WP2 - PR.I.S.C.I.LLA EDUCATIONAL PROGRAMME FOR YOUTH WITH I.D.

Module 3: Potential Risks in using Social Media

Document Created by: EDRA

PR.I.S.C.I.LLA EDUCATIONAL PROGRAMME FOR YOUTH WITH I.D.	
Module 3: Potential Risks in using Social Media	
Module Summary	In this module, you will learn about the risks that can happen when using social media. These risks include cyberbullying (when people are mean to you online), grooming (when an adult pretends to be someone your age and tricks you into sharing pictures or engaging in intimate activities) and phishing (when someone tries to steal your identity or passwords). You will also learn how to spot these risks and how to stay safe while using social media. Risks can also happen in online games. In video games, people can chat with you and sometimes ask for personal information or say inappropriate things. The same safety rules apply.
Learning Outcomes of the module	By the end of this module, you will be able to: 1. Understand what cyberbullying, grooming, and phishing are. 2. Recognize situations where these risks might happen. 3. Learn tips and steps to stay safe from these risks.
Educational principles adopted	This module is designed to help you: ● Take positive risks by using social media safely. ● Feel in control of your online actions. ● Build your independence in using social media. ● Make safe choices with confidence

PR.I.S.C.I.LLA

Contents of the module	In the previous modules, we learned that social media is a space full of possibilities. It's a place where we can discover interesting information, share our thoughts and feelings on different topics, and connect with people who share our interests.

However, it's important to remember that the online world also has its risks. To enjoy social media safely, we need to understand these risks and learn how to protect ourselves from them. This way, we can make the most of our online experiences while staying safe.

Now we will introduce to you some of the most common risks: cyberbullying, grooming and phishing.

What is Cyberbullying?

Cyberbullying happens when people use social media or online platforms to send mean messages, post hurtful comments, or spread rumors. Cyberbullies often hide behind fake accounts.

Examples of Cyberbullying:

- Someone comments on your photo: "You look so weird! No one likes you."
- A group of people sends nasty messages in a group chat, making you feel excluded or upset, e.g. "Let's ignore her and not let her be part of the group anymore."
- Someone sends you a private message saying: "You're so stupid. Stop posting things online."

Practical tips to avoid cyberbullying

1. **Don't respond.** If someone sends you mean messages, don't reply.
2. **Save the evidence.** Take screenshots of mean messages or comments to show a trusted adult.
3. **Block and report.** Use the platform's tools to block the bully and report their behavior.
4. **Talk to someone you trust.** Share your feelings with a parent, teacher, or friend.
5. **Be kind online.** Treat others with respect to help create a positive online environment.

What is Grooming?

Grooming is when an adult uses the internet to manipulate and trick a young person into sharing

Case scenarios **Introduction**	Explain to participants that they will hear/read three different stories, each presenting a situation that took place online. These stories are designed to help them understand some of the risks they may encounter while using social media and the internet. After reading each story, guide the participants through a discussion by asking them specific questions. Encourage them to reflect on the situation, identify the risks involved, and think about the best ways to respond safely. The goal of this activity is to help participants recognize online dangers and develop strategies to protect themselves.
Case scenario 1	**The case of Lucia** Lucia is 19 years old and enjoys drawing. She often shares her artwork on social media. One day, someone sends her a message saying, "Hi! I love your drawings. You're so talented! Can we be friends?" Lucia feels happy and replies, "Thank you! Sure!" After a few days, the person starts asking Lucia personal questions like, "Where do you live?" and "Can you send me a picture of yourself?" They also tell Lucia, "Don't tell anyone about our chat—it's our secret." 1. What could happen if Lucia shares personal information with someone she doesn't know online? a) They might use the information to trick or harm her. b) They might become her best friend. c) Nothing; sharing personal information is always safe. 2. What should Lucia do when the person asks for her picture? a) Send it quickly to be polite. b) Say no and block the person.

	c) Ask the person why they need the picture. 3. If Lucia feels unsure about this situation, what is the best step to take? a) Talk to a trusted adult about the messages. b) Ignore her feelings and keep chatting. c) Ask her friends if they think it's okay.
Case scenario 2	**The case of Luca** Luca shares a funny photo of himself on social media. Someone comments, "You look so stupid!" and other people start laughing and writing mean things about him. Luca feels upset and doesn't know what to do. He wonders if he should delete his account or reply angrily to the comments. 1. What is the first thing Luca should do about the mean comments? a) Ignore the comments and take screenshots for evidence. b) Post a reply saying mean things back. c) Delete his account immediately. 2. Who should Luca talk to if he feels hurt by the comments? a) A trusted adult like a teacher, parent, or caregiver. b) The person who posted the comments. c) No one; he should keep it to himself. 3. What is a good way for Luca to handle cyberbullying in the future? a) Avoid sharing anything online again.

	b) Block and report the people who are being mean.
	c) Write a long post explaining how hurt he feels.
Case scenario 3	a) The email asks for her personal information.
	b) The email is written in a friendly tone.
	c) The email includes the name of the store.
	1. If Ana thinks this email is suspicious, what should she do?
	a) Report the email as phishing and delete it.
	b) Forward the email to her friends to check if it's real.
	c) Ignore the email but keep it in her inbox.
Additional Material	
Resources	

Activity of Module	
Name of the Activity	Risk spotting
Objectives	You will practice identifying potential risks in different online scenarios and discuss the appropriate actions we should take to stay safe.
Learning Methodologies	Learning by doing, Practical exercises and interactive activities
Time allocated for the Activity	30 minutes
Resources Needed	Cards with scenarios

	Paper and pens if you want to write down your answers.
Instructions	In this activity, you'll see pictures or hear short stories about things that might happen online. Your job is to:

In this activity, you'll see pictures or hear short stories about things that might happen online. Your job is to:

1. Decide if the situation is risky or safe.

2. Say why you think it is risky.

3. Explain what you would do to stay safe.

Example

Let's start with a simple example to help you understand how the activity works:

A stranger sends you a message saying, "You're so cool! Can we meet?"

Ask yourself:

- Is this risky?

- Why might it be risky?

- What should you do in this situation?

Answer:

Yes, this is risky because you don't know the person. They might not be who they say they are. You should ignore the message, block the person, and tell a trusted adult.

Now, you'll see different online situations. For each one, think carefully and answer the following questions:

- Is it risky or safe?

- Why do you think it is risky or safe?

- What would you do to stay safe?

PR.I.S.C.I.LLA

Scenario 1:
Someone online says: "I can help you get a lot of followers if you send me your password."

Scenario 2:
A friend posts a funny photo of you without asking first.

Scenario 3:
Someone comments on your post, "You're so ugly, everyone hates you."

Scenario 4:
You get an email that says, "Congratulations! You've won 1.000 €! Click here to claim your prize."

Scenario 5:

You are in an online group chat about your favorite video game. Someone in the chat asks, "What's your birthday? We want to celebrate it with you!"

Scenario 6:

You get a message from someone saying, "We are looking for people to work from home. Just send your name, address, and bank details to start!"

Scenario 7:

You take a group photo with your friends at a park and want to post it on social media. One of your friends says they don't want their picture online.

Scenario 8:

A stranger sends you a message saying, "You're so cool and pretty! I'd love to talk more. Can you tell me more about yourself?"

Sample answers

Sample answer scenario 1

- This is risky because they might use your password to take over your account.

- You should never share your passwords with anyone. Block the person and report them.

Sample answer scenario 2

- This could be risky because the photo might embarrass you or share private information.

- You should ask your friend to delete the photo and explain why it's important to ask for permission.

Sample answer scenario 3

- This is cyberbullying because the comment is mean and could hurt your feelings.

- You should take a screenshot of the comment, block the person, and tell an adult you trust.

Sample answer scenario 4

- This is risky because it's probably a phishing scam to steal your personal information.

- You should delete the email and report it as spam. Never click on links from emails like this

Sample answer scenario 5
- This is risky because sharing your birthday in a public chat can lead to identity theft or unwanted contact.
- You should avoid giving out personal details like your full birthday in public spaces. If someone asks, politely say you don't share personal information online.

Sample answer scenario 6

- This is risky because it's likely a scam designed to steal your personal or financial information.
- You should delete the message immediately and report the sender. Never share sensitive information like your address or bank details with people you don't know.

Sample answer scenario 7

- This is safe only if you respect your friend's wishes and don't post the picture. Ignoring their request would not be safe or kind.
- You should make sure to ask everyone in the photo for permission before posting it online. If someone says no, choose a different photo or don't post at all.

Sample answer scenario 8

- This is risky because strangers who give compliments might be trying to groom you or gain your trust for unsafe reasons.
- You should not respond to the message. Block the person immediately and tell a trusted adult about what happened.

Reflection

After finishing the scenarios, take some time to think about what you've learned.

Ask Yourself:

- Which risk surprised you the most?

- How did you feel deciding what to do in each situation?

- What will you do differently next time you're online?

	Talk with the group or your teacher about your answers. Sharing your thoughts can help you feel more confident about staying safe online.
	Conclusion
	You've done a great job spotting risks and thinking about how to stay safe online. Remember:
	✔ If something feels wrong online, trust your feelings.
	✔ Don't share personal information or passwords with people you don't know.
	✔ Always talk to someone you trust if you're unsure about a situation.

Activity of Module	
Name of the Activity	Role-playing
Objectives	You will practice how to respond to different online risks by acting out situations in small groups. This activity will help you feel more confident about what to do if you face these risks in real life. You'll Learn: ✔ How to respond to common online risks. ✔ How to make smart, safe choices when something feels wrong. ✔ How to ask for help when you need it.
Learning Methodologies	Role play

Time allocated for the Activity	30-40 minutes
Resources Needed	- Scenario cards or printed sheets with the scenarios. - A safe space for small groups to role-play.
Instructions	You'll work in small groups to act out different situations. Each group will receive a scenario about an online risk. One person will act as the person facing the problem, and the others will play different roles, like a friend, the risky person, or a trusted adult. After acting out the scenario, we'll talk about what happened and how to handle it. **Scenario 1** **Story:** Someone online says, "You're so talented! Can I see more pictures of you? I promise I won't share them with anyone." **Roles:** - Person being asked for pictures. - The stranger. - A trusted adult or friend the person talks to for advice. **Action Steps:** - Refuse to send pictures. - Block the stranger. - Talk to the trusted adult about what happened.

Scenario 2

- **Story:** Someone comments on your post, "This is so dumb. Why do you even bother?" Other people start liking the comment and writing mean things too.

- **Roles:**

  o   The person being bullied.

  o   The bully.

  o   A trusted adult or friend the person talks to.

- **Action Steps:**

  o   Do not reply to the mean comments.

  o   Take screenshots as evidence.

  o   Block and report the bully.

Scenario 3

- **Story:** You get an email that says, "Congratulations! You've won a new phone! Click this link to claim your prize."

- **Roles:**

  o   The person receiving the email.

  o   The scammer who sent this e-mail.

  o   A friend or trusted adult giving advice.

- **Action Steps:**

  o   Do not click the link.

  o   Delete the email and report it as spam.

o   Talk to a trusted adult if you're unsure.

Discussion

After each group has acted out their scenario, come together as a large group to discuss:

- What made the situation risky?
- What did the person do to stay safe?
- How did it feel to practice this situation?
- What would you do if this happened to you in real life?

Conclusion

You've done an excellent job practicing how to handle online risks! Remember:

- Always trust your instincts—if something feels wrong, it probably is.

- Block and report people who make you uncomfortable.

- Talk to a trusted adult if you're unsure about what to do.

Activity of Module	
Name of the Activity	Risk Sorting Game
Objectives	You will practice identifying safe and risky online behaviors by sorting examples into "Safe" or "Risky" categories.

Learning Methodologies	Practical exercises and interactive activities
Time allocated for the Activity	20 minutes
Resources Needed	● Cards with online actions. ● Two labeled areas: "Safe" and "Risky" (on a board or table).
Instructions	Let's test what you've learned about online risks! In this activity, you'll see examples of things people might do online. Your task is to decide whether each example is "Safe" or "Risky." You'll work in pairs or small groups. Each group will receive cards with examples of online actions. Your job is to place each card into the "Safe" or "Risky" category on the board or table. After sorting the cards, we'll discuss your choices as a group. Let's try an example together: **Example Card:** "Sharing your full name and address in your profile." Is it Safe or Risky? **Answer:** Risky. Sharing personal information can make you vulnerable. Now it's your turn! Here are the cards you need to sort: ● "Accepting a friend request from someone you don't know." ● "Posting a picture of your favorite hobby."

	● "Clicking on a link from an email that says you've won a prize." ● "Blocking someone who sends you mean messages." ● "Sharing your phone number in a public post." ● "You get a friend request from someone with no profile picture and no posts on their account." ● "You share a photo of your favorite book with no other personal details." ● "You receive a message saying, 'Send me your location so we can hang out!' from someone you don't know." ● "You post a picture of your school's name on social media." ● "Your friend tells you they're being bullied online, and you encourage them to talk to a trusted adult."

Sample answers:

1. "Accepting a friend request from someone you don't know."

Answer: Risky. Accepting requests from people you don't know can be unsafe because they might not be who they say they are. Always make sure you only connect with people you trust.

2. "Posting a picture of your favorite hobby."

Answer: Safe. Sharing your interests, like a picture of your favorite hobby, is fine as long as it doesn't include private details like your location or school name.

3. "Clicking on a link from an email that says you've won a prize."

Answer: Risky. This is likely a phishing scam. Clicking on the link could give scammers access to your information

or harm your device. Delete the email and don't click the link.

4. "Blocking someone who sends you mean messages."

Answer: Safe. Blocking someone who is mean to you online is a smart way to stop the negativity. It's also important to report their behavior and tell a trusted adult.

5. "Sharing your phone number in a public post."

Answer: Risky. Sharing your phone number in a public post is unsafe because anyone can use it to contact you or find out personal details. Keep your phone number private and only share it with people you trust directly.

6. "You get a friend request from someone with no profile picture and no posts on their account."

Answer: Risky. Accepting requests from unknown or suspicious accounts can lead to unsafe interactions.

7. "You share a photo of your favorite book with no other personal details."

Answer: Safe. Sharing general interests without revealing private information is okay.

8. "You receive a message saying, 'Send me your location so we can hang out!' from someone you don't know."

Answer: Risky. Sharing your location with strangers can be dangerous.

9. "You post a picture of your school's name on social media."

Answer: Risky. Sharing your school's name can help strangers figure out where to find you.

10. "Your friend tells you they're being bullied online, and you encourage them to talk to a trusted adult."

Answer: Safe. Supporting a friend and helping them seek help is the right action to take.

Discussion

After sorting the cards, discuss your answers with the group.

- Did everyone agree on which actions were risky?

- What made some actions safer than others?

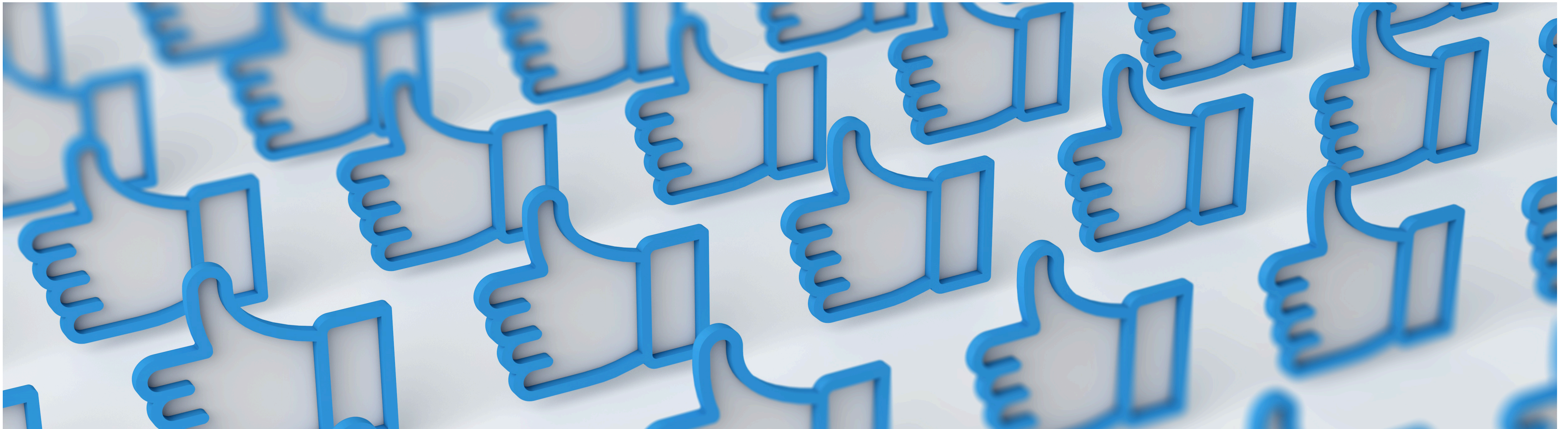- How can you remember to stay safe in similar situations?

Conclusion

Great job sorting the risks! Now you know how to spot safe and risky behaviors online. Remember, when in doubt, always ask a trusted adult.

A stranger sends you a message saying, "You're so cool! Can we meet?

PR.I.S.C.I.LLA
Preventing Incident of Sexual Cyberbullying
in Intellectual disability

Someone online says: "I can help you get a lot of followers if you send me your password."

A friend posts a funny photo of you without asking first.

Someone comments on your post, "You're so ugly, everyone hates you"

You get an email that says, "Congratulations! You've won 1.000 €! Click here to claim your prize

You are in an online group chat about your favorite video game. Someone in the chat asks, "What's your birthday? We want to celebrate it with you!"

You get a message from someone saying, "We are looking for people to work from home. Just send your name, address, and bank details to start!"

You take a group photo with your friends at a park and want to post it on social media. One of your friends says they don't want their picture online.

Funded by
the European Union

PR.I.S.C.I.LLA
Preventing Incident of Sexual Cyberbullying
in Intellectual disability

A stranger sends you a message saying, "You're so cool and pretty! I'd love to talk more. Can you tell me more about yourself?"

Scenario card 1:

Story: Someone online says, "You're so talented! Can I see more pictures of you? I promise I won't share them with anyone."

Roles:
- Person being asked for pictures.
- The stranger.
- A trusted adult or friend the person talks to for advice.

Action Steps:
- Refuse to send pictures.
- Block the stranger.
- Talk to the trusted adult about what happened.

Funded by
the European Union

PR.I.S.C.I.LLA
Preventing Incident of Sexual Cyberbullying
in Intellectual disability

Scenario card 2:

Story: Someone comments on your post, "This is so dumb. Why do you even bother?" Other people start liking the comment and writing mean things too.

Roles:
- The person being bullied.
- The bully.
- A trusted adult or friend the person talks to.

Action Steps:
- Do not reply to the mean comments.
- Take screenshots as evidence.
- Block and report the bully.

Scenario card 3:

Story: You get an email that says, "Congratulations! You've won a new phone! Click this link to claim your prize."

Roles:
- The person receiving the email.
- The scammer who sent this e-mail.
- A friend or trusted adult giving advice.

Action Steps:
- Do not click the link.
- Delete the email and report it as spam.
- Talk to a trusted adult if you're unsure.