

TEACHING STUDENTS INTERNET SAFETY THROUGH AN ARTIFICIAL INTELLIGENCE MOBILE APPLICATION



INTERNET SAFETY

LESSON PLANS



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



This license lets distribute, remix, adapt, and build upon your work, even commercially, as long as they credit you for the original creation.

www.isafetyapp.eu

Link to the iSafetyApp:

<https://play.google.com/store/apps/details?id=com.bgs.safetyscapegame>

Link to videos related to the topics of the lessons:

<https://www.youtube.com/@isafetyapp>

Link to the flipbook version: <https://heyzine.com/flip-book/873e360354.html>



IX Liceum Ogólnokształcące
im. Kazimierza Jagiellończyka
w Toruniu


Innovation Frontiers
Mind is the limit

 **technologos**
pushing the boundaries



CONTENTS

ADDICTION.....	4
CYBERBULLYING.....	18
FAKE NEWS	24
GROOMING	33
PHISHING	39

ADDICTION

Addiction Behaviors and Symptoms

1 Online behavior

- Excessive use of social networks
- Excessive web browsing and searching
- Excessive gaming
- Excessive visiting on websites
- Excessive visiting gambling websites
- Excessive online shopping

Symptoms 2

- persistent and repetitive use of internet
- Unable to stop an activity or reduce the time on internet
- Internet is the only way to feel satisfaction and happiness
- isolation from family and friends
- low school performance

3 Physiologically

- Uninterested to participate on activities, hobbies, family events
- Feel guilty and telling lies about time spending on internet
- Internet as a means of escape from bad mood

Physically 4

- Dry eyes
- Headaches
- Migraines
- musculoskeletal problems
- Sleep Disorders



LESSON PLAN 1

Group: Students aged 14-18

Time: 45 min

Topic: Internet addiction: introduction to the issue.

Aims:

- to present in a symbolic way how addictions work;
- to teach Students what addictions are;
- to present the definition, reasons and common symptoms of addictions;
- to familiarise Students with the phenomena of Internet addiction;
- to help Students perform a quasi self-diagnosis.

Objectives:


By the end of the lesson students will be able to:

- define what addictions are;
- name examples of addictions;
- name reasons and symptoms of addictions;
- 'diagnose' themselves.

Materials: interactive board, video, handouts for Students

Procedure:

TIME	ACTIVITIES	INTERACTION PATTERN	COMMENTS
7 min	Lead-in Discussion	Teacher – students	<p>In this part of the lesson T doesn't say anything about the topic and purpose of the lesson. Here, T performs an 'experiment' showing the nature and the mechanism of getting addicted.</p> <p>T asks a volunteer (he/she will represent a person who is slowly getting addicted) to come and stand in front of the class - his/her task would be to free himself/herself out</p> <p>T asks another volunteer (this one will represent addiction and the process of getting addicted) to come and try to hold and stop volunteer no. 1 (he/she will probably be able to run away easily). T repeats the procedure – each time new volunteers representing addiction stay and hold volunteer no. 1 until volunteer no. 1 can't escape any longer</p> <p>T asks Ss what they think they have just seen, what the scene symbolises, and wait for Ss' answers.</p> <p>T summarises the scene.</p>
5 min	Warm-up	Teacher – students	<p>T writes on the board the word 'ADDICTION' and brainstorms Ss – they need to give their associations with the word.</p> <p>In this part of the lesson, T doesn't comment, suggest or give any hints concerning the main topic of the lesson i.e. Internet addiction.</p>

10 min	Lead-in Presentation of the topic Discussion	Teacher – students	T shows to Ss the following video: https://www.youtube.com/watch?v=N5dauIYZTs4 T asks Ss about what they have just watched, what they think about the video and the boy. T tries to elicit from Ss the word 'Internet addiction'.
7 min	Discussion	Teacher – students	T talks with Ss about this particular dependence, asks how they understand and define it and if they can give any specific examples of reasons why people become addicted, and behaviour which could be characteristic for an addicted person. Later T presents the definition of Internet addiction and discuss it with Ss: <i>Internet addiction is characterized by excessive or poorly controlled preoccupations, urges or behaviours regarding computer use and internet access that lead to impairment or distress*.</i> (* https://pubmed.ncbi.nlm.nih.gov/18399706/ , DOA 15.03.2023)
7 min	Working with handouts Discussion	Whole class Individual work Teacher – students	T gives handouts to Ss (attachement no. 1). Ss reflect on their use of the Internet and self-diagnose. If Ss answer 'YES' more than twice it can mean they have a problem with using the Internet in a healthy way.  Mind that this exercise is not and cannot be used as a REAL tool to diagnose anybody. A diagnosis should be performed only by a qualified specialist. This exercise aims only to make Ss aware of the amount and quality of their time spent on the Internet.
7 min	Pre-summary exercise Discussion	Whole class Individual work Teacher – students	Ss receive the attachment no. 2 and complete the sentences with own ideas. Later T asks volunteers to share their ideas with the rest of the group.
2 min	Summary	Teacher	T summarises the lesson and everything that happened during the lesson.

LESSON PLAN 2

Group: Students aged 14-18

Time: 45 min

Topic: FOMO vs JOMO: what are they?

Aims:

- to sensitise Students to and make them aware of their free time management skills;
- to present and teach Students about the concepts of FOMO;
- to provide Students with information about healthier lifestyles characterised by JOMO;
- to teach Students create ways of spending their time without using cellphones.

Objectives:

By the end of the lesson students will be able to:

- define in their own words what FOMO is;
- define in their own words what JOMO is;
- describe behaviour characteristic for each of the aforementioned phenomena;
- create ways of spending their time without using mobile phones;
- choose and live a healthier lifestyle.

Materials: interactive board, video, card stock, drawing aids, magazines

Procedure:

TIME	ACTIVITIES	INTERACTION PATTERN	COMMENTS
7 min	Lead-in Discussion	Teacher – students Whole class Individual work	<p>In this part of the lesson T doesn't say anything about the topic and purpose of the lesson.</p> <p>T takes Ss' mobile phones away, puts them in a visible place and tells Ss they have to do something and get busy for the next 5 minutes without using their phones.</p> <p>T doesn't give any suggestions or comments on what Ss might do – it's their task to come up with an idea.</p> <p>After 5 minutes T asks Ss what they did and if it was easy or difficult to figure something out on their own, how they felt and if there is anything they would change about their situation. If nobody mentions their phones, T asks how they feel about the fact that they are taken away and Ss can't use and check them out right now.</p>

3 min	Presentation of the topic Discussion	Teacher – students	<p>T asks Ss if they know what FOMO is and elicits ideas of what it stands for.</p> <p>T presents and explains the concept of FOMO – Fear Of Missing Out:</p> <p><i>[It] is a unique term introduced in 2004 and then extensively used since 2010 to describe a phenomenon observed on social networking sites. British psychologists elaborated and defined it as “pervasive apprehension that others might be having rewarding experiences from which one is absent”, FoMO is characterized by the desire to stay continually connected with what others are doing*</i></p> <p>T makes sure Ss understand the definition and if there's a need, explains it in an easier way.</p> <p>T discusses with Ss specific examples of reasons why people might suffer from FOMO, and behaviour which could be characteristic for such people</p> <p>(*https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8283615/, DOA 07.04.2023)</p>
10 min	Lead-in	Teacher	<p>T briefly presents to Ss the contradicting concept – JOMO (Joy Of Missing Out):</p> <p><i>JOMO means proudly living life in the slow lane and deriving pleasure from social exclusion*</i></p> <p>Later T shows the TEDxBasel video: <i>JOMO no FOMO: Keeping curiosity afloat in a sea of rising information</i> by Barbara Krieger:</p> <p>https://www.youtube.com/watch?v=YK_QHBQWTlg</p> <p>T briefly summarises the lesson up to this point.</p> <p>(*https://www.bbc.com/worklife/article/20190718-jomo, DOA 07.04.2023)</p>
20 min	Project	Group work	<p>T divides Ss into groups. Their task is to create posters presenting the notion of JOMO, what people can do to 'join' the lifestyle it represents, and demonstrate ideas of spending less time on their mobile phones.</p>

5 min	Presentation Summary	Whole class Teacher	Ss present and summarise their posters. T sums up the meeting and everything that happened.
-------	-------------------------	------------------------	--

LESSON PLAN 3

Group: Students aged 14-18

Time: 45 min

Topic: How to stay safe and use new technologies wisely.

Aims:

- to make Students reflect on friendships they make on the Internet;
- to familiarise Students with Robin Dunbar's theory concerning number of friends people need;
- to make Students aware of problems they might be facing on the Internet;
- to teach Students about wise and safe usage of the Internet;
- to provide Students with information on where they can look for help.

Objectives:

By the end of the lesson students will be able to:

- reflect on and verify the quantity and quality of online friends they make;
- use the Internet wisely and in a safe manner;
- name addiction treatment centres;
- name addiction treatment centres' phone numbers and websites.

Materials: interactive board

Procedure:

TIME	ACTIVITIES	INTERACTION PATTERN	COMMENTS
1 min	Lead-in	Teacher	T states the topic of the lesson: <i>How to stay safe and use new technologies wisely</i>
3 min	Warm-up Discussion	Teacher – students	T asks Ss to name social media websites they use and/or know and writes their answers on the board

8 min	Discussion	Teacher – students	<p>T asks Ss to go to their social media accounts and say:</p> <ul style="list-style-type: none"> • how many friends they have • how many of these friends they know personally • how often they meet with those friends • what they generally know about their online friends <p>(T might create an online survey using e.g. Google Forms or Mentimeter and provide a link to Ss to get and show to the group an overall results)</p> <p>T summarises the results and asks if Ss know how many friends one person really needs – according to a British anthropologist and biologist, Robin Dunbar, it is 150.</p> <p>T might recommend reading Dunbar's book: <i>How Many Friends Does One Person Need?</i> as homework and later perform a lesson on its basis.</p>
20 min	Discussion	Teacher – students	<p>T asks Ss what dangers might it bring if they make friends with people they don't really know. When Ss finish, T writes (or circle these answers if Ss gave such) on the board:</p> <ul style="list-style-type: none"> • grooming • phishing • scam • cyberbullying <p>T discusses with Ss each danger – its characteristics, how people can recognise them, how they can protect themselves*</p> <p>(*Here T can use materials and videos prepared by iSafetyApp teams)</p>
10 min	Individual task	Whole class Individual work Teacher – students	<p>T tells Ss to go back to their accounts and asks them to scan their social media friends and delete the ones Ss don't really know or whose profiles look questionable. T doesn't force Ss to do that (they have to be ready for such steps) but tries to emphasise once again how important it is to know who they invite to their virtual life.</p> <p>After the task, T talks with Ss if it was easy or difficult for them to do that, what and how they feel now, what they learnt through this and previous exercises.</p>

3 min	Summary	Teacher	T summarises the lesson and distributes the leaflets with contact details of addiction treatment centres in Poland.
-------	---------	---------	---

LESSON PLAN 4

Lesson plan: Internet addiction

Lesson objective: To make students aware of the dangers of Internet addiction and to promote healthy habits of using digital media.

Duration: Approximately 45 minutes

Materials:

- Multimedia projectors
- Boards and markers
- Sheets of paper and pens
- Notes with important information about Internet addiction

The course of the lesson:

1. Introduction (5 minutes): a) The teacher starts the lesson by asking students how often they use the Internet and what their favorite websites or applications are. b) Then the teacher asks if any of the students have heard of the term "internet addiction" and how they understand it.
2. Explanation of the concept of Internet addiction (10 minutes): a) The teacher displays the definition of Internet addiction on a multimedia projector. b) Through discussion with students, the teacher explains the symptoms and consequences of Internet addiction, such as:
 - Decrease in school achievement
 - Problems with social relationships
 - Sleep disorders
 - Health problems related to lack of physical activity
 - Negative impact on emotional development
 - Difficulty controlling the time spent online
3. Presentation of statistics (10 minutes): a) The teacher presents some statistics on Internet addiction to students, such as the number of hours spent online by the average person per day or statistics on computer game addiction. b) Students have the opportunity to ask questions about these statistics.
4. Group discussion (15 minutes): a) Students are divided into small groups. b) Each group is given a scenario where one of the characters is addicted to the Internet. c) The groups are to discuss the consequences of such an addiction and how this person can be helped. d) After some time, the groups present their answers to the whole class.
5. Summary and discussion of the strategy (5 minutes): a) The teacher summarizes the conclusions of the group discussions and presentations. b) Discuss self-control techniques with students, such as:
 - Setting time limits for Internet use
 - Planning activities outside the virtual world
 - Encourage face-to-face conversations with friends and family
 - Avoid using electronic devices before bedtime
 - Using the Internet in a useful way, eg for learning

6. Homework (5 minutes): a) The teacher asks students to write a short essay on the benefits and risks of using the Internet and how to avoid Internet addiction. b) The teacher explains that the homework will be checked and discussed in the next lesson.

Conclusion: The teacher emphasizes that the Internet is an extremely useful tool, but it requires conscious and responsible use. It encourages students to talk to their parents or teachers if they have concerns or concerns about their online use.

Time spent on the Internet | Worksheet

The table below will help you to see how much and how you spend your time online. If it is difficult for you to estimate the time for individual activities – put them in order: 1 – the most amount of time, 7 – the least amount of time.

How much time do you spend in front of the computer per day:	
playing computer games?	
on social networks?	
reading the news?	
in chat rooms and online forums?	
getting ready for school?	
watching movies, series, short videos?	
browsing websites?	
other (what?):	

Have you ever wondered if you might have a problem with Internet addiction? Questions below will help you think about whether you have a problem with the amount of time you spend online.

1. Do you neglect your school duties because you spend time on the Internet?YES NO
2. Do you stay up late at night, spending time on the Internet despite being tired?YES NO
3. Do you browse the Internet weven though you already feel bored?YES NO
4. Do you feel angry, depressed, irritated when you are unable to use the Internet?YES NO
5. You don't know what's going on with your friends and family because you prefer to spend time online?YES NO
6. Do you hide how much time you spend online? Do you underestimate or don't tell the truth about how much time you spend online?YES NO
7. Do you use the Internet to deal with sadness, anger, guilt, fear?YES NO

1. The Internet is
2. On the Internet there are
3. An addiction is.....
4. People are getting addicted because
5. Symptoms of addiction are
6. I can protect myself from getting addicted to the Internet by

1. The Internet is
2. On the Internet there are
3. An addiction is.....
4. People are getting addicted because
5. Symptoms of addiction are
6. I can protect myself from getting addicted to the Internet by

1. The Internet is
2. On the Internet there are
3. An addiction is.....
4. People are getting addicted because
5. Symptoms of addiction are
6. I can protect myself from getting addicted to the Internet by

CYBERBULLYING

HOW TO STOP CYBERBULLYING

Do not forward messages, photos or videos that might hurt you or other people

1

2

Do not send messages when you do not agree about the content

If you see something on internet that doesn't seem right inform an adult that you trust

3

4

If any person or incident on internet makes you feel bad or inconvenient inform an adult that you trust

If you suspect or you know that a friend or a classmate is a cyberbullying victim, you should inform an adult that you trust

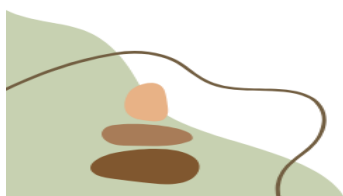
5

6

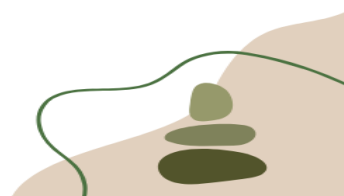
Do not respond to the cyberbullying because that might make it worst

Do not feel shame if someone is cyberbullying you. It is not your fault!

7



iSafetyApp



LESSON PLAN 1

Duration: 45 minutes.

Level: primary and secondary school

Aims:

- To make sure young people realize that once something is posted online, they can't get it back.
- Understanding what cyberbullying is and how it can affect others.
- Understanding that cyberbullying can have serious consequences

Objectives - Upon the end of the lesson students will be able to:

- Negotiate in relationships, recognizing that actions have consequences in the online world as well as in the offline world
- understand what cyberbullying is and know how to seek help or advice.
- resist the pressure to do wrong and recognize when others need help and how to support them.

Presentation (15 minutes)

Ask students to define cyberbullying - give them a few minutes to come up with a definition. Share with the whole class - what are the similarities and differences between each group's findings and discussions? Is there a general class consensus? Share with the class one of the generally accepted definitions - "Cyberbullying is the use of information and communication technologies, in particular mobile phones and the Internet, to intentionally annoy someone else" (you can also use other definitions from sources other than this scenario). Ask the class what they think about cyberbullying. Is it something that concerns them? Who do they think is most at risk? The desired answer that should be pursued in the classroom: Anyone can be, but those who are more vulnerable in the real world are more vulnerable in the online world.

Practice (20 minutes)

Share a cyberbullying case study with your students. Choose a more local example. Ask students to work in small groups to find similar cyberbullying stories online. Are there any common aspects? Discuss the following with students: What could have been done to prevent incidents of cyberbullying? When could action be taken to stop the chain of events? What can people who have fallen victim to cyberbullying do? It is important that students understand how to report a concern if they are victims of cyberbullying, and they should remember to keep any evidence they have about the bullying.

Summary (10 minutes)

Discuss with students, as part of the recapitulation, how ubiquitous technology can lead to a loss of inhibitions. Try to conclude that it is important for students to remember to stop and think before doing anything online.

LESSON PLAN 2

Duration: 45 minutes.

Level: primary and secondary school

Aims:

- To make sure young people realize that once something is posted online, they can't get it back.
- Understanding what cyberbullying is and how it can affect others.
- Understanding that cyberbullying can have serious consequences

Objectives - Upon the end of the lesson students will be able to:

- Negotiate in relationships, recognizing that actions have consequences in the online world as well as in the offline world
- understand what cyberbullying is and know how to seek help or advice.
- resist the pressure to do wrong and recognize when others need help and how to support them.

Presentation (15 minutes)

Ask students to define cyberbullying - give them a few minutes to come up with a definition. Share with the whole class - what are the similarities and differences between each group's findings and discussions? Is there a general class consensus? Share with the class one of the generally accepted definitions - "Cyberbullying is the use of information and communication technologies, in particular mobile phones and the Internet, to intentionally annoy someone else" (you can also use other definitions from sources other than this scenario).

Ask the class what they think about cyberbullying. Is it something that concerns them? Who do they think is most at risk? The desired answer that should be pursued in the classroom: Anyone can be, but those who are more vulnerable in the real world are more vulnerable in the online world

Practice (20 minutes)

Share a cyberbullying case study with your students. Choose a more local example. Ask students to work in small groups to find similar cyberbullying stories online. Are there any common aspects?

Discuss the following with students: What could have been done to prevent incidents of cyberbullying? When could action be taken to stop the chain of events? What can people who have fallen victim to cyberbullying do? It is important that students understand how to report a concern if they are victims of cyberbullying, and they should remember to keep any evidence they have about the bullying.

Summary (10 minutes)

Discuss with students, as part of the recapitulation, how ubiquitous technology can lead to a loss of inhibitions. Try to conclude that it is important for students to remember to stop and think before doing anything online.

LESSON PLAN 3

TIME: 45 MIN

LEVEL: primary and secondary school

AIMS:

- Expanding students' knowledge about the phenomenon of cyberbullying.
- Look at the impact cyberbullying has on each person in the peer group.
- Supporting teenagers in finding common or similar developmental goals of the peer group in which they function.
- Activating the sense of co-responsibility for relations in the group.

OBJECTIVES - after the end of the lesson, the student will be able to:

- indicate the definition of cyberbullying,
- determine where the phenomenon of cyberbullying comes from, what destructive actions it leads to and how to prevent it.

PRESENTATION - 15 MIN

Divide the participants into 4 groups. Ask students in the first and second groups to spend a few minutes on the question: What do you think the teenager wants to be like?, and ask the students in the third and fourth groups to think about the question: What a teenager should be like according to adults? Ask each group to list at least three characteristics in response to the question. Then the groups create their own boards (a large sheet of paper, e.g. a flipchart), writing down all the features that appeared during the group discussion. The next step will be to discuss the results of the groups' work. Ask groups one and two to present their work in the forum. At the end of the presentation, connect (glue) the boards of both groups together and summarize the exercise, noting the similarities in the work of both teams. In this way, you will get a picture of what teenagers expect of themselves. Then ask the third and fourth groups to present their results. Summarize the exercise similarly to groups one and two. This is where the image of adults' expectations towards teenagers is created. At the end of the presentation, ask students to make free associations to the following questions: Which teenage characteristics listed are common to these images? Which contradict each other? During the activity, students can react vividly to the question about the expectations of adults. Your task in this part of the exercise is to listen and gather ideas, not to judge or give explanations in this area.

PRACTICE - 20 MIN

Ask students to get into pairs or groups of three. Before starting the activity, make sure that students in individual teams do not show each other the assignment they will receive. Give each group one of the four descriptions:

- 1) Anne has been practicing handball since her early school years as the only one in her class.
- 2) Anne has been training handball since her early school years as the only one in her class. She is often praised for her diligence by teachers. They like that despite 4-5 workouts a week, he finds time to prepare for lessons.
- 3) Anne has been practicing handball since her early school years as the only one in her class. She is often praised for her diligence by teachers. They like that despite 4-5 workouts a week, he finds time to prepare for lessons. She is often teased by her classmates, especially when her classmates ask her about things related to the last game. They write offensive things about her on the Internet.
- 4) Anne has been training handball since her early school years as the only one in her class. She is often praised for her diligence by teachers. They like that despite 4-5 workouts a week, he finds time to prepare for lessons. She is often teased by her classmates, especially when her classmates ask her about anything related to the last

game. They write offensive things about her on the Internet. After another knee injury, the coach told Anne's parents that the girl should consider giving up the game.

After reading the story of the teenage girl, students in their groups have a few minutes to think about the answers to two questions - What does Anne think about herself? What do her peers think about her? and write down your answers on a piece of paper. During this time, prepare a table on the board or a large sheet consisting of two columns: one will contain the answers to the question: What does Anne think about herself?, and the other: What do her peers think about her? As you create the table, ask students to continue not to show the stories they received, but to observe the different groups' answers and try to guess how and why they differ. In conclusion, discuss the topic of self-esteem. It is an often used term to describe the image we have of ourselves. Together with the students, look for elements that interact with this image by relating to Anne's story.

SUMMARY - 10 MIN

In the summary, pay attention to several elements: 1. Each student, as a member of a given group, is affected by what is happening in it. Even when it seems that he is only a witness to the situation. 2. Each student has a certain attitude to this situation and emotions related to it - you can get scared, feel compassion for the victim, anger towards the perpetrator, be surprised, feel relieved that you are not a victim, wonder what will happen now, wait for the adults' reaction. 3. Try to separate the emotions that students talk about from their assessment of the situation, noting that both are related. Help name the emotions mentioned. 4. Show that emotions and thoughts (judgment) are related. 5. Pay attention to the fact that we cannot judge emotions - they are a reaction independent of man, they are all important because they inform about what we need and want.

LESSON PLAN 4

Duration: 45 minutes

Level: primary and secondary school

Aims:

- Familiarize students with the definition of cyberbullying
- Make students aware of the causes of cyberbullying
- Awareness of the consequences of cyberbullying
- Be aware of how to deal with cyberbullying.
- Learning to work in a group to express one's own opinion without offending.
- Sensitivity to the dignity of other people.

Objectives - after completing the lesson, the student will be able to:

- indicate the definition of cyberbullying, its causes and consequences.
- indicate what to do when faced with cyberbullying.

Presentation - 15 minutes

At the beginning, the teacher asks the students some questions, the children raise their hands up in response: 1. Who uses social media such as facebook, snapchat, instagram, youtube, tiktok,? 2. Who posts photos? 3. Who comments on posts, photos of friends? 4. Who shares posts, photos of other people? 5. Who sends private messages to other people? Then the teacher divides all students into subgroups (so that there are no more than 6 people in each group). Each group gets a large sheet of paper and writing utensils. Groups should be divided proportionally into two topics: • WHAT IS CYBERBULLYING? - groups with this topic are to write down

everything they think falls under this term (examples may be suggested). • WHAT IS NOT CYBERBULLYING? - groups with this topic are asked to list everything that they do not think is covered by this term. After 10 minutes, the groups finish their work. The teacher asks each group to present what they wrote down. The teacher writes down on the board, in separate parts, what the students present, asking the students: • what they meant, • asks for elaboration on the thought, asks for examples, • paraphrases the words of the students.

PRACTICE - 20 MIN

The teacher divides all students into 6 subgroups. Each group gets a large sheet of paper and writing utensils. Each group is given one of the following topics: 1. How might the recipient of cyberbullying feel? (it is important that the list includes: anger, sadness, depression, apathy, fear, impotence, frustration, loneliness, feeling of rejection). 2. What can be the consequences of cyberbullying for its recipient? (it is important to include on the list: deterioration of well-being, loss of self-confidence, reduced self-esteem, cutting off from the peer group, isolation, giving up hobbies, interests, depression, suicide attempt, suicide, aggression directed at someone else). 3. Why and what is someone bullying online? (it is important that they are on the list: someone could experience violence, hate, the need to relieve anger, frustration, the need to attract attention, the need to be noticed, the desire to express one's opinion, the need to influence the opinion of others, i.e. trolling, the need to kill boredom, the need to have fun, the need to improve well-being, the need to feel better, i.e. improving self-esteem). 4. What can be the consequences of cyberbullying for its creator? (it is important that they are on the list: being reported to the website administrator, kicked out of the forum / discussion group, blocked, ridiculed against the group, legal consequences (no one is anonymous on the Internet)). 5. What should and should not be done if you become a victim of cyberbullying? (it is important that they are on the list: you should tell a trusted adult about it, report it to the website administrator, portal, do not respond to hate with hate, keep it only for yourself). 6. What should and should not be done when witnessing cyberbullying? (it is important that they are on the list: support the victim in person or through a supportive comment, help report this fact to the site administrator, do not share the post, comment, respond to harassment with harassment, do not react). After the time has finished, the groups end their work. The teacher asks each group to present their list. After each group has finished presenting, you can ask the other groups if they want to add anything. Each of the sheets can be attached to the board or in another visible place.

SUMMARY - 10 min

The teacher divides the class, a group of students into 4 subgroups. Each group gets a sheet of paper and writing utensils. Each group draws the beginning of one of the 4 sentences and has to finish their sentence. It is important that the content of the sentences is the result of the decision of the whole group.

1. When you cyberbully me, I feel
2. When cyberbully my friend, my friend feels....
3. When you cyberbully me, I have the right to.....
4. When you cyberbully my friend, my friend has the right to.....

Then all the groups face each other, still remaining in their groups, but so that they are all facing each other. Then each group takes turns reading a complete sentence aloud.

FAKE NEWS

CHECKLIST

How to spot fake news

■ Consider the source

Is there an author? Check out their credentials on relevant issues.

■ Supporting sources?

Click on links or check with official sources. Do they support the story?

■ Ask the experts

Ask a librarian, or consult a fact-checking site.

■ Read beyond

Headlines can be outrageous in an effort to get clicks. What's the whole story?

■ Check your biases

Consider if your own beliefs or concerns could affect your judgement.

■ Look before you share

Don't share posts or stories that you haven't checked out first.



Co-funded by
the European Union



LESSON PLAN 1

Lesson topic: True or False? That is true and false information.

Target group: Secondary school students.

General Objective: The student knows what false information is and is able to distinguish it from true information.

Specific goals:

- the student is able to verify information in the media
- the student makes a critical selection of sources
- the student distinguishes between the concepts of: manipulation, disinformation, post-truth, stereotype, information bubble, virality
- the student recognizes the above phenomena in texts and characterizes them.

Methods and forms of work:

- problem method
- creating a poster/mental map
- work in groups
- working with press releases - real and fake.

Materials, teaching aids:

- terms and definitions
- board. Chalk or flichart and sheets of paper, markers helpful in making a poster
- multimedia screen, work cards in electronic form,
- work cards in paper form

Key competences:

- competencies in understanding and creating information
- language competences
- digital competences
- personal, social and learning competences
- civic competences.

Course of classes:

1. Presentation of the topic and general objective of the classes. The teacher writes the topic "True or False" on the board and presents the purpose of the lesson: The student knows what false information is and can distinguish it from true information.

The teacher introduces the topic:

The amount of information that we are bombarded with every day makes it impossible for us to analyze them all. As a consequence, we are susceptible to manipulation and it is increasingly difficult for us to distinguish truth from falsehood. That is why it is so important to recognize true and false information.

2. The teacher writes on the board or flipchart the password: false information and asks for associations with mines. Students explain the concepts. Then completes the terms that are related to the topic and which were not provided by the students and briefly describes them. An associogram appears on the board with the following

slogans: manipulation, disinformation, post-truth, stereotype, information bubble, virality, fake-news, fact-checking, messages that manipulate, trolling, harmful and dangerous content, deepfake, propaganda.

3. The teacher asks students to formulate a definition of false information and then summarizes the statement: False information is texts, photos and/or videos containing false information, attracting attention, functioning on television, newspapers, social media, conquering the Internet and bringing, among others, material benefits to those who create and disseminate them, and to the detriment of people and institutions about which they talk and show.

4. Students are divided into groups of four and receive worksheets prepared by n.

You can prepare the material yourself, based on current events and the time of the classes, tailored to a given country, region, etc. They can contain various information, both true and false: article headlines, excerpts from tabloids, photos, Facebook posts.

The task is to distinguish true from false information and to justify why, according to the students, the presented content is true or false.

5. Students work in their groups for a few minutes and then present their thoughts to the class.

The teacher presents the materials of each group to the class (displays on the screen), representatives of the individual groups discuss what is on the worksheet, assess which materials are true and which are false, discuss and evaluate, give arguments for and against the theses.

The teacher moderates students' presentations and corrects misjudgments regarding true and false information contained in the worksheets.

6. At the end of the lesson, the teacher summarizes the achievement of the lesson objectives and informs about the degree of students' ability to recognize truth from falsehood in social media, the press or the Internet.

LESSON PLAN 2

Lesson topic: How to recognize fake news? How to fight disinformation?

Objectives: Understanding the phenomenon of fake news. Students learn how to recognize fake news and fight disinformation. Why is fake news created?

Forms and methods of work: discussion, group work

Materials: flipchart, markers, a few plain sheets of paper and pens, a computer connected to a projector with the ability to display presentations or websites, participants can use smartphones with an internet connection

Course of classes:

1. Conversation with students: how do they understand the term "fake news"? The teacher makes sure that the students understand the meaning of the English words fake and news. I'm trying to motivate as many people as possible to answer this question. Write down all the passwords that come up on a board/flipchart.
2. Using a previously prepared presentation or a page in the Internet encyclopedia, n-l presents a dictionary definition of fake news, making sure that the password is understandable for students.
3. The teacher divides the students into groups, e.g. of several people, and asks each group to prepare answers to one of the following questions (the questions can be modified, added or reduced depending on the number of groups):
 - Why do false information appear in the public space? Why, for what purpose does someone create them?
 - Are false information, lies, manipulations new phenomena? When did they appear in public space?
 - What facilitates the spread of fake news? What methods and tools are used to spread false information?
 - Give examples of fake news, which content would you call fake news?
 - How to recognize false information? What characterizes them? Which sources are unreliable?
 - What sources of information can be considered credible (sufficient for correct verification of statements) and those that may be helpful (guiding to credible sources)? justify.
 - What is disinformation, how to recognize it and how to react to it?
 - What are the consequences of fake news? What are the consequences of false information shared on the web and other media?
 - How to defend yourself against manipulation, lies and false information? Are there organizations/institutions dealing with this phenomenon? What is their job?Each group gets one question, a large sheet of paper and a felt-tip pen. Answers are written on a large sheet of paper. Students can use their smartphones.
5. Each group presented items from its list in turn. He presents his posters and discusses the answers to the questions put to them. If something is missing, students from other groups complete the statement, say what else they think should be on the poster . The teacher moderates the meeting, asks additional questions, adds a comment.
6. As a summary of classes, n-l informs about the achieved goals of the lesson.

LESSON PLAN 3

Lesson topic: True or False? That is true and false information.

Target group: Secondary school students.

General Objective: The student knows what false information is and is able to distinguish it from true information.

Specific goals:

- the student is able to verify information in the media
- the student makes a critical selection of sources
- the student distinguishes between the concepts of: manipulation, disinformation, post-truth, stereotype, information bubble, virality
- the student recognizes the above phenomena in texts and characterizes them.

Methods and forms of work:

- problem method
- creating a poster/mental map
- work in groups
- working with press releases - real and fake.

Materials, teaching aids:

- terms and definitions
- board. Chalk or flichart and sheets of paper, markers helpful in making a poster
- multimedia screen, work cards in electronic form,
- work cards in paper form

Key competences:

- competencies in understanding and creating information
- language competences
- digital competences
- personal, social and learning competences
- civic competences.

Course of classes:

1. Presentation of the topic and general objective of the classes. The teacher writes the topic "True or False" on the board and presents the purpose of the lesson: The student knows what false information is and can distinguish it from true information.

The teacher introduces the topic:

The amount of information that we are bombarded with every day makes it impossible for us to analyze them all. As a consequence, we are susceptible to manipulation and it is increasingly difficult for us to distinguish truth from falsehood. That is why it is so important to recognize true and false information.

2. The teacher writes on the board or flipchart the password: false information and asks for associations with mines. Students explain the concepts. Then completes the terms that are related to the topic and which were not

provided by the students and briefly describes them. An associogram appears on the board with the following slogans: manipulation, disinformation, post-truth, stereotype, information bubble, virality, fake-news, fact-checking, messages that manipulate, trolling, harmful and dangerous content, deepfake, propaganda.

3. The teacher asks students to formulate a definition of false information and then summarizes the statement: False information is texts, photos and/or videos containing false information, attracting attention, functioning on television, newspapers, social media, conquering the Internet and bringing, among others, material benefits to those who create and disseminate them, and to the detriment of people and institutions about which they talk and show.

4. Students are divided into groups of four and receive worksheets prepared by n.

You can prepare the material yourself, based on current events and the time of the classes, tailored to a given country, region, etc. They can contain various information, both true and false: article headlines, excerpts from tabloids, photos, Facebook posts.

The task is to distinguish true from false information and to justify why, according to the students, the presented content is true or false.

5. Students work in their groups for a few minutes and then present their thoughts to the class.

The teacher presents the materials of each group to the class (displays on the screen), representatives of the individual groups discuss what is on the worksheet, assess which materials are true and which are false, discuss and evaluate, give arguments for and against the theses.

The teacher moderates students' presentations and corrects misjudgments regarding true and false information contained in the worksheets.

6. At the end of the lesson, the teacher summarizes the achievement of the lesson objectives and informs about the degree of students' ability to recognize truth from falsehood in social media, the press or the Internet.

LESSON PLAN 4

Lesson topic: How to recognize fake news? How to fight disinformation?

Objectives: Understanding the phenomenon of fake news. Students learn how to recognize fake news and fight disinformation. Why is fake news created?

Forms and methods of work: discussion, group work

Materials: flipchart, markers, a few plain sheets of paper and pens, a computer connected to a projector with the ability to display presentations or websites, participants can use smartphones with an internet connection

Course of classes:

1. Conversation with students: how do they understand the term "fake news"? The teacher makes sure that the students understand the meaning of the English words fake and news. I'm trying to motivate as many people as possible to answer this question. Write down all the passwords that come up on a board/flipchart.

2. Using a previously prepared presentation or a page in the Internet encyclopedia, n-l presents a dictionary definition of fake news, make sure making sure that the password is understandable for students.

3. The teacher divides the students into groups, e.g. groups of several people, and asks each group to prepare answers to one of the following questions (the questions can be modified, added or reduced depending on the number of groups):

- Why do false information appear in the public space? Why, for what purpose does someone create them?
- Are false information, lies, manipulations new phenomena? When did they appear in public space?
- What facilitates the spread of fake news? What methods and tools are used to spread false information?
 - Give examples of fake news, which content would you call fake news?
- How to recognize false information? What characterizes them? Which sources are unreliable?
- What sources of information can be considered credible (sufficient for correct verification of statements) and those that may be helpful (guiding to credible sources)? justify.
- What is disinformation, how to recognize it and how to react to it?
- What are the consequences of fake news? What are the consequences of false information shared on the web and other media?
- How to defend yourself against manipulation, lies and false information? Are there organizations/institutions dealing with this phenomenon? What is their job?

Each group gets one question, a large sheet of paper and a felt-tip pen. Answers are written on a large sheet of paper. Students can use their smartphones.

5. Each group presented items from its list in turn. He presents his posters and discusses the answers to the questions put to them. If something is missing, students from other groups complete the statement, say what else they think should be on the poster . The teacher moderates the meeting, asks additional questions, adds a comment.

6. As a summary of classes, n-1 informs about the achieved goals of the lesson.

Here are some tasks that can be assigned to students in a lesson about fake news on the Internet:

1. Research task: Ask students to select any article or news item from the Internet and check if the information in it is true. Ask them to use various sources of information, such as credible websites, research papers, or government publications, to verify the credibility of the article. Then ask them to share their conclusions and what criteria they used to judge the credibility of the information.
2. Simulation games: Ask students to take part in a simulation game in which they will have to identify false information. Prepare a set of messages, some of them will be true and others will be false. Students will have to check the credibility of the information by analyzing the sources, context, author, etc.
3. Depending on the level of difficulty, you can adjust the amount of information or add additional clues.
4. Case Study: Give students some examples of known cases of false information that have had high impact, such as popular rumors, political disinformation, or false advertising. Ask students to analyze these cases and answer questions about why the information was misleading, how it affected people, and what the effects of the false information were. Students could also be asked to share ways in which this false information could have been avoided.

5. **Creating Information:** Ask students to create a fake news or article on their own to mislead readers. Then ask them to take turns with another student and share their materials. The second student will have to identify false information and point out why it is false. This exercise will help students understand how easy it is to be misled by the manipulation of information.
6. **Group Discussions:** Divide the class into small groups and assign them different instances of false information. Ask the groups to discuss the effects of this information on society, what are the methods of combating disinformation, and what are the responsibilities of those who spread false information. Then ask the groups to share their findings with the rest of the class.

When assigning these tasks, it is worth paying attention to differences in students' skills and knowledge, adjusting them to the appropriate level and complexity. Also, encourage students to share their findings and discuss together about fake news on the Internet.

Checking the credibility of information on the Internet is a key skill in the era of easy access to information. Here are some steps you can take to assess the credibility of information:

1. **Check the source of the information:** Starting with the source itself, check whether it is a reputable website, institution, company or an unknown source. Pay attention to the domain (whether it is an official government, university, credible organization) and the reputation rating of the site.
2. **Check Author:** Analyze the author information. Check if he or she has the appropriate qualifications, experience or knowledge of the subject. Look for information about the author outside of the page to see if he or she is an expert in the field.
3. **Verify the message with different sources:** Check if similar information is confirmed with other, independent sources. If the information appears only on one page or is not confirmed by other reliable sources, it may be worth being careful.
4. **Check the date of publication:** Make sure the information is up to date. Often, older articles may be outdated or inappropriate for the current situation.
5. **Analyze language and tone:** Pay attention to the language used in the text. Is it objective or does it appear to be biased or emotional? Be wary of information that is overtly emotional or overly simplistic.
6. **Verify internal sources:** If the article contains quotes, references or references to other sources, verify that these sources actually exist and support the claims made.
7. **Check the context of the information:** Try to understand the context in which the information is presented. Sometimes information can be manipulated or taken out of context to mislead readers.
8. **Check Reliable Fact-Checking Sites:** There are many websites that specialize in fact-checking and fact-checking. Search these sites to see if the information has been verified and is reliable.
9. **Trust your intuition:** If something seems suspicious or untrue, trust your intuition and maintain a healthy skepticism. It's better to be careful than to believe false information.

Remember that checking the reliability of information takes time and effort. It is important to be a responsible consumer of information and develop critical thinking skills so as not to be misled by online disinformation.

Here are some examples of websites that specialize in fact-checking and fact-checking:

1. **Snopes (www.snopes.com):** Snopes is one of the oldest and most famous fact-checking sites. It assesses the credibility of various information, rumors and myths concerning various areas of life.

2. FactCheck.org (www.factcheck.org): FactCheck.org is a non-profit project that analyzes and verifies political information in the United States. It focuses on checking the veracity of political statements, advertisements and public claims.

3. PolitiFact (www.politifact.com): PolitiFact is another popular fact-checking website that focuses on analyzing and verifying political statements in the United States. Assigns ratings to the degree of truthfulness of statements, ranging from "True" to "Pants on Fire" (a complete lie).

4. Full Fact (fullfact.org): Full Fact is a UK fact-checking organization that checks information and political statements in the UK. Their goal is to provide independent and accurate information.

5. AFP Fact Check (factcheck.afp.com): Agence France-Presse (AFP) is an international news agency that also has a fact-checking division. They analyze and verify information, photos and videos that are widely distributed.

6. BBC Reality Check (www.bbc.co.uk/news/reality_check): The BBC Reality Check is a section on the BBC website that researches and verifies various information, rumors and claims in current events.

It is also worth noting that many countries and regions have national or local fact-checking sites that focus on verifying information in the context of their country. Therefore, it is worth looking for sites that are relevant to the specific region in which you are located.

GROOMING

SEXTING



Sexting means sending sexual text messages. It includes sending nude and seminude photos and explicit videos of yourself. It happens via texts or direct messages on social media.

RISKS FOR ADULTS



The major risk of sexting for adults is sharing explicit images and videos to unknown person. They could leak your images or sell them to websites as revenge porn. If someone accidentally seen your images, it will ruin your character.

RISKS FOR TEENS



Teens also have same risks similar to adults but they may have vast effects on them which creates huge problems. Sexting media leak can lead to cyberbullying which will cause stress, depression, anxiety and self harm.

LEGAL PROBLEMS



People who are under 18 could lead to legal charges. The people who are sharing the images of minors will be charged on child pornography or sex offender which will influence adolescents future.

How to avoid?

- ▶ Contact Authority figure
- ▶ Navigate the conversation in different direction
- ▶ offer refusal
- ▶ Set limits on social media
- ▶ Educate teens on what to do
- ▶ Think before sending messages or explicit images
- ▶ Confronting the person



LESSON PLAN 1

Let's talk about grooming

Objectives: Familiarization with the subject of dangerous contacts online or via, including the phenomenon of child grooming.

Organizing knowledge about Child Grooming,

Recognizing the stages of grooming aimed at establishing contacts with a minor

The student recognizes and characterizes various manifestations of cybercrime, which is grooming

Recognition of signals indicating manipulation attempts.

Work methods and techniques: brainstorming, presentation, discussion

Forms of work: individual

Materials: blackboard and chalk, presentation, film

The course of the lesson:

1. The teacher introduces students to the topic of the lesson. He informs that the Internet, on the one hand, offers many opportunities, and on the other, it is also a space where students encounter various threats. One of them is the dangerous friendships they can make online. In the virtual world, young people contact not only their peers or friends from the yard, but also with friends from the Internet, who do not always have good intentions towards them. That's why it's worth talking about child grooming.

2. The teacher writes the term child grooming on the board and asks the students to write their associations under it (brainstorming).

3. The teacher summarizes the record on the board and presents the definition of child grooming in a presentation.

Child grooming - activities undertaken to befriend and emotionally bond with a child in order to reduce his resistance and later sexually exploit him. It is also a mechanism used to induce a child into prostitution or participation in child pornography. Colloquially, child grooming is understood as grooming children via the Internet. (definition from https://pl.wikipedia.org/wiki/Child_grooming).

4. The teacher plays a video about the topic of the lesson - "CHILD GROOMING | PROTECT THE CHILD" – a film on the youtube channel – Protect the Child, the film lasts 3.40 minutes. and presents a teenager writing messages via instant messenger with a stranger, complaining about her life situation, problems at school and at home, misunderstanding on the part of her friends and parents. The interlocutor shows support and persuades the girl to meet. (https://www.youtube.com/watch?v=_Gy_8QomMpI).

5. After watching the videos, the teacher asks the students to talk about the specificity of child grooming and indicate what its individual stages are. Students share their observations. The teacher organizes the messages and presents the individual stages of grooming in the presentation:

Grooming is a long-term process. It can be divided into 4 stages:

- Getting to know the victim and making friends – at this stage, the pedophile collects the first, basic information about the child, eg: interests, difficulties, needs. He assesses his chances.
- Deepening the relationship - convincing the child that he is dealing with a trustworthy person with similar interests and problems, a potential friend. Strengthening the relationship by referring to previous conversations. The child feels heard. This is conducive to further and deeper confessions.

- Situation analysis - assessment of the risk of exposure. There are questions about where the computer is located? Do parents know about their relationship? There are requests not to save conversations. Then the topics related to sexuality and male-female relationships begin. Intimate questions are asked, often delicate at the beginning so as not to scare the child, e.g.: has he had a boyfriend/girlfriend, has he already kissed? As time goes by, the questions get bolder.
 - Suggestions for specific actions - the pedophile prepares the child for meeting in reality or performing other activities, eg masturbation while talking on the Internet. At the same time, he tries to present his parents in a bad light (as enemies) and himself in a good light (an ally). There is also blackmail - failure to comply with the request will destroy the friendship, just like telling someone else about it, e.g. parents.
7. At the end of the lesson, the teacher summarizes the lesson and adds that you should be careful when meeting someone online. Because not everyone is who they say they are. You can never be 100% sure who is really on the other side of the screen.

LESSON PLAN 2

Lesson topic: Legal aspects of grooming

Objectives: Students will learn about grooming laws

Learn the right ways to respond to attempts to make contact online by strangers.

Students know where to look for help

Developing critical thinking skills.

Methods and techniques of work: presentation, discussion, work in pairs

Forms of work: individual; work in pairs.

Materials: mobile phones or computers (computer lab at school), presentation, film

The course of the lesson:

1. The teacher introduces the students to the subject of the classes, says that sometimes it happens that someone dishonest, with bad intentions, tries to establish contact with children/young people via the Internet. It tempts with promises and gifts. He pretends to be the only person who can understand the young man's feelings, taking advantage of the fact that sometimes his virtual interlocutor is dissatisfied, sad or feels lonely. It gives attention and interest, draws the victim away from other people whom she trusted so far. It is difficult to break such contact, even if it is no longer comfortable for both parties. Sometimes the offender will blackmail you with revealing secrets that the child has told him in confidence. He may insist on meeting in secret or ask for things (such as sending private, intimate photos or videos, such as those in which the victims are incompletely dressed).

The teacher draws the students' attention to the fact that a person inciting a child to such behavior commits a crime under Polish law.

2. The teacher asks students to look in pairs for information on the Internet regarding legal aspects related to child grooming. Students should search for relevant provisions from the Penal Code, including information on penalties provided for by Polish law.

3. Students present the results of their searches. The teacher asks for the records on child grooming related to persuading a minor to participate in sexual activities.

6. The teacher summarizes the students' statements and presents the collected information in the presentation:
How to help? Where to look for help?

LESSON PLAN 3

Lesson topic: Grooming - online grooming

Objectives: Students will learn about online grooming and its dangers

Working methods and techniques: brainstorming, discussion,
Materials: blackboard, worksheets

The course of the lesson:

1. A reminder of the meaning of grooming:

Child grooming, i.e. the process of seducing a child using modern communication technologies, can take various forms. Sometimes it's a sexually suggestive comment under a photo or video of a minor on social media. However, in many cases it is a long-term process that lasts even months. It usually leads to the sexual exploitation of a child in the real world or to the production of illegal content with his participation. Child grooming is a crime under Polish law.

2. Students are divided into groups of several people. Each group receives a worksheet with questions about online grooming. Half of the groups get card A, the other half get card B. Students discuss, write down their ideas and

Card A

Think together about how an online criminal will try to introduce himself to a potential victim in order to force them to take a certain action. Enter your ideas below:

- What can a criminal/manipulator operating in the network say?
- How can it behave?
- What can it convince?

Card B

Consider together what elements prove that you are a victim of grooming and how to prevent it? Enter your ideas below:

- Why can't everyone online be trusted?
- What are the signs of manipulation?
- What to protect against online grooming?

3. Individual groups A and B present the results of their work, others supplement the statements of their predecessors. The teacher directs the discussion. Worksheets of all groups are hung on the school board.

4. Lesson summary. The teacher emphasizes the naive ways of seducing minors on the Internet and warns against it and shows how to avoid being a victim of grooming.

LESSON PLAN 4

Duration: about 45 minutes

Lesson Objectives:

1. Understanding the concept of grooming in the context of the Internet.
2. Understanding the techniques used by criminals to gain trust and manipulate victims.
3. Raising students' awareness of the risks of grooming.
4. Providing practical tips on how to protect yourself from grooming.

The course of the lesson:

1. Introduction (5 minutes):

- Greeting students and introducing the topic of the lesson.
- Explain that the lesson will be about grooming in an internet context.
- Asking the question: "Do any of you know what grooming is?".

2. Grooming Definition (10 minutes):

- Clarification of the definition of grooming: the process of manipulating, trusting and exploiting individuals, especially children and young people, for intentional criminal activities.
- Discuss that grooming often takes place online where criminals use various manipulation techniques.

3. Grooming techniques (15 minutes):

- Presentation of various grooming techniques, such as: flirting, feigning friendship, highlighting common interests, giving gifts, threats and blackmail.
- Discuss how criminals use these techniques to gain the victim's trust and lead them into a trap.
- Emphasize that grooming is manipulation and exploitation, not blame.

4. Risks and Consequences (10 minutes):

- Explaining the risks of grooming, such as: physical and emotional abuse, cyberbullying, blackmail, identity theft, and loss of privacy.
- Discuss the consequences for grooming victims, both short and long term.
- Emphasize the need to report grooming and seek help.

5. Prevention and protection (15 minutes):

- Provide practical tips to prevent grooming, such as: not sharing personal information, choosing your online friends carefully, limiting the time you spend online, being aware of red flags.
- Discussing the importance of communicating with trusted people, such as parents, teachers, or counselors, if you have suspicions or concerns about grooming.
- Identify resources and organizations that offer help and support to victims of grooming.

6. Summary (5 minutes):

- A summary of the most important points covered in the lesson.
- A reminder that it's important to keep yourself safe online and to be aware of the risks of grooming.
- Encouragement to ask questions and further reflect on grooming.

End of the lesson.

It is important that the lesson is conducted in an empathetic and age-appropriate manner. Provide a safe space to ask questions and share any experiences you may have. In addition, the teacher should point out that there are specialist organizations that offer help to victims of grooming, and students should know where and how to seek help if needed.

Task card - A lesson on grooming

Activity 1: Definition of grooming (5 minutes)

Ask students to share their definition of grooming.

Explain that grooming is the manipulative actions of an adult to make contact with a child for the purpose of sexual abuse.

Ask students if they are aware of what forms of grooming can be.

Activity 2: Discuss Grooming Tactics (10 minutes)

Discuss with students the different tactics groomers use, such as trust building, emotional manipulation, blackmail, threats, promises of rewards, etc.

Ask students to share examples of such tactics or situations where they might occur.

Activity 3: Identifying Warning Signs (15 minutes)

Provide students with the different warning signs that may indicate the presence of grooming activities, such as: sudden changes in behavior, secrecy with parents or guardians, excessive use of the Internet, extreme reactions to privacy talks, etc.

Ask students to create a list of warning signs on a whiteboard or flipchart.

Activity 4: Internet safety rules (10 minutes)

Introduce internet safety rules that can help students avoid grooming situations, such as:

Never share private information such as name, address, telephone number, etc.

Be careful when making friends online and don't socialize with people you don't know in person.

Do not accept invitations from unknown people to private chats.

Report suspicious situations to parents, teachers or other trusted adults.

Activity 5: The role of social support (10 minutes)

Talk to students about the role of social support in grooming situations.

Mention that it's important to tell your parents, teachers, carers, or other trusted adults about these situations.

Please note that whatever the situation, the victim is not responsible for what happened and should always receive help and support.

Activity 6: Summarize and reflect (5 minutes)

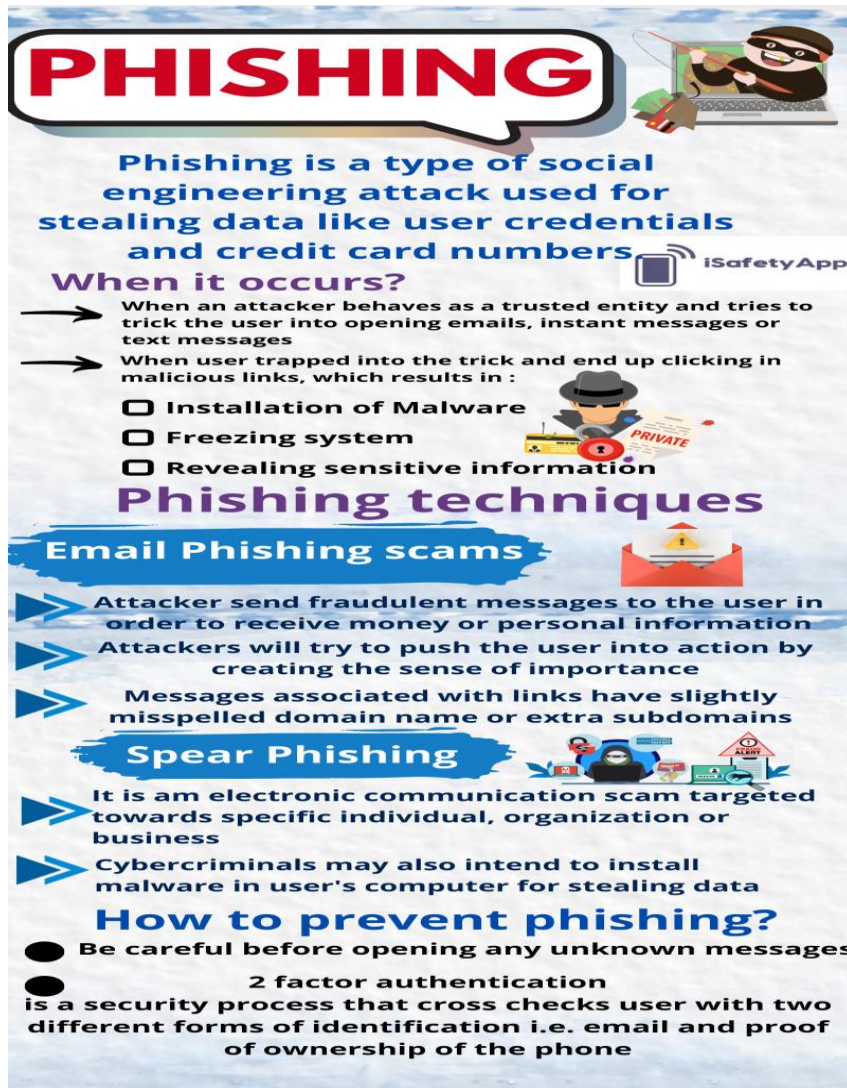
Ask students to summarize the most important things they learned in the grooming lesson.

Encourage students to reflect on how they can protect themselves and others from grooming.

Thank students for their active participation in the lesson and emphasize the importance of raising awareness about grooming.

It is important for the teacher to be ready for possible difficult questions and reactions from students and to provide them with emotional support. Presenting information with moderation and care is key when teaching a lesson on such a sensitive topic.

PHISHING



PHISHING

Phishing is a type of social engineering attack used for stealing data like user credentials and credit card numbers.

When it occurs?

- When an attacker behaves as a trusted entity and tries to trick the user into opening emails, instant messages or text messages
- When user trapped into the trick and end up clicking in malicious links, which results in :
 - Installation of Malware
 - Freezing system
 - Revealing sensitive information

Phishing techniques

Email Phishing scams

- Attacker send fraudulent messages to the user in order to receive money or personal information
- Attackers will try to push the user into action by creating the sense of importance
- Messages associated with links have slightly misspelled domain name or extra subdomains

Spear Phishing

- It is an electronic communication scam targeted towards specific individual, organization or business
- Cybercriminals may also intend to install malware in user's computer for stealing data

How to prevent phishing?

- Be careful before opening any unknown messages
- 2 factor authentication is a security process that cross checks user with two different forms of identification i.e. email and proof of ownership of the phone

LESSON PLAN 1

IDENTITY THEFT AND PHISHING SCAMS

Key concepts

Consumer protection of financial records, protection of one's identity through paper and online

Summary

This lesson introduces students to identity theft and phishing, including common methods used in the crime of identity theft.

Overview & Lesson Objectives

This lesson is intended for high school students. The lesson teaches students how to protect their identities while making purchases online and in everyday financial life. The activities rely on a variety of interactive and visual formats designed to be interesting and fun.

Students will be able to:

- List the common techniques used to steal one's identity
- Become aware of electronic phishing ploys
- Describe and evaluate methods to protect financial records
- Explain how to take action if your identity is stolen
- Explain behavior to operate more safely online and with mobile devices

Time Allocation: 15 – 20 Minute Prep

35 – 40 Minutes Engagement

Materials:

- Access to the internet in the classroom

Lesson Begins: Setting the Stage

State the Objective: Tell the students what they will be able to do upon conclusion of the lesson.

“Today we are going to learn about a fast-growing financial crime: identity theft. You will be able to list the common techniques used to steal one's identity and know how to report that one's identity is stolen. You will be able to list some behaviors to protect your financial records and personal information and to operate more safely online and with mobile devices.”

Lesson Continues

If you have ever heard a parent or a relative say when they opened their credit card bill, “Wow, I did not charge all of these items." I did not buy a 500 euro watch!" it is possible that they were a victim of identity theft. People who are dishonest and unethical (and they are often very smart) will try to make their money by stealing yours. Identity theft is a crime.

Open the lesson with a definition of new terms and phrases, asking students if they know what they are.

Definitions:

Identity theft is when a person acquires and then uses your name, address and Social Security Number in order to apply for a credit card in your name or purchase products in your name.

Phishing occurs with electronic communication such as e-mail or text messaging. It is when someone pretends to be someone or something they are not to acquire your passwords, credit card or bank account information, or other personal information.

The top methods for stealing a person's identity are:

1. "Dumpster Diving": going through a person's or household's trash to look for credit card offers, bills, bank account numbers, pay stubs, anything with Social Security numbers, birth dates, bank or credit account number, or other personal information.
2. Skimming: stealing credit card numbers with a small hand-held unit that can store your credit card number with a quick swipe of your card.
3. Phishing: pretending to be a legitimate financial institution, government agency, or company through an e-mail, a pop-up message, a text message, etc.
4. Changing your address: Completing a change of address card at the Post Office to defer your mail to another location other than your home. Or hacking into your e-mail or online accounts to change your address or steal your personal information.
5. Stealing: stealing mail from a person's U.S. postal service mailbox, or stealing your mailed Income Tax Return; stealing wallets or purses; bribing employees who have access to employee personnel records.
6. Unsecured Websites: online purchase sites where the URL does not start with "https", indicating it is not secure and opens you to the chance that identify theft occurring.

Ask students if they can think of other, unscrupulous methods for attempting to steal one's identity or cleverly disguise phishing. Ask them if they have ever received a spam text message (it is likely that they have).

Ask students to come up with a list of the harmful things that could occur if your identity is stolen, for example:

- Someone could withdraw money from your bank account using a debit card or credit card in your name.
- Your credit score could drop if you exceed your credit limit.
- You have to take the time and go through the expense of cancelling accounts, getting new accounts and account numbers, etc.

Deterring Identity Theft:

Ask students to come up with a list of behaviors to deter thieves from stealing their identity, such as:

- Shred financial documents that are not being kept for safeguarding. [This allows a teacher to cover the kind of information that should be held and for how long (in years).
- Do not give out personal information over the phone or over the internet unless you are absolutely sure who you are dealing with.
- Choose computer and electronic passwords with care by avoiding birth dates, your mother's last name, etc.
- Try not to have your postal mail pile up in your mailbox for several days; if you are going to be away for a few days, have your mail held at the post office until you return.
- Do not click on suspicious links in e-mail or complete forms with your account number and password. Check the web address.
- Be suspicious about regular bills that do not arrive on time, denials of credit for no apparent reason, calls or letters about purchases you did not make, charges on your financial statements that you do not recognize.
- Use a password to access your mobile devices such as your cell phone, tablet (iPad), etc., just as you would have a password to get access to your e-mail accounts.

Lesson Closes

Review with students the importance of securing their personal information and keeping an eye out for persons trying to steal information through electronic means.

Additional Engagement Opportunities / Resources

Pair and Share

Students (pairs) interview one another about the lesson content. They must summarize the partner's feedback in either written report or verbal format

Sample questions:

- How can you better safeguard your personal information?
- What should you be careful to review online to avoid responding to phishing scams?
- Describe why it is important to protect one's financial documents/identity.
- What can you do to protect your identity from being stolen?
- What steps should you take if your identity is stolen?
- What is the name of the government organization that can assist you if you're a victim of identity theft?

What's left out? Supply students with statements that have some information missing. This can be done verbally or it can be done on a board. Ask students to provide the missing information.

Samples:

Stealing credit card numbers with a small hand-held unit that can store your credit card number with a quick swipe of your card is called _____.

o Answer is "skimming"

Pretending to be a legitimate financial institution, government agency, or company through an e-mail, a pop-up message or a text message is a form of _____>

o Answer is "Phishing"

Peer Education through Skits, Videos: Often learning is reinforced or students learn best by teaching others. Have students write a script and act it out in class with the objective of teaching each other (their peers) about the lesson. A student skit could show identity theft or phishing in action and/or the proper steps for preventing it or reporting it once it occurs. Students could invent very clever scenarios that will keep them on alert in the future. These should be prepared by students and performed in another class period that follows this lesson.

LESSON PLAN 3

Lesson topic: Awareness and prevention of phishing

Lesson Objective: To educate students about the dangers of phishing and provide them with the tools and guidance to identify and avoid such attacks.

Lesson duration: 45 minutes

Materials needed: Multimedia projectors or access to computers, blackboard or flipchart, notebooks or sheets of paper for students.

I. Introduction (5 minutes)

- Welcome students and introduce the purpose of the lesson.
- Discussing the definition of phishing as a type of Internet attack in which cybercriminals impersonate credible institutions or individuals in order to obtain confidential information.
- Asking an open question: Have any of you heard of phishing? What do you know about it?

II. Lecture (15 minutes)

- Presentation of examples of different forms of phishing, such as fake emails, websites, SMS messages, etc.
- Discussion of the techniques used by phishing attackers, such as emotional manipulation, creating urgency, etc.
- Discuss the consequences for phishing victims, such as loss of personal information, identity theft, loss of money, etc.

III. Case study (15 minutes)

- Display various examples of phishing emails or web pages on multimedia projectors or computers.
- Dividing students into groups and assigning them specific examples to analyze.
- Each group analyzes the example assigned to them and tries to identify features that may indicate a phishing attempt.

IV. Discussion and conclusions (10 minutes)

- Joint discussion on the analyzed examples of phishing.
- Discuss the characteristics students have noticed that can help identify phishing attacks.
- Emphasize the importance of being suspicious and careful when using the internet.

V. Phishing prevention (10 minutes)

- Providing practical tips for preventing phishing, such as:
- Not opening suspicious emails, especially from unknown senders.
- Check the sender's email address and pay attention to any suspicious items.
- Avoid clicking on suspicious links and downloading attachments from unknown sources.
- Encourage students to use authorized websites and apps.
- Educating students about the consequences of sharing their confidential information online.

VI. Summary (5 minutes)

- Repetition of the main points covered in the lesson.
- Emphasize the role of awareness and caution in preventing phishing.
- Encourage students to ask questions and report any suspicious situations.

VII. End of lesson (2 minutes)

- Thank students for participating in the lesson.
- Encourage students to share what they learn with siblings and others to help prevent phishing.

It is also important to provide students with resources such as leaflets or posters that can remind them to use the internet safely and identify phishing.

Task card - Lesson about phishing

Activity 1: Definition of Phishing (5 minutes)

- Ask students to share their definition of phishing.
- Explain that phishing is a type of online attack where cybercriminals impersonate credible institutions or individuals in order to obtain confidential information.
- Ask students if they have heard of phishing before and what their understanding is.

Activity 2: Phishing examples (10 minutes)

- Display various examples of phishing emails, web pages or SMS messages on a multimedia projector or computer.
- Ask students to analyze these examples and identify features that may indicate a phishing attempt.
- Discuss the different forms of phishing, such as fake emails asking you to update your login details, websites that pretend to be banks, etc.

Activity 3: Recognizing the characteristics of phishing (15 minutes)

- Divide students into groups and assign each group an example of a phishing email or website.
- Ask groups to analyze the example and identify features that may indicate a phishing attempt, such as: wrong sender email address, suspicious links, spelling or grammar errors, lack of personalization of messages, etc.
- Each group should present their findings to the rest of the class.

Activity 4: Preventing Phishing (10 minutes)

- Give students practical tips on how to prevent phishing, such as:
 - Never open suspicious emails or attachments.
 - Be careful when clicking on links, especially those received from unknown sources.
 - Double-check website URLs before providing any confidential information.
 - Avoid sharing sensitive information, such as passwords or credit card details, on unknown and untrusted websites.
 - Use antivirus and security software to help detect and block phishing.

Activity 5: Practical exercises (10 minutes)

- Prepare several situations where students need to recognize whether a message or website is a phishing attempt.
- Ask students to participate in these exercises and decide whether the situation is safe or suspicious.
- Discuss the correct answers and justifications.

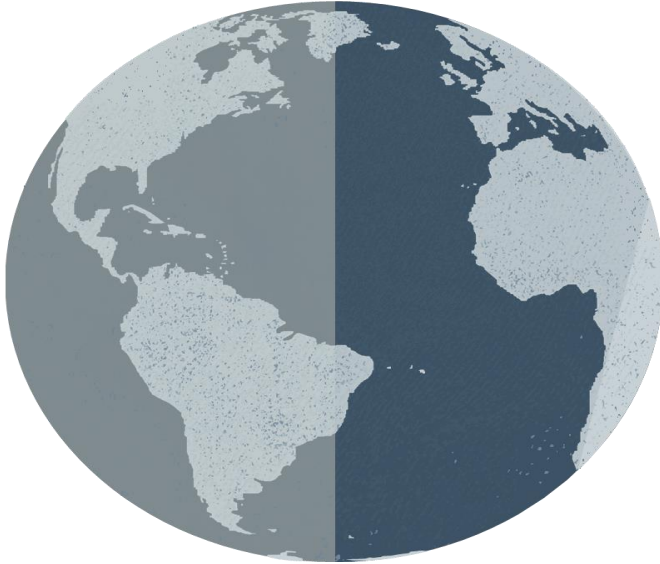
Activity 6: Summarize and reflect (5 minutes)

- Ask students to summarize the key points they learned from the lesson on phishing.
- Encourage students to reflect on how they can protect themselves and others from phishing.
- Thank students for their active participation in the lesson and emphasize the importance of caution and awareness when using the Internet.

It is important that the teacher is ready for students' questions and provides them with support in case of difficulties. Encourage students to ask questions and share their concerns or experiences about phishing.



iSafetyApp



TEACHING STUDENTS INTERNET SAFETY THROUGH
AN ARTIFICIAL INTELLIGENCE MOBILE APPLICATION



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

www.isafetyapp.eu