#DigitSafe

Boosting digital safe spaces and resilience

Digital Resilience Handbook

CONEXX-EU

inova aspire

CESUR Tu Centro Oficial de FP

radio alma 101.9

Co-funded by the
Erasmus+ Programme
of the European Union

#DigitSafe

“#DigitSafe-Boosting digital safe spaces and resilience” aims at empowering young people to become resilient and safe digital citizens, enabling them to address some of the challenges and negative impacts of the digital era.

Project partners:

CONEXX-EU

inova
aspire

CESUR
Tu Centro Oficial de FP

СДРУЖЕНИЕ "ПРОФЕСИОНАЛЕН ФОРУМ ЗА ОБРАЗОВАНИЕТО" СОФИЯ

radio
alma
101.9

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

The **#DigitSafe-Boosting digital safe spaces and resilience** project following the EU Youth Strategy 2019-2017 in line with the EU Youth Goal 4 “Information & Constructive Dialogue” aims at empowering young people to become resilient and safe digital citizens, enabling them to address some of the challenges and negative impacts of the digital era.

#DigitSafe project pursues fostering a wider and deeper knowledge amongst young people on the two key topics of Cybersecurity & Hate Speech and Security & Privacy, in particular amongst the most vulnerable groups of young people, building safer digital common spaces and practices as well as boosting their capacities in terms of digital resilience.

This project also wants to achieve the following three specific main objectives:

- To **promote digital citizenship among young people** in participating countries by, in accordance with the EU Youth Strategy 2019-2027, empowering them with practical and compiled information about Security & Privacy, Hate Speech & Cyberbullying.
- To provide young people, especially the ones with fewer opportunities who often lack information and data literacy, with the necessary competences to enhance their **digital resilience**.
- To develop an innovative methodology that translates the compiled relevant information in a single handbook into a **multichannel public awareness campaign**, utilizing the most common audiovisual communication practices and language, tools and trends amongst young people. A multimedia and multichannel strategy that exploits the current content creation vast number of possibilities accessible to every user offered by the current social media landscape, aimed at strengthening the ability of the youth to make rational choices, knowing their digital rights.

This Digital Resilience Handbook on Cyberbullying, Hate Speech, Security & Privacy will offer in a comprehensive and unified way, guidance, practical information (legal resources, psychological resources, tips, open learning resources and other training resources) and key recommendations on different issues for youth to acquire a more in-depth knowledge of their rights, digital risks and threats in the context of these topics. It will raise awareness on

the opportunities and resources available to build skills for dealing with issues arising from young people's current digital lives. It will empower youth to become engaged digital citizens and foster a safer digital world. It will curate a vast amount of information, unifying it in a more useful and comprehensive way.

This Handbook will be divided into two modules:

1. **Cyberbullying & Hate Speech**
2. **Security & Privacy**

This will provide information not only regarding legal framework, raising awareness and prevention but also it will offer action guidelines as well as tips and recommendations.

1. Cyberbullying

1. CYBERBULLYING

1.1 What is Cyberbullying?

At the European level, multiple definitions of cyberbullying have been found, incorporating one or other aspects depending on the specific characteristics of each of the countries in which the study has been carried out (Belgium, Bulgaria, The Netherlands and Spain). However, the study developed in 2016 by the Policy Department of Citizen's Rights and Constitutional Affairs belonging to the European Parliament "Cyberbullying among Young People"[1] has produced a fairly accurate and homogeneous definition that can be used transnationally in the European Union.

"Cyberbullying describes those situations in which bullying is taking place on the internet mostly through mobile phones and social media. Cyberbullying corresponds, thus, to an equally aggressive and intentional act, carried out through the use of information and communications technologies (ICTs)."

As with offline Bullying, Cyberbullying usually involves the following 3 key participants, the conduct must occur intentionally and repeatedly and there must be an imbalance in the power relations between the aggressor and the victim:

1. **The perpetrator**. Person carrying out the aggression.
2. **The victim**. Person who suffers the aggression
3. **Bystanders**. Those who see what is happening between the bully and the victim but they are not directly involved in the bullying.

In relation to the persons involved, it is important to highlight that there is an important difference between bullying and cyberbullying and it is that the perpetrator (the bully) can stay anonymous in the case of cyberbullying, he/she can hide under a false identity (or someone else's identity) and it could be even several people hiding behind this identity. Nonetheless, Cyberbullying leaves an electronic trail - which can serve as evidence and a means to stop such behavior. Unfortunately, despite these differences, face-to-face bullying and cyberbullying often occur in parallel.

[1] Céline Chateau. (2016). Cyberbullying among Young people. European Parliament. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Furthermore, there are key features of Cyberbullying which facilitates its identification and comprehension:

Cyberbullying is malicious and never accidental. The cyberbully has the clear and conscious goal to harm the victim, to cause pain, humiliate him/her, to make him/her suffer physically or mentally.

It is performed from a position of power. The cyberbully always has an advantage and he/she holds a position of superiority. Depending on the environment in which Cyberbullying is taking place, it could mean committing cyberbullying with a group against one victim who is alone. As well, aggressors can take advantage of a non-aggressive or vulnerable victim, unable to defend himself/herself.

It is repetitively aimed at intimidating, angering or embarrassing the victims. An isolated aggressive action is not Cyberbullying yet. It becomes Cyberbullying when the aggression is repeated over and over again against the same person (or the same people).

Digitalisation has multiplied the channels through which bullying can be perpetrated via the Internet. However, some of the most common ways in which Cyberbullying victims are attacked are as follows:

- **Social networks**
- **Messaging platforms**
- **Gaming platforms**
- **Mobile phones**

In order to clarify which actions would fall under Cyberbullying, here are some examples that would fall within these illegal actions:

- Spreading lies or posting embarrassing photos/videos of someone on social media.
- Sending offensive messages or threats through messaging platforms.
- Sending malicious messages under someone else's identity.

1.2. Learn about the importance of Cyberbullying and its consequences. Raise awareness, how to identify it:

Identifying Cyberbullying

One key way in which to tackle Cyberbullying is being able to identify it and looking out for the warning signs. There is no universally agreed definition of cyberbullying internationally or on a European level. However, the European Commission defines cyberbullying as:

'Repeated verbal or psychological harassment carried out by an individual or a group against others through online services and mobile phones.'[2]

According to the Council of Europe, cyberbullying is distinctive from other types of bullying due to the risk of public exposure, the complex roles of observers and the size of the audience that comes with digital technologies and communication.[3]

WiredSafety, the largest online safety, education and help group in the world, disagrees with the proposal that cyberbullying must be 'repeated' to be classified as cyberbullying. Rather, some serious incidents of cyberbullying may not need to be repeated to qualify as cyberbullying. For example:

- Sextortion, sext-bullying and significant reputational attacks (e.g. those relating to sexual preference, sexual activity and other types of reputational attacks constituting defamation).
- Death threats or threats of serious bodily harm to the target or someone close to the target, designed to distress the target.[4]

In order to create a more tolerant and safe world online, cyberbullying must be tackled on a wider scale at both an individual and organisational level.

[2] 'Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.8.

[3] https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)

[4] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Council of Europe (2017)

According to a 2016 report by the European Parliament, the direct involvement of children in the development of solutions and policies relating to cyberbullying has been recognised as one of the most effective methods for coping with the issue.[5] Additionally, a 2017 report to the Council of Europe, concluded that in order to tackle cyberbullying, young people's voices should be represented and heard at a European and national level.[6] It is clear, therefore, that the voices of young people should be at the forefront of these discussions.

The consequences of Cyberbullying cannot be taken lightly or regarded as mere jokes, as it not only denies the emotions and suffering of the victim but also normalises this type of violence in the digital environment. Cyberbullying's consequences can be long-lasting and can affect the victims in many ways. In some extreme cases, Cyberbullying can even lead to suicide. #DigitSafe Consortium has reached these conclusions following intensive research carried out at European level in four countries and the testimonies of cyberbullying victims collected by the project. Social Networks and Cyberbullying among Teenagers developed by the JRC has helped to understand the scope of the consequences of cyberbullying in the victims that suffer it. We could highlight as the main consequences of Cyberbullying:

- **Mental and emotional consequences**

Victims may feel sad, ashamed, embarrassed, stupid, depressed, angry and anxious. Victims usually lose their interest in the things they used to love, they develop a lower self-esteem or they feel isolated, incapable of communicating with their peers. Sometimes victims of cyberbullying can become "victims-aggressors", replicating the behavior and bullying others.[7]

In other words, there is a real chance of Cyberbullying causing deep psychological harm to the victims. Victims of Cyberbullying are[8]:

1. More likely to suffer from **depression** and **anxiety**.

[5] Cyberbullying among Young People', Directorate General for Internal Policies (European Parliament), 2016, p.11

[6] Bullying, Perspectives, Practices and Insight, ancie Richardson, Elizabeth Milovidov, Roger Blamire, Council of Europe (2017) p.44

[7] Joint Research Centre (2013). Social Networks and Cyberbullying among Teenagers. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

[8] https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/preventing-bullying-and-violence [accessed 27/05/2022)

2. More likely to suffer from **poor academic achievement and behaviour problems at school**.
3. Students who experience violence and bullying are more likely to have **difficulty developing basic democratic competences such as empathy**, **respect for others**, **openness to other cultures and beliefs**, **tolerance and self-efficacy**.

- **Physical consequences**

Due to the stress and anxiety that a victim suffers, this can lead to **physical problems** such as feeling tired because of sleeping disturbances or experiencing real **health symptoms** such as stomach aches or headaches.

- **Legal consequences**

The feeling that they are being ridiculed or bullied by others often prevents the victims of cyberbullying from reporting or trying to deal with the problem. This, together with the slow evolution in the legal classification of the crime, means that it often goes unpunished, and it encourages the repetition of attacks.

Raising awareness of Cyberbullying to prevent it is essential. The first step in identifying cyberbullying is to have a clear definition of what it involves. Furthermore, in Europe, in order to prevent cyberbullying, policy decisions have been taken and numerous programmes have been defined and implemented. Nevertheless, the impact that this phenomenon has means that European institutions need to continue to research, to legislate and to encourage collective and individual actions in order to address it.[9]

[9] Rizza C, Martinho Guimaraes Pires Pereira A. Social Networks and Cyber-bullying among Teenagers. EUR 25881. Luxembourg (Luxembourg): Publications Office of the European Union; 2013. JRC80157

Addressed to young people

Cyberbullying Research Center[10] has developed a series of structured tips on how to proceed in order to prevent Cyberbullying and secure ourselves as users. Prevention is always the best option to fight against this problem. In addition, we have selected these tips precisely because most of them have parameters that are much more oriented towards children than young adults:

- **Stay up to date with privacy settings**

Social Media sites and programs are modifying and updating their privacy settings frequently. Make sure that you are familiar with the new profile options and keeps as much information as possible restricted to those you really trust.

- **Restrict access to your contact information**

Do not give out your email or phone number to people that you do not know. Also, keep your email and phone number off of social media sites. You never know who might have access to them and you cannot trust everyone who is a “friend” or “follower”.

- **Learn Internet etiquette**

To prevent potential problems with other Internet users, learn social conventions related to interaction in cyberspace. For example, do not write in all caps. This can be perceived as yelling to some. Also resist using sarcasm online as it can be easily misinterpreted.

- **Don’t send inappropriate pictures or videos**

Remember that today’s boyfriend or girlfriend can be tomorrow’s scorned lover. You do not want someone with inappropriate pictures or videos of you posting them online and sharing them with the rest of the world. Don’t put yourself in the position of having to worry about this.

[10] Cyberbullying Research Center. (2021.)Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online

- **Google yourself**

You should always know what is being said about you. It is often surprising to find information you thought was private show up in public databases, new articles or on social media pages that have been indexed by search engines.

- **Do not accept friend requests from strangers**

If you do not know the person who is sending you a friend or follower request, ignore it. Most social media sites and apps also give you the option to block the user if you like.

- **Use site – based controls**

Disable search options on certain social media sites to prevent anyone in the general public from searching for you or messaging you. This allows you to have more control over who you interact with online, as you are the only one who can initiate it.

- **Keep your information protected**

If using a public computer or wireless, be sure to log off of any site you are on when you walk away from that computer – even for a minute. In fact, do it on your other mobile devices too if there is a chance that someone might come by and use your account to be funny or mischievous. Do not give passwords out to anyone and change your password frequently. Also, make sure your phone and tablet have a passcode and are locked down.

- **Be skeptical in online interactions**

Even among people you trust, it is risky to reveal too much information because you never know for sure if the person you think you are communicating with is really there- or if they are alone.

- **Guard against me and people**

Remember that some people have a lot of time on their hands and all they want to do is make life miserable for others. Don’t let them. Resist putting too much personal or private information online that could be used to harass or humiliate you and resist interacting with them in any way. As conventional wisdom indicates. Don’t feed the internet trolls!

Addressed to teachers and parents

It is important for organisations, schools, workplaces and individuals to commit themselves to tackling cyberbullying because of the impact that cyberbullying can have on victims. The research developed by Cyberbullying Research Center in 2021 “Cyberbullying: Identification, prevention and Response in 2021”[11] give an extensive explanation of how teachers and parents could address Cyberbullying in terms of identification and prevention:

Educating the community about a responsible use of the devices focused on digital citizenship is maybe the most important preventive step regarding educational institutions and its teachers/professors. Instilling discipline in students who engage in harassing or threatening others and letting them know what they are doing is more than wrong, it is a crime.

It is essential to include in various areas of the education institution curricula appropriate online content to discuss Cyberbullying among other digital threats. Furthermore, the messages could be reinforced in other classes, especially in those that utilizes technology and digital tools. Establishing and reinforcing a respect and an integrity environment in the educational institutions is crucial where violations and harassment are satiated formally or informally.

Moreover, developing new and creative strategies to fight cyberbullying is getting more and more important nowadays, particularly to face minor forms of harassment and prevent them. Researchers Hinduja and Patchin (2021) from the Cyberbullying Research Centre give different examples:

“Students may be required to create anti-cyberbullying posters to be displayed throughout the school, or a public service announcement (PSA) video conveying an anti-bullying and/or a pro-kindness message.

Older students might be required to give a brief presentation to younger students about the importance of using technology in ethically-sound ways.

[11] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

The point here, again, is to condemn the behaviour (without condemning the child) while sending a message to the rest of the school community that bullying in any form is wrong and will not be tolerated".[12]

In other words, it is important not just for formal education but start to introduce in the formal education at school non-formal and informal activities to fight and prevent Cyberbullying from a creative point of view.

On the other hand, parents *"must demonstrate to their children through words and actions that they both desire the same end result: that the cyberbullying stops and that life does not become even more difficult"*.[13]

Cyberbullying Research Centre (https://cyberbullying.org/) highlights how critical it is, as a parent, not to be dismissive of their children's perspective, but to validate their voice and opinion. **It is vital that targets of cyberbullying and bystanders know that the adults, since they have knowledge of the cyberbullying situation, "*will intervene rationally and logically, and not make the situation worse*"**.[14]

How should parents react if they discover their own child is a cyberbully? Firstly, they need to explain to him/her/them how that behavior is provoking and inflicting harm and pain in the real world. After that, parents should be able to give him/her/them the opportunity to move on and end that behaviour. Researchers Hinduja and Patchin (2021) propose parents "*to cultivate empathy by intentionally putting them in situations that make them uncomfortable and that can soften their heart*". Children need to know that every action, even if it is online, has serious consequences.

From the parents' side, it is essential to start paying greater attention to their children's behaviour and actions online.

[12] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
[13] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf
[14] Hinduja and Patchin.(2021). Cyberbullying: Identification, prevention and Response: https://cyberbullying.org/Cyberbullying-Identification-Prevention-Response-2021.pdf

1.3. Guidelines: how to deal with Cyberbullying victims? (Procedures, empathy, the importance of listening, emotional support, psychological support):

The compilation of procedures and tips on how to proceed has been mainly shaped by the more than completed proposals of the Cyberbullying Research Center and Amnesty Jeunes (https://jeunes.amnesty.be/).

When you are victim yourself

If you are a victim, we would like to advise you with a series of steps to follow if you are suffering from cyberbullying:

- **Seek help**

First of all, you need to talk, discuss with relatives or professionals!

- **Report the content**

If the Cyberbullying has been produced through a social network, report the content to that platform. This is not always effective, but it is important that the social network knows who the accused is so that they can take action, sometimes after several reports.

- **Protect yourself**

Change your password, increase the privacy of your posts, remove personal information such as your email address, phone number or links to other accounts.

- **As a temporary measure, delete your account or change your nickname**

Try to disconnect from social networks for a while, block the person who is the source of the cyberbullying.

- **Reply and remind the person who is harassing you of the legal framework by pointing out that online harassment is a crime punishable by law.**

- **If it happens in the work environment, talk to your employer.**

Let your employer know if the person harassing you is a co-worker, or if the bullying is occurring on a work-related forum or blog. If the harassment prevents you from doing your job, your employer needs to know about it.

- **Cut ties**

Don’t befriend those who are mean or try to get them to warm up to you. If you feel like you need to respond to the person who is mistreating you, do it respectfully. Do not try and rationalize or make friends with anyone who is cruel towards others.

- **Do not relate**

Those who cyberbully want you to react. The problem is that if you respond angrily, the one doing the bullying may feed off of that response and continue (and even escalate the severity of) the cyberbullying. Plus there could be consequences for your response.

- **Contact the Internet Service Provider (ISP)**

Try to contact the Internet Service Provider of the person who is harassing you if they have been identified. The ISP can then contact the person or perhaps close their Internet account directly.

- **File a complaint by going to a police station**

Take evidence of the attack (for example, screenshots). The police will take note of your complaint and all the information related to your complaint and put it into a report. They will give you a copy of the report and a certificate of complaint. The report is then sent to the public prosecutor's office, i.e. to the magistrates responsible for the investigations. Ask for the number of the report to be able to follow the case and to know which public prosecutor's office (of which commune) is competent.

- **Report the cyberbullying by publicly**

Share screenshots of the bully (be sure to hide the bully's username and profile picture so that you are not accused of defamation).

As a colleague (at work or at school)

In this area, Save the Children[15] has very accurately pointed out some guidelines on how to act in the case of bullying:

- You may feel fear or rejection in this situation, but take action.
- If you see that you cannot stop it on your own and that it is not the best thing to do, ask an adult or a person in charge for help. This is not snitching, it is being supportive of those in need.
- Support the colleague who is being bullied. No one deserves to be treated badly.
- Propose conducting training or develop materials to raise awareness at your educational institution or company to prevent cyberbullying and seek help.

As a teacher

Teachers have to pay attention to different signs that can show that a child is being cyberbullied. Some of these signs can be a rapid increase or decrease in device use or an emotional response to what is happening on their device. If a child hides their screen or device when others are near and avoid discussion, this should be taken into account.

In addition, teachers also have to help kids how to identify, respond and avoid cyberbullying. Some guidelines would be:

- Communication is very important so **if you ever think a child is being cyberbullied, speak to them privately and ask about it**. You can also speak to a parent about it. Teachers can be a mediator between the child, parents and school.
- **Promote a safe class environment**. Help children develop emotional intelligence so that they can learn self-awareness and self-regulation skills and learn how to have empathy for others.
- Encourage students to pay attention to signs that can help them identify when something happens on digital media that makes them feel uncomfortable, worried, sad or anxious.

[15] Save the children. Advice for students on how to deal with bullying. https://www.savethechildren.es/publicaciones/consejos-para-estudiantes-frente-al-bullying-o-acoso-escolar

- Teach them to think before posting.
- Explain to students the three ways they can and should respond if they witness cyberbullying: if you support the target of the bullying you are an ally, if you try to stop the cyberbullying you are an upstander and if you are a victim of cyberbullying you have to report it to an adult.

As a parent

It is very likely for kids not to recognize that they are being cyberbullied because they might feel ashamed. It is very common for the youth to suffer silently. They may be afraid that parents will react by restricting their online access, they may feel embarrassed that they cannot take care of the bullying themselves, they may be afraid that parents will handle things in a way that escalates the bullying, or that they will not understand the problem.

For these reasons, if parents see any signs in their kids they must take action immediately. First of all, **try to talk with your child and listen to him/her/them**. The best way to do it is engaging him/her/them in conversation about what is going on in a calm manner. Take your time to understand exactly what happened and the context in which it occurred. It is very important for your kid that you do not minimize the situation. Since social media has become an extension of children's day to day lives, a nasty comment or text can be devastating for him/her/them. Praising your child for doing the right thing by talking to you about it is a good way to boost confidence between you two.

Once you know about it, **offer comfort and unconditional support** as cyberbullying victims often experience a feeling of isolation. Show your child that this situation can be dealt with in a way that does not involve online retaliation. Make your child feel safe, it must be the foremost priority as well as letting your child know that it is not their fault.

After that, **try to collect as much evidence as possible**. Print out or make screenshots or recordings of conversations, messages, pictures, videos, and other items which can serve as clear proof that your child is being cyberbullied. Keep a record of any and all incidents to assist in the investigative process. Also, keep notes on relevant details like location, frequency, severity of harm, third-party involvement or witnesses, and the backstory.

The next step is to **contact the content provider**, since cyberbullying always violates the Terms of Service of all legitimate service providers. They should take action on this matter so that your child does not suffer from it again.

If the cyberbully is a classmate or goes to the same school as your child, you should **notify the school as soon as possible** since they might have rules for responding to cyberbullying. Parents can also contact the police in case the situation mentioned does not help the situation to get better.

If it is necessary, try to seek counseling for your child. Children may benefit from speaking with a mental health professional. They might prefer to dialogue with a third party who may be perceived as more objective.

1.4. Prevention measures

There is no foolproof way to prevent a child from being cyberbullied. However, there are different ways to reduce the likelihood they will be targeted.

First of all, **it's important to use passwords** on everything and not share these passwords with anyone. A good way to improve kids' security online is using the privacy tools and settings provided by social media. We have to make sure children are aware of the privacy settings and tools offered by the organization and go through each social media and set the privacy settings to the most secure one. This means making accounts private, preventing people from tagging them and so on.

Kids have to know that it is important to keep personal stuff private. They should never share their address, cell phone number, or email address online. They should be careful about sharing too much information about where they go to school, especially if they have friends or followers online that they don't know really well.

They also have to know that they have to log out when using public devices such as public computers or laptops at school or the library. This includes logging out of email, social media accounts, their school account or any other account they may open.

Last but perhaps most importantly, **children should be aware that if they are ever the victims of cyberbullying they must report it to their parents or teachers**.

1.5. How to report cyberbullying

(legal framework, institutions, NGOs, etc.)

One of the most significant aspects of reporting Cyberbullying is that most European countries do not have specific legislation on Cyberbullying. Despite the importance, the large number of cases and the concern among young people, legislation has not yet made progress in this area. This has made the work of institutions and organisations essential to help to identify cases, denounce them and give support to the victims.

Belgium

- **Legal framework**

Cyberbullying is understood as a "criminal offense" in Belgium, thus it is a subject of criminal punishment. Nonetheless, as in many other countries, there is no specific criminal law with regard to Cyberbullying. However, this does not mean that the criminal offence goes unpunished, but rather that through other Belgian laws:

Art. 442 bis & art. 442 ter of the Belgian Criminal Code = Harassment.

"Anyone who tells harmful lies in public that might damage someone else's honour or reputation commits a breach of article 442 of the Belgian Penal Code".

Art. 145.3bis of the Law of 13/06/2005 with regard to electronic communication, defamation and slander
Art. 448 of the Belgian Criminal Code= Public insults
Art. 422 bis of the Belgian Criminal Code = Stalking
Art. 383 of the Belgian Criminal Code= Public indecency

In the world of work, Cyberbullying is a relatively recent and unexplored phenomenon, despite the ubiquitous use of ICTs in today's working environments and modalities recently adopted ILO Violence and Harassment Convention, 2019 (No. 190), and its accompanying Recommendation No. 206, which include within their scope violence and harassment occurring also through work-related communications, including those made possible by information and communication technologies. In Belgium, these provisions are incorporated into occupational Safety and Health (OSH) legislation.

- **Institutions & NGOs**

In Belgium, if Cyberbullying occurs in an educational institution, internal regulations and internal rules allow these institutions to put sanctions against it. Apart from that, there are some organisations and platforms that give support and orientation to those victims that are looking for help before the legal process that in most of the cases, is complex, difficult and traumatic for the young person.

CyberHelp (https://smartcity.brussels/news-750--the-cyberhelp-app-combats-cyberbullying)

A joint initiative by the Belgian Federal Police, Mons University, the Wallonia-Brussels Federation. It is an **app against cyberbullying**, to report it through your own smartphone. The app includes a button which enables them to make a screen grab of their chat history with a cyberbully and a second button through which they can then send this content to the people in charge of dealing with such situations at their education institution. In 2021, the CyberHelp team will be presenting the app to 12,000 students by making around 100 visits to schools in Wallonia and Brussels.

Amnesty Jeunes Belgium (https://jeunes.amnesty.be/)

Télé-Accueil Bruxelles (https://tele-accueil.be/bruxelles/)

Télé-Accueil is a **telephone and chat service**. Anyone wishing to find "someone to talk to" will find by through 107 number, an attentive ear, free of charge, 24 hours a day, 7 days a week, in anonymity and confidentiality. It is a great option for those victims who, out of embarrassment or inability to know how to deal with cyberbullying, cybercrime or hate speech, receive assistance and a person to listen and advise them.

Spain

When cyberbullying takes place there are several things to be aware of. Firstly, do not reply to or forward cyberbullying messages and block the person who is bullying you. It is important to keep evidence of cyberbullying. Record dates, times and descriptions of cyberbullying. It is possible to report bullying both on the platform where it takes place and legally, e.g. to the police.

When reporting through the platform, first review their terms and conditions or rights and responsibilities sections. These terms describe content that is or is not appropriate and then report cyberbullying to the social media site so they can take action against users abusing the terms of service.

On the other hand, when cyberbullying implies threats of violence, child pornography or sending sexually explicit messages or photo or stalking and hate crimes, it is considered to be a crime. In these cases, it should be reported to the police.

There are foundations that offer support and help to those children or adolescents and their families who do not know how to deal with this issue or how to report it. For example:

Cybersmile (https://www.cybersmile.org/who-we-are)

It is a nonprofit organization committed to digital wellbeing and tackling all forms of bullying and abuse online.

AEPAE (https://aepae.es/plan-nacional)

It is an Association for the Prevention of Bullying in Spain. The aim of this association is to develop preventive behaviour in children and adolescents aimed at conflict resolution in the school environment.

INFOACOSO (https://infoacoso.es/telefonos-de-ayuda-contra-el-acoso-y-el-bullying)

This association offers a guide on its website on how to act if you are being cyberbullied and where to call to report it, depending on the community of Spain you live in.

The Netherlands

In the Netherlands, the following institutions and bodies may help you if you are a victim of cyberbullying:

- **MiND** (https://www.mindnederland.nl/) The internet discrimination hotline which registers and evaluates reports of discrimination on the internet.
- Approach an antidiscrimination service in your area. All municipalities in the Netherlands have a an antidiscrimination service whereby you can approach the service with a question or complaint about discrimination.
- Call the national discrimination helpline (0900 235 5345)
- Contact the police if you have been harassed, intimidated, threatened or worse.

Some of the services mentioned above are specific to those who have faced discrimination. Discrimination is usually defined as the unequal treatment of another person based on their ethnicity, sex, gender or genetic features. Discrimination is prohibitted under EU law:

Article 21: '*Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.*'[16]

As cyberbullying takes many forms, you may feel as though you are a victim of cyberbullying which is not specifically discriminatory. In these instances, some suggestions are:

- Report cyberbullying to the school/ work (if you are being bullied by someone in your place of education/ employment).
- Stop Online Bullies is a Dutch tailored intervention scheme for lower educated cyberbullying victims, aimed at teaching victims how to cope with cyberbullying and its negative effects.
- Block and report the cyberbully on your social media channels.
- Block and report the bully's number.

[16] Article 21 EU law: Non discrimination https://fra.europa.eu/en/eu-charter/article/21-non-discrimination#:~:text=EU%20Charter%20of%20Fundamental%20Rights,-Previous%20title&text=1.,2.

- Request information from your local police department.
- File an official report with the police (if this is perceived as the best course of action after discussion with the police department).

In the Netherlands, specific responsibilities are placed upon schools to combat and prevent cyberbullying. For example, the KiVa programme aims to improve the safety of students in schools and has been financed by grants from the Dutch Ministry of Education.

The KiVa programme (https://www.kivaprogram.net/) is a Finish research and evidence based anti-bullying programme which was originally developed by the University of Turku and has been implemented in schools globally. It is based on three main elements: prevention, intervention and monitoring.[17]

- **Prevention**. preventative actions such as the KiVa curriculum are implemented in schools to focus on the prevention of bullying.

- **Intervention**. KiVA intervention techniques target children who have been directly involved in bullying. The goal is to provide schools and students with solution focused tools.
- **Annual monitoring**. Annual surveys for both students and staff within KiVa schools are used to monitor the effectiveness of the programme and provide information on how to improve their anti-bullying work.

From programmes such as KiVa, lessons can be learnt and applied to individuals and organisations across the world. It is evident that a focus on preventative measures is crucial to ensuring that all forms of bullying are dealt with. This can be applied to cases of cyberbullying via educational campaigns. These measures ensure that people are able to use the internet safely.

[17] What is KiVa? https://www.kivaprogram.net/what-is-kiva/

Bulgaria

Cybercrimes, including cyberbullying, privacy and security risks online, are reported to the Cybercrime Department of the Ministry of Interior of Bulgaria. It is a general reporting mechanism for non-urgent signals for cybercrime (dedicated primarily to cyber-fraud and child-pornography). The programme is coordinated by the Cybercrime Department (www.cybercrime.bg) at the General Directorate for Fighting Organized Crime of the Ministry of interior.

Through an online form cyberbullying, cyber-fraud, child-pornography can be reported. For urgent cases people are advised to report to the general emergency telephone number 112.

There is also a state-managed mechanism for support and counseling children and youth on different matters, including cyberbullying, hate speech and privacy and security risks online. This mechanism is the **National Telephone Line for Children** 116 111 that is managed and administered by the State Agency for Child Protection with the aim of supporting all children and their families in Bulgaria. The operators who answer the calls are trained psychologists who 24 hours a day, 7 days a week, anonymously and completely free of charge, are ready to listen, support, consult and guide the callers on all issues that concern them.

2. Hate speech

2. HATE SPEECH

2.1. What is Hate Speech?

There is no universally accepted definition of hate speech. In this section, we will outline a couple of definitions which are outlined in both EU law and by leading organisations combating hate speech. Hate speech is defined by EU law as:

'(Illegal) *The public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin*.'

Whilst the Framework Decision relates to racism and xenophobia, the majority of Member States have extended their national laws to include other grounds such as sexual orientation, gender identity and disability.[18] INACH (the leading network in the EU and globally combat cyber hate) defines hate speech as:

'*The intentional or unintentional public discriminatory and/ defamatory statements; intentional incitement to hatred and/ or violence and/ or segregation based on a person's or a group's real or percieved race, ethnicity, language, nationality, skin colour, religious beleifs or lack thereof, gender, gender identity, sex, sexual orientation, political beleifts, social status, birth, age, mental health, disability, disease*.'[19]

Under EU law, freedom of speech and expression are protected, leading some to believe that there is a conflict between the protection of freedom of speech and expression and the criminalisation of hate speech. Many experts propose that this supposed 'conflict of interest' between criminalising hate speech and protecting freedom of speech is misunderstood.

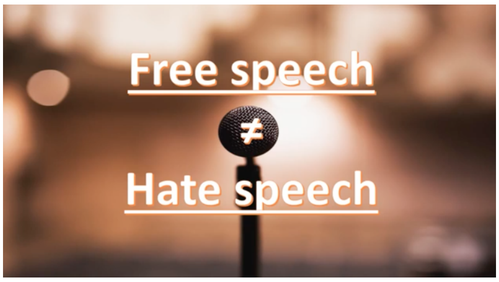
In fact, the International Covenant on Civil and Political Rights (ICCPR) prohibits 'any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.'[20]

[18] Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf

[19] INACH definition of hate speech https://www.inach.net/cyber-hate-definitions/

[20] ICCPR Article 20 (2)

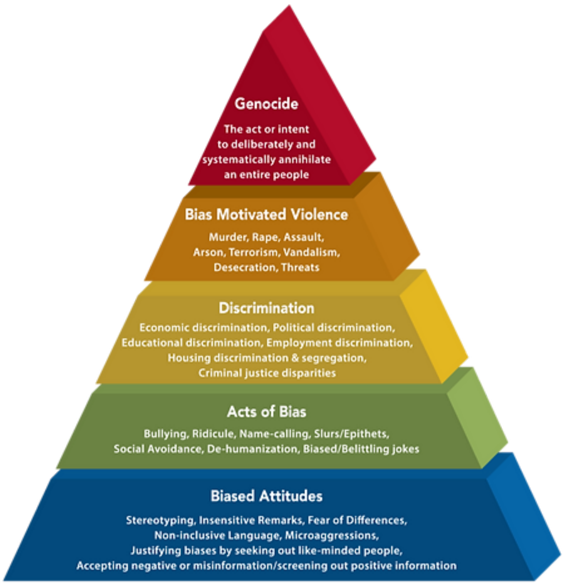
This short video explains further this misconception and why freedom of speech is not absolute.



https://www.youtube.com/watch?v=V0HhyVLX0ZA

The ‘Pyramid of Hate’ (shown below) signifies the danger of all forms of hate speech.[21]

The pyramid of hate is used to exemplify how hate speech has historically (and continues) to be a precursor to extreme violence. It aims to highlight how hate speech can pose a threat to others by contributing to the pyramid of hate and violence. Tackling hate speech, therefore, is essential to creating a more peaceful and tolerant world.


Genocide
The act or intent to deliberately and systematically annihilate an entire people
Bias Motivated Violence
Murder, Rape, Assault, Arson, Terrorism, Vandalism, Desecration, Threats
Discrimination
Economic discrimination, Political discrimination, Educational discrimination, Employment discrimination, Housing discrimination & segregation, Criminal justice disparities
Acts of Bias
Bullying, Ridicule, Name-calling, Slurs/Epithets, Social Avoidance, De-humanization, Biased/Belittling jokes
Biased Attitudes
Stereotyping, Insensitive Remarks, Fear of Differences, Non-inclusive Language, Microaggressions, Justifying biases by seeking out like-minded people, Accepting negative or misinformation/screening out positive information

[21] https://www.rightsforpeace.org/hate-speech

2.2. How to Prevent Hate Speech

Hate speech is tackled at EU level by the Audiovisual Media Services Directive (AMSD) which requires national authorities in every EU country to ensure that audiovisual media services do not contain incitement to hatred.[22] Additionally on an EU level, the Commission agreed with Facebook, Microsoft, Twitter and Youtube a 'Code of Conduct on countering illegal hate speech online.' The implementation of this code of conduct is regularly monitored with a network of organisations across the EU.[23]

How can you on an individual level prevent hate speech?

One way to combat hate speech is to **block and report accounts of hate speech that you encounter online** (see the next section on tips on how to report hate speech). The United Nations recommend committing to following practices to prevent hate speech[24]:

- **Pause**. Restrain from making any hateful comments yourself and/or sharing such content.
- **Fact check**. Make sure that you spot false and biassed information before spreading misinformation.
- **Challenge**. Spread your own counter speech and challenge hate speech wherever possible.
- **Support.** Take a public stand and extend solidarity to targets of hate speech.
- **Report**. Check out the community guidelines of social media platforms you use and report instances of hate speech which violate these guidelines. For more serious cases you may wish to file a complaint with the police (e.g. when there is incitement to violence).
- **Educate**. Share educational resources and public campaigns or start conversations with your friends and family.

[22] Code of Conduct- Illegal Online Hate Speech Questions and Answers, (European Commission 2016) https://ec.europa.eu/info/sites/default/files/code_of_conduct_hate_speech_en.pdf

[23] The EU Code of Conduct on Tackling Illegal Hate Speech https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[24] United Nations- how to deal with hate speech? https://www.un.org/en/hate-speech/take-action/engage

- **Commit**. Consider joining an NGO or initiative that works to address hate speech within your community.

To learn more about hate speech and ways to prevent it, test yourself by taking this quiz by the United Nations: https://www.un.org/en/hate-speech/take-action/test-yourself

2.3. How to report Hate Speech

INACH is a leading network within the EU and globally that works to combat cyber hate. It is a foundation under Dutch law and is based in Amsterdam but has 32 members from 28 countries. Its website offers an online reporting platform to report any incidents of cyber hate. As well as offering a complaints and reporting service against cyber hate, INACH uses the data from all the complaints received to write reports and analyses. In doing so, they attempt to influence the public, social media companies and international institutions which aids their work in lobbying for international legislation against cyber hate.

In addition to reporting instances of cyber hate via INACH, users can also directly report any incidents of hate speech through the social media channel in which they encounter it. The council of Europe website provides information on how to report on social media channels[25]. There are some cases whereby you do not need to have an account to report.

Some European countries have introduced national reporting procedures and mechanisms for hate speech, hate crime and cyberbullying as part of the European Councils 'No Hate Speech Youth Campaign'. You can find the list of countries and their reporting procedures on the Council of Europe website[26]. Other suggestions for reporting hate speech include:

- Report the hate speech to the police.
- Report to an authoritative body for example, a civil or administrative court.
- Report to an NGO for example, MiND is the national reporting centre in the Netherlands for hate speech and discriminatory content.
- Talk to someone you trust- e.g. a parent, friend, teacher.

[25] Reporting on Social Media Channels https://www.coe.int/en/web/no-hate-campaign/reporting-on-social-media-platforms#{%2237117289%22:[]}

[26] https://www.coe.int/en/web/portal

3. Cybersecurity and Privacy

3. CYBERSECURITY AND PRIVACY

3.1. Why is personal data protection important?

The term personal data protection is defined in Art. 4 (1) of the General Data Protection Regulation:

'Personal data are any information which are related to an identified or identifiable natural person. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data.'

In the next paragraphs we will further explore the types of data that require protection.

Data protection is important, since it prevents the misuse of the information of an individual or an organization, it aims to prevent different privacy and security risks, such as fraudulent activities, hacking, phishing and identity theft (described in the next section).

The type of data that requires protection

Vital information, such as **names, addresses, emails, phone numbers, health information or bank details** are all data that should be carefully stored and protected. If such information gets in the wrong hands, it can compromise people's safety in many forms, including personal integrity, physical safety and financial security. Stolen information can also be used to create fake profiles and commit fraud. Examples of personal data include:

- Name and surname
- Home address
- An email address such as name.surname@company.com
- Identification Card Number
- Location data (for example the location data function on a mobile phone)*
- Internet Protocol (IP) address
- Cookie ID*

- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Examples of data that is not considered personal data include:

- Company registration number
- An email address such as info@company.com
- Anonymised data: personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

Who is responsible for protecting our data?

Data protection is the process of safeguarding important information from corruption, compromise or loss. The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates.

Therefore, organizations that store and manage personal information are responsible for guaranteeing that it is safeguarded from corruption, compromise or loss. In the European Union, the General Data Protection Regulation (GDPR) (https://gdpr-info.eu/) protects the personal data of the EU citizens. It is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018.

Key Elements of Data Protection

One very important data protection model is the CIA triad, where the three letters of the name represent the three elements of data protection: *Confidentiality*, *Integrity*, and *Availability*. This model was developed to help individuals and organizations develop a holistic approach to data protection. The three elements are defined as follows:

- Confidentiality: The data is retrieved only by authorized operators with appropriate credentials.
- Integrity: All the data stored within an organization is reliable, precise, and not subject to any unjustified changes.
- Availability: The data stored is safely and readily available whenever needed.

According to the General Data Protection Regulation (GDPR), there are also several principles of personal data protection that organizations collecting and managing it must comply with:

- **Lawfulness, fairness and transparency**. Processing must be lawful, fair, and transparent to the data subject.
- **Purpose limitation**. The data controller must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- **Data minimization**. The data controller should collect and process only as much data as absolutely necessary for the purposes specified.
- **Accuracy**. The data controller must keep personal data accurate and up to date.
- **Storage limitation**. The data controller may only store personally identifying data for as long as necessary for the specified purpose.
- **Integrity and confidentiality**. Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- **Accountability**. The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates. There is also little tolerance for downtime that can make it impossible to access important information.

As explained above, organizations that collect, store and manage personal data are responsible for guaranteeing that this data is not misused and is available to authorized personnel at any time. The GDPR guarantees this through concrete legal requirements and sanctions for the organizations who do not comply with them. On the other hand, individuals can maintain security against outside parties’ unwanted attempts to access their data, as well as protect their privacy from those they don’t consent to sharing their personal information with.

3.2. Types of personal data and privacy threats and crimes

- **Identity theft**

Identity theft **is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud**, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation. The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name.

Identity theft occurs when someone steals your personal information, such as your Social Security number, bank account number, and credit card information. Identity theft can be committed in many different ways. Some identity thieves sift through trash bins looking for bank accounts and credit card statements. More high-tech methods involve accessing corporate databases to steal lists of customer information. Once identity thieves have the information they are looking for, they can ruin a person's credit rating and the standing of other personal information.

Identity thieves increasingly use computer technology to obtain other people's personal information for identity fraud. To find such information, they may search the hard drives of stolen or discarded computers; hack into computers or computer networks; access computer-based public records; use information-gathering malware to infect computers; browse social networking sites; or use deceptive emails or text messages.

Types of identity theft

Financial identity theft

In financial identity theft, **someone uses another person's identity or information to obtain credit, goods, services, or benefits**. This is the most common form of identity theft.

Social Security identity theft

If identity thieves obtain your Social Security number, they can use it to apply for credit cards and loans and then not pay outstanding balances. Fraudsters can also use your number to receive medical, disability, and other benefits.

Medical identity theft

In medical identity theft, someone poses as another person to obtain free medical care.

Synthetic identity theft

Synthetic identity theft is a type of fraud in which **a criminal combines real (usually stolen) and fake information to create a new identity, which is used to open fraudulent accounts and make fraudulent purchases**. Synthetic identity theft allows the criminal to steal money from any credit card companies or lenders who extend credit based on the fake identity.

Child identity theft

In child identity theft, someone uses a child's identity for various forms of personal gain. This is common, as children typically do not have information associated with them that could pose obstacles for the perpetrator. The fraudster may use the child's name and Social Security number to obtain a residence, find employment, obtain loans, or avoid arrest on outstanding warrants. **Often, the victim is a family member, the child of a friend, or someone else close to the perpetrator.** Some people even steal the personal information of deceased loved ones.

Tax identity theft

Tax identity theft occurs when someone uses your personal information, including your Social Security number, to **file a bogus state or federal tax return in your name and collect a refund**.

Criminal identity theft

In criminal identity theft, **a criminal poses as another person during an arrest** to try to avoid a summons, prevent the discovery of a warrant issued in their real name, or avoid an arrest or conviction record.

Unemployment identity theft

Someone uses your personal information to claim (and receive) unemployment benefits.

- **Online sexual harassment**

Online sexual harassment is defined as **unwanted sexual conduct on any digital platform and it is recognised as a form of sexual violence**. Online sexual harassment encompasses a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public). It can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against.

Types of online sexual harassment

Non Consensual sharing of intimate images and videos

A person's sexual images and videos being shared without their consent or taken without their consent. This includes a range of behaviours, such as:

- Sexual images/videos taken without consent ('creep shots' or 'upskirting')
- Sexual images/videos taken consensually but shared without consent ('revenge porn')
- Non-consensual sexual acts (e.g., rape) recorded digitally (and potentially shared)

Exploitation, coercion and threats

A person receiving sexual threats, being coerced to participate in sexual behaviour online, or blackmailed with sexual content. This includes a range of behaviours, such as:

- Harassing or pressuring someone online to share sexual images of themselves or engage in sexual behaviour online (or offline).
- Using the threat of publishing sexual content (images, videos, rumours) to threaten, coerce or blackmail someone ('sextortion').
- Online threats of a sexual nature (e.g., rape threats).
- Inciting others online to commit sexual violence.
- Inciting someone to participate in sexual behaviour and then sharing evidence of it.

Sexualised bullying

A person being targeted by, and systematically excluded from, a group or community with the use of sexual content that humiliates, upsets or discriminates against them. This includes a range of behaviours, such as:

- Gossip, rumours or lies about sexual behaviour posted online either naming someone directly or indirectly alluding to someone.
- Offensive or discriminatory sexual language and name calling online
- Impersonating someone and damaging their reputation by sharing sexual content or sexually harassing others
- Personal information shared non-consensually online to encourage sexual harassment (‘doxing’)
- Being bullied because of actual or perceived gender and/or sexual orientation
- Body shaming
- ‘Outing’ someone where their individual’s sexuality or gender identity is publicly announced online without their consent

Unwanted sexualisation

A person receiving unwelcome sexual requests, comments and content. This includes a range of behaviours, such as:

- Sexualised comments (e.g., on photos)
- Sexualised viral campaigns that pressurise people to participate
- Sending someone sexual content (images, emojis, messages) without them consenting
- Unwelcome sexual advances or requests for sexual favours
- ‘Jokes’ of a sexual nature
- Rating peers on attractiveness/sexual activity
- Altering images of a person to make them sexual

Sexual harassment of this kind can make a person feel any of the following:

- Threatened or scared
- Exploited
- Coerced
- That their dignity is violated
- Humiliated or degraded
- Shamed or judged
- Upset
- Sexualised
- Discriminated against because of their gender or sexual orientation
- Feel guilty or that they are to blame

The experience and impact of online sexual harassment is unique to the individual and can be felt both in the short-term but also can have long-term impacts on mental health and wellbeing. Long-term impacts can be amplified because of re-victimisation if content is re-shared online, or because the initial trauma of the incident resurfaces much later. It is important to recognise that there is no single way that a young person may experience online sexual harassment and that it might also affect others who witness it.

- **Phishing**

Phishing attacks are **the practice of sending fraudulent communications that appear to come from a reputable source**. It is usually performed through email.

The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is a common type of cyber attack that everyone should learn about in order to protect themselves.

Sometimes hackers are satisfied with getting your personal data and credit card information for financial gain. In other cases, phishing emails are sent to gather employee login information or other details for use in more malicious attacks against a few individuals or a specific company.

Phishing starts with a fraudulent email or other communication designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he/she/them is/are coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.

Cybercriminals start by identifying a group of individuals they want to target. Then **they create email and text messages that appear to be legitimate but actually contain dangerous links, attachments, or lures that trick their targets into taking an unknown**, risky action.

Phishing risks include:

- Money being stolen from your bank account
- Fraudulent charges on credit cards
- Lost access to photos, videos, and files
- Fake social media posts made in your accounts
- Cybercriminals impersonating you to a friend or family member, putting them at risk

In brief:

- **Phishers frequently use emotions like fear, curiosity, urgency, and greed to compel recipients to open attachments or click on links**.
- **Phishing attacks are designed to appear to come from legitimate companies and individuals**.
- Cybercriminals are continuously innovating and becoming more and more sophisticated.
- It only takes one successful phishing attack to compromise your network and steal your data, which is why it is **always important to “think before you click”**.

In order to avoid phishing, CISCO (https://www.netacad.com/) gives the following tips:

1. **Avoid unknown senders**. Check names and email addresses before responding.
2. Don’t trust links or attachments in **unsolicited emails**.
3. **Be suspicious of emails marked “urgent”**.
4. Beware of messages with **mistakes in spelling or grammar**.
5. **Don't be lured by “deals”**. They are usually too good to be true.
6. **Consider using a secure email provider**.
7. **Never give out personal or financial information** based on an email request.
8. When receiving email from known institutions (government, banks, your doctor), **go directly to the source instead of clicking on links in the email**.
9. **Be wary of generic greetings, such as “Dear sir or madam”**.
10. Understand your **service provider’s policy for tracking and stopping phishing**.
11. Don’t give a stranger or unsolicited help access to your computer.

- <u>Internet fraud and scams</u>

Internet fraud involves using **online services and software with access to the internet to defraud or take advantage of victims**. The term "internet fraud" generally covers cybercrime activity that takes place over the internet or on email, including crimes like identity theft, phishing, and other hacking activities designed to scam people out of money.

Internet scams that target victims through online services account for millions of dollars worth of fraudulent activity every year, and the figures continue to increase as internet usage expands and cyber-criminal techniques become more sophisticated.

Cyber criminals use a variety of attack vectors and strategies to commit internet fraud. This includes **malicious software**, **email** and **instant messaging services to spread malware**, **spoofed websites that steal user data**, and **elaborate, wide-reaching phishing scams**.

Internet fraud can be broken down into several key types of attacks, including:

Phishing (explained in details above): The use of email and online messaging services to dupe victims into sharing personal data, login credentials, and financial details.

Data breach: Stealing confidential, protected, or sensitive data from a secure location and moving it into an untrusted environment. This includes data being stolen from users and organizations.

Denial of service (DoS): Interrupting access of traffic to an online service, system, or network to cause malicious intent.

Malware: The use of malicious software to damage or disable users' devices or steal personal and sensitive data.

Ransomware: A type of malware that prevents users from accessing critical data then demanding payment in the promise of restoring access. Ransomware is typically delivered via phishing attacks.

Business email compromise (BEC): A sophisticated form of attack targeting businesses that frequently make wire payments. It compromises legitimate email accounts through social engineering techniques to submit unauthorized payments.

Some examples include:

- **Greeting Card Scams**

Many internet fraud attacks focus on popular events to scam the people that celebrate them. This includes birthdays, Christmas, and Easter, which are commonly marked by sharing greeting cards with friends and family members via email. Hackers typically exploit this by installing malicious software within an email greeting card, which downloads and installs onto the recipient's device when they open the greeting card.

- **Credit Card Scams**

Credit card fraud typically occurs when hackers fraudulently acquire people's credit or debit card details in an attempt to steal money or make purchases. To obtain these details, internet fraudsters often use too-good-to-be-true credit card or bank loan deals to lure victims. For example, a victim might receive a message from their bank telling them they are eligible for a special loan deal or a vast amount of money has been made available to them as a loan. These scams continue to trick people despite widespread awareness that such offers are too good to be true for a reason.

- **Online Dating Scams**

Another typical example of internet fraud targets the plethora of online dating applications and websites. Hackers focus on these apps to lure victims into sending money and sharing personal data with new love interests. Scammers typically create fake profiles to interact with users, develop a relationship, slowly build their trust, create a phony story, and ask the user for financial help.

- **Lottery Fee Fraud**

Another common form of internet fraud is email scams that tell victims they have won the lottery. These scams will inform recipients that they can only claim their prize after they have paid a small fee. Lottery fee fraudsters typically craft emails to look and sound believable, which still results in many people falling for the scam. The scam targets people's dreams of winning massive amounts of money, even though they may have never purchased a lottery ticket. Furthermore, no legitimate lottery scheme will ask winners to pay to claim their prize.

- **The Nigerian Prince**

A classic internet fraud tactic, the Nigerian Prince scam approach remains common and thriving despite widespread awareness. The scam uses the premise of a wealthy Nigerian family or individual who wants to share their wealth in return for assistance in accessing their inheritance.

It uses phishing tactics to send emails that outline an emotional backstory, then lures victims into a promise of significant financial reward. The scam typically begins by asking for a small fee to help with legal processes and paperwork with the promise of a large sum of money further down the line.

The scammer will inevitably ask for more extensive fees to cover further administration tasks and transaction costs supported by legitimate-looking confirmation documents. However, the promised return on investment never arrives.

Tips for avoiding internet frauds and scams:

It is vital to never send money to someone you met over the internet, never share personal or financial details with individuals who are not legitimate or trustworthy, and never click on hyperlinks or attachments in emails or instant messages. Once targeted, internet users should report online scammer activity and phishing emails to the authorities.

Credit card fraud can also be avoided by keeping a close eye on bank accounts, setting up notifications on credit card activity, signing up for credit monitoring, and using consumer protection services. If users suffer credit card fraud, they must report it to the relevant legal authorities and credit bureaus.

Spam

Spam is any kind of **unwanted, unsolicited digital communication that gets sent out in bulk**. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

Spam is not an acronym for a computer threat, although some have been proposed (stupid pointless annoying malware, for instance). The inspiration for using the term “spam” to describe mass unwanted messages is a Monty Python skit in which the actors declare that everyone must eat the food Spam, whether they want it or not. Similarly, everyone with an email address must unfortunately be bothered by spam messages, whether we like it or not.

Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch many of these types of messages, and phone carriers often warn you of a “spam risk” from unknown callers. Whether via email, text, phone, or social media, some spam messages do get through, and you want to be able to recognize them and avoid these threats. Below are several types of spam to look out for:

- Phishing emails (already described above)
- **Email spoofing**. Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple.
- **Tech support scams**. In a tech support scam, the spam message indicates that you have a technical problem and you should contact tech support by calling the phone number or clicking a link in the message.
- **Malspam**. Short for "malware spam" or "malicious spam," malspam is a spam message that delivers malware to your device. Unsuspecting readers who click on a link or open an email attachment end up with some type of malware including ransomware, Trojans, bots, info-stealers, cryptominers, spyware, and keyloggers. A common delivery method is to include malicious scripts in an attachment of a familiar type like a Word document, PDF file, or PowerPoint presentation. Once the attachment is opened, the scripts run and retrieve the malware payload.
- **Spam calls and spam texts**. Have you ever received a robocall? That's called spam. A text message from an unknown sender urging you to click an unknown link? That's referred to as text message spam or "smishing," a combination of SMS and phishing. If you're receiving spam calls and texts on your Android or iPhone, most major carriers give you an option to report spam. Blocking numbers is another way to combat mobile spam.

Cyber hacking

Anyone who uses a computer connected to the Internet is susceptible to the threats that computer hackers and online predators pose. These online villains typically use phishing scams, spam email or instant messages and bogus websites to deliver dangerous malware to your computer and compromise your computer security.

Computer hackers can also try to access your computer and private information directly if you are not protected by a firewall. They can monitor your conversations or peruse the back-end of your personal website. Usually disguised with a bogus identity, predators can lure you into revealing sensitive personal and financial information, or much worse.

While your computer is connected to the Internet, the malware a hacker has installed on your PC quietly transmits your personal and financial information without your knowledge or consent. Or, a computer predator may pounce on the private information you unwittingly revealed. In either case, they will be able to:

- Hijack your usernames and passwords
- Steal your money and open credit cards and bank accounts in your name
- Ruin your credit
- Request new account Personal Identification Numbers (PINs) or additional credit cards
- Make purchases
- Add themselves or an alias that they control as an authorized user so it’s easier to use your credit
- Obtain cash advances
- Use and abuse your Social Security number
- Sell your information to other parties who will use it for illicit or illegal purposes

In order to protect yourself from these threats, you can do the following:

1. Continually **check the accuracy of personal accounts and deal with any discrepancies right away**.
2. Use **extreme caution** when entering chat rooms or posting personal web pages.
3. **Limit the personal information** you post on personal web pages.

4. Carefully monitor requests by online "friends" or acquaintances for predatory behavior.
5. **Keep personal and financial information out of online conversations**.
6. Use **extreme caution when agreeing to meet an online "friend"** or acquaintance in person.

7. **Use a 2-way firewall.**
8. **Update your operating system regularly.**
9. **Increase your browser security settings.**
10. **Avoid questionable Websites**
11. Only **download software from sites you trust**. Carefully evaluate free software and file-sharing applications before downloading them.
12. **Don't open messages from unknown senders**.
13. Immediately **delete messages you suspect to be spam**.
14. Make sure that you have the **best security software products installed on your PC**: Use antivirus protection and get anti spyware software protection.

Cyber stalking

Cyberstalking refers to **the use of the internet and other technologies to harass or stalk another person online**.

This online harassment, which is an extension of cyberbullying and in-person stalking, can take the form of emails, text messages, social media posts, and more and is often methodical, deliberate, and persistent. Most of the time, the interactions do not end even if the recipient expresses their displeasure or asks the person to stop. **The content directed at the target is often inappropriate and sometimes even disturbing, which can leave the person feeling fearful, distressed, anxious, and worried**.

When it comes to cyberstalking, those who engage in this behavior use a variety of tactics and techniques to harass, humiliate, intimidate, and control their targets. In fact, many of those who engage in cyberstalking are technologically savvy as well as creative and come up with a multitude of ways to torment and harass their targets. Here are some examples of things people who cyberstalk might do:

- **Post rude, offensive, or suggestive comments online**.
- **Follow the target online** by joining the same groups and forums.
- Send **threatening, controlling, or lewd messages** or emails to the target.
- Use technology to threaten or blackmail the target.
- **Tag the target in posts excessively**, even if they have nothing to do with them.

- Comment on or like everything the target posts online.
- **Create fake accounts to follow the target on social media**.
- Message the target repeatedly.
- **Hack into or hijack the target's online accounts**.
- Attempt to extort sex or explicit photos.
- Send unwanted gifts or items to the target.
- **Release confidential information online**.
- Post or distribute real or fake photos of the target.
- **Bombard the target with sexually explicit photos of themselves**.
- Create fake posts designed to shame the victim.
- Track the target's online movements by installing tracking devices.
- **Hack into the target's camera on their laptop or smartphone as a way to secretly record them**.
- Continue the harassing behavior even after being asked to stop.

Just like stalking, cyberstalking has the potential to cause a wide range of physical and emotional consequences for those who are targeted. For instance, it's not uncommon for those who are being harassed online to experience anger, fear, and confusion. They also might have trouble sleeping and even complain of stomach trouble.

The ways of preventing cyberstalking are very similar to the ones recommended for preventing other cyber threats, as all of them are connected and function in a similar way. Some of the tips include:

- **Create strong passwords**. Make sure you have strong passwords for all your online accounts as well as strong passwords for your devices. Then, set a reminder on your phone to regularly change your passwords. **Choose passwords that would be difficult to guess but are easy for you to remember**.

- **Be sure to log out every time**. It may seem like a pain, but make sure you log out of email, social media accounts, and other online accounts after using them. This way, if someone were able to get into your device they would not have easy access to your accounts.

- **Keep track of your devices**. **Don't leave your phone sitting on your desk at work or walk away from an open laptop**. It only takes a minute or two for someone to install a tracking device or hack your device. So, make sure you keep these things in your possession or that you secure them in some way.
- **Use caution on public wifi**. Recognize the fact that if you use public wifi at hotels or at the local coffee shop, you are putting yourself at risk for hacking. Try to refrain from using public wifi or invest in VPN.
- **Practice online safety habits**. In other words, make it a priority to only accept friend requests from people you know and keep your posts private. You also should consider having one email address that is specifically for your online activity. Use this email when you do your online shopping or join loyalty programs.
- **Take advantage of security settings**. Go through each of your online accounts—especially your social media accounts—and ensure that you are using the strongest privacy settings as possible. You can even establish settings where people cannot tag you or post pictures of you without your approval first.
- **Create generic screen names**. Rather than using your full name online, consider developing a gender-neutral screen name or pseudonym. By doing so, you are making it harder for people to find you online. You also should leave the optional sections, like your date of birth or your hometown, blank.
- **Keep locations secure**. Consider disabling the geolocation settings in photos. You also should refrain from posting your location in real time and instead post photos showing where you have been after the fact.
- **Be careful with online dating sites.** Refrain from using your full name on online dating sites. You also should avoid giving out personal information like your last name, address, email, and telephone number until you have met in person and established a level of trust.
- **Perform a social media audit**. It's always a good idea to go through your social media accounts and remove photos or posts that provide too much information about you

or that create an image you don't want out there. Keep in mind, too, that even if you have blocked someone on social media, they may be able to still see your account by using another person's account or by creating a fake profile.

The ways to cope with cyberstalking, in case it is already happening, include:

- **Tell the person to stop**. Respond only once to the person cyberstalking you and tell them to stop contacting you. You don't need to say anything specific or explain your answer, just ask them to never contact you again.
- **Block the person**. Make sure you block the person cyberstalking you from all your accounts. You should block them on social media and on your smartphone.
- **Refuse to respond to any contact**. If the person cyberstalking continues to find ways to contact you, do not respond to anything they post or send you.
- **Change email address and screen names.** Consider getting a new email address and changing your online screen names to make it harder for the person cyberstalking you to reach you.

If you have asked the person cyberstalking you to stop and their behavior continues, it's important to take action against them. This includes contacting the appropriate authorities and collecting evidence of their actions. You also may want to consider talking with an attorney. **Here are the key points that will need to be addressed when taking action**. Your local law enforcement can let you know if there is anything else you can do in order to stay safe.

- **Save evidence of everything**. Even though you may feel like destroying everything, it's important to keep copies of everything the person cyberstalking you has sent. Make a copy for yourself and a copy for law enforcement.
- **Notify your local police**. It's important to notify the police and file an official complaint if you're being cyberstalked. Even if they cannot do anything right away, having an official complaint on file is important if the behavior persists or escalates.
- **Report them to the site or service they used**. If the person cyberstalking you harassed you through Facebook, Instagram, Twitter, Snapchat, YouTube, Gmail, or

some other method, let the appropriate authorities know what you're experiencing. Many times, these organizations take complaints of cyberstalking seriously and will address the matter.

3.3. How to report cybersecurity threats on social media/institutions

All social networks have established mechanisms for reporting different types of cybersecurity threats, including online hate speech, identity theft, sexual harassment, cyberbullying, etc. Below you can find information about some of the most popular social networks:

- **Facebook**

Facebook security issues have multiple categories. There may be an abusive content or hate page you want to report or maybe someone is impersonating you on Facebook, etc. The best way to report abusive content or spam on Facebook is by using the Report link near the content itself.

To report a profile:

1. Go to the profile that you want to report by clicking its name in your Feed or searching for it.
2. Click "…" to the right and select Find support or report profile.
3. To give feedback, click the option that best describes how this profile goes against their Community Standards, then click Next.
4. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn't ask you to submit a report, but it uses your feedback to help their systems learn. Click Done.

To report a post:

1. Go to the post that you want to report.
2. Click "…" in the top right of the post.
3. Click Find support or Report post.

4. To give feedback, click the option that best describes how this post goes against Facebook’s Community Standards. Click Next.
5. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn’t ask you to submit a report, but they use your feedback to help their systems learn. Click Done.

To report a photo or video:

1. Click on the photo or video to expand it. If the profile is locked and you can't view the full-sized photo, click Find support or Report photo.
2. Click “…” to the right of the photo or video.
3. Click Find Support or Report Photo for photos or Report Video for videos.
4. Select the option that best describes the issue and follow the on-screen instructions.

To report a message that goes against Facebook’s Community Standards:

1. From any page on Facebook, click the Messenger icon in the top right.
2. Open the message.
3. If you opened the message as a pop-up window, click the setting icon.
4. Click Something's wrong.
5. To give feedback, click the option that best describes how this message goes against Facebook’s Community Standards.
6. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn’t ask you to submit a report, but they use your feedback to help their systems learn.

To report a page:

1. Go to the Page you want to report by clicking its name in your Feed or searching for it.
2. Click more below the Page's cover photo.
3. Select Find support or Report page.
4. To give feedback, click the option that best describes how this Page goes against Facebook’s Community Standards.

5. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn’t ask you to submit a report, but they use your feedback to help their systems learn.

To report a group:

1. Go to the group that you want to report by clicking its name in your Feed or searching for it.
2. Click more below the group's cover photo.
3. Select Report group.

To report an event:

1. From your Feed, click Events in the left menu.
2. Go to the event that you want to report.
3. Click “…” and select ‘Report event’.
4. To give feedback, click the option that best describes how this profile goes against Facebook’s Community Standards.
5. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn’t ask you to submit a report, but they use your feedback to help their systems learn.

To report a comment:

1. Go to the comment you want to report.
2. Click “…” next to the comment.
3. Click Give feedback or Report this comment.
4. To give feedback, click the option that best describes how this comment goes against Facebook’s Community Standards. If you can't see any options that fit, click Something else to search for more.
5. Depending on your feedback, you may then be able to submit a report to Meta. For some types of content, Facebook doesn’t ask you to submit a report, but they use your feedback to help their systems learn.

To report an ad on Facebook:

1. Go to the ad you want to report by clicking its name in your Feed or searching for it.
2. Click "…" next to the ad that you want to report
3. Click Report ad and then follow the on-screen instructions.

- **Instagram**

Report posts

If you see a post, message or account you think goes against Instagram's Community Guidelines, you can report it. You can report individual pieces of content by tapping the three dots above a post, holding on to a message, or by visiting an account and reporting directly from the profile. For more information, visit Instagram's Help Center https://help.instagram.com/

Report accounts

Accounts in violation of Instagram's Community Guidelines can be reported in-app or via a web form. For more information you can refer to the Help Center.

Report comments

1. If you see a comment that's spam or intended to bully or harass you or someone else, report it.
2. Open the conversation in the Instagram app.
3. Tap and hold the individual message you'd like to report.
4. Tap Report.
5. Select a reason for why you're reporting the message and then tap Submit Report.
6. For more information, visit the Help Center.

Report messages

If you receive a message that feels inappropriate, tap and hold the individual message to report it. For more information, visit the Help Center.

Report stories

1. If you see someone's story and think it goes against Instagram's Community Guidelines, you can report it.
2. Open the story.
3. Tap the 3 dots at the bottom of the photo or video you'd like to report.
4. Tap Report, then follow the on-screen instructions.
5. For more information, visit the Help Center.

- **TikTok**

For questions, concerns, or issues with your profile, you can find information and support in the TikTok Help Center (https://support.tiktok.com/en/). In the 'Safety' section, you can go to 'Report a problem' and report a LIVE video, a LIVE comment, a video, a comment, a direct message, a sound, a hashtag, and you can also report someone. The steps are very easy to follow, you just need to find the option Report and follow the instructions.

For questions, concerns, or issues with TikTok's privacy policy or fraud, you can find support in this link https://privacytiktok.zendesk.com/hc/en-us/requests/new . You will be redirected to an online form where you can request information about your data, report a privacy violation or ask about a particular privacy issue.

- **Twitter**

In the Help Center of Twitter (https://help.twitter.com/en/safety-and-security) you can find information and support in case of compromised and hacked accounts, about privacy, spam and fake accounts, sensitive and offensive content, abusive behavior and its reporting.

To report a Tweet:

1. Navigate to the Tweet you'd like to report on twitter.com or from the Twitter for iOS or Twitter for Android app.
2. Select the "…" icon.
3. Select Report.
4. Select who the report is for: Myself, Someone else or a specific group of people, or Everyone on Twitter.

5. Next, Twitter will ask you to provide more information about the issue you're reporting. Twitter may also ask you to select additional Tweets from the account you're reporting so they have better context to evaluate your report.
6. Twitter will then make sure they have your information correct by confirming what you're reporting as well as additional context you've shared, and what rule it may have violated.

7. Twitter will include the text of the Tweets you reported in follow-up emails and notifications to you. To opt-out of receiving this information, you can uncheck the box next to Updates about this report that can show these Tweets.
8. Once you've submitted your report, Twitter will provide recommendations for additional actions you can take to improve your Twitter experience.

To report an account:

1. Go to the account profile and select the "…" icon.
2. Select Report.
3. Select who the report is for: Myself, Someone else or a specific group of people, or Everyone on Twitter.
4. Next, Twitter will ask you to provide additional information about the issue you're reporting. They may also ask you to select Tweets from that account so they have better context to evaluate your report.
5. Twitter will then make sure they have your information correct by confirming what you're reporting as well as additional context you've shared, and what rule it may have violated.
6. Twitter will include the text of the Tweets you reported in follow-up emails and notifications to you. To opt-out of receiving this information, you can uncheck the box next to Updates about this report that can show these Tweets.
7. Once you've submitted your report, Twitter will provide recommendations for additional actions you can take to improve your Twitter experience.

To report an individual message or conversation:

1. Select the Direct Message conversation and find the message you'd like to report. (To report the entire conversation, click the "…" icon).
2. Select the information "i" icon and select Report @username.
3. If you select It's abusive or harmful, Twitter will ask you to provide additional information about the issue you're reporting. They may also ask you to select additional messages from the account you're reporting so they have better context to evaluate your report.
4. Once you've submitted your report, Twitter will provide recommendations for additional actions you can take to improve your Twitter experience.

- **When is it considered a crime?**

Spain

In Spain **the consequences of cybersecurity crimes go from five years in prison to fines up to 2.700 €**.

Stalking becomes a crime when someone is repetitively restricting one's feeling of safety and when they make the victim feel humiliated, insulted, threatened. Unsurprisingly, anyone practicing this has to face several consequences that go from three months to two years of imprisonment or the payment of a fine to the victim a daily amount of money that judges decide. A daily fine of 15 € during six months amounts to a total of 2.700 €.

The **disclosure of secrets** also has consequences in Spain since it is a serious crime. Any person who "*without the authorisation of the person concerned, disseminates, discloses or transfers to third parties audiovisual images or recordings*" can face imprisonment or the payment of fines as well. The **dissemination of sexual images** is even more serious and can have further consequences.

Moreover, it is necessary to talk about **identity theft**. It is the appropriation of a person's identity. In other words, impersonating that person, assuming their identity to others. An example could be the creation of an account on a social network trying to impersonate another person in order to collect information or for any other purpose. It is punishable by imprisonment of six months to three years.

These cybersecurity threats need stopping. Therefore, in Spain there is one way of taking it to a legal level. First of all, **any victim who wants to take action must firstly collect proof of what is happening** and then **report it at the police station as soon as possible**. After doing it they will contact you after having checked it and they will assess the situation. If they find it convenient, the report will start a new process and legal actions will be taken.

Belgium

Cyber security is the result of a set of security measures that minimize the risk of disruption or unauthorized access to information and communication (ICT) systems. It includes all reasonable and acceptable measures to protect the ICT of citizens, businesses, organizations and government from cyber threats. Cyber security involves protecting systems (such as hardware, software and related infrastructure) and networks, as well as the data they contain.

The Belgian National Risk Assessment 2018-2023 of the National Crisis Centre considers cyber security as one of the main risks that Belgium will face in the coming years. Inside this cluster, **cybercrime** and **hacktivism** are identified as national priority risks.

This definition is taken from the "Center for Cyber Security in Belgium[27], the national authority for cybersecurity in Belgium which also specifies the 4 main threats to which Cyber security aims to respond: foreign military and intelligence services, terrorism, hacktivism and cybercrime. In this report, the cybersecurity that we will be focusing on will be mainly related to hacktivism and cybercrime because of their most commonly used attack methods, social media, and due to the direct impact they have to the overall security of every citizen, including young people.

In July 2016, the Security of Network and Information Systems Directive (NIS Directive) (https://www.itgovernance.eu/nl-be/nis-directive-be) was adopted, which was transposed into Belgium law on 7 April 2019: Act establishing a framework for the security of network and information systems of public interest for public safety. Article 7 of this directive

[27] Center for Cyber Security Belgium (2022, May).Cybersecurity Strategy Belgium 2.0 2021-2025. Available: https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

(reproduced in article 10 of the Belgian NIS Act) requires member states to draw up a national strategy for the security of network and information systems. Until the publication of the Belgian Network and Information Systems (NIS) Law in May 2019, the country didn't have a complete legislation on cyber security.

This great step was achieved thanks to the European Union Agency for Cybersecurity (ENISA) that contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Apart from that, we could highlight the following legislation that will be used depending on the cybercrime is pursued:

- Belgian Criminal Code: art. 550 (b) "Hacking", art. 210bis "IT fraud.
- Act of 1 July 2011 on the security and protection of critical infrastructures.
- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- Act of 7 April 2019 establishing a framework for the security network and information systems of general interest for public security.
- Royal Decree of 12 July 2019, implementing the law of 7 April 2019, establishing the framework for the security network and information systems of general interest for public security.
- Regulation (EU) 2019/881 OF 17 April 2019 on ENISA.
- Commission Implementing Regulation (EU)2018/151 of 30 January 2018 laying down rules for the application of Directive EU 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing security risks.

The Netherlands

In 2021, nearly 2.5 million people in the Netherlands aged 15 or over reported that they had fallen victim to cybercrime; this accounts to nearly 17% of the population.

The Dutch parliament has enacted legislation on cybercrime which prevents the following:

- Article 138a: Any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system.
- Article 138b: the unlawful serious hindering of data processing.
- Article 232: forgery of any electronic token that has evidentiary value and the usage of such tokens as if they were genuine.

Cybercrime is defined as '*crime involving digital forms of identity fraud, fraud when buying or selling online, hacking and cyber bullying (slander, stalking, blackmail and threats of violence committed online).*'[28]

Cybercrimes relating to individual, organisational and governmental privacy are criminalised under Dutch law (in accordance with the articles above). Common cybercrimes reported in the Netherlands are **Hacking**, **Online shopping fraud** and **Cyber bullying**[29]. Common cybercrimes, as identified by the Dutch Government, are as follows[30]:

- Phishing: using fake email messages to get personal information from internet users.
- Misusing personal information (identity theft).
- Hacking: shutting down or misusing websites or computer networks.
- Spreading hate and inciting terrorism.
- Distributing child pornography.
- Grooming: making sexual advances to minors.

The National Cyber Security (NCSC) (https://english.ncsc.nl/) is responsible for overseeing digital security in the Netherlands[31]. It does so by: Continuously monitoring all suspect sources on the internet, advising organisations on how to protect themselves from online threats and monitoring developments in digital technology and updating security systems.

Bulgaria

[28] The Netherlands in Numbers : https://longreads.cbs.nl/the-netherlands-in-numbers-2020/what-about-cyber-crime/#:~:text=Hacking%2C%20online%20shopping%20fraud%20and%20cyber%20bullying&text=Hacking%20was%20most%20common%2C%20mentioned,such%20as%20stalking%20or%20threats.

[29] Ibid

[30] Forms of Cybercrime: https://www.government.nl/topics/cybercrime/forms-of-cybercrime

[31] Fighting Cybercrime in the Netherlands: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands

"Cybercrime" (also called "computer-related crime" or "high-tech crime") should be understood as "*criminal acts committed through the use of electronic communication networks and information systems, or against such networks and systems*".

In fact, the term refers to three categories of criminal acts. The first covers traditional types of crime such as fraud or counterfeiting, although in the context of cybercrime this category refers in particular to crimes committed through electronic communication networks and information systems ("electronic networks"). The second concerns the publication in electronic media of illegal content (such as child pornography or content inciting violence and connected to hate speech and discrimination). The third includes crimes specific to electronic networks, such as attacks against information systems, denial of service and hacking.

Bulgaria has ratified the Convention on Cybercrime adopted by the Council of Europe in 2001, and its protocols. Based on this, the Criminal Code of Bulgaria includes definitions and sanctions related to cybercrimes. The Criminal Code outlines different types of cybercrimes:

- Cyber fraud is defined under Art. 212a
- A special form of destruction and damage using digital tools is defined under Art. 216, para. 2
- A specific manner of violation of the secrecy of the correspondence is defined under Art. 171.
- Child pornography is also specifically criminalized.
- The cyber crimes outlined in Chapter 9 of the Criminal Code (Art. 319a to Art. 319f of the Criminal Code). They affect the public relationships that ensure the proper functioning of computers, computer systems, computer resources and computer networks, as well as the lawful creation and use of information. These include unauthorized access, alteration, damage, destruction of data or programs, the introduction of a virus or the spread of passwords.
- The first concerns the copying or use of computer data without permission through getting unauthorized access to computer resources (Article 319a).
- The next type of computer crime is counterfeiting or destruction of a computer program or data (Article 319b). This includes the adding, modifying or deleting a

computer program or computer data, making them inauthentic or inconsistent with the original programs and data.

- The introduction of a computer virus into a computer or information network is referred to in Art. 319d, para 1 of the Criminal Code.
- Article 319e, para 1 of the Criminal Code, includes the distribution of computer or system passwords, when this leads to disclosing personal data or personal secret. The penalty is up to one year in prison.

In terms of online privacy and security, it is important to mention that the Bulgarian regulations are related to the GDPR, which is regulated by the Commission for Personal Data Protection (https://www.cpdp.bg/). It is an independent state body that protects individuals in the processing of their personal data and in accessing such data, as well as control over compliance with the Personal Data Protection Act. It is an independent, collegial body and consists of a chairman and four members. The members of the commission and its chairman are elected by the National Assembly on the proposal of the Council of Ministers for a term of 5 years and may be re-elected for another term. One of the most important roles of the Commission is to refer matters related to infringement of the GDPR to the Court of Justice in Bulgaria.

3.4. How to avoid security data risks

One of the most important things to do in order to keep our data protected is to have a strong password. It will be very useful since nowadays cybercriminals keep thinking of new and innovative ways to hack accounts and get ahold of personal data. Some potential consequences of weak passwords include data breaches, identity theft, computer hijacking, blackmail and loss of privacy.

Therefore, in order to prevent people from suffering these consequences, here are instructions on how to create a strong password that you can rely on.

- **Never use personal information**. It might seem obvious, but many people use their own personal information when creating their password. It is recommended not to use names, birthdays, addresses or phone numbers.

- **Include a combination of letters, numbers, and symbols**. The more random characters you use, the more complex your password will be.
- **Prioritize password length**. It will lessen the chances of falling victim to a cyberattack.
- **Never repeat passwords**. People are used to always choosing the same password. This is a huge mistake since it puts them at risk of credential stuffing attacks.
- **Avoid using real words**. Hackers use malicious programs that can process every word found in a dictionary to crack passwords. Therefore, using invented words can help to create a strong and secure password.

Additionally, in order to keep your information protected it is recommended to **use only websites you trust**. Many people do not know how to check if a website is safe or not, thus, some tips will be given:

1. First of all, **check if the URL has the correct spelling**, is secured with “https” and has some sort of indicator that it is verified, such as a lock sign.
2. Secondly, **websites that look unsafe usually are**. If the website owner is not investing in the appearance and user experience, they probably are not investing in the security of the site. Therefore, these sites are prone to malware, which could be threatening to your security.
3. Thirdly, **you must be able to check that there is contact information available as well as an accessible privacy policy**. These are usually found at the very bottom of the homepage. Another useful tip is to read some testimonies and reviews for the site from other people so you can get to know experiences that other people had using these websites.

There are also other practices that can put digital security at risk such as **using public WIFI**. It is true that this service that some hotels and airports provide is free, but it does have a price. These free WIFI hotspots allow hackers to position themselves between the person using it and the connection point, so instead of talking directly with the hotspot, people are sending their information to the hacker, who then relies on it. Hackers then have access to every piece of information people send out on the Internet: important emails, credit card information and security credentials. Once hackers have that information, they can access your systems as if they were you.

In order to prevent you from being hacked this way, it is recommended that you keep WIFI off when you do not need it and when you have to use these types of connections do it with a VPN. A VPN is a virtual private network since it will help your information to be strongly encrypted. If you really need to use this free WIFI, try not to do online banking, shopping or working. Something that can help is also turning off Bluetooth and file-sharing.

How can individuals protect their personal data?

1. Secure your accounts

In the past decade, data breaches and password leaks have struck big companies such as Facebook, Home Depot, Marriott, Yahoo, etc., and governmental institutions have also suffered from cyberattacks through which third unauthorized parties have obtained access to citizens' personal information (e.g. the attack on the Bulgarian National Revenue Agency in 2019).

If you have online accounts, it is possible that hackers have leaked data from at least one of them. In order to check that, you can search for your email address on **Have I Been Pwned?** (https://haveibeenpwned.com/) to cross-reference your email address with hundreds of data breaches (*a "breach" is an incident where data is inadvertently exposed in a vulnerable system, usually due to insufficient access controls or security weaknesses in the software*).

There are other ways to identify possible indications that an account has been hacked, your identity stolen, or your data breached in some other way. Educate yourself on the warning signs of a potential breach and create positive habits for monitoring your personal data security to identify potential attacks or breaches before they escalate to devastation. Read up on data protection tips and on information outlining the common warning signs of a data breach or hack, such as this list of **"15 signs you've been hacked—and how to fight back"** (https://www.csoonline.com/article/3617849/15-signs-youve-been-hacked-and-how-to-fight-back.html).

If your account has been hacked, your data lost, or device stolen, consider it a learning opportunity. Find out exactly what went wrong and how you could have protected your data by taking better precautions. While you are fixing things, it’s a good time to take a step back, and ask yourself a more basic question: What was the reason for the breach? If it was your bank account, the answer may be obvious.

In other cases, such as e-mail, it can be for a host of reasons: from using it to send spam, to requesting money from your contacts, to getting password resets on other services. An attacker may even be trying to gain access to your business. Knowing why you were targeted can also sometimes help you understand how you were breached.

A way to increase the level of digital security and to protect our personal data is to **use a password manager** to generate and remember different, complex passwords for every account. This is one of the most important things people can do to protect their privacy and security today. **LastPass** /https://www.lastpass.com/) and **1password** (https://1password.com/) can help you to do so, generating passwords, monitoring accounts for security breaches, suggesting changing weak passwords, and syncing your passwords between your computer and phone. **Don't use Social Security numbers, phone numbers, addresses, or other personally identifiable information as passwords**.

Another suggestion is to also use two-step authentication whenever possible for your online accounts. Most banks and major social networks provide this option. As the name suggests, two-step authentication requires two steps: entering your password and entering a number only you can access. For example, step one is logging in to Facebook with your username and password. In step two, Facebook sends a temporary code to you in a text message or, even better, through an app like Google Authenticator, and you enter that code to log in.

2. Protect your web browsing

Companies and websites track everything we do online. Every ad, social network button, and website collects information about your location, browsing habits, and more. The data collected reveals more about you than you might expect. Even if you don't share your personal information publicly on social media, chances are good that the websites you visit regularly provide all the data advertisers need to pinpoint the type of person you are. This is part of how targeted ads remain one of the Internet's most unsettling innovations.

A browser extension like **uBlock Origin** (https://ublockorigin.com/) blocks ads and the data they collect. The uBlock Origin extension also prevents malware from running in your browser and gives you an easy way to turn the ad blocking off when you want to support sites you know are secure.

You can combine uBlock with **Privacy Badger** (https://privacybadger.org/), which blocks trackers, and ads will not appear everywhere. To slow down stalker ads even more, disable interest-based ads from Apple, Facebook, Google, and Twitter. A lot of websites offer means to opt out of data collection, but you need to do so manually. Doing this won't eliminate the problem completely, but it will significantly cut down the amount of data collected.

Installing the **HTTPS Everywhere** (https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp) extension also helps protect your personal information. It automatically directs you to the secure version of a site when the site supports that, making it difficult for an attacker, especially if you're on public Wi-Fi at a coffee shop, airport, or hotel, to digitally eavesdrop on what you're doing.

3. Use antivirus software on your computer

Viruses might not seem as common as they were a decade ago, but they still exist. Malicious software on your computer can wreak all kinds of havoc, from annoying pop-ups to convert bitcoin mining to scanning for personal information. If you're at risk for clicking perilous links, or if you share a computer with multiple people in a household, it's worthwhile to set up antivirus software, especially on Windows computers. If your computer runs Windows 10, you should use Microsoft's built-in software, **Windows Defender**. You can also have an extra layer of protection if you install an antivirus program.

4. Update your software and devices

Phone and computer operating systems, Web browsers, popular apps, and even smart-home devices receive frequent updates with new features and security improvements. These security updates are typically far better at thwarting hackers than antivirus software.

All three major operating systems can update automatically, but you should take a moment to double-check that you have automatic updates enabled for your OS of choice: Windows, macOS, or Chrome OS. Although it’s frustrating to turn your computer on and have to wait out an update that might break the software you use, the security benefits are worth the trouble. Your phone also has automatic-update options but sometimes you need to manually approve the installation of updates.

5. Don’t install software that you don’t know and trust fully

Every weird app you install on your phone and every browser extension or piece of software you download from a sketchy website represents another potential privacy and security hole. Countless mobile apps track your location everywhere you go and harvest your data without asking consent, even in children’s apps. stick to downloading programs and browser extensions directly from their makers and official app stores.

It is good to know which apps have access to your location, contacts, microphone, and other data. Disable permissions where they don’t make sense. For example, Google Maps needs your location to function, but your notes app doesn’t. In the future, think about app permissions as you install new software; if an app is free, it’s possibly collecting and selling your data.

6. Disable Bluetooth when not using it

Bluetooth technology has offered incredible conveniences to the mobile world, but it also opens the door for vulnerabilities. Most threats exploiting Bluetooth connectivity are dependent on the active Bluetooth connection, and while they aren't typically devastating or dangerous, they're certainly inconvenient and can be serious. Bluetooth attacks depend on exploiting the permission request/grant process that is the backbone of Bluetooth connectivity. Regardless of the security features on your device, the only way to completely prevent attackers from exploiting that permission request/grant process is to power off your device’s Bluetooth function when you’re not using it; not putting it into an invisible or undetectable mode, but completely turning it off.

7. **Be overly cautious when sharing personal information**

This tip applies to both the online and offline worlds: who is asking for your personal information, such as your Social Security number or credit card information? Why do they need it? How will they use it? What security measures do they have in place to ensure that your private information remains private? All these important questions must be clearly answered before you provide your personal data to anyone.

8. **Watch out for impersonators**

Related to the previous tip, there are many impostors who attempt to trick unsuspecting consumers into giving out their sensitive personal information by pretending to be the individual's bank, credit card company, or other entity. **This can happen by phone or online, via phishing emails or websites designed to mimic the authentic company's look and feel**.

Make sure you know who is getting your personal or financial information. Don’t give out personal information on the phone, through the mail or over the Internet unless you’ve initiated the contact or know who you’re dealing with. If a company that claims to have an account with you sends email asking for personal information, don’t click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

9. **Don't share too much information on social network platforms**

Social networking has become a way of life for many individuals, but sharing too much personal information on your social media profiles can be dangerous. For instance, many hackers have successfully guessed passwords through trial-and-error methods, using combinations of common information (such as children's names, addresses, and other details) easily found on users' social media profiles.

Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.

10. Customize your social network privacy settings

Social networks like Facebook enable users to customize their privacy settings. On Facebook, for instance, you can choose who is able to see the content you post and who is able to view information on your profile, such as your place of employment, birth date, and hometown.

Always choose the highest level of privacy possible to ensure that your personal data doesn't end up in the hands of someone with malicious intent. The content you post online will be around for a long time, but you can customize privacy settings on most social media sites. This will affect who can contact you and who can see the information you post.

Be choosy: while it's fun to share information, keep your online reputation in mind. And if you over-disclose information publicly, it could be used by identity thieves to hijack your identity.

11. Don't forget to sign out

Signing into online services is necessary when you need to access your personal accounts, but many users forget to sign out when they're finished using a service.

When accessing account-based websites via a public computer (or a shared device), be sure to logout of the service when a session is over. Just because a new website is accessed following a visit to a site you've logged into doesn't mean the next user can't hit the back button and access your logged in account. Some systems are set up to automatically save information, as well, so be sure to see if this feature can be disabled.

12. Don't open emails from people you don't know

If you receive an email from a source or individual you don't recognize, don't open it, and definitely avoid clicking any links or file attachments.

There is a golden rule to dealing with spam emails: if it looks like a spam message, it probably is; so delete it without clicking or downloading anything. Such messages may contain software that tells the sender you've opened the email, confirming you have an active account, which may lead to even more spam messages. Some malware programs can steal your email address and use it to resend spam messages under the guise of a legitimate address. For example, imposters could pose as someone you know, like a friend, relative, or colleague. If the message in question appears to come from someone you know, contact them outside of your email.

13. Don’t save passwords in your browser

The common practice of 'remembering passwords' in browsers is a dangerous practice. Indeed, should someone gain access to your computer or mobile device, they'd be able to easily access any accounts for which you've stored login credentials in your browser. While it may make logging in more convenient, it's a risky habit in terms of data protection. Keep an eye out for these pop-ups and be sure to deny them.

14. Don’t use social media credentials to register for or sign in on third-party sites

It seems like a convenient option: Simply register for a website or online service using your Facebook or LinkedIn account, and as long as you’re signed in to that social network, signing in to the third-party site is fast and easy. Doing so can jeopardize your privacy, however.

Although it is a convenient option, signing into another account with your Facebook username and password can mean giving the other site all the information Facebook has gathered about you. Worse, if someone hijacks your social login information, they can also gain access to these third-party accounts.

15. Choose a safe, reputable email provider

Be sure your email provider guarantees proper security. You need to make sure your email provider uses technology like **DMARC** to stop phishing and minimize risks. The good news is that Google does it, Yahoo does it, Microsoft supports it, AOL supports it, so if you're on one of those, you're on your way to minimizing privacy and security risks.

4. Non-formal Education

4. NON-FORMAL EDUCATION

In this section we will mention national contexts of non-formal ways of raising awareness on Cyberbullying and Hate speech.

● The Netherlands

There are other non-formal ways in which people have become more aware of issues relating to staying safe online. Cybersecurity is not just talked about in formal or specific education; through **news stories**, **influencers** online, **parents** and **teachers**, and victims speaking out, awareness is raised in different ways.

Cybersecurity and privacy

Tackling or regulating cybersecurity and privacy is often associated with official institutions and bodies or formal education. However, non-formal education regarding this also has an impact.

Chantal Stekelenburg (https://twitter.com/mifare_lady) is part of the **Women in Cybersecurity Community Association (WICCA)** (https://womenofwicca.nl/) and has gained a large online following. She has spoken out about cybersecurity and mainly focuses on encouraging women to become security enthusiasts and experts.

Cyberbullying

Influencers and other individuals who have spoken out about cyberbullying have had an important effect on how people view this issue and how educated people are regarding this. Many young people often feel ashamed to speak out in a formal or official way, through filing reports or alerting staff at school or within other institutions. Thus, non-formal approaches are useful as they allow people who have experienced cyberbullying to relate to others, feel less alone and more likely to speak out.

A news article in 2018 reported that a Dutch appeals court upheld a prison sentence for a man convicted of cyberbullying many young men and women, many from the Netherlands. He had pressured girls into performing sexual acts in front of webcams. This story gained lots of attention in the media and can be seen as a clear example of non-formal education regarding cyberbullying and cybercrime. Essentially, **the more attention that is drawn to cases such as this, the more awareness is raised and the better equipped people become to prevent and report such**.

Hate Speech

The importance of non-formal education extends to hate speech, as people speaking out against this is vital. There have been important campaigns based on this issue.

There is a national campaign in the Netherlands, as part of the wider **No Hate Speech Youth Campaign** (https://www.coe.int/en/web/no-hate-campaign) from the Council of Europe, which aims to mobilise young people to combat hate speech and promote human rights. This encourages people to report hate speech and directly tackle it. Online activists consequently have a platform and community where they can share ideas and unite against this issue, empowering people to denounce hate speech.

● Spain

When talking about non-formal education ways of raising awareness about cyberbullying and hate speech in Spain, it is impossible not to mention the important role of culture, influencers and big marketing campaigns.

Cyberbullying

Influencers are indeed a potential reference for people. With millions of followers, this new profession is able to reach a higher target through social media and online platforms. The methodology is simple and effective, while people are consuming social media during their free time, they are also receiving all this information transmitted by the influencers without making any extra effort.

In Spain there are many examples of influencers that have used their spotlight to raise awareness about cyberbullying. For instance, **Y luego ganas tú (Nube de Tinta)** is a book of short stories in which the authors (5 Spanish influencers) tell, through their own stories and fictions that draw on reality, the problem of bullying at school.

A problem that is getting out of hand as a society: one out of every two students in Spain claims to have suffered some kind of bullying or cyberbullying. These influencers are Javier Ruescas (@javier_ruescas), Manu Carbajo (@karbajo), Jedet Sánchez (@lajedet), María Herrejón (@hersimmar) y Andrea Compton (@andreacomptonn). They are popular in Spain for their fight for social rights and visibility.

Another example of an effort on fighting cyberbullying is the podcast called **Estirando el chicle** (https://www.youtube.com/c/Estirandoelchicle?app=desktop) driven by Carolina Iglesias y Victoria Martín. In this podcast, multiple famous people are interviewed bringing up topics like cyberharassment or LGBTIQA+ visibility. In fact, the podcast has gained a lot of recognition with prizes like the Ondas Award for the best podcast or digital broadcasting programme for being "*a groundbreaking programme in terms of language and approach that mixes humor, interviews and social content without prejudice*".

In addition, it would also be relevant to mention how the famous shampoo brand H&S has also contributed to the fight against bullying. In the campaign **'Stop bullying'** (https://www.hys.es/es-es/frena-el-bullying/) many spanish public figures, like Marta Pompo or Ibai, attempt to raise awareness by telling their own experiences with hate speech in social media. In addition, an educational microsite will be activated on the H&S website with advice for pupils, teachers and parents to get them to take an active role in bullying situations. As well as information pills to raise awareness among the different parties involved.

- **Belgium**

From Belgium, we would like to highlight a communication campaign against cyberbullying by young people and highlight one of its most important influencers:

‘WAT TEGEN WAT PESTEN’ Campaign

Youth Platform **WAT WAT** (https://www.watwat.be/) works together with influencers and young people to discuss bullying among youngsters through tips and experiences. With a Facebook messenger dilemma game, WAT WAT sparks the conversation about bullying (“*Bullying or being bullied, trolling or liking, bully or pimple head: the choice is yours*”).

They developed a campaign during the Flemish “Anti-Bullying Week” to make children and young people aware of what bullying is, what you can do about it and what consequences bullying has. True stories were publicly shared: Angel (16) was forced to eat GFT waste by her bullies. In the week against bullying she, together with Yasmien Naciri (27), Margot (22) and Jorrit (23), shared her story and showed her scars from years of bullying. These courageous stories encourage young people to think, to talk about it, and to help each other.

WAT WAT calls on everyone to do more against bullying such as make a statement by hanging up the campaign posters in classrooms or youth rooms and make bullying a topic of discussion in a group with the game methodology with the hashtag #tegenpesten (#againstbullying)

On the other hand, **Angèle** (angele_vl), the most successful Belgian singer of the moment, is also the most followed influencer on Instagram in the country with 3,6 million (Statista, 2019). Not only that, the artist is quite committed to equal education and the end of hate speech against women and the LGTBI+ community, and this is reflected in her songs.

- **Bulgaria**

Cyberbullying has been addressed through several online campaigns and organizations that work for its prevention and for raising awareness among young people, parents and teachers about this social issue. An example of such an online campaign is the Guidelines on Cyberbullying developed by **Safenet.bg** (https://cyberbullying.safenet.bg/)

Here in a very visual way young people can see examples of cyberbullying and can share if they have experienced something similar; they can report an incident through the link provided. They can also read some useful information, tips and advice about cyberbullying and how to react to it.

Safenet.bg also has a YouTube channel (https://www.youtube.com/@safenetbg948) where there are videos related to cyberbullying, online hate speech, etc., aiming to raise awareness among young people about these issues in a more attractive and visual way.

The telecommunication company **Yettel** also has a YouTube channel (https://www.youtube.com/@YettelBulgaria) developed in 2020, where there are diverse videos for young people with information about different online risks that young people can face, such as fake profiles, cyberbullying, dangerous links, risks on TikTok and YouTube, in games, etc.

5. Conclusions

5. CONCLUSIONS

Throughout this handbook Cyberbullying, Hate Speech, Cibersecurity and Privacy have been explained and contextualized. Their definitions can vary along different countries, however they are considered as an aggression to other people. In the case of Cyberbully there are normally three actors (the perpetrator, the victim and bystanders), in the case of Hate Speech, it is harder to establish a common scenario, but it equally involves a person who discriminates and the receptor who is discriminated against.

This handbook includes different ways of identifying, dealing and reporting cyberbullying and hate speech, of course, it will depend on who is the victim (yourself, a colleague, your children, etc.) but also on the legal framework of the country. For example, in Spain you can report it to the police while in Netherlands there is a national discrimination helpline. In addition, it is shown why concepts like data protection or CIAD triad are important as well as types of privacy threats such as identity theft, online sexual harassment, phising or frauds.

In conclusion, this document does not only offer definitions or key concepts regarding Cyberbullying, Hate speech, Cibersecurity and Privacy it also serves as a guide to prevent, react and report these kinds of abuses.

6. References

6. REFERENCES

101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022. (2022, May 26). Digital Guardian. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

A, D. (2020). *Cyberbullying (for Parents) - Nemours KidsHealth*. Nemours KidsHealth. https://kidshealth.org/en/parents/cyberbullying.html

A. (2018). *Report security vulnerabilities | TikTok Help Center*. TikTok. https://support.tiktok.com/en/safety-hc/reporting-security-vulnerabilities/reporting-the-security-vulnerabilities.

Assistant Secretary for Public Affairs (ASPA). (2019b, December 4). *Report Cyberbullying*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/how-to-report

Assistant Secretary for Public Affairs (ASPA). (2021, May 21). *Tips for Teachers*. StopBullying.Gov. https://www.stopbullying.gov/cyberbullying/tips-for-teachers

C, S. (2021). *Password security: How to create strong passwords in 5 steps*. Norton. https://us.norton.com/internetsecurity-privacy-password-security.html.

Caroline Rizza. (2013). *Social networks and Cyber-bullying among teenagers: EU Scientific e political report*. https://doi.org/10.2788/41784

Celine Chateau. (2016). *Policy department Citizen¡s rights and constitutional affairs*. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Center, C. R. (2021, October 18). *Preventing Cyberbullying: Top Ten Tips for Adults Who Are Being Harassed Online*. Cyberbullying Research Center. https://cyberbullying.org/preventing-cyberbullying-adults

CISCO. (2021). *Think Before You Click [Slides]*. CISCO. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf

Commission for Personal Data Protection, available. (2019). FOLD. https://www.cpdp.bg/?p=element&aid=12

Convention on Cybercrime (No. 185). (2001, November). Convention on Cybercrime. https://rm.coe.int/1680081561

Cyberbullying Research Center. (2022). *Cyberbullying Fact Sheet: Identification, Prevention, and Response*. https://cyberbullying.org/cyberbullying-fact-sheet-identification-prevention-and-response

Defining online sexual harassment. (2021, December 15). Childnet. https://www.childnet.com/what-we-do/our-projects/project-deshame/defining-online-sexual-harassment/

Digital Guardian. (22–05-26). *101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Online Safe in 2022*. https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe.

Facebook - Meld je aan of registreer je. (2018). Facebook. https://www.facebook.com/unsupportedbrowser

Griffin, M. (2020, March 5). *Advice on what to do if your child is a victim of cyberbullying*. Laya Healthcare. https://www.layahealthcare.ie/thrive/family/what-to-do-if-your-child-is-victim-of-cyber-bullyi/.

How to Protect Your Digital Privacy. (2019). The Privacy Project Guides - The New York Times. https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

Identity Theft. (2022, June 12). Investopedia. https://www.investopedia.com/terms/i/identitytheft.asp

Instagram Help Center. (2018). Instagram. https://help.instagram.com/192435014247952?helpref=uf_permalink

J. (2013). *Social Networks and Cyber-bullying among Teenagers*. JRC Publications Repository. https://publications.jrc.ec.europa.eu/repository/handle/JRC80157

L. (2021, 28 enero). *Ciberdelincuencia en el código penal - Letslaw*. LetsLaw. https://letslaw.es/ciberdelincuencia/

L.J. (2022, June 2). *Delitos en redes: de cinco años de cárcel a multas de hasta 2.700 euros*. Diario Noticias de Álava. https://www.noticiasdealava.eus/vivir-on/internet-y-ciencia/2022/04/24/delitos-redes-consecuencias/1183252.html.

Lex.bg - Р—Р°РєРѕРЅРё, РїСЂР°РІРёР»РЅРёС†Рё, РєРѕРЅСЃС‚РёС‚СѓС†РёСЏ, РєРѕРґРµРєСЃРё, РґСЉСЂР¶Р°РІРµРЅ РІРµСЃС‚РЅРёРє, РїСЂР°РІРёР»РЅРёС†Рё РїРѕ РїСЂРёР»Р°РіР°РЅРµ. (2017). Lex.Bg. https://www.lex.bg/laws/ldoc/1589654529

P. (2020). *Why is Data Protection Important?* PECB. https://pecb.com/article/why-is-data-protection-important

S, G. Cyberstalking: Prevention, Consequences, and Coping. (2021, August 17). Verywell Mind. https://www.verywellmind.com/what-is-cyberstalking-5181466

Safety and security. (2018). Twitter. https://help.twitter.com/en/safety-and-security

W, The Dangers of Hacking and What a Hacker. (2020). © Copyright 2004 - 2022 Webroot Inc. All Rights Reserved. https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-hackers

What Is Internet Fraud? Types of Internet Fraud. (2019). Fortinet. https://www.fortinet.com/resources/cyberglossary/internet-fraud

What is personal data? (2018, August 1). European Commission - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

What Is Phishing? (2022, May 5). Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#%7Ehow-phishing-works

Wilkey Oh, E. (2020, March 15). *Teachers' Essential Guide to Cyberbullying Prevention*. Common Sense Education. https://www.commonsense.org/education/articles/teachers-essential-guide-to-cyberbullying-prevention

Ф. (2009). *Киберсигурност*. Фондация. https://www.netlaw.bg/bg/a/kiber-sigurnost

If you want to know more about #Digitsafe, visit our website www.digit-safe.com

Or contact us at info@digit-safe.com

www.digit-safe.com
info@digit-safe.com