/episodes</a>

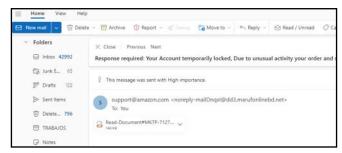
### **Phishing**

Phishing is a form of social engineering attack that happens when a victim is tricked into opening a masquerade email, text message, etc., that seems to be legitimate. The victim trusts the reliability of the content, as in most of cases they have the same corporate branding (same logos, colors, etc.).

Subsequently, the email asks the receiver click on a link, download a file, etc., that can cause the installation of malware to steal credentials. Also, clicking to the link might let persons get to a fake website that looks identical as the original one, where they are asked to provide sensitive information such as passwords, bank accounts, etc.

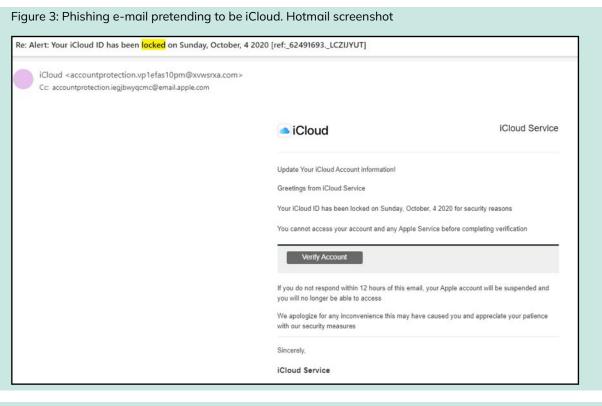
### **Examples:**

Email coming from an attacker who is pretending to be Amazon. The attacker is asking to download a document for reading further details about the unusual activity of the account. However, the file could be infected with malware.



Phishing e-mail pretending to be Amazon. Hotmail screenshot

Illegitimate email from iCloud. The email is asking the victim to click at the button to verify information in order to unlock the account. In this case, normally after clicking the button, victims will be directed to a fake website where they will start a "sign in" process that includes typing their password.



Email pretending to be sent by an important bank from Spain. As in the previous examples, the attacker is trying to make the victim think that their bank account has been locked. By clicking the "Information confirmation" button, the victim will be tricked to provide their bank information.

Figure 4: Phishing e-mail pretending to be CaixaBank. Hotmail screenshot



### What happens when the attacker gets the personal information?

Below are some examples of what the attackers do after having access to the victims' credentials and sensitive information:

- Data breaches
- Doxing: Publishing the victim's personal or professional information online.
- Asking victims for money in order to get back their documents, pictures, information, etc.
- Asking victims for money to have access to their computer, accounts, etc.
- Modification in the victim's computer's systems
- Locking out accounts, without the possibility for getting them back
- Directing victims to malicious sites, spam, etc.
- Having access to the network of a company, etc.
- Getting money from bank accounts.
- Buying things.
- etc.

### **Examples of real cases from Facebook:**

#### **Identity theft**

Identity theft is when the attacker steals personal and confidential information, and uses it for fraudulent activities.

Figure 5: Example of phishing case 1. Facebook screenshot



Figure 6: Example of phishing case 2. Facebook screenshot



The most common information that thieves look forward to stealing are:

- Full victims' names
- Victims' birth dates and places of birth
- Social security numbers
- Physical address
- Email address
- Phone number
- Passport number or ID number
- Drive license
- Financial account numbers
- Banking PINs
- Credit card information: Number, expiration dates, security codes, holder's

name.

- Memberships, affiliations
- Employer and employee information

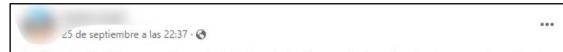
Identity can be stolen through different ways, but the most common ones are through phishing or by creating similar social media profiles with stolen pictures from the victim's social media public posts.

### Some of the fraudulent activities committed by the identity thief are:

- Financial fraud: Identity thieves use the stolen information to apply for loans, credit cards, make unauthorized payments, etc.
- Medical Fraud: To fraudulent get prescription medications, medical treatments, insurance benefits, etc.
- Tax Fraud: They may submit fictitious tax returns in the victim's name in an attempt to obtain refunds or other financial advantages.
- Social Engineering: By manipulating the stolen data, identity thieves can trick other people into disclosing more private information, launching a chain reaction of fraudulent activities.
- Contact friends and family: Identity thieves get into the social media account or create a similar profile of the victim to contact friends. Attackers pretend to be the victims and tell their friends that they are passing through a bad situation. After making a close contact with them, thieves proceed to ask them for money.
- Employment Fraud: They might use stolen data to get jobs, which might cause problems for the victim's employment history, taxes, benefits, etc.
- Criminal Activity: Thieves may use of the stolen identity for illegal purposes, such as eluding police authorities, providing fake identities to police, etc.

#### **Examples of real cases from Facebook:**

Figure 7: Example of identity theft case 1. Facebook screenshot



My identity theft happened in early July, they locked me out of my Facebook account, and took my personal and business identity. Ruined my website, stole my yahoo emails. They captured my URL, and placed fake windows on my page, when I googled Facebook help, I would come in contact with them. Went to the police, and filed several reports. I am looking for new ID theft protection programs. Do not like the one I have now. I heard Aura is very good. They went as far as trying to scam me again acting like web developers, asking me to get rid of my web host and security. Police asked me to block them, as they were harassing me nonstop. A friend of mine said I need to get a new Apple ID, and a new computer. He thinks they might have placed malware on my computer, as I noticed I would see email appear and disappear, on my phone, and MacBook.

Figure 8: Example of identity theft case 2. Facebook screenshot



Hey also my identity theft was someone using my KIDS social security number!! They used my maiden name to open bank accounts, offshore accounts, apply for car loans, utilities for a home, then they straw bought a house!! They made credit cards and used them to pay for all sorts of stuff! They caused people to get investigated by the feds and now they are in trouble with crime rings and they have been giving out my picture and saying that I was the one that was doing all of the finical fraud!!

### How to prevent phishing and identity theft?

- Do not open attachments in emails without knowing who the sender is and confirming that they actually sent you that email. Also, confirm with them that the email contains an attachment and that they know what it is.
- Ignore emails with incorrect spelling (Amason instead of Amazon or Instagr. am instead of Instagram, etc.).
- Try to get directly from the legitimate website, instead of the link of the email.
   For example, get into your Amazon account directly from the website to check if the account is really locked.
- Do not click links (URLs) in emails unless you know who sent you the link.-Make your brain and passwords stronger. Although they might be difficult to be memorized, the use of complex passwords can prevent you to become a victim of these attacks. Avoid date of birth, pets' names or other easy details that the thief can try as password.
- Do not use your pets' names, etc. in the questions to reset your password.
- Use different passwords for different sites.
- If possible, use the two-factor authentication in your accounts. This is an extra layer where first the users type their usernames and passwords. After this, the account asks them for further infor-

- mation, for example a code that users receive through a text message on their mobiles.
- Never enter to pop-up windows. Some of them might not be safe.
- Log out and reboot your computer whenever you finish using it.
- Scan your computer frequently.
- Use antivirus program and keep it update. Ensure that the program is from legitimate companies.
- Use a firewall.
- Update your operating system. System updates have new security patches that will help you to have the computer more protected.
- Do not enter to websites that your browser notifies you that could not be safe.



### **Disclosure of information (Doxing and Outing)**

Disclosure of information can be done in several ways and purposes:

### **Doxing or Doxxing**

Doxing/doxxing is when someone reveals personal information about someone, without their permission. Some of the information is posted in online media is:

- Home addresses
- Signature
- Workplace details
- Passwords
- Personal phone numbers
- Social security numbers
- Family background
- Education details
- Personal photos
- Personal videos
- Private correspondence
- Criminal history
- Embarrassing personal details
- Bank account
- Credit card information
- National registration identity card number
- etc.

The evolution of the term "doxing" starts in the 1990s, from the word "documents". The term "dropping dox" originated when "documents" was abbreviated to "docs" and subsequently "dox." Dropping dox was a tactic employed by cybercriminals to reveal the true identities of rival cybercriminals. They lost their anonymity when they disclosed their true names, making them visible to law enforcement and any others attempting to locate them.

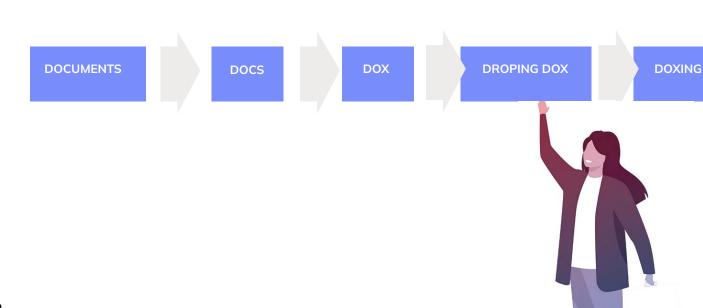


Figure 9: The evolution of the "Doxing" term. Own creation. Source: Keeper Security

### How do attackers compile information?

#### **Usernames tracking**

Do you tend to use the same usernames on different accounts? You are more vulnerable of a doxing. For attackers it is easy to track your username, leading them to all your websites, applications, social media profiles, etc.

#### **Domain Search**

The details of domain name website owners are kept in a registry and are frequently accessible to the public. The buyer of the website domain needs to keep private their personal details, during the purchasing procedure. In the opposite, attackers will be able to find personal information, such as phone number, address, etc.

### **Phishing**

Is a form of social engineering attack that happens when a victim is tricked into opening a masquerade email, text message, etc., that seems to be legitimate. Consult all the details of phishing in the subchapter "Masquerading, Catfishing, Phishing, Digital identity theft".

#### **Packet sniffing**

Data is structured in packets when they travel on the internet. When an attacker intercepts and reads private data traveling over a network, it is known as packet sniffing.

Threat actors mostly use packet sniffing to target sensitive data, including unencrypted email messages, financial information and login passwords. Since anybody may join a public WiFi network, packet sniffing usually happens when a victim is connected to it.

#### Checking on social media profiles

Many people do not include private settings in their social media profiles, making strangers have direct access to pictures, information, educational and work profiles, family members, financial situation, locations, etc.

#### **Tracking IP Addresses**

They attacker can obtain the victim's IP address and track their physical location. Through social engineering techniques, the attacker uses the IP address to convince the victims' ISP to provide more information about the victim.

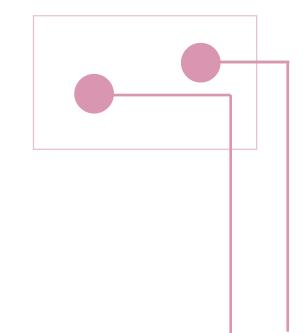
#### Mobile number tracking

Atackers can use your mobile number to look for more information about the victim. Searching the mobile number can lead to different social media, white pages websites, etc.

European Union Agency for Fundamental Rights's staff, 2020, A long way to go for LGBTI equality, European Union Agency for Fundamental Rights.

Doxing can be done with different intentions, such as:

- Revenge or punishment intentions
- Cause alarm
- Cause fear of violence or incite violence
- Intimidation
- Humiliation
- Cause harassment
- Damaging the reputation of the victim
- Etc.



For some people from the LGBTQ+ community, the journey of self-discovery and disclosure of their gender identity or sexual orientation is a personal process. It is critical to understand that each person has a different procedure. Some people can disclose their LGBTQ+ identity early in life, while other persons can take years to understand and accept their identities. Furthermore, some persons might have concerns in disclosing this information, as they could face different challenges in their lives, such as:

- Discrimination and stigma
- Harassment
- Violence
- Rejection by family and friends
- Work Consequences
- Rejection by schools
- Legal Consequences (in some countries)
- Lack of Support Networks
- Religious and Cultural Beliefs
- etc.

The process of self-discovery and disclosure can be violated by other persons. In the digital world, one type of cyberbullying is called Outing. Outing is disclosing the sexual orientation or gender identity of a person, without their permission.



In digital communities, outing can have far-reaching negative impacts, especially because when the identity is revealed, there is no way of taking back this message. Although pictures, videos or other information can be deleted, the main objective of the message is already disclosed.

### Why outing is a concern in our modern society?

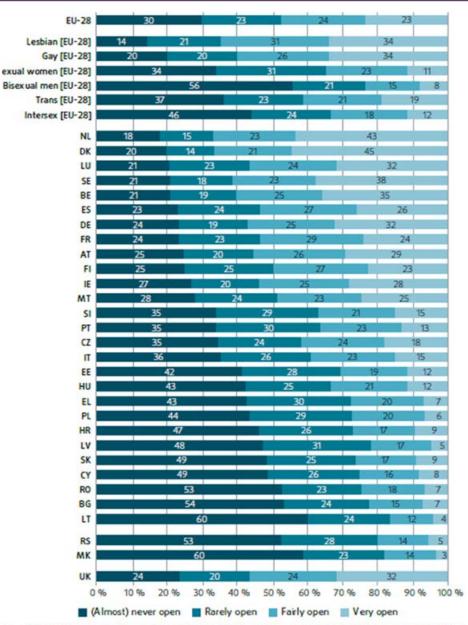
The study "A long way to go for LGBTI equality" from the European Union Agency for Fundamental Rights, provides figures about the disclosure rates in Europe:

- 53 % of LGBTI people surveyed are almost never or rarely open about being LGBTI.
- 23 % say that they are very open.

### Younger LGBTI respondents are less open than older respondents:

- Respondents aged 15 to 17: only 5% are very open.
- Respondents aged 18 to 24: only 12% are very open.
- Respondents older than 55: 36 % are very open.
- LGBTI respondents with higher education levels (27 %) are nearly twice as likely to be very open than the ones with lower education levels (14 %).
- 61 % of respondents always or often avoid simple displays of affection in public, i.e. holding hands.





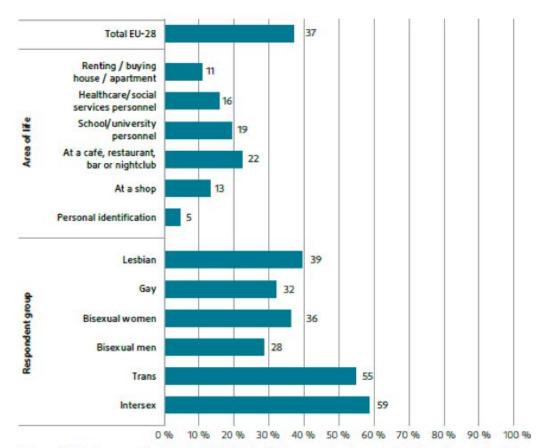
- es: The EU-28 aggregate includes the United Kingdom (UK) because the reference period of the data collection is from when the UK was a Member State.
  - Out of all respondents who provided a valid answer of at least one sub-question from battery G1 (n = 139,363; in EU, n = 137,085); weighted results.
  - b The presented percentages are based on answers to question G1: "To how many people among the following groups are you open about yourself being [RESPONDENT CATEGORY]? (A. Family members (other than your partner(s)); B. Friends; C. Neighbours; D. Work colleagues; E. Schoolmates / University co-students; F. Immediate superior/head of department; G. Customers, clients, etc. at work; H. Medical staff/health care providers".

rce: FRA, EU-LGB II II 2019

- 1 in 3 (33 %) always or often avoid certain places for fear of being assaulted, threatened or harassed.
- 26 % of respondents hide being LGBTI at work.

A person can take it seriously while deciding to reveal their sexual orientation or gender identity, due to existing external factors. Discrimination is not a self-perception or fear. Discrimination is real towards LGBTQ+ people of all ages, in all environments, with concerning figures detailed in the study "A long way to go for LGBTI equality":

- 21 % felt discriminated at work in the year before the survey of this study was carried out (2019).
- 10 % felt discriminated when looking for work in the year the survey of this study was carried out (2019).
- 37 % felt discriminated in other areas different than work: school, university, housing, café, restaurant, bar, night club, healthcare or social services, shops, or after showing an ID document. 55% of trans and 59% of intersex feel discriminated in these life areas.
- 53% of respondents aged 15-17 experienced discrimination in some area of life.
- 41% of respondents aged 18+ experienced discrimination in some area of life.
- Of the recent incidents of discrimination, just 11% were reported to the nation's equality body or another organisation.



otes: The EU-28 aggregate includes the United Kingdom (UK) because the reference period of the data collection is from when the UK was a Member State.

- Out of all respondents who were discriminated against in at least one area other than employment in the 12 months before the survey (n = 126,709); the totals vary in individual areas of life; weighted results.
- b The presented percentages refer to respondents who answered 'yes' to at least one situation in question C1: "During the last 12 months, have you personally felt discriminated against because of being [RESPONDENT CAT-EGORY] in any of the following situations: C. When looking for a house or apartment to rent or buy (by people working in a public or private housing agency, by a landlord); D. By healthcare or social services personnel (e.g. a receptionist, nurse or doctor, a social worker); E. By school/university personnel. This could have happened to you as a student or as a parent; F. At a café, restaurant, bar or nightclub; G. At a shop; H. When showing your ID or any official document that identifies your sex".
- Besides 'yes', respondents could answer 'no' and 'don't know'. The percentage of respondents who answered 'don't know' to all relevant situations did not exceed 0.5.4 % in any breakdown category in the chart.

Source: FRA, EU-LGBTI II 2019

European Union Agency for Fundamental Rights's staff, 2020, A long way to go for LGBTI equality, European Union Agency for Fundamental Rights.

Figure 11: Respondents who felt discriminated against due to being LGBTI in area other than employment in the 12 months before surve in EU-28, by area of life and group (%).Source: FRA, EU-LGBTI II 20:

### **Teaching Unit: The outing case of Channing Smith**

**Duration**: 2 hours

The aim of the activity is to increase awareness about the negative consequences of the intervention and violation of the disclosure process of people from LGBTQ+ communities.

**Step 1:** Ask your learners to make research about the case of Channing Smith from Tennessee.

**Step 2**: Ask them to answer the following questions:

- Who was Channing Smith?
- At what age he became a cyberbullying target?
- How was he involved in outing?
- Had Channing disclosed his sexuality publicly before the main attack?
- What happened after the messages where leaked? How did classmates react? What did Channing Smith do?
- Why was Channing Smith disappointed about the attackers?
- What do you think about the last message of Channing Smith?
- Where did Channing Smith live? Did he live in a rural area or in a city?
- How did the school's principal react after the students' tribute?

If your learners are having troubles to find all the answers, you can provide them the following news:

- From The Washington Post "A teen's intimate messages to another boy were leaked by classmates. Hours later, he killed himself, his family says": <a href="https://www.washingtonpost.com/nation">https://www.washingtonpost.com/nation</a>
- From The NBC "Tennessee teen dies by suicide after being outed online": https:// www.nbcnews.com/
- From The New York Times "A Teenager Killed Himself After Being Outed as Bisexual. His Family Wants Justice": <a href="https://www.nytimes.com/">https://www.nytimes.com/</a>

**Step 3**: Review and discuss your learners' answers.

**Step 4:** Make the following reflection questions:

Do you think that cyberbullying can have different consequences for victims who live in a rural town, that the ones who live in cities?

- What actions could have been done before committing suicide?
- How can these incidents be prevented in your environment (school, work, etc.)?
- How outing someone without their permission can affect their mental well-being?

- What kind of support can you offer to persons from LGBTQ+ to protect their rights?
- What actions and initiatives you think are necessary so people from LGBTQ+ communities do not hide their gender identities or sexual orientations?

**Step 5:** Ask your learners to get divided into groups. Ask each group to identify main quotes of Channing Smith's family and friends. For example, from Joshua Smith (Channing Smith's brother):

"Nobody deserves
to die as they are
figuring their way
through this complex journey called
life"

Ask them to select quotes and create a collage to raise awareness about outing and its negative consequences. Motivate your learners to:

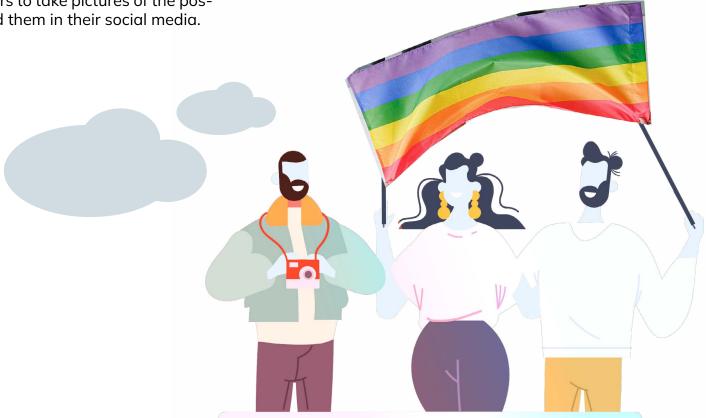
- Select a creative grid design that fits all the messages.
- Combine different textures
- Combine different colors to create eye-catching contrasts.
- Use 3D and other creative techniques.

**Step 6**: Present the collages. Each group should give the reason of the selected quotes. Paste the collages in your facilities. Also, ask your learners to take pictures of the posters and upload them in their social media.

### Spoiling alert! Do not read it, until you finish the case

Studying this case is relevant for promoting and facilitating the inclusion of LGBTQ+ Communities. The case of Channing Smith is a touching demonstration of how common is the violation of privacy. The act of outing Channing Smith led him an extreme detrimental impact in his overall well-being, causing him to take his own life. This case shows how some people can underestimate the privacy, rights and values of others. It is important to:

- Respect and preserve people's freedom to express who they are, whenever they want.
- Understand that a person's sexual orientation and gender identity is a private and personal matter.
- Disclosing the gender identity and or sexual orientation of a person, without their permission, is a violation of their privacy.
- Allowing and supporting them to disclosure this information with others, on their terms and time frames, is a way to honor their process.
- Offer support and acceptance.



### **Exclusion**

The Cambridge Dictionary defines exclusion as "the act of not allowing someone or something to take part in an activity or to enter a place".

Unfortunately, it is too typical for exclusion to be used as a cruel kind of bullying among young communities. This kind of discriminatory conduct is not only part from our real world but also into the digital one. Speaking about the digital world, exclusion is an intentional act of not including a person in online groups, etc.

People frequently utilize exclusion, either in both contexts to establish their dominance; denigrate others, or follow behaviors from their peers.

Some examples of exclusion can be:

- Not inviting a person to a group chat where they organize different face-to-face activities.
- Exclude someone in participating in discussions, such as online forums, online communities, etc.
- Not adding a person to a chat group of friends in order to speak negative things about them.
- Asking others to unfriend the victim from

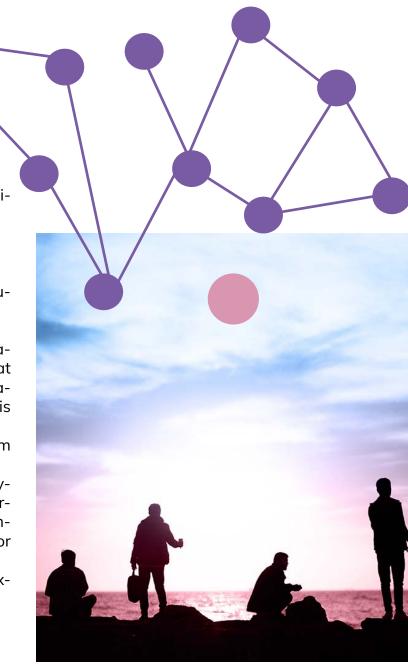
social media accounts.

• Ignore the victim when sharing their opinion, asking questions, etc.

etc.

Some negative consequences about exclusion are:

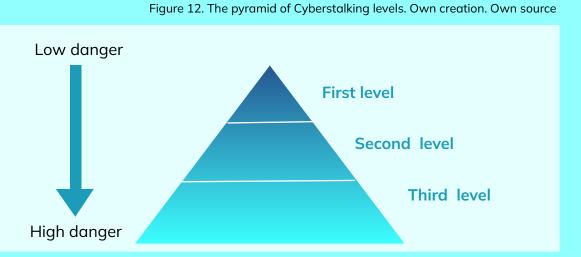
- In some cases, the victim has a face-to-face friend relationship with the group that is excluding them. Not knowing the reason behind the exclusion, will affect this relationship.
- The excluded person can become victim of other cyberbullying attacks.
- It can accelerate the process of being cyberbullied in other ways. Excluded persons do not know what others are planning, not having chances to prevent or defend themselves.
- Digital exclusion causes isolation and exclusion in the real world.
- etc.



### Cyberstalking

Cyberstalking is when a person has an obsessive control, tracking and harassment of someone, by using digital technologies.

Cyberstalking actions can escalate and get out of control in a fast way, putting the victims life in real danger. Cyberstalking has different levels of escalation:



Like many other internet hazards, cyberstalking in many cases begins discreetly and inoffensive. Victims may not initially give much attention to the early indicators of cyberbullying. The first level can start with jokes, harmless messages, compliments or even passive-aggressive conducts through online media. However, cyberstalking can evolve into a medium level where cyberstalkers can start with harassment, disrespectful messages, etc., raising concerns and distress on victims. Moreover, cyberstalking can evolve to a third level, in which cyberstalkers continue with intimidation, threats, harmful attacks, aggression where the victim is in danger, not only in the digital world, but in the real one. In some cases, stalkers commit physical harm to their victims.

Some behaviors of cyberstalking are:

- Tracking someone's movements using location (GPS) technologies such as apps, GPS gadgets, etc.
- Searching where the victim will go and make "accidental" encounters.
- Sending repeated unwanted messages through email, instant messaging, texting, etc.
- Over insisting messages or requests of "love" or sex.
- Obsessive contact through several online accounts.
- Use spying apps.
- Telling the victim that they are controlled, without hiding possibilities.
- Constant aggressive messages and threats.
- etc.

Regretfully, cyberstalking may become an extremely prevalent problem in love relationships, especially when one or both partners display extreme jealously and a constant need of control the other's actions. Cyberstalking tactics in these situations can take many different shapes, frequently indicating a lack of trust, low self- esteem, and low securities. Sadly, in our unprepared society, many of the following cyberstalking tactics are normalized in relationships:

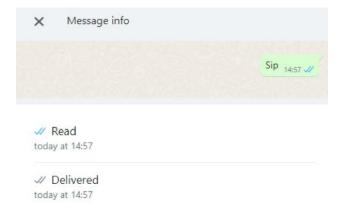
- Keeping a close eye on the partner's online activities.
- Checking constantly the time of their last online connection.
- Keeping an eye on their social contacts, asking to know who they are speaking with and why.

- Requesting access to their personal gadgets or communication platforms.
- Requesting the GPS location of the partner.
- Asking the partner why they viewed a message but did not reply right away.

Some hints that could let you know that you are a victim of cyberstalking, or at risk of becoming one are:

- Obsessive control of each of your online movements.
- Constant engagement with most of your posts.
- Contacting, controlling and following friends and family members.
- Contstant and obsessive questions: Who are you with? Where are you? What are you doing?
- Do not take your request of leaving you alone.
- etc.





### What is the difference between harassment and cyberstalking?

The terms of harassment and cyberstalking might sound similar, however there are some differences between them:

In cyberstalking the attacker is involved in an obsessive behavior.

- Cyberstalking attacks towards one victim are more frequent than in harassment.
- Cyberstalking can last for long periods of time.
- At first, persons might not be aware that they are victims of cyberstalking. They might not experience distress or fear on the first instance.

### **Teaching Unit: The pyramid of cyberstalking**

**Duration:** 90 minutes

The main aim of the exercise is to raise awareness about the alarming and fast escalation of cyberstalking behaviors. Learners will be able to review the consequences that these obsessive behaviors cause in victims.

**Step 1:** Ask your students to watch the video made by the ABC News, Nightline, published by Kenyanese:

Nightline| A Woman's Affair that Morphed into Cyber-stalking Horror . A video that explains the case of Courtney Allen, a woman who was a victim of cyberstalking that caused damaging consequences in her life and family:



ABC News, Nightline. Kenyanese YouTube Channel. Nightline| A Woman's Affair that Morphed into Cyber-stalking Horror. link

**Step 2**: Ask your participants to analyse the cyberstalking behaviours from the video and classify them into the main levels of the cyberstalking pyramid:

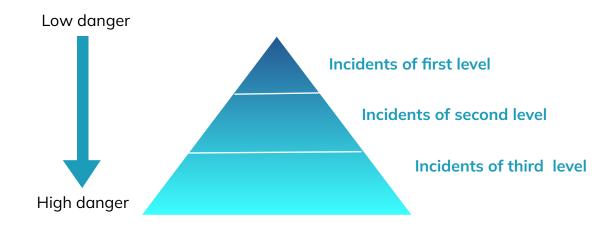


Figure 13: The cyberstalking pyramid. Own creation. Own source

**Step 3:** Show results among the group.

**Step 4:** Ask to the group the following reflection questions:

- What do you think about the escalation of this case?
- At what level do you think is important to take counteractive measures? Why?
- Do you think cyberstalking happens more

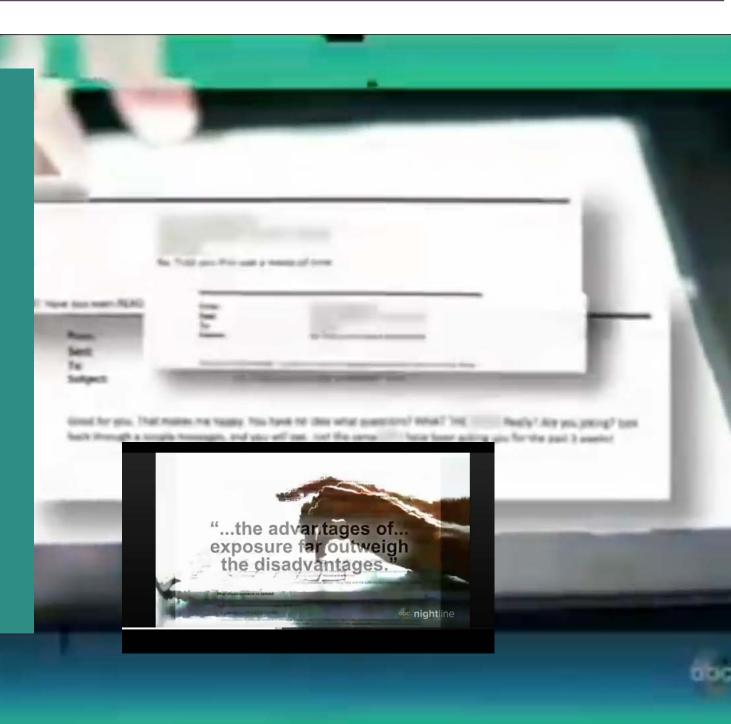
- frequently in persons from a specific sex or gender identity?
- Do you think cyberstalking cause real life repercussions?
- Why is important to take counteractive measures as soon as possible?

### Spoiling alert! Do not read it, until you finish the case

The lessons learned from Courtney Allen's case serve as a clear warning that cyberstalking may constitute a threat in both, the physical and online worlds.

Reviewing this case is important to become aware of how crucial it is to identify and stop cyberstalking, at its very beginning (first phase). Many times, people would underestimate the situation and ignore the initial indications of cyberstalking because they believe there is no imminent risk.

On the other hand, when victims do not resolve and stop the situation, cyberstalking can escalate in a disturbing and fast way. The more it escalates, the more complicated it is to stop cyberstalkers. It might have terrible repercussions that might greatly affect our lives.



### **Electronic insults:** Flaming and trolling

Electronic insults is a type of cyberbullying that are available in all media.

### **Flaming**

According to the Social Media Victims Law Center, flaming is "a form of cyberbullying that involves repeatedly posting insulting and intimidating language at another user in an online forum. Social media, chatrooms, YouTube, gaming rooms, or any online platform where users can share content are common places for flaming cyberbullying. Flames are often personal and intended to cause a recipient to feel shame and humiliation."

### **Trolling**

Trolling is the purposeful publishing of offensive and provocative information online in an effort to sabotage conversations, provoke or evoke strong feelings in other people.

Trolls can exhibit a range of disruptive activities, such as disseminating fake information; use irony and sarcasm to provoke reactions; send inflammatory messages, etc. The objective of trolls is to have fun by inciting chaos, manipulating others, etc.





Ah, that's why, I think there are more people from .. What a dam

#### Me too dam

- and they asked you for more DAM?
- -We have naval mines and we can't stop the crossing by boat... damn, that's strong
- -Naaaaa, better to bomb... really, how people are...
- -Go to the Canary Islands and see for yourself how the QUEMA people are
- Reread what you have written and you will realize the immense nonsense you have said...
- -: Whatever you say, geniuses

It's obvious that you didn't do the Nini military service You, for sure, have never seen a mine in your life, Hulio...

- Seriously, the people from VoX are getting more and more stupid every day...
- Please, let's keep the good vibes in the group. Insult each other if necessary, but in private, please. Thank you!
- How did this lead to that?

- -Naaaaa, better to bomb...really, how the people are...
- -Go to the Canary Islands and see for yourself how the QUEMA people
- -Reread what you have written and you will realize the immense nonsense you have said...
- Whatever you say, geniuses

It is clear that you did not do the military service Nini

- You, for sure, have never seen a mine in your life, Hulio...
- -: Seriously, V..X members are getting more and more stupid every
- Please, let's keep the good vibes in the group. Insult each other if necessary, but privately, please. Thanks!
- How did this lead to that?

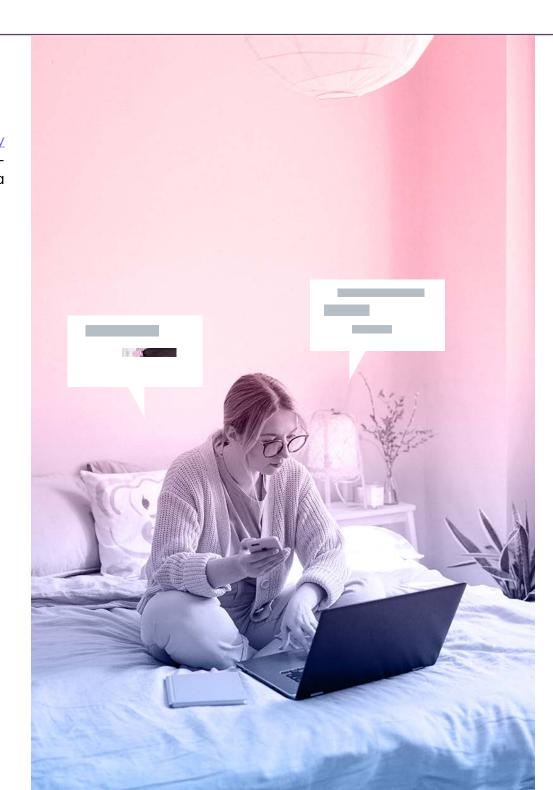
### **Happy slapping**

The Cambridge Dictionary defines happy slapping as "the activity of attacking someone and filming the attack, especially with a mobile phone".

Why happy slapping is a concern in our modern society?

### <u>Save the Children</u> provides some concerning figures in their website:

- Approximately 76,643 young people in Spain have been victims of happy slapping during their childhood.
- 61% of cases happy slapping, the aggressors are friends or colleagues.
- The average age at which they suffered happy slapping for the first time was 14 years old.



In our modern and unprepared society, it has become increasingly prevalent to see constant videos shared on social media, websites, blogs, and various online platforms, that show different acts of aggression (physical, verbal, sexual). What is truly concerning is the tendency for these videos to be presented in a seemingly humorous manner. On the other side, a significant reason behind the creation and dissemination of happy slapping lies in the desire for becoming viral and the pursuit of financial gain and fame.

This has led in a concerning trend where acts of violence, pranks, confrontation, etc. are often trivialized for the sake of entertainment.

In the digital era, where social media algorithms reward the increased visibility and followers, creators often intentionally craft content that pushes the boundaries of acceptability. This "funny" content blurs the lines between reality and amusement, where viewers are not aware about the gravity of these situations.

According to Save the Children happy slapping has the following common patterns and phases:

### First phase:

- Prior Agreement: Usually, there is an agreement among two or more individuals on when and how to attack another person. Usually, the victim is someone who has already been bullied or cyberbullied.
- The pretext: Bullies typically search for a pretext to isolate the person who they plan to attack. They look for places where they can be alone and where anybody can stop the aggression.
- Physical Aggression: In most of the times the aggression is done by more than one person, where some of them are ready to record the incident and the others attack the person. There are some other cases, where an aggressive incident emerges without previous planning, and others capture the moment.

### **Second phase:**

Share the images: After the completion of the first phase, the second phase consists in sharing this aggressive content through different online media. The victim suffers continuing harm as a result of both, the attack and the constant reproduction in digital devices.



Happy slapping is a phenomenon where we should raise important questions about the desensitization of violence; the reduction of empathy in our society; and the consequences of normalizing aggression in our digital interactions. Happy slapping is increasingly blurring the lines between real life and virtual reality.

Youth communities and other groups need to be aware about the ethical implications of the content they consume and share, in order to reach a safe and healthy online environment.

### Teaching Unit: The erosion of empathy and respect

**Duration:** 3 hours

The aim of this activity is to increase awareness about the blurred lines among being funny losing empathy and respect towards others. Also, this exercise looks forward to becoming aware of how "funny" moments lead to uncontrolled situations that can change our lives forever.

**Step 1:** Ask your learners to watch the following video:

Try not to laugh (prank edition) #shorts #funny: A video from Awesome Chimp that shows happy slapping incidents: <a href="https://www.youtube.com/watch?v=FRdgTgKxnx4">https://www.youtube.com/watch?v=FRdgTgKxnx4</a>



### Step 2:

Ask the following reflection questions:

Was this video funny for you?

Take a look at the following image:



- How many views the video has?
- When was the video published?
- How many likes the video has?
- How fast can a victim become viral?
- How do you think these persons felt at that moment?
- How do you think these persons feel now that they become viral?
- Do you think they can become target of more "funny" incidents?
- Some of these people might be chosen randomly; which ones you think they could be victims of happy slapping?
- Do you think the ones who were not chosen randomly are involved in a healthy environment (at work, with their family/friends, etc.)?

**Step 3:** Take a look to each of the following real comments from this video and determine the level of awareness of the person who wrote it:

Level 1: Not aware of happy slapping.

**Level 2:** Medium aware - people might not know what happy slapping is, but they know that these videos are not ethical. Despite this, they laugh about them.

**Level 3:** Totally aware about happy slapping and consequences.

- That plastic wrap liked that first girl so much it kept her glasses. That and the mirror had me Imao.
- Banana prank .. and the laugh after.
- The first one got potential. She can be a star.
- Dude with the mirror in the bed was thinking to himself "Now you know how I feel every morning".
- Never prank someone next to a road, and don't prank employees of a business.
- Pranking store employees when they are on shift is a great way to get arrested.
- Pranks in private with people you know, yes, funny. Pranks with strangers for the internet, no, you're asking for trouble.
- It's scary how people have normalized

- pranking strangers while they're minding their own business.
- Me convinced I'm not gonna laugh. Me laughing so hard after the first clip.
- This was great!!! I laughed so hard.
- The 3 plastic wrapped doorway had me crying thank you, I needed that!
- Even she was surprised by her own appearance.
- Invisible danger prank, works every time.
- The rat pranked should be jailed. No sense of respect for private space.
- The rubber banana prank, blanket ghost prank, mirror prank, and plastic-wrap prank were all diabolical... and hilarious! they were also the only humane pranks in this video, as it is dangerous to prank someone near a road (especially when there's traffic), and it is wrong to prank strangers in a public area (such as a grocery store).
- WARNING: If you frighten someone and they have a heart attack, you could be charged with murder and certainly break your pocket.
- That first prank should never be done on road sidewalks especially when the victim's first escape option in response is towards the road.
- Lawyers reaction: someone IS getting sued.
- Warning: never ever throw even a fake mouse at a person who has musophobia. If it's a woman on the edge she will beat you down then pick you up so she

- can put you down again.
- These examples are how to lose people's trust in you.
- That banana slap was personal.
- The mirror was the best haha.
- It's all fun and games until someone gets hurt and you find out you're paying their hospital bills.

**Step 4:** Show to the group the following comment:

"It's all fun and games until someone gets hurt and you find out you're paying their hospital bills".

Ask your learners to research about the case of Gavin Waterhouse which incident happened at Keighley, in 2008. Learners should answer the following questions:

- What happened? Describe the incident
- Who were involved in the happy slapping attack?
- Who was Gavin Waterhouse?
- Who is Mark Masters?
- Who is Sean Thompson?
- How old were the involved persons on

that time?

- Who recorded the attack?
- What was the duration of the video?
- What was the attitude of the attackers?
- What happened to Gavin Waterhouse?
- What sentence did Mark Masters, Sean Thompson and the girl who recorded the video receive?

If your learners are having troubles to find all the answers, you can provide them the following websites:

- From the Guardian: Girl jailed for filming 'happy-slap' killing
- From YorkshireLive: The cruel killing that put Bradford at the centre of a landmark 'happy slapping' case, link
- From Mail Online: Teenage girl jailed for two years for filming 'happy slap' killing on mobile phone <u>linkl</u>
- From BBC News: 'Happy slap' teenagers sentenced link

**Step 4:** Review as a group the answers. Ask the following reflection questions:

- Do you think the attackers knew at that time the seriousness of the situation?
- Do you think the girl, who recorded the incident, was aware that she was participating in a crime?
- How the 15 seconds video changed the life of the girl?
- After attackers finished, they went away laughing and started to share the video. By doing this, what value do you think the attackers were giving to the life of Gavin Waterhouse? How do you feel about this?
- Do you think the society is aware of happy slapping?
- Do you think youth communities have lost empathy and respect values?
- Do you think groups of other ages have also lost these values?
- Do you think happy slapping happens more frequently in persons from a specific sex or gender identity?
- Do you think it is easy that a happy slapping incident can get out of control, leading to harmful damages?
- How can you prevent these events?
- What would you do if you were witnessing a happy slapping incident?



#### Spoiling alert! Do not read it, until you finish the case

The importance of studying these previous cases of happy slapping lies in the unambiguous contrast between the initial motivations of the attackers and the consequences that arises. In many instances, the perpetrators engage in happy slapping as a misguided form of enjoyment, with a casual desire to have fun at the expense of others.

Some of the video comments show passive spectators, who inadvertently normalize these behaviors, by laughing about these moments.

The gravity of the situation is not realized until things get complicated. It is crucial to be aware that happy slapping carries severe repercussions. Happy slapping attackers can face legal repercussions, such as imprisonment. Mark Masters was sentenced to 7 years; Thompson to 6 years and the teenage girl (who recorded the video) to 2 years. On the other side, victims struggle with not just physical injuries but also with emotional scars. Unfortunately, Gavin Waterhouse is one of many victims who are not here to share their stories.

We can participate actively to reduce these events; it is important to:

Avoid consuming these kinds of videos;

• Do not share happy slapping content;

• Do not participate in happy slapping;

 Intervene whenever we are witnessing an event;

• Report to authorities whenever we see a happy slapping incident;

• Help the victim.



#### **Sextortion or Online Sexual Coercion**

"Sextortion" or "online sexual coercion" are some of the terms known for obtaining online sexual content (mostly pictures and videos) through different tactics such as threats.

According to the FBI, sextortion can occur on a variety of digital platforms, including chat services, websites, applications, and online games where users gather and engage. Under some circumstances, the first communication with the criminal could be a threat. The person might say to have an image or video of the child and threaten to share it unless the victim provides more pictures. Another way sextortion could start is when children think they are speaking with a friend who is similar in age, expressing interest in a romantic connection, or someone who seems to be giving something of value.

After obtaining one or more videos or photographs, the perpetrators use threats of publishing or even physical violence to force the victim to provide further material. When children are caught up in this pattern, they frequently feel ashamed, afraid, and confused, which discourages them from asking for help or reporting the abuse.

According to the <u>Department of Homeland</u> <u>Security</u> from the United States and Europol, some other tactics used by perpetrators are:

- Creating a fake relationship with the victim.
- Secretly capturing pornographic chat messages and videos.
- Contacting the child through different identities.
- Pretending to be someone of a different sex.
- Hacking accounts for obtaining sexual pictures or videos.
- Threatening to terminate one's life if the victim declines to provide sexual pictures.
- Analyzing the victim's friends list and other publicly accessible social media accounts to learn more about them and to look for any more personal information that can damage their reputation.
- Reciprocity "If you show me, I'll show you."
- First offering the child/youngster something in return for sexually explicit content, such cash or drugs.
- Pretending to be employed by a modeling agency.

The FBI, has also seen an increase of financial sextortion, where perpetrators obtain sexually material and then threatens the child to publish it, unless they send gift cards or money. The demanded sum can vary, and the perpetrator frequently exposes the victim's sexually explicit content regardless of whether the payment is made or not. The

FBI states that this escalating danger has tragically led to an alarming number of suicide cases.



<u>Europol</u> provides some concerning figures in their website:

- Online predators are now targeting victims as young as 7 years old.
- Female child victims are subjected to a higher degree for sexually explicit material, with 84% falling victim to this coercion, whereas male child victims experience this at a rate of 53%.
- Male victims are more frequently targeted for financial exploitation, with 32% facing such threats compared to just 2% of female child victims.



# **Teaching Unit: The case of Ashley Reynolds**

**Duration:** 2 hours

The aim of this activity is to raise awareness about the importance of reporting to the police about online sexual coercion.

**Step 1**: Provide to your learners the following statement:

In 2009, when she was 14 years old, Ashley Reynolds was a joyful teenager who had a deep passion for sports, excelled both in her academics and her social life. She also liked to maintain a journal, one that she lovingly filled with entries meant for her "future self" to discover. Unfortunately, in this year something happened to her, that she could not tell anyone, not even her diary.

**Step 2:** Ask your learners search on the internet for more information about Ashley Reynolds's case.

You can provide them the following videos for more support:

Victim of Sextortion Speaks Out: A video where Ashley Reynolds speaks about her case (https://www.youtube.com/watch?-v=ixAYkkub4Pw).

Special Agent Discusses Sextortion Case: A video where an FBI agent comments about the perpetrator (https://www.youtube.com/watch?v=miR-8uBbVrU).

**Step 3:** Ask them to answer the following questions:

- Who is Ashley Reynolds?
- What happened to her?
- Why was she complying with the requests of the perpetrator?
- What were the reasons behind her denial to tell her parents or someone else about it?
- Who is Lucas Michael Chansler?
- What different tactics was Lucas using with his victims?
- How many teenage girls were victims

from Lucas's tactics?

- How was Lucas caught by the police?
- What was Lucas' sentence?
- How many victims know that Lucas is in jail?
- If your learners are having troubles to find all the answers, you can provide them the following websites:
  - From FBI: Sextortion. Help Us Locate Additional Victims of an Online Predator: <a href="https://www.fbi.gov/news/stories/">https://www.fbi.gov/news/stories/</a>
  - From CNN: FBI: Sextrortion a growing threat: <a href="https://edition.cnn.com/">https://edition.cnn.com/</a>
  - From Thorn: Ashley Reynolds: I Want People to Remember My Sextortion Story: <a href="https://www.thorn.org/blog/sextortion-remember-my-story/">https://www.thorn.org/blog/sextortion-remember-my-story/</a>

**Step 4:** Review and discuss your learners' answers.

**Step 5:** Make the following reflection questions:

- What do you think will happen if Ashley had asked for help at the first moment?
- Why is important to contact the police in these cases?
- What do you think about the FBI agent, Larry Meyer's declaration? "We know that youngsters don't always make sound

decisions. Today, with a smartphone or digital camera, an individual can take an inappropriate picture of themselves and 10 seconds later have it sent to someone. Once that picture is gone," he said, "you lose all control over it, and what took 10 seconds can cause a lifetime of regret."

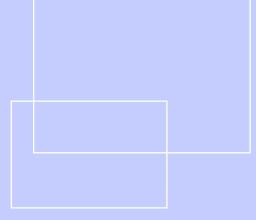
 How gender is involved in these bad practices?

# Spoiling alert! Do not read it, until you finish the case

The importance of this case is that the report from Ashley's parents to the National Center for Missing and Exploited Children (NCMEC's CyberTipline) was relevant for catching Lucas Michael Chansler. His caught was a relief for almost 350 female teens, although 250 victims might not know that the perpetrator is in jail. The police are making efforts to find these girls to reduce their fears of having future threats as well as provide them assistance. If you think that you might know someone who could be one of these girls, do not hesitate to share the FBI website

Lucas Michael Chansler had some years to contact and extort almost 350 victims. Therefore, the faster a victim reports an incident, the less time the perpetrator will have to contact future prospects.





Cyberbullying roles

Most incidents of cyberbullying include a complicated dynamic in which individuals are involved in 3 main roles. These roles are divided according to their actions:

**BULLING VICTIM** 

**BYSTANDERS** 

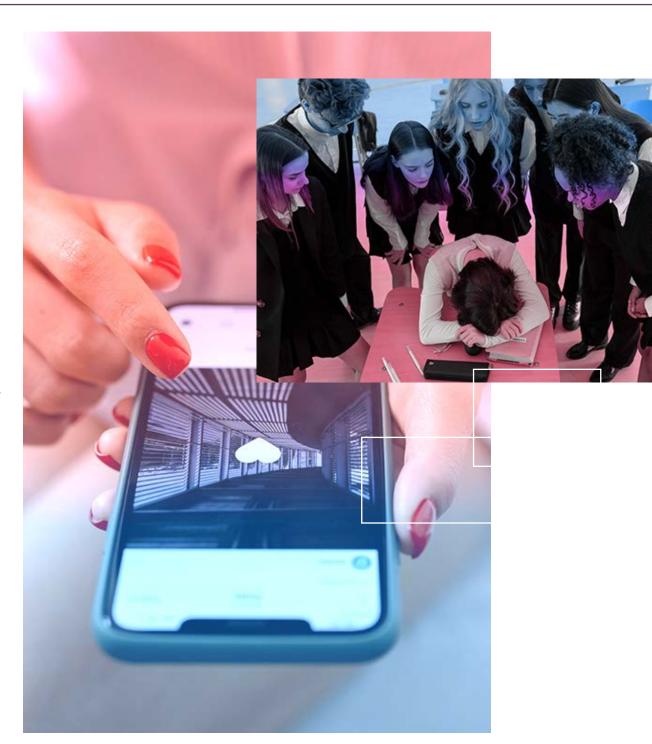


# **Bully**

The bully is a group or a person who initiates any harmful behavior that is included into the cyberbullying types, described in the chapter "Cyberbullying typology".

The bully can adopt many identities. They can be someone the victim knows, for example, a friend, classmate, peer, etc. Bullies can also be someone completely different, such a stranger they met only online. Also they could be a complete stranger.

For this reason, cyberbullying is a more complicated phenomenon than bullying because perpetrators can come from the victim's close social circle or from a larger online community. This increases a wider variety of possible motives, strategies and results.



# **Teaching Unit: Test: Am I a bully?**

The main objective of this test is to provide learners an opportunity for introspection and self-assessment to determine if they have ever engaged in cyberbullying behavior. This test is a self-evaluation where learners will have to be honest with themselves. Learners will not share their answers to prevent any judgments. The purpose of the test is not to condemn but to promote self-awareness and a responsible digital conduct.

# **Step 1:** Ask your learners to individually answer the following questions:

- 1- Have you ever published fake posts under the victim's name?
- 2- Have you ever disclosed private information, private conversations or a secret from a friend?
- 3- Have you ever disclosed the gender identity or sexual preference from anyone?
- **4.** Have you ever coerced a person to send you pictures or other information?
- **5.** Have you ever shared inappropriate pictures of videos from a friend?
- 6- Have you ever threated someone online?
- 7- Have you ever sent constant insults to someone?
- 8- Have you ever entered to a person's personal accounts without permission?

- 9- Have you ever controlled the life or locations of someone, for example a partner?
- **10-** Have you ever created a fake website from another person?
- 11- Have you ever done something online to someone that could damage their well-being (cause anxiety, fear, sadness, etc.)?
- **12-** Have you ever say comments that attack a persons' reputation?
- **13.** Have you spied on someone through online means?
- **14-** Have you ever sent a virus to a friend on purpose?
- **15-** Have you ever contacted anybody pretending to be someone else?
- **16-** Have you ever fought with bad language and insults in any online media?
- 17- Have you ever used the personal information of somebody to any type of benefit?
- **18-** Have you ever excluded someone from online media?
- 19- Have you ever recorded "funny" videos or pictures that harm the persons who are in them (affecting their reputation, violence, etc.)?
- 20- Have you ever established a fake relationship with someone online?

- **21-**How often are you involved in these situations (either starting the behavior or participating in a group)?
  - Almost daily
  - At least once per week
  - Once per 2 months
  - It happened on few times



**Step 2:** Ask your learners to count their answers:

Questions numbered from 1 to 20: Each "yes" answer is 1 point. Each "no" answer is 0 points.

Question number 21:

- Answer a: 20 points
- Answer b: 15 points
- Answer c: 10 points
- Answer d: 5 points

**Step 3:** Provide your learners the following results:

- From 15 to 30 points: you are a bully at high level.
- From 10 to 14 points: you are a bully at medium level.
- From 6 to 10 points: you are at risk of becoming a bully.
- From 1 to 5 points: congratulations, you have good online interactions.

**Step 4:** Ask your learners to write the answers of the following reflection questions. It is important that they write them so they can become accountable for their thoughts, behaviors and actions. Their answers will only be for themselves and will not be unveiled:

- Now that you know the results of your test, what score did you get?
- How do you feel about the score?
- What consequences do you think your behaviors are causing to other people?
- How can you improve these negative behaviors?
- Do you think you need additional help to reduce these behaviors? If your answer is yes, consider that your youth worker can offer you support with no judgment.

It is important to let learners know that some of them might have been involved in cyberbullying, due to the lack of knowledge about its consequences. Therefore, this test will be useful to bridge this knowledge gap and make some individual reflections about their online interactions and frecuency of their behaviors.

# **Victim and Vulnerable groups**

The victim is a person targeted by the bully. Now-a-days most of people, especially youth communities, spend a large portion of their lives interacting online. Therefore, there is always a chance that someone becomes a target. Sadly, the terrible fact of cyberbullying is that it has no boundaries. It can affect any person, no matter their age, background, physical appearance, etc. Now-adays cyberbullying attacks any person from any personality (outgoing, introverted, confident, bashful, etc.) without making any distinctions.



#### **Vulnerable groups**

Throughout the book, you will find concerning statistics about people who tend to become victims. Some groups are more likely to become victims in specific types of cyberbullying.

- Adolescents, youngsters and young adults are more at risk.
- People from LGBTQ+ communities tend to become victims of outing.
- Girls tend to be more involved in sexual coercion.
- People who constantly interact on the internet are more at risk of becoming cyberbullied.
- Public figures
- Influencers or people with a high number of followers
- etc.

Cyberbullying, when is directed to some people, has the potential to act as a catalyst to generate and contribute to hate speech. The <u>United Nations</u> Strategy and Plan of Action on Hate Speech define hate speech as "any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are."

These persons are part of groups based on:

- Their religion
- Ethnicity
- Nationality
- Race
- Colour
- Descent
- Gender
- Other identity factor

Whenever we interact online, it is important to notice that in hate speech, bullies can disguise their comments and pretend to be the victims. They can describe themselves as the good group and take advantage of the differences that exist with the other group to denigrate, etc. For example, in the study "Helping young people recognize and respond to online hate" from Kids Help Phone, mentions that one of the recurrent themes found from hate speech perpetrators is that they romanticize their past and blame victims as guilty for its declination.

In the unexpected case that you are involved as a victim of cyberbullying, due to a specific characteristic of yourself, it is important to remember that blaming yourself is not an option. Placing the blame to oneself shifts the accountability from the attacker to the victim. It is relevant to understand that becoming a target of cyberbullying is not a reflection of your characteristics, but a reflection of the harmful behavior and actions of the perpetrator.



#### The circle of roles

Different studies have demonstrated that in bullying, cyberbullying or any other type of aggression can lead to a concerning scenario: a fluidity of roles within the same person. This implies that in many times one person can frequently move between the roles.

This highlights the ways in which people's experiences and behaviors may alter over time due to a diversity of variables such social dynamics, personal experiences, lack of resilience, environmental influences, etc.

#### From victim to bully

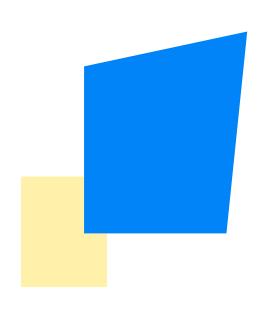
Some persons who were victims in one incident, might subsequently become bullies in future events. Therefore it is important to work on the mental health whenever a person becomes a target.

#### From bully to victim

Although we could think that bullies tend to always be in this role, they are also at risk to become victims, due to factors as:

- Exposure of their Actions: If the actions of perpetrators are reported or publicly exposed, they can become subject to reprisals from the victim or other persons (public condemnation, criticism, etc.).
- Changing Social Dynamics: Peer relationships may change socially, which can alter the balance of power. In the event that a bully loses their position of dominance within a social group, they may become the target of cyberbullying.
- Peer pressure: Peers can try to modify the behavior of the bully. Perpetrators can become victims if they resist changing.





# **Bystanders**

Bystanders are the main witnesses. They are those persons who see cyberbullying occurs but are not personally participating.

Bystanders have the power to make a significant difference in influencing how cyberbullying turn out. Therefore, bystanders can be divided according to the action they decide to implement:

**Outsiders:** Are those who watch bullying occur but decide not to get involved or do something about it. For example, people who are staring about the online comments from the bully, without sharing, reacting, etc.

**Defenders:** They take the action of addressing the incident in different ways. Defenders can interfere, publicly or privately, to stop cyberbullying. They can also report these bad actions. Furthermore, they can provide support to victims. For example, defenders can report a fake profile to Facebook and tell about the incident to main authorities (youth workers, etc.).

Reinforcers: They accept and encourage the behavior of the perpetrator. They can unintentionally reinforce the negative conduct by laughing, cheering or applauding during or after the attack. For example, in Facebook, reinforcements can be done through positive reactions (like, love, ha-ha).

Assistants: They support the bully and joins in the incident. For example, the bully creates a website for ruining the victim's reputation and assistants help in sharing the website to all the community.



Figure 16: Example of reinforcement in social media. Facebook screenshot

# **Teaching Unit: Step on or stand for**

**Duration:** 45 minutes

The main aim of the activity is to acquire knowledge and awareness of the reasons that make bystanders intervene or not in a cyberbullying situation.

**Step 1:** Cut each of the following statements into individual pieces of paper:

# Reasons of why bystanders intervene in a cyberbullying situation:

- Consider that cyberbullying is wrong.
- Is a friend of the victim.
- They are used to act under ethical values.
- Have realized that the cyberbullying is harming the victim.
- Consider the victim as innocent.
- Feels empathy towards the victim.
- They are sure that authorities (youth workers, etc.) will counteract the incidents.
- They are worried about the mental and physical health of the victim.

# Reasons of why bystanders do not intervene in a cyberbullying situation:

- Fear of becoming also a victim by the bully.
- They do not know the victim or are not friends.
- They do not have tools or knowledge of how to address the cyberbullying incident properly.
- Are not aware about the cyberbullying consequences on the victim.
- They do not think that authorities (youth workers, etc.) will counteract the incidents.
- Feel that they will lose power or reputation.
- They think that is not their problem.
- They are friends of the bully.

Make more statements to ensure that each of your learners have one.

**Step 2:** Ask your learners to place the piece of paper inside the balloon. Your learners should inflate the balloon and tie it with the rope on their leg.



**Step 3:** Make 2 groups ensuring that statements of why bystanders intervene or not are mixed.

**Step 4:** 1 person from each group should come to the middle. They will try to step on the other's balloon. The first person that steps on the balloon will have to pick up the statement and go back to the group. The group will have 20 seconds to decide if the statement is:

- A reason of why bystanders intervene in a cyberbullying situation.
- A reason of why bystanders do not intervene in a cyberbullying situation.

If the answer of the group is correct, they will win 1 point.

The team who gets more points will be the winner.

**Step 5:** Put the different statements in a chart and review the last result.

Reason of why bystanders interve- ne in a cyberbullying situation	Reason of why bystanders do not intervene in a cyberbullying situation
Answers:	Answers:

Figure 17: Answer chart: Reasons of why bystanders intervene or not. Own creation. Own source.

**Step 6:** Ask the following reflection questions:

- Why bystanders play a crucial role in cyberbullying incidents?
- If you were a bystander, what would you do? What role would you play?
- What can happen if you decide to be...
  - 1. Outsider?
  - 2. Defender?
  - 3. Reinforcer?
  - 4. Assistant?

This activity is important for youngsters learn that being a defender bystander can help the person who is suffering cyberbullying. Being an outsider, reinforcer or assistant is basically stepping on the victim. However, youngsters can decide to stand for the victim and avoid the escalation dangers that these incidents can cause.

# **Conditions for cyberbullying**

# Image: Digital identity and personal branding

Digital identity is the information compiled in the online world that identifies a person. For example, name, address, age, social media profiles, pictures, etc.

Personal branding is a strategic effort of how one person wants to be perceived by others. For example, is how influencers of healthy food show different actions to demonstrate that they are having healthy lives. It will be very rare to find pictures or videos about not taking care of themselves.

Now-a-days many people take care about their digital identity and personal branding, in order to keep a good reputation. What a person does online can have a direct consequence in the real life. Therefore, a good digital identity and personal branding helps people in several ways such as networking and academic/professional growth opportunities.

Taking care about digital identity and personal branding is an open door for perpetrators in different ways:

- Perpetrators know that attacking these aspects could be of high importance to the victim. This will facilitate the attack, for example, it will be easier to ask for money for giving back information, not uploading pictures, etc.
- For reaching a strong digital branding, people tend to publish publicly their achievements, personal information, acquisitions, going to good places, travelling, etc. Sharing this information without privacy settings, make a person become vulnerable to cyberbullying.
- Some people share their opinions according to their digital brand. This can generate insults and harassment of others who do not agree.
- Although people have never heard about digital branding, the truth is that most of us only publish the "good" pictures. Most of persons take care of their reputation. Bullies can destroy this reputation by spreading fake gossips, uploading embarrassing pictures, etc.



# Digital narcissism and social digital voyeurism

#### Digital narcissism

Some people with narcissistic behaviors can be engaged as bullies, due to their specific characteristics in their personality:

- Strong need for attention
- They constantly look forward to being admired.
- They feel more important than others.
- Liked to be recognized even without achievements.
- Do not take care about the needs of others.
- They spend time only with those that they feel as equally important.
- Look down on people they consider as "not important".
- Manipulate others to get what they want.
- Become angry when they do not catch the others' attention.

Also narcissists, in their way for looking for attention, they can contribute in the escalation of the cyberbullying incidents.

However, these characteristics also make a narcissist person vulnerable to be cyberbullied. Bullies can exploit these characteristics and involve narcissists in denigration.

#### Social digital voyeurism

The Cambridge Dictionary defines voyeurism as "the activity of getting pleasure from secretly watching other people in sexual situations or, more generally, from watching other people's private lives."

Extrapolating this definition to the online world, digital voyeurism is secretly watch



other people's online lives and interactions.

Social digital voyeurism can lead easily to cyberbullying, as some of the characteristics are:

- They secretly have access and monitor the victim's profiles.
- They monitor the victim's online activities.
- They make things to have access to private information or conversations.
- They track the victim's behaviors.
- Digital voyeurism is carried out without the victim's authorization. In many cases the victim is not aware of this.

Some examples of cyberbullying incidents in digital voyeurism are:

- Constant observation can lead to cyberstalking.
- Perpetrators involved in digital voyeurism can gather and disclose information.
- Create easily fake stories and rumors, which are credible, as they have an obsessive control of the victim's life.
- They can gather information for manipulating the victim.
- Create fake profiles with the victim's information.
- etc.

#### **Self-esteem**

Self-esteem is how persons perceive and value themselves. Self-esteem plays a relevant role in cyberbullying:

#### **Bullies**

In some cases, low self-esteem is a condition for some persons to become bullies:

- Persons with low self-esteem have more probabilities of being insecure. They become bullies to project their insecurities to victims. For example, they can attack people they perceive as more confident, to acquire a sense of superiority.
- A perpetrator with low self-esteem can target individuals who appear to be living the "perfect life", due to feelings of envy and jealousy.
- They raise their self-esteem as they boost a false sense of power and authority.
- Bullies with low self-esteem look for validation. The number of likes and positive reactions can increase their self-esteem.
- Low self-esteem can lead to frustration which can be expressed through cyberbullying incidents.

#### **Victims**

In some cases, low self-esteem can serve as a condition for certain people become a victim of cyberbullying:

- Persons with low self-esteem can project vulnerability, being for bullies an easy target.
- Persons with low self-esteem do not find enough confidence to look for support. They can think that nobody cares about them.
- Victims with low self-esteem can facilitate the escalation of cyberbullying.
- Victims with low self-esteem can believe the message of the bully, being more likely to internalize and accept harassments.



# **Teaching Unit: Celebration of being myself**

**Duration:** 3 hours

The main aim of the activity is to increase learners' self-esteem through the self-assessment of their essential values. Learners will acquire a deep understanding about what really is important in their lives, what drive their actions, etc.

**Step 1**: Ask your learners to answer individually the following questions:

- I like who I am because:
- I am really good at:
- I feel good about my:
- I am a good friend because:
- I will try to make healthy digital interactions as I will:
- The characteristics that I like the most of myself are:
- I am a good team member because:
- My friends think I have a good:
- My natural qualities are:
- My greatest talent is:
- I mean a lot to:
- I enjoy doing:
- I help others by:
- Somewhere I feel happy is:
- My goals are:
- I can achieve my goals because I am:
- I have succeeded at:

- Describe something that makes you feel proud:
- Describe something that makes you different from a family member or friend:

**Step 2**: Ask them to create a big poster with their answers. Ask them to be creative; they can use images, style and techniques that they want.

**Step 3:** Ask each learner to present their poster to the rest of the group.

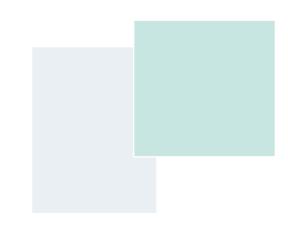
**Step 4**: Ask the following questions:

- How would the world be if all looked the same?
- How would the world be if all had the same personality?
- Why is it good to celebrate each other's differences?
- Why is important to respect the other's differences?

**Step 5:** Write each of your learners' names on separated pieces of paper. Fold them and put them in a bag. Each learner will take one paper from the bag. The student should write a positive message to that person. This

message should be kind, validating some of the information that they shared on their poster.

The importance of this activity is that learners will be empowered to align their actions with their authentic values, reinforcing their self-esteem. Learners, especially youngsters, are in a journey of self-discovery. Therefore, this activity will help them to discover, accept and appreciate themselves, boosting their self-esteem. Also learners will understand that each person's differences make them unique.



# **Impulsivity and Recklessness**

Impulsivity and recklessness can be a condition to cyberbullying in different ways:

- Impulsive people can post online or send messages without considering how it might affect other people.
- Being impulsive means that they do not think twice before taking the action. This careless and hurried communication might result in unpleasant information, insults, or nasty remarks that contribute to cyberbullying.
- Engaging in risky online activities, such as disseminating fake information, taking part in hazardous challenges, or motivating others to engage in harmful actions, are examples of reckless conduct. These behaviors may lead to the escalation of cyberbullying incidents.
- Impulsive and reckless people might have a lack of judgment while interacting with others online. This can lead them to be engaged in cyberbullying incidents without knowing the real repercussions.

 Sometimes, impulsive people can be involved in cyberbullying in order to have immediate gratification, sense of power, entertainment, etc.



# **Gender roles/identity**

Identity and gender roles have a big impact on cyberbullying dynamics. They can be precondition for cyberbullying in different ways, including the following:

- Unfortunately some members of our society still have stereotypes and discrimination towards persons from a different identity or sexual orientation than theirs.
   Some of these members can attack online to one or several people who belong to these groups through insults, harassment, etc.
- Cyberbullies may marginalize people online based on their gender. This might be making someone feel uncomfortable in digital places, disseminating false information about their gender identity, or purposefully excluding them from online organizations.
- Gender identity and conventional beauty standards frequently collide. Cyberbullies may use appearance-based or body-shaming tactics to attack people who they perceive as "different" from conventional gender norms.

 Microaggressions are discriminatory comments that are subtle and frequently inadvertent. They might be directed at a person based on their gender identity or expression. Such remarks reinforce negative preconceptions, which in turn lead to cyberbullying.

In other chapters of the book, you will see how some types of cyberbullying have a big influence on gender identity and sexual orientation.



#### **Peer-pressure**

Peer pressure is the influence from members of a group, to another member, to execute an action. There is no doubt that peer pressure is a condition to boost cyberbullying incidents, due to the following reasons:

- They try to fit in the group.
- Fear of being excluded if they do not start or participate in cyberbullying acts.
- They feel afraid to becoming the victim if they do not participate.
- Group dynamics have a direct influence in behaviors.
- The person feels more committed to be "loyal" in the group, even if this goes against their values.
- Prefer to be bullies than victims.
- Lack of confidence to stop the group's actions.
- Accept the group's norms.
- etc.



## **Privacy**

Privacy is an important asset in a person's life; therefore it can become a valuable treasure for bullies to hunt.

The persons who are more vulnerable to become victims are:

- Persons with low privacy settings.
- Persons who expose their private information in public settings (social media, websites, etc.).
- Persons with no antivirus protection.
- Persons who do not control their friends networks in social media.
- Persons who constantly share all their daily activities and locations.
- Persons with lack of skills to identify phishing attacks.
- etc.

Attacking the person's privacy can lead to cyberbullying incidents such as:

- Masquerading, phishing, digital identity theft.
- Doxing and outing
- Cyberstalking
- Online sexual coercion
- Etc.

Go to the corresponding section to find more information about each of these cyberbull-ying typologies. Also, consult section "Advices for protecting from cyberbullying" to find some clues of how to take care of your privacy and interactions in the digital world.



## **Empathy**

#### **Teaching Unit: Walking on my shoes**

**Duration:** 3 hours

The main aim of the activity is to acquire knowledge about empathy in a group.

**Step 1**: Ask your students to draw one of their shoes that they like the most.

**Step 2:** Ask your students to write on the front side:

- 5 things about yourself that people can find in your social media.
- 5 things about yourself that nobody would know, unless you told them.

**Step 3:** On the other side of the shoe, ask your learners to write a line from a book, lyric or a famous person's quote that represents an important part of their lives. They should explain on that side why they chose that line.

Step 4: Ask them to decorate the shoe.

**Step 5:** Ask your learners to present their shoes with the rest of the group.

**Step 6:** Ask the following reflection questions:

• When a person is being victim of cyber-bullying:

- How do you think they might be feeling in this cyberbullying incident?
- Describe what it might be like to be in the victim's shoes
- How do you think victims are feeling?
- If you were in their position, what would you need from others?
- How can you offer understanding for what they are going through?
- Think about one day in the victim's lives. How do you imagine it would be like?
- What words or actions can make them feel more valued?
- Name one moment where someone was empathetic with you? How did you feel?
- How can empathy resolve conflicts?
- How can you use empathy to improve relationships?

The importance of this activity is to realize that empathy is a powerful tool for the prevention and counteraction of cyberbullying. Through the figurative act of "walking in someone else's shoes," learners are able to understand the victims' emotions, challenges, weaknesses, etc. This perspective can help them in identifying the possible harm that our acts can cause, encouraging to reconsider their actions before they get worse.



# Environments where cyberbullying takes place

## **Primary interactions**

In cyberbullying, it is more frequent that a person becomes victim within their primary interactions.

Cyberbullying can be manifested at schools and friendships in the following contexts:

- Students/friends might create fake social media accounts on the name of the victim to bully other students.
- Students/friends can hack the e-mail account of the victim and erase homeworks.
- Students/friends can humiliate others through comments or rumors on social media platforms, such as Instagram.
- Students/friends can take pictures of their peers to embarrass them.
- Students/friends can send online threats to their classmates.
- Private social media groups can be created for excluding the victim and spread harmful content.
- Friend might reveal private information or secrets.
- Fake accounts can be created to send

E-mails, under the "victim's" name.

- Exclusion of people from academic works or ludic activities.
- Public shaming.

In the case of schools and NGO's, cyberbullying is a pressing concern that disrupts the educational environment. For this reason, it is important for these entities to follow the tips below for preventing cyberbullying in these organizations:

- Raise awareness about cyberbullying.
- Provide knowledge about cyberbullying (types, consequences, etc.).
- Provide digital education.
- Provide tools for healthy digital interactions.
- Promote collaboration within the entire NGO/school community.
- Offer a clear and efficient flow of communication among learners, staff and parents.
- Promote a culture of EU values.
- Establish clear rules and policies.
- Establish clear and effective protocols for addressing cyberbullying.
- Promote values of friendship and trust.



## Couple

# Teaching Unit: True partner VS toxic partner

**Duration**: 1 hour

The main aim of the activity is to find out the characteristics of a partner or friend in a healthy relationship. Also learners will raise awareness about the toxic behaviors that can cause cyberbullying incidents.

**Step 1:** Ask your learners to draw the silhouette of a toxic partner. Give them some time to fill in the drawing with characteristics that the toxic partner should have, in order to have an awful relationship that can cause cyberbullying. Also ask them to write in which types of cyberbullying this toxic partner might be involved.

**Step 2:** Ask your learners to draw the silhouette of a true partner. As before, they should fill in the drawing with characteristics that they should have to reach a healthy relationship, especially in the digital world.

**Step 3:** Ask your learners to present individually their assignments. This will be useful for other learners that have interiorized toxic behaviors as normal attitudes.

#### **Answers example:**

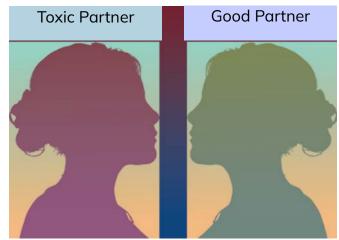


Figure 18: Partner's silhouettes. Source: Pixabay

#### **Toxic partner:**

- Online harassment: Insults, online treats, etc. through social media, private messages, instant messages and email.
- Sharing sensitive pictures for revenge purposes.
- Excessive jealousness, asking constantly where the partner is.
- Asking to whom are they talking to.
- Denigrating the partner as \*\*\*ch because of having friends.
- Monitor daily online interactions.
- Have the password to get into the partner's mobile without permission.
- Emotional manipulation through social media posts.
- Threatening the partner on exposing private information or pictures.
- Ask friends to harass the partner.

- Making online gossips to ruin the reputation of the partner.
- Using phrases like "I am punishing you because it is good for you".
- The toxic partner makes the decision of the couple.
- etc.

#### **Good partner**

- Respectful communication through social media, private messages, instant messages, email, etc.
- Trustworthy: will keep the partner's sensitive information in private and will never share it.
- Motivates the partner to hang out with their friends and establish new relationships.
- Respect the partner's private conversations with other people.
- Admiring the partner in public and private.
- Not tracking location or online interactions.
- Respect privacy. Do not ask for any passwords.
- Encourage independence and personal growth.
- Apologizes and forgives.
- Supports the partner from any problem.
- Uses healthy conflict resolution techniques.
- Healthy intimacy.
- Involvement in mutual decision-making.
- etc.

In order to prevent cyberbullying incidents, it is imperative that you carefully engage in healthy interactions with your partner, staying away of any behavior that can trigger such incidents.

Any relationship starts with open communication, empathy, and understanding. Avoiding destructive actions on the digital world is a measure to prevent from turning into cyberbullying.

Although you have a good partner, it is important that both of you discuss if it is necessary to be involved in sharing sexual content. Both of you should be aware that in the digital world there are perpetrators that can use this content to get money from you, etc.

Furthermore, try to find how your partner expresses from previous relationships. Ask how they managed breaking up in previous relationships. Actions and expressions about their rupture will give you an insight in how your partner might act in case of a rupture with you. If your partner was involved in revenge actions, consider twice sharing information that can put you in danger in case they break up.



#### Social

In the digital world, cyberbullying goes beyond primary interactions and extends into social interactions. This creates a complex and pervasive problem that affects people in a wider scale. The dynamics of cyberbullying in social interactions can be present in different online spaces from people who belong to our primary interaction groups and people outside these groups, such as strangers.

Because of their large number of users, social media platforms are important places for cyberbullying to happen. People could be the target of harmful actions including public humiliation, internet harassment campaigns, etc., for example, it is common to find several haters on Twitter.

Some other platforms, such as some online chats, offer anonymity where bullies may feel more empowered to do destructive acts without fear of repercussions, which exacerbates the impact of victims. Also, people can keep their true identities behind a fake profile in which they attack other users, for example Instagram comments.

Gaming communities are also a place for cyberbullying. People might experience verbal abuse, targeted harassment based on how well they play the game, or being kicked out of in-game events in these kinds of settings. Because gaming is inherently competitive, tensions can rise, creating a toxic environment that is harmful to the mental health of individuals who are targeted.

Cyberbullying may also flourish in other digital contexts, such as comment sections of YouTube, Twitch, forums, etc. People might run across hurtful remarks, hurtful language, or the dissemination of damaging information, which creates an atmosphere where the lines between social and main contacts become blurred and the risk of widespread injury increases.



# Teaching Unit: Stereotypes and cyberbullying

**Duration:** 1 hour

The aim of the activity is the acquisition of awareness and acceptance of the existence of stereotypes and prejudices. Learners will comprehend how stereotypes can facilitate cyberbullying on victims with specific characteristics.

**Step 1:** Write on each stamp a word for describing a character which our society can have either good or bad perceptions. For example, blond, junkie, rich, kleptomaniac, actor, migrant, corrupt, Muslim, Christian, Roma, doctor, teacher, youngster, old person, poor, prostitute, director, president, white person, lawyer, police, prisoner, etc. Each of your learners should have one stamp.

**Step 2:** Provide randomly a stamp to each person.

**Step 3:** Each person will have to paste the stamp on the back of another learner. They should not reveal what is written on the stamp.

**Step 4:** Learners will have to move around the class to discover their assigned charac-

ter. Other learners will have to give them some clues such as characteristics, what the society think about them, etc. Their peers' feedback will help them to discover who they are.

**Step 5:** Ask to the group the following reflection questions:

- Were you able to identify who your character was?
- What characteristic made you guess your assigned character?
- What comments or characteristics caught your attention in a positive way?
   Were there any good comments?
- What comments caught your attention in a bad way?
- In general, how do you think the society perceive your character?
- Do you think this perception is fair?
- Do you think that the comments you received represent all persons from the same group?
- How do you think the bad characteristics and comments you received can lead to cyberbullying?
- If your character only received positive comments, how would you use this power in cyberbullying?

- Do you think is fair to attack a person the perpetrator does not know, due to stereoytpes?
- How stereotypes have affected a healthy integration of all your peers in the digital world?
- Why should your community do to not discriminate others due to stereotypes?

This activity is important to realize that in many times stereotypes and prejudices are present in cyberbullying episodes. In many cases, especially within youth communities, a group can be more on the side of the bully, as their speeches are full of prejudgments and stereotypes. Youngsters should become aware that a label does not represent a person, neither a group. Therefore it is important to analyse the words of the bullies in order not become bystanders who judge others without even knowing them.

## **Cyber-bullying means**

# **Teaching Unit: Cyberbu**llying public and private means

**Duration**: 1 hour

The main aim of the activity is to acquire knowledge about the means used by bullies to attack in the digital world.

**Step 1:** Divide your learners into 2 teams.

**Step 2**: Provide one balloon of a different color to each team.

Step 3: Divide the learning area in half, having each team in one half (such as a volleyball court).

**Step 4:** Assign to each group 5 points.

**Step 5:** Each team will simultaneously throw a balloon at the other team to start the game. Consider it as a volleyball variant in which each team uses two balloons rather than the customary one. They can only use hands to pass the balloon.

will stop. This team will have to answer the following question:

> What media are used by bullies in their cyberbullying attacks?

**Step 7:** The group will have 15 seconds to answer. If the group answers correctly, nothing will happen. If they answer wrong, they will lose 1 point. Answers cannot be repeated. Although answers can be easy, participants will, sooner or later, get no more ideas. The game will end when the first team lose all their points.

Each of the answers should be written in a piece of paper and paste it on a board.

**Step 8:** Once the game is over, review all the answers and make brainstorming in case all the ideas were not covered during the game.

**Step 9:** Separate together each of the media that can be used for cyberbullying throu-

#### **Answers example:**

#### **Public Interaction Networks:**

- Social Media Platforms: the comments section and posts.
- Public Forums
- Public Chat rooms
- Websites
- Online gaming chat rooms
- Message boards
- Video sharing platforms: the comments section and sharing videos to the public.
- Photo sharing apps: the comments section and sharing pictures to the public.
- Virtual world communities
- Podcast comments
- Educational and professional portals



#### **Private Interaction Networks:**

- Social Media Platforms: private messages
- SMS
- E-mail
- Online gaming private messages
- Instant messaging apps
- Video sharing platforms: the comments section and sharing videos only to the victim.
- Photo sharing apps: the comments section and sharing pictures only to the victim.
- Anonymous messaging apps
- Online dating apps
- Educational and professional portals: private messages

**Step 10**: Ask to the group the following reflection questions:

- What are the risks for the victims when the bully uses public media?
- What are the risks for the victims when the bully uses private media?
- How can the level of visibility or privacy affect the dynamics of cyberbullying?
- How can cyberbullying be prevented or addressed in private networks where interactions are less visible?
- How can a bystander intervene in a public cyberbullying incident?
- How can a bystander intervene in a private cyberbullying incident?
- The importance of this activity is to understand that even cyberbullying is done through private and public interactions, the severity and impact of each action is almost the same. In public and private cyberbullying attacks, victims can have serious personal and social consequences, which are detailed in chapter "Consequences of cyberbullying"

Reporting can be more difficult in private incidents. Therefore, if you are a victim of private attacks, look immediately for support, before it escalates.

If you are a bystander and you are not 100% sure that a person is being attacked, try to contact them and offer support. Do not hesitate to report the incident immediately whenever you are sure.



# Consequences of cyberbullying

## Legal

Europe's legal framework for fighting against cyberbullying might differ from one country to another, as each country has their unique system of policies and laws. The diverse legal frameworks are a reflection of the socio-cultural contexts and legislative priorities of individual nations. Countries in Europe and the world might not have a specific law for cyberbullying, however they can have different laws that can address some parts of the cyberbullying, for example:

- Laws against harassment and defamation which can address incidents of cyberbullying. Their purpose is to protect people from derogatory comments, unfavorable rumors, persistent online harassment, etc.
- Laws concerning to privacy and data protection, for example, the General Data Protection Regulation (GDPR) in the European Union.

Fundamentally, the GDPR defines people's rights in the digital age to take more control over their personal information, including:

- The right of a person to give explicit consent before processing their personal data:
- Easier access to their personal data;
- The right to delete and rectify their data;
- The right to decline the use of their personal information for "profiling" purposes:
- Data portability rights among service providers.

Furthermore, the GDPR clearly places requirements on those who process data. The GDPR carefully lays out the procedures and requirements needed to guarantee its compliance, creating a foundation that places a premium on the ethical and responsible management of personal data.

Most importantly, the GDPR establishes a system of penalties intended to deal with any violations of its rules. These penalties are essential for people responsible for breaking the regulations, which emphasizes how important privacy and data protection are in today's digital world.

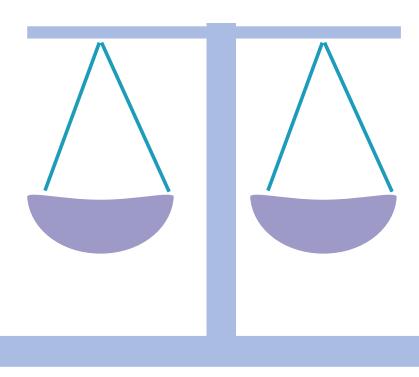


If victims have suffered a violation of their privacy, for example doxing, they might be able to take legal actions against the bully.

- Laws for addressing the safety of children and young minors. These regulations can prevent children from being victims of sextortion, coercion, harassment, etc.
- Laws for Criminal Violations. Cyberbulying incidents might be illegal with severe penalties such as jail. For example, many countries in Europe and the rest of the world, consider the unauthorized recording and publishing of digital sexual consent with jail penalties.
- Laws prohibiting online hate speech. In some countries, there could be legal repercussions of cyberbullying incidents that contain offensive or discriminatory content that targets people because of their race, sexual orientation, religion, ethnicity, etc.

It is important that people, who are victims of cyberbullying, become aware of the laws and policies available in their countries. In this way, it will be easier for victims to address the situation in a more effective way. The relevance of reporting cyberbullying incidents as soon as possible is essential before it escalates. It is of highly importance to contact the police in situations such as:

- Severe harms are caused:
- When the situation starts to escalate;
- When the victim's safety is at risk;
- When the situation is getting out of control;
- Etc.



#### Personal

#### Low self-esteem

The Cambridge Dictionary defines self-esteem as "the belief and confidence in your own ability and value". Cyberbullying can seriously and negatively affect a person's self-esteem, as:

- The victim can internalize negative comments and posts, leading to a negative self-perception.
- Victim can acquire feelings of worthlessness, questioning their value as a person, or their valuable contributions in a group.
- Being excluded can affect their self-esteem.
- Happy slapping can amplify a perceived loss of dignity and respect.
- Victims can start questioning their abilities and worth.
- Avoidance to join social events can lower the opportunity for building positive self-esteem experiences.
- Acquiring doubts of their physical appearance.
- Etc.



# Mental health consequences

#### **Emotional consequences on victims**

Although for bullies can be funny, for the victims can decrease the quality of their lives in less than one day.

It is important to identify and comprehend the variety of strong feelings that victims of cyberbullying frequently experience.

First of all, cyberbullying may cause intense feelings of humiliation and embarrassment, as in most of the cases these events are persistent and visible to the public. Events such as sextortion, happy slapping etc., can emerge these feelings, where the victim is object of disrespect and fun by the rest of the community.

Aside from embarrassment, victims also frequently experience anger. Strong emotions of anger and resentment can be triggered by the unfairness of being cyberbullied. Injustice and the lack of capacity to stop these incidents can cause frustration and overwhelming. Furthermore, people could feel sad, as in most of times they cannot control the unfavorable story that is being told about them.

In addition, victims of cyberbullying typically feel helpless in their situation. Bullies can give victims the impression that they are significantly more powerful than them, which makes them feel even more powerless.

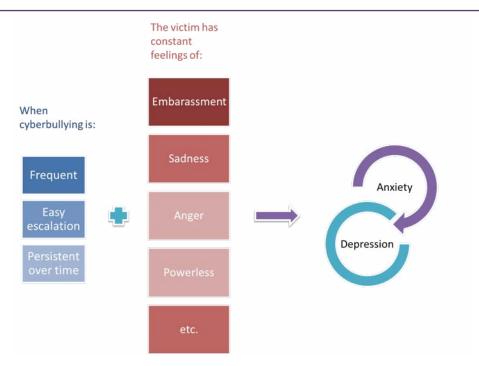


Figure 19: The evolution of mental health in cyberbyllying. Own creation. Own Source

Unfortunately, cyberbullying can have the characteristic of escalating, being frequent and/or be persistent over time. This can generate, that the victim constant experiences the feelings above and much more. The persistent exposure of these feelings can lead to depression and anxiety.

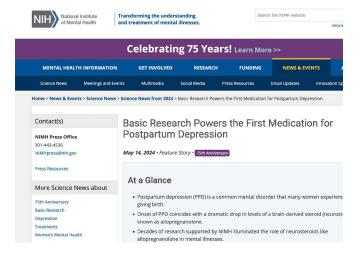
Anxiety levels can rise when victims are subjected to cruel comments, critical messages, or public humiliation on a regular basis. A reason for this could be that memories of previous traumas arise. Moreover, victims might have anxiety due to fear that they will be attacked again.

The continuing tension and psychological torment brought on by cyberbullying may cause depression. Victims can have depression as a result of their constant feelings of helplessness, loneliness, sadness, powerless, etc. The National Institute of Mental Health, defines depression as "a common but serious mood disorder. It causes severe symptoms that affect how a person feels, thinks, and handles daily activities, such as sleeping, eating, or working."

#### **Behavioral consequences on victims**

As mentioned above, cyberbullying can cause depression on victims. Depression can be manifested in a range of behaviors that can happen individually or socially (see the "Social" section from this chapter):

Changes on sleep patterns: Depression can interfere with sleep cycles, resulting in not being able to sleep, wake up very early or excessive sleep. Sleep disturbances can affect people's humor, as they will experience constant fatigue during the day; anxiety and overthinking at nights; etc.



Changes on appetite: A victim's appetite may fluctuate significantly, leading to excess consumption in food or a decrease in appetite. This can lead to eating disorders which can affect their physical health.

**Difficulty in concentration:** Depression can affect cognitive functioning, making it difficult to concentrate, think clearly, make judgments and take wise decisions.

Substance consumption: As a coping method, some victims can turn to drugs or alcohol. The constant abuse of these substances can lead to addiction problems, causing dangerous consequences in the person and their social circles (family, partner, friends, etc.).

Hopelessness or pessimism: Cyberbullying victims might become stuck in a vicious circle of hopelessness, believing that their now-adays problems will never improve. They frequently have difficulty seeing a better future, which might make their mental health worse.

Diminished Vitality, Tiredness or a Slow-down: Victims might have a severe loss of energy, and feel exhausted all the time. Tiredness can be in a physical and mental way. Depression can make the person carry out their daily tasks more slowly.

Increased Impulsivity: The lack of concentration and making decisions can facilitate the impulsivity of a person. Impulsivity can lead to risky actions or behaviors which can make the victim be part of a worse scenario.

Issues with Sexual Performance and Desire: Depression can have a big effect on the person's libido and ability to have sexual relations. The loss of interest can affect the victims' relationships and sexual dysfunctions, contributing to a worse emotional distress.

These behaviors can vary on each person. However, it is important to recognize and comprehend these behaviors that emerge on cyberbullying victims. In this way, we can support the persons to look for help from a professional therapist, in order to work on their mental health. Addressing cyberbullying incidents with a mental-health expert can empower the victim to counteract and stop the situation.

## **Teaching Unit: The Feeling Wheel**

**Duration:** 1 hour

The main aim of the activity is to raise awareness of how the involved parties feel in a cyberbullying incident.

**Step 1:** Divide learners into different groups.

Step 2: Provide them the Feeling Wheel

**Step 3:** Ask your learners to take a look to the wheel and answer the following questions:

- How do bullies feel while executing cyberbullying incidents?
- How do victims feel? Try to assign feelings according to each of the cyberbullying types.
- How could bystanders feel?

For using the wheel, it is important that learners start with the inner circle and then move to the circles from the outside to assign a feeling. Learners can also use the blank spaces from the outer circle to add more feelings.

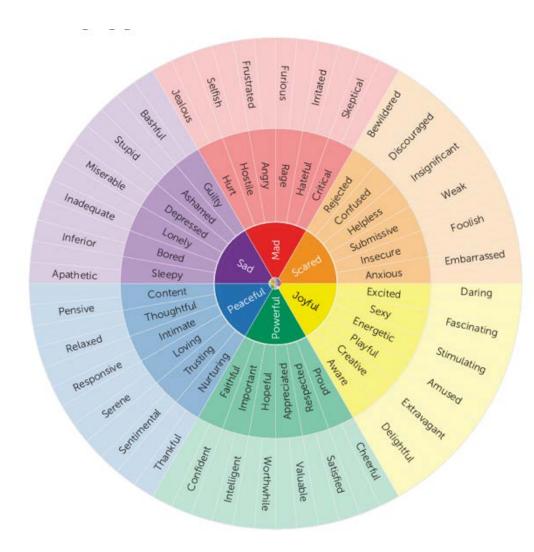


Figure 20: The Feeling Wheel. Creation, All The Feelz . Source: Gloria Willcox

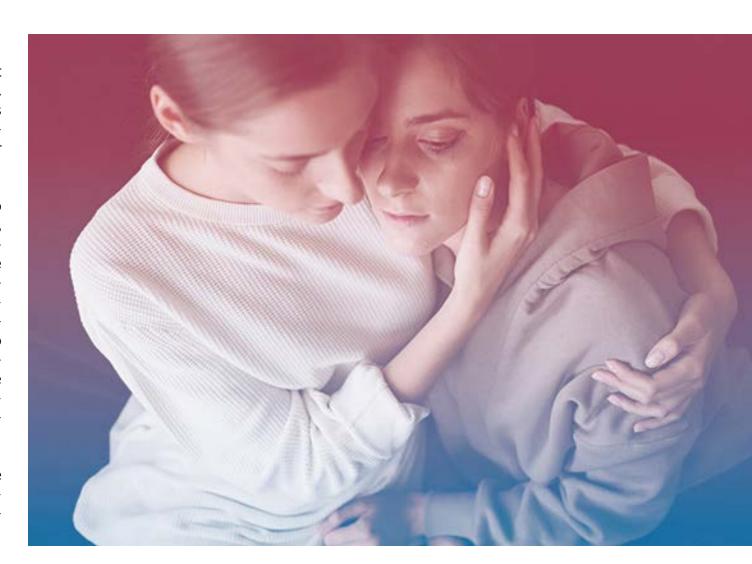
**Step 4:** Ask to each group to write on a board their answers.

**Step 5:** Compare feelings and make a final chart with all the ideas.

Sometimes for ourselves it is difficult to get the ideal word to describe how we feel. However, understanding other people's emotions might be much more difficult, especially if we have not personally lived their experiences.

For this reason, this activity is important to understand the feeling scenarios of bullies, victims, and bystanders. This activity works as empathy tool that will put us in the "shoes" of the persons who experience cyberbullying. We will be able to better understand the emotional situation and vulnerability that victims go through. We will also recognize the intentions, fears, and occasionally regrets of cyberbullies, as well as the complicated range of feelings that bystanders experience when they are indirectly engaged in these incidents.

In this way, we will develop a stronger sense of empathy and awareness, which are essential for counteracting and preventing cyberbullying.



### **Physical consequences**

#### **Physiological effects**

Cyberbullying victims can develop physiological symptoms, due to the constant mental health distress they are experiencing:

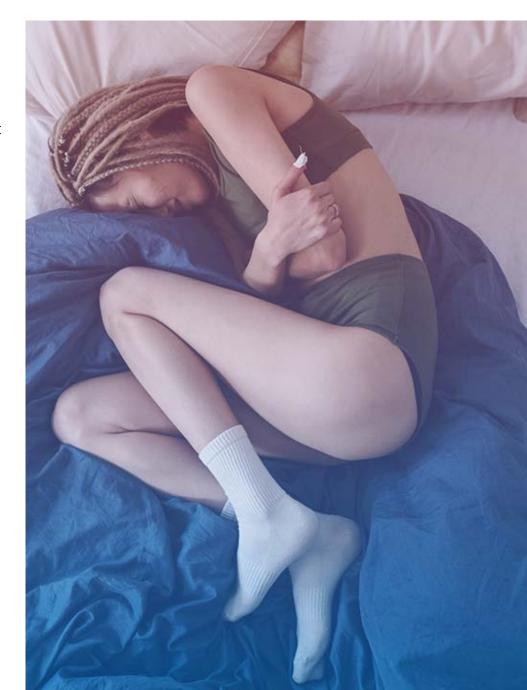
Muscles tension: Stress can lead to tense muscles, especially in shoulders, neck and back. This can generate constant pains in the body.

**Digestive Problems:** The digestive system can be affected, due to stress of cyberbull-ying incidents, causing stomachache, indigestion, gastritis, stomach ulcers, diarrhea, IBS-irritable bowel syndrome, etc.

**Headaches and migraine:** They can emerge due to extended periods of stress and worry.

**Skin Issues:** Stress can affect the skin, causing acne, psoriasis, rashes, wrinkles, face flushing, etc.

Weakened immunological System: Longterm stress can compromise immunological function, leaving sufferers more vulnerable to infections and diseases. They could discover that they are becoming sick more often. Cardiovascular Problems: Extended periods of worry and stress can raise blood pressure and put people at higher risk of developing heart-related problems.



#### **Self-harm**

Depression can lead to self-harm as a result of the deep emotional pain, hopelessness, despair, etc. that victims of cyberbullying experience. Self-harm is a response where victims can use it, due to complicated reasons such as emotional release, regaining control, self-punishment, release endorphins, etc. Fortunately, self-harming is not a universal response and not all persons practice it.



## **Suicidal thoughts**

In cyberbullying victims can start to have abstract thoughts about ending their lives such as "what happens if I kill myself?", "would somebody miss me?", "who would go to my funeral?", etc.

Suicidal thoughts are very dangerous because if they are not controlled, the person might change it into an action. Persons might start thinking on different techniques, dates and places to take off their lives.

Cyberbullying is dangerous. When the victim does not see an ending on the situation; considers that the incident will devastate their life; etc., the previous thoughts can be executed to relieve their pain.

Whenever we identify that a person is having suicidal thoughts, it is very important not to underestimate its importance. Sometimes these thoughts could be expressed as "jokes". Therefore, we need to be open to talk about this topic with the person and get help. Remember that your action can mark the difference for the person to have the brighter future needed.

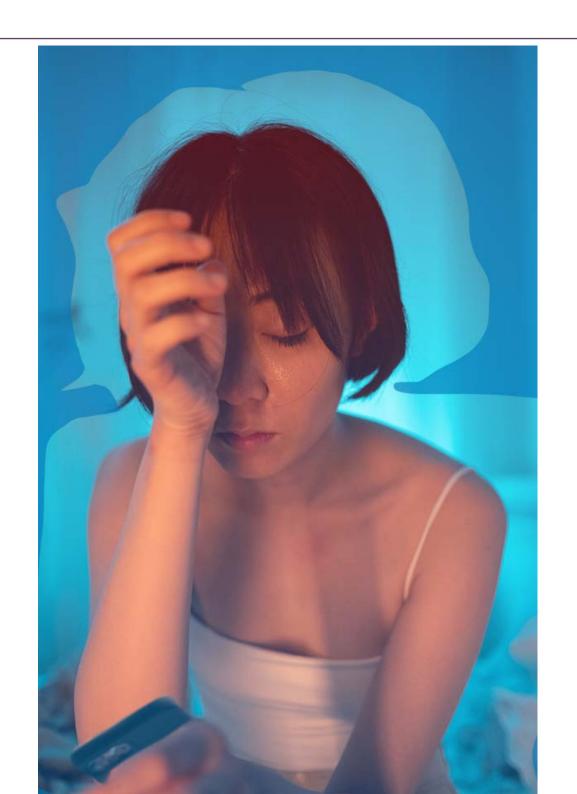
### Social

Cyberbullying have far-reaching social consequences that affect victims in many ways:

#### **Isolation**

The most noticeable consequence is social isolation. In order to protect themselves, victims frequently feel forced to set apart from social connections, either in the digital world or in the real one. The fear of continue being harassed, humiliated, damaging their reputation, etc. reduce the possibilities of social interaction, thus, develop positive relationships. Let's not forget that one type of cyberbullying is exclusion, decreasing the quality of the victims' friendships.

This isolation on one hand obstructs the growth of interpersonal abilities, and in the other hand intensifies emotions of not having friends. Constant isolation can reinforce the idea of victims that is "better to be on my own".



#### **Quitting from enjoyed activities**

Sometimes, persons who are being cyberbulied can quit from activities that once they enjoyed. 2 of the main reasons of this are:

**Fear:** The fear of encountering further harassment may cause victims to disengage from hobbies, sports, or community involvement that once brought them joy.

Loss of interest: Depression can cause that people lose interest in activities that once gave them fun. They can also have a lack of motivation to go to these events or start new ones. For victims it can be really challenging to regain their enthusiasm in these activities.

The withdrawal of these activities, reinforce their isolation, affecting their social and emotional well-being.

# Decrease the quality of personal relationships

Cyberbullying can have a negative effect on the victim's relationships (friends, family, partners, colleagues, etc.). If the mental health is affected, there is a high probability that relationships are also harmed. The emotional distress caused by cyberbullying, make victims to become more irritable, leading to misunderstandings and conflicts.

On the other hand, victims might distance themselves from friends and family, interacting with them in a more unpleasant way and with a more distanced attitude.

Damaged relationships can take time, communication and understanding to be repaired. Furthermore, it is important to highlight that working on mental health is indispensable to reach healthy relations.

It is essential not to take things personally whenever a person who has depression affect your relationship. It is relevant to understand that they are passing through a very hard time.



#### **Academic or professional**

#### consequences

As explained above, cyberbullying and depression can decrease the victim's concentration, performance and capabilities to make good decisions. As a consequence, victims can struggle with their academic studies of professional tasks, where trying to meet their objectives can become a big challenge. This can affect them in several ways:

#### **School**

- Low grades.
- Do not learn the subjects.
- Avoiding going to school.
- Losing scholarships, career opportunities, etc.
- Early dropouts.
- etc.

#### Work

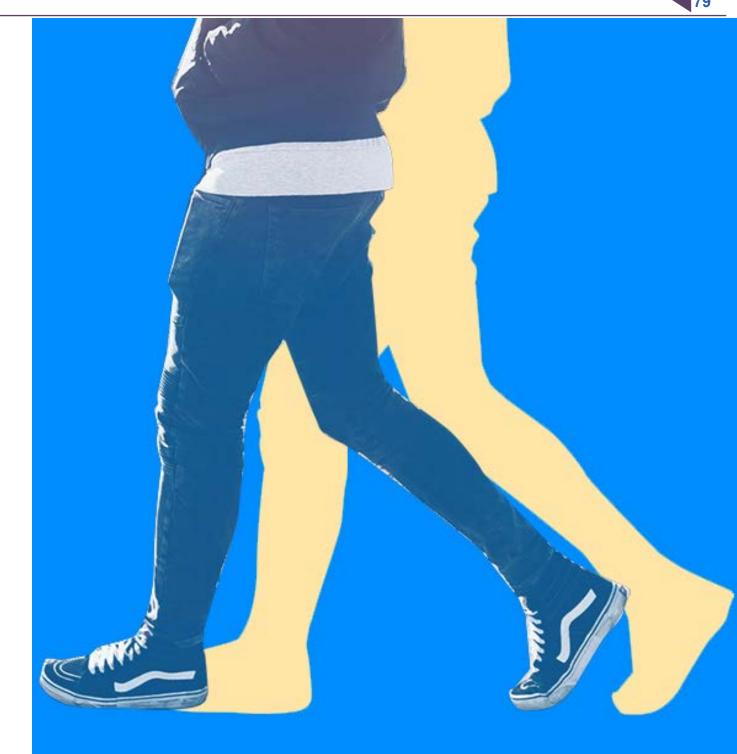
- Low performance.
- Constant mistakes.
- A lack of control over work.
- Losing the opportunity of being promoted.
- Job loss.
- etc.



#### **Involvement in high-risk activities**

Some victims of cyberbullying might get involved in risky activities, due to factors such as:

- Use it as a coping strategy or a reaction to their negative feelings.
- Looking for escape from emotional pain.
- Attract attention to unconsciously communicate their emotional suffering.
- Depression can lead to reckless behavior and impulsivity.
- Etc.



# Critical thinking to counteract cyberbullying: an integrated response

# What to do if you are a victim of cyberbullying?

If you start being cyberbullied, do not hesitate to follow this process:

- **Keep calm:** Although these kinds of messages can cause you fear or other feelings, it is important that you keep calm and do not reply instantly.
- Record: In social media, posts can be deleted and changed easily, therefore you need to save the evidence as fast as you can:
  - Take screenshots;
  - Save the post if the application lets you;
  - Save the date, time;
  - Try to do some research about the person who is cyberbullying you: profile account, email, etc. Look for information that can facilitate their contact.

Look for support:

- Contact the police or an emergency center in case you are in real danger.
- If you are not in danger, report the message to the main administrators of the social media application or website. Ask for the message to be removed after you saved the evidence (in case you need it for the future).
- Do not keep the information for yourself.
  Tell the persons you trust the most about
  what happened and send them the evidence. They will help in case something
  happens.

**React:** If you assessed that the situation is not dangerous, you can try the following options:

- Reply with a proper manner. Remember that being aggressive will not make the situation better.
- Block the contact.
- Ignore the message. Remember the old saying "Don't feed the troll!"

If the situation is getting out of control regarding your mental health, ask for support to an expert (psychologist).



# As a youth worker, what to do if your learner notifies a cyberbullying incident?

If one day one of your learners notifies you a cyberbullying incident, you can follow this process:

- Active Listening: Provide to the victim
  a space of trust and listen deeply their
  thoughts. This space should be given as
  soon as possible, in which you can pay
  100% of your attention. Do not underestimate the situation.
- Keep calm: As a leader it is important that you keep calm, otherwise you can increase the victims' feelings and emotions, which will make the process more complicated.
- Analyse the situation and keep records.
- Describe the main situation.
- Help the victim to record all the evidence:
  - Take screenshots;
  - Save the post;
  - Save the date, time;
  - Try to do some research about the person who sent the message: profile account, email, etc.;
  - Look for information that can facilitate their contact.

Look for support:

- If the victim is in an immediate dangerous situation, contact the police and your organisation's security team.
- If the victim is not in danger, ask for support to:
  - The person responsible to solve the problem. If you are the person who needs to solve the problem, make an intervention under healthy conflict resolution techniques.
  - The administrators of the social media or website to delete the message.
  - Any other entity who could help.

If the victim is under 18 years old, contact their parents or tutors and notify them about the situation. If the victim is older than 18 years old, convince them to notify the ones they trust the most.

Follow up the case to make sure that the victim receives the necessary support. If you consider the situation has affected the victim's mental health, recommend them to go to an specialist (psychologist), to address these challenges.

**Supervise the bully**: In case that the bully belongs to the same learning environment, do constant supervisions to prevent a new incident.



## What to do if you are a bystander?

The dynamics of a cyberbullying episode can be influenced by a variety of measures used by bystanders during and after the incident.

#### **During the incident**

One intervention is standing up for the person being cyberbullied. By voicing their disapproval of the cyberbullying conduct, bystanders can take proactive steps to support and protect the victim. Furthermore, a bystander can disseminate a strong message that cyberbullying is not acceptable in the environment. Once the action is intervened and bullies are publicly evidenced, they can quit from their harassing behavior.

One effective measure to deal with cyberbullying is to step in as a group. It shows that cyberbullying is not accepted in the community when a number of bystanders come together and confront the bully. This will give the victim a fast support. Bully will think twice to continue with future incidents as they will know that there is a peer group who will not tolerate cyberbullying.

Bystanders can also use more subtle tactics, such as changing the topic to blur a cyberbullying scenario. Bystanders can successfully lessen the impact of the episode, by guiding the group away from the bad energy originated. This strategy is useful for not confronting the perpetrator directly.

Reflection is a powerful tool for counteracting cyberbullying. Asking the bully to explain their actions or intentions might cause the bully to reflect on their conduct. This can make the bully change their behaviors. This approach fosters empathy and provides a positive dialogue about the negative effects that can cause to a victim.

Bystanders can effectively diffuse tension during a cyberbullying episode by using comedy to lighten the severe situation. Humor can assist to change the emotional tone and lessen the bully's incentive to carry out their acts. However, it should be used sensitively and with caution in order not to hurt anybody. Additionally, it can foster a more relaxed environment that facilitates understanding and collaboration.

Finally, as some bullies tend to denigrate their victims, bystanders can make comments that give back the value of the person. If bullies see that the victim is respected and cherished by the rest of the group, they will quit from these behaviors. Furthermore, validation can give back the victim's self-esteem and the harmful consequences of cyberbullying can be mitigated.



#### After the incident

Contacting the cyberbullied person in private is a useful measure of providing support. If bystanders express to the victim support and confidentiality, victims can have a safe space to talk about their experience and feelings. Also victims will become aware that they are not alone to deal with this. This can help the victim to develop resilience and cope with the problem.

In certain cases, as long as they consider that they will not put their lives at risk, bystanders can contact the bully privately. This measure works, especially when bystanders and bullies have a close relationship. If bystanders talk to the perpetrator about their harms and consequences, they might change their actions. The bully will reevaluate the repercussions which might make them quit. However it is important that bystanders take precautions to protect themselves when using this strategy, as it might lead to unexpected results.

The reporting of bullying to an authority (police, youth worker, parent, or organization manager, etc.) is a crucial action that bystanders need to undertake. With this, bystanders will guarantee that the cyberbullying event will be appropriately handled. Reporting is crucial for:

- Making the bully responsible for their acts.
- Protect the victim from future incidents.
- Preventing the victim to be more in danger.
- Create an environment where
- etc.



# Advices for protecting from cyberbullying

In order to prevent for being involved as a victim of cyberbullying, follow the below advices that will help you to protect your online interactions:

#### Social media for friends

Making your social media profiles posts "friends only" can help you protect your data by limiting who can see your updates and private information to people you know and trust.

Being selective when accepting friend requests on social media is another important tactic. It is better to only accept requests from people you have really met and are familiar with, in order to keep your online presence safe and controlled. Do not give full access of your posts to people you have just met.

Your safety will be further increased if you configure your social networks to only accept requests from friends and from friends of friends. It will be a filter to reduce the likelihood of strangers who pretend to be friends from another friend.

Although having lots of contacts who see your content can be fun, this easy step lowers the chance of being exposed to possible threats or unwanted attention by letting you keep control over who may see your posts. In this way, people you do not really know will find hard to reach to your personal information, activities, contacts, pictures, etc.

# Do not post publicly your private information

For your protection, be careful while disclosing private information on social media (ID number, address, phone number, etc.). Whenever you can, restrict the accessibility of your primary contact information (education, job, location, etc.). Also be aware that not all sections of the profile are mandatory, so avoid filling in spaces where you can disclose this information.

Always use a private message over a public post when you need to communicate sensitive information with a friend, such your phone number. Furthermore, do not share your private information to friends if they do not need them for a real specific good purpose.



# Do not post publicly your private information

For your protection, be careful while disclosing private information on social media (ID number, address, phone number, etc.). Whenever you can, restrict the accessibility of your primary contact information (education, job, location, etc.). Also be aware that not all sections of the profile are mandatory, so avoid filling in spaces where you can disclose this information.

Always use a private message over a public post when you need to communicate sensitive information with a friend, such your phone number. Furthermore, do not share your private information to friends if they do not need them for a real specific good purpose.

These measures lessen the possibility that your personal information may end up in the wrong hands and preventing cyberbullying incidents such as identity theft, cyberstalking, etc.

#### Do not use your real name

Using a gender-neutral screen name or pseudonym rather than your real name on social media platforms can offer an additional degree of security. Using a pseudonym helps you remain anonymous and protect your identity from potential dangers. It will be harder for perpetrators to find out your real-life details. However, use this anonymity in a responsible way.

#### **Turn off geolocation settings**

Your physical location may be accidentally revealed by geolocation technologies, raising security risks. Hence, it is important to:

- -turn off the GPS on your phone.
- -disable geolocation settings on your different accounts (social media, apps, etc.).

This will reduce the possibility that you unintentionally share your location to others that could reach you in the real world. In this way, you will improve your personal safety and privacy.

#### Strangers might be dangerous

In terms of personal safety, it is relevant to be aware that the communication with strangers might be risky. People that you only have met online, might not always have good intentions. Their interactions can lead to cyberbullying in the form of sextortion, cyberstalking, catfishing, etc. This will put your privacy and well-being compromised.

Cyberbullying perpetrators can be really cunning and seem incredibly kind in order to gain your confidence and obtain private information. It is important to stay aware and have in mind that this kindness could be only a mask. This mask can be taken once perpetrators obtain what they want.

Never give personal information to somebody you have not met in the real world. Also, do not send images or videos that include sensitive material; remember that these materials can be used against you, affecting your finances, reputation, etc.

#### Manage your passwords properly

Never share your passwords. They are the keys to your digital existence. Even with someone you trust, sharing your credentials might come with unanticipated threats. Giving someone your password essentially gives them access to your online environment, which may contain private messages, financial data, sensitive emails, private documents, etc. This raises the possibility of identity theft and the compromising of other important online assets. In addition you are exposing yourself to potential privacy violations and unauthorized access to your accounts.

Furthermore, selecting secure passwords that are difficult to guess is essential. There is a serious security risk when using passwords that are simple to figure out. For example, including in your passwords birth dates, pet names, popular terms, etc. Malicious actors that have access to your social media accounts or publicly accessible information about you, may be able to crack these kinds of passwords.

Now-a-days strong passwords are mandatory to improve your online security. Make a password difficult to be hacked using a mix of capital and lowercase letters, digits and special characters.

Below, you will find tips for the proper management of your passwords that you need to apply in a frequent basis:



Figure 21: Proper mangement of passwords. Own creation. Own resource

- Use a different password for each account
- Regularly update passwords
- Enable Two-Factor Authentication

# Different accounts for different purposes

Your digital privacy and security are improved by keeping your email addresses separate. Think about the habit of keeping different email accounts for different purposes, each with a particular function in your online life. One way to handle business/academic contact is to set up a unique email address for work/education-related correspondence, particularly if you deliver documents, through that account. You can designate a different email address for social media and less formal personal communications. You may use a third email address—often called a "spam" email—to sign up for subscriptions, specials, or any other circumstance where you could expect a larger number of promotional material.

Your personal and business correspondence is shielded from potential risks by this segregation of email addresses. In this way, the attacker might not be able to access every element of your online identity, even if one of your email addresses is hacked.

Although the "spam email" might not have as much importance as the rest, it is relevant that it should be protected from any hacking attempts. Perpetrators may try to get to this email and if they succeed, they will be able to access to all your subscriptions.

#### **Limit permissions**

Be cautious when allowing access when registering for new apps, games, completing online tests, etc. Your social network account information is requested by many apps, and although this may seem harmless, it might put your security at danger.

Additionally, some applications' security features might not be strong enough to shield your data from any dangers. Under such circumstances, a doxing hacker may penetrate the app's security and have access to all of your personal data. It is best to register for applications using a distinct username and password rather than giving access to one of your social media accounts in order to reduce these hazards.

#### **Avoid phishing**

In chapter "Masquerading, Catfishing, Phishing, Digital identity theft" you will find different measures to prevent to become a victim.

#### Use a VPN

Essentially, a virtual private network, or VPN, covers your IP address and encrypts your internet traffic to improve online privacy and security. VPN can tangentially improve your general internet security, which can reduce the probability of being part of cyberbullying incidents:

- Anonymity: A VPN will hide your IP address, making more difficult for perpetrators to link your online interactions to your real location.
- Safe Data Transmission: By encrypting your internet traffic, a VPN will reduce the possibility of intercepting your communications, including private messages and sensitive data.

# The THINK Tool for a healthy online communication

Building a healthy communication in our virtual communities is essential to addressing and preventing cyberbullying. Healthy, especially respectful, communication can boost empathy, understanding and responsibility for our actions. Analysing our thoughts before speaking, can help to promote a culture where people feel secure, supported, and included.

An important tool for assessing the words we use and the ideas we explore, on a regular basis, is the acronym THINK. These acronym's letters function as a guide for evaluating the impact and quality of our words and ideas.

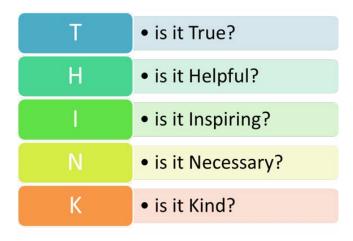


Figure 22: Think tool. Own creation. Author unknown

#### T - is it True?

Truth is the main basement of enhancing a good attitude, good communication and good relationships. We need to make sure what we are saying or thinking is factually correct before expressing information or giving our point of view. Expressing lies or accepting misleading information can cause mistrust, confusion and harm to the implicated persons.

#### H - is it Helpful?

Sometimes our truth statements can harm others. Not only our ideas and words should be honest, but they should also have a purpose. Before saying something, we should consider whether it would be beneficial for the person or the main situation. Will our words offer support, guidance or answers? If not, it might be best to keep it silent.

#### I - is it Inspiring?

Inspiration is a potent energy that has the capacity to motivate and raise ourselves and everyone around us. Our minds should be filled with positive, encouraging and inspiring thoughts. In most of times, our inner dialogue is expressed in our daily behaviours and communitacion. If our inner dialogue is positive, we will be able to create an inspirational environment with other people.

#### N - is it Necessary?

We need to think about whether our ideas or words are necessary in the specific situation. Excessive or unnecessary information might impede our ability to communicate and think clearly, making it more difficult to concentrate on the things that are really important.

#### K - is it Kind?

The golden rule that has to govern both, our internal dialogue and our relationships with other people, is kindness. We need to evaluate if the words and ideas we express are done with respect and empathy. A kind comment can make a big impact in our own and other people's wellbeing.

If we comply with the 5 letters, we will become more mindful in our ideas, words and actions. We will reach a healthier and productive communication which will contribute positively in our interactions and relationships, within the digital world.

## Teaching Unit: The tree of the healthy digital environment

**Duration: 1 hour** 

The objective of this exercise is to stimulate creative thinking and engagement in fostering a positive online atmosphere.

**Step 1**. Divide your learners into different groups.

Step 2. Each group will have to draw a tree. Ask your participants to write down in the tree's roots, the best practices for reaching a healthy digital environment. They will also need to think about different personal and social consequences after reaching a healthy environment. Each of the positive consequences should be included in different tree's fruits, such as apples.

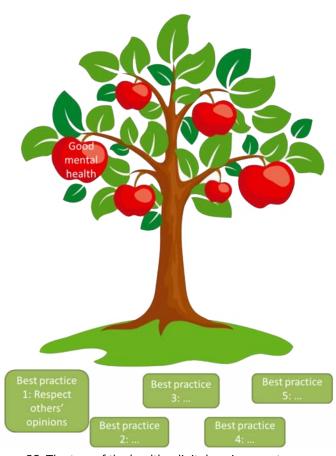


Figure 23: The tree of the healthy digital environment.

**Step 3:** Ask each group to present their trees.

**Step 4:** Make some reflections and conclusions as a group.

**Step 5**: Paste the trees in your facilities. Also, ask your learners to take them pictures and publish them in their social media.

## **Teaching Unit: The rainbow of hearts**

**Duration**: 2 hours

The aim of this activity is to create a safe environment for LGBTQ+ learners. The activity will raise awareness in all learners (no matter their sexual orientation or gender identity) to counteract cyberbullying; and promote a culture of respect. This activity might contribute to facilitate the process of self-discovery and disclosure in learners from this community. With this, all learners will be able to work in an inclusive room, where everyone is accepted as they are.

**Step 1**: Make a rainbow on cardboard. The size of the rainbow will depend on the size of the group and the hearts to be made.

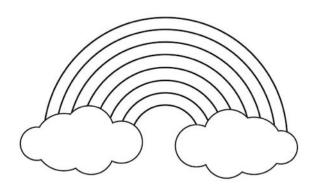


Figure 24: Rainbow example.

**Step 2:** Gather sheets of paper in the colors of the LGBTQ+ flag. Cut these sheets into square shapes. Give each student two squares.

**Step 3:** Each student will have to create 2 hearts. Provide them the following instructions:

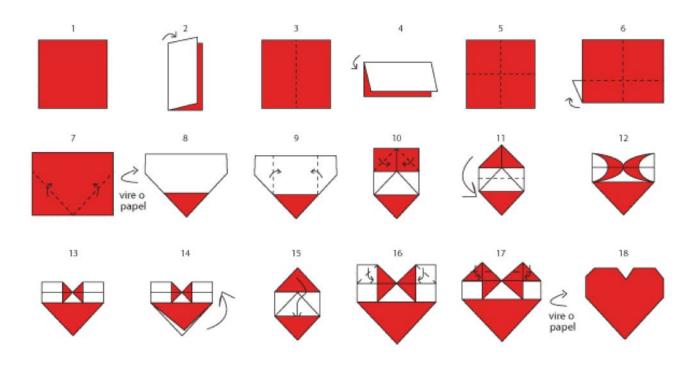


Figure 25: Instructions for creating a heart. Source: comofazerartesanatos.com



**Step 4**: Each student will have to write a message to each heart:

- **Heart 1:** Give a message so a person from the LGBTQ+ community feels supported.
- **Heart 2:** Give a message to prevent discrimination and cyberbullying against persons from the LGBTQ+ community.

**Step 5:** Ask each learner to share their hearts with the rest of the group and paste them in the rainbow.

**Step 6:** Paste the heart in the learning room.

The rainbow will serve as a safe space sign, to let learners know that the environment is LGBTQ+ friendly. Learners should know that youth workers and the organisations' staff:

- Are willing to challenge any type of language, harassment or cyberbullying actions.
- Support any person from this community in their journey of self-discovery and disclosure.

### **Teaching Unit: Roll the** dice!

**Duration**: 90 minutes

The aim of the activity is to practice the main knowledge acquired from the previous chapters.

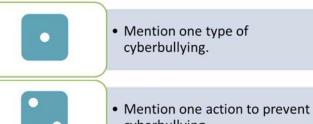
**Step 1:** Divide your learners into groups.

**Step 2:** Get into Google.com and type "roll dice". If you have a big screen, project the dice tool:



Figure 26: Dice tool. Screenshot. Source: Google.com

**Step 3:** Draw or print the following image:



cyberbullying.



· Mention one action to counteract cyberbullying.



· Mention one cyberbullying example.



• Mention one good practice for reaching a healthy online environment.



· Mention a bad habit that damages online interactions.

Figure 27: Roll the dice. Own creation. Own Source

**Step 4:** 1 person of each group will click the "roll" button. The group will have to provide an answer, according to the image from Step 3. They will have 2 minutes to prepare and write the answer on the following answer chart:

Types of cyberbullying	Actions to prevent cyberbullying	Ations to counteract cyberbullying	Cyberbullying examples	Good practices for reaching a healthy online environment	Bad habits that damage online interactions
Answers:	Answers:	Answers:	Answers:	Answers:	Answers:
Figure 28: Roll the dice answer chart. Own Creation. Own Source					

If the answer is correct, the group will win 1 point. The first group that gets 10 points will be the winner.

**Step 5:** Take a look to the answers included in the chart and make some reflections as a group.

## Teaching Unit: The anti-cyberbullying T-shirt movement

**Duration:** 3 Days (total 10 hours)

The main aim of the activity is to empower learners as ambassadors in anti-cyberbull-ying, within the learning organization.

The creation of the T-shirt can be done within the class or at home.

**Note:** Therefore, it is important that this activity is made after the whole group acquires knowledge and understanding of all the chapters of this book.

#### Day 1

**Step 1:** Tell your learners that during the next days they will create a T-shirt using ideas to promote anti-cyberbullying to the rest of the members of the organisation. Learners should start making a sketch design, in order to capture all their ideas. Sketching will also help them to:

- Make a list of the materials that they will use for decorating the T-shirt
- mprove creative skills
- Develop different ideas in the brain that can be changed in paper, rather than doing them directly on the T-shirt.
- Enhance confidence in which ideas can be turned in tangible results
- etc.

Below are some beautiful ideas that you can give to your students, so they can consider them in their sketches:

- Painting
- Use patches



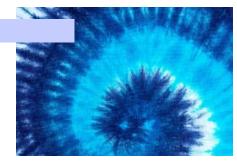


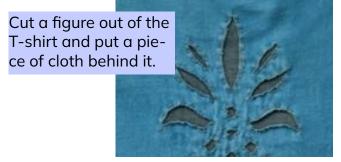






Tie dye





**Step 2:** Set a special date and ask your learners to bring the T-shirt to class and the materials needed. Due to environmental purposes, it is recommended that they take an old T-shirt that they do not longer use.

#### Day 2

**Step 3:** On the fixed date, learners will have to design their T-shirts according to their previous sketches.

#### Day 3

**Step 4:** Set a new date so learners can bring the T-shirt on. The main idea is that learners become anti-cyberbullying ambassadors. They will initiate a proactive movement for raising awareness about cyberbullying. It is important that they promote a healthy environment on both, in real and online youth communities.

Beyond just being visually attractive, these T-shirts will have a deeper meaning; they will be a badge for the ambassadors. The rest of the learners and staff from the organization will be able to easily identify them. Hence, ambassadors should be able to wear their T-shirt in future days. These young activists will clearly communicate to their peers that they:

- Can solve their doubts about cyberbullying.
- Provide advices to reach a healthy online environment.
- Support victims on incidents.
- Motivate other learners to talk about their experiences.

Anti-cyberbullying ambassadors will become an important figure in the organization for eradicating cyberbullying. They will also contribute in creating an environment under principles of kindness, respect and empathy.



# References

American Psychological Association Dictionary of Psychology, Bullying (<a href="https://dictionary.apa.org/bullying">https://dictionary.apa.org/bullying</a>)

UNICEF's staff. Cyberbullying: What is it and how to stop it. What teens want to know about cyberbullying (<a href="https://www.unicef.org/end-violence/how-to-stop-cyberbullying">https://www.unicef.org/end-violence/how-to-stop-cyberbullying</a>)

The Cambridge Dictionary, harassment (<a href="https://dictionary.cambridge.org/dictionary/english/harassment">https://dictionary.cambridge.org/dictionary/english/harassment</a>)

Marc Dahan, 2022, What are masquerade attacks and how to avoid them, Comparitech.

Aranza Trevino, Anne Cutler, Darren Guccione, 2023, What Is Doxxing?, Keeper Security.

Fortinet's staff. What is Doxing? (<a href="https://www.fortinet.com/lat/resources/cyberglos-sary/doxing">https://www.fortinet.com/lat/resources/cyberglos-sary/doxing</a>)

Randy McCall, 2004, Online Harassment and Cyberstalking: Victim Access to Crisis, Referral and Support Services in Canada, Concepts and Recommendations, Victim Assistance Online Resources. The Cambridge Dictionary, Catfish (<a href="https://dictionary.cambridge.org/dictionary/english/catfish">https://dictionary.cambridge.org/dictionary/english/catfish</a>)

MTV Channel, Catfish (<a href="https://www.mtv.com/shows/catfish-the-tv-show">https://www.mtv.com/shows/catfish-the-tv-show</a>)

European Union Agency for Fundamental Rights's staff, 2020, A long way to go for LGBTI equality, European Union Agency for Fundamental Rights.

Allyson Chiu, 2019, A teen's intimate messages to another boy were leaked by classmates. Hours later, he killed himself, his family says, The Washington Post.

Tim Fitzsimons, Alexander Kacala and Minyvonne Burke, 2019, Tennessee teen dies by suicide after being outed online, NBC.

Emily S. Rueb, 2019, A Teenager Killed Himself After Being Outed as Bisexual. His Family Wants Justice, The New York Times.

Joshua Smith, 2019, The Washington Post and other newspapers.

The Cambridge Dictionary, exclusion (<a href="https://dictionary.cambridge.org/dictionary/english/exclusion">https://dictionary.cambridge.org/dictionary/english/exclusion</a>)

eSafety Commissioner's staff. Cyberstal-king (https://www.esafety.gov.au/key-is-sues/staying-safe/cyberstalking)

ABC News, Nightline. Kenyanese YouTube Channel. Nightline| A Woman's Affair that Morphed into Cyber-stalking Horror (https://www.youtube.com/watch?v=HG-82d\_3Lk8Q).

Social Media Victims Law Center's team of expert legal content, 2023, What Is Flaming on the Internet?, Social Media Victims Law Center

The Cambridge Dictionary, Happy slapping (<a href="https://dictionary.cambridge.org/dictionary/english/happy-slapping">https://dictionary.cambridge.org/dictionary/english/happy-slapping</a>)

Save the Children's staff, 2019. Happy slapping, cuando la violencia se hace viral (https://www.savethechildren.es/actualidad/happy-slapping-violencia-online-menores)

Awesome Chimp YouTube Channel. Try not to laugh (prank edition) #shorts #funny (https://www.youtube.com/watch?v=FRd-gTgKxnx4)

Angela Balakrishnan and agencies, 2008,

Girl jailed for filming "happy slap" killing, The Guardian.

Andrew Robinson, 2020, The cruel killing that put Bradford at the centre of a landmark 'happy slapping' case, YorkshireLive.

MailOnline's staff, Teenage girl jailed for two years for filming 'happy slap' killing on mobile phone (https://www.dailymail.co.uk/ news/article-538291/Teenage-girl-jailed-years-filming-happy-slap-killing-mobile-phone.html)

BBC News's staff, 2008, 'Happy slap' teenagers sentenced (http://news.bbc.co.uk/2/hi/uk\_news/england/bradford/7294680.stm)

FBI's staff. Sextortion (https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/sextortion)

Department of Homeland Security'staff. Sextortion, it's more common than you think (https://www.ice.gov/features/sextortion)

Europol's staff, 2017, Online sexual coerción and extortion as a form of crime affecting children, European Union Agency for Law Enforcement Cooperation.

Europol's staff. Police across Europe issue

warning about the online coercion and extortion of children (<a href="https://www.europol.europa.eu/">https://www.europol.europa.eu/</a>)

FBI-Federal Bureau of Investigation Youtube Channel. Victim of Sextortion Speaks Out (https://www.youtube.com/watch?-v=ixAYkkub4Pw)

FBI-Federal Bureau of Investigation Youtube Channel. Special Agent Discusses
Sextortion Case (<a href="https://www.youtube.com/watch?v=miR-8uBbVrU">https://www.youtube.com/watch?v=miR-8uBbVrU</a>)

FBI's staff, 2015, Sextortion. Help Us Locate Additional Victims of an Online Predator (<a href="https://www.fbi.gov/news/stories/sextortion">https://www.fbi.gov/news/stories/sextortion</a>)

CNN's staff, 2015, FBI: Sextrortion a growing threat (https://edition.cnn.com/2015/07/08/politics/fbi-sextortian-growing-threat/index.html)

Thorn's staff, 2017, Ashley Reynolds: I Want People to Remember My Sextortion Story (https://www.thorn.org/blog/sextortion-remember-my-story/)

FBI's staff, 2015, Sextortion. Help Us Locate Additional Victims of an Online Predator (https://www.fbi.gov/news/stories/sextortion)

United Nations, Understanding Hate Speech, <a href="https://www.un.org/en/ha-te-speech/">https://www.un.org/en/ha-te-speech/understanding-hate-speech/what-is-hate-speech/</a>

Kids Help Phone, 2022, Helping young people recognize and respond to online hate, <a href="https://kidshelpphone.com">https://kidshelpphone.com</a>

Stopbullying's staff. Bystanders are Essential to Bullying Prevention and Intervention (https://www.stopbullying.gov/resources/research-resources/bystanders-are-essential)

Mayo Clinic's staff, Narcissistic personality disorder (https://www.mayoclinic.org/diseases-conditions/narcissistic-personality-disorder/symptoms-causes/syc-20366662)

Childhub's staff, Stereotypes and Prejudices, Childhub.org

The Cambridge Dictionary, voyeurism (<a href="https://dictionary.cambridge.org/dictionary/english/voyeurism">https://dictionary.cambridge.org/dictionary/english/voyeurism</a>).

Council of the European Union's staff, 2022. The general data protection regulation (<a href="https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/">https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/</a>)

The Cambridge Dictionary, self-esteem (<a href="https://dictionary.cambridge.org/dictionary/english/self-esteem">https://dictionary.cambridge.org/dictionary/english/self-esteem</a>)

The National Institute of Mental Health's staff. Depression (https://www.nimh.nih.gov/health/topics/depression)

Sherri Gordon, 2022, The Real-Life Effects of Cyberbullying on Children, Verywell family.

American Society for the Positive Care of Children's staff, Effects of cyberbullying (https://americanspcc.org/impact-of-cyberbullying/)

World Health Organization's staff, 2023, Depressive disorder (depression) (<a href="https://www.who.int/news-room/fact-sheets/detail/depression">https://www.who.int/news-room/fact-sheets/detail/depression</a>).

Gloria Willcox, 1982, The Feeling Wheel, Transactional Analy sis Journal, 12:4, 274-276, DOI: 10.1177/036215378201200411

All The Feelz' staff. The Feeling Wheel (<a href="https://allthefeelz.app/feeling-wheel/">https://allthefeelz.app/feeling-wheel/</a>)

Kapersky's staff. Tips to protect yourself from Cyberstalkers (<a href="https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking">https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking</a>) Fortinet's staff. What is Doxing? (<a href="https://www.fortinet.com/lat/resources/cyberglos-sary/doxing">https://www.fortinet.com/lat/resources/cyberglos-sary/doxing</a>)











Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.