MODULE 3

POTENTIAL RISKS IN USING SOCIAL MEDIA

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

1

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**

⚠ **Grooming**

⚠ **Phishing**

You will also learn how to spot these risks and how to stay safe while using social media.

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 protect yourself from these risks.

4

Module Summary

This module is designed to help you:

○ Take positive risks by using social media safely

○ Feel in control of your actions online

○ Build your independence in using social media

○ Make safe choices with confidence

Cyberbullying

It 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.

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.

Grooming

It happens when an adult uses the internet to manipulate and trick a young person into sharing personal information, sending private photos, or engaging in unsafe behaviors.

Tips to avoid grooming

1. **Do not share personal information.** Never give out your address, phone number, school name, or passwords.

1. **Be careful with photos.** Don't send your pictures to people you don't know.

1. **Trust your feelings.** If someone online makes you feel uncomfortable, stop talking to them.

1. **Talk to a trusted adult.** If you feel unsure about someone online, tell a parent, teacher, or caregiver.

1. **Block and report.** Use the platform's settings to block the person and report their behavior.

Phishing

It happens when someone pretends to be a trusted person or company to steal your information, such as passwords, account details, or money. They often use fake emails, messages, or websites to trick you.

Tips to avoid phishing

1. **Don't click on unknown links.** If you receive a message or email from someone you don't trust, ignore it and don't click on any links the message contains

1. **Check the sender.** Look closely at the sender's email address or username. Fake messages often have small spelling mistakes.

1. **Keep your passwords safe.** Never share your passwords with anyone.

1. **Be careful with prizes.** If someone says you've won something amazing, but it feels strange or too easy, it's probably not real.

1. **Use secure websites.** Make sure a website name starts with "https://" and shows a padlock symbol.

2

Case scenarios

Now we will read three on-line situations that will help you to understand some of the risks you may encounter while using social media and the internet.

After reading each story we will 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 you recognize online dangers and develop strategies to protect yourself.

Lucia's case

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."
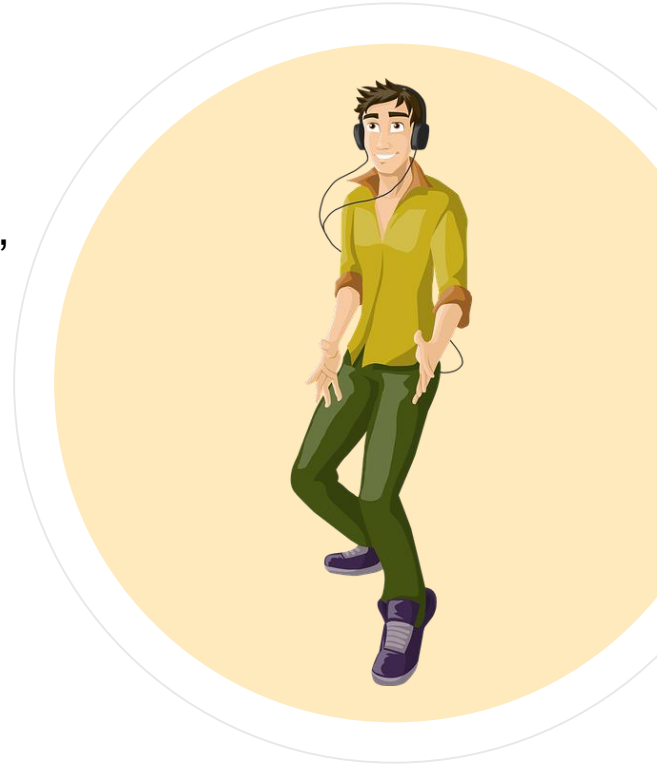
Lucia's case – let's discuss

1. What could happen if Lucia shares personal information with someone she doesn't know online?

2. What should Lucia do when the person asks for her picture?

3. If Lucia feels unsure about this situation, what is the best step to take?
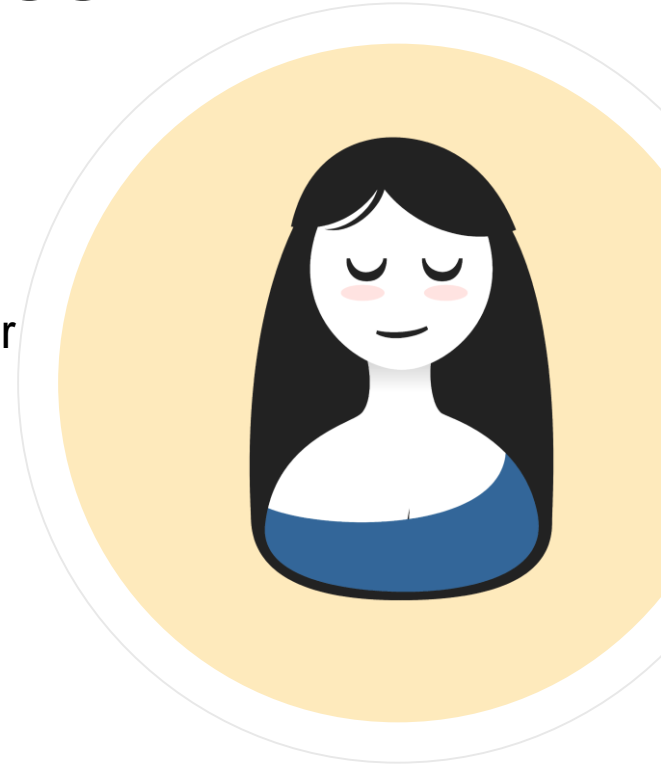
Luca's case

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.
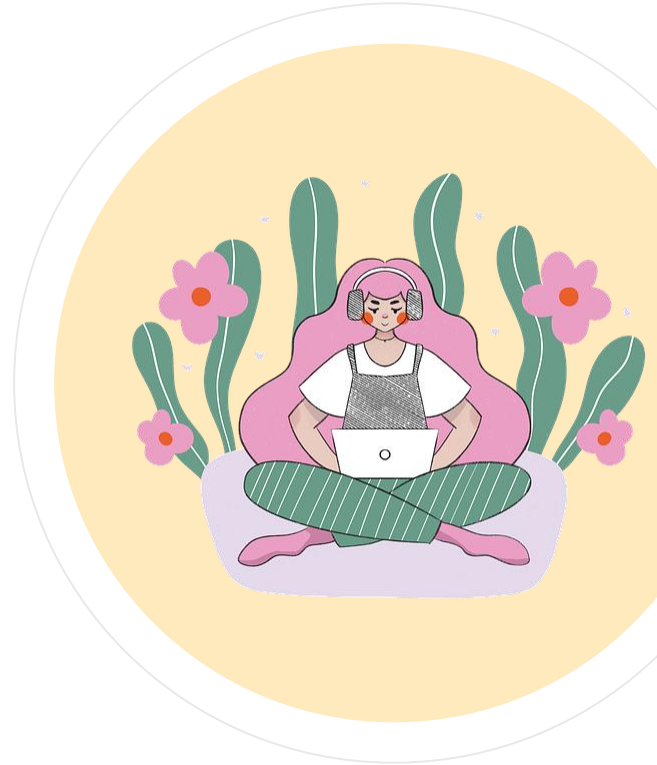
Luca's case – let's discuss

1. What is the first thing Luca should do about the mean comments?

2. Who should Luca talk to if he feels hurt by the comments?

3. What would be a good way for Luca to handle cyberbullying in the future?

Ana's case

Ana receives an email that looks like it's from her favorite online store. The email says, "Congratulations! You've won a 50 € gift card! Click here to get your prize." Ana is excited, but she isn't sure if it's real. She notices the email address looks strange and the link doesn't match the store's website.

Ana's case – let's discuss

1. What should Ana do before clicking the link?

2. What is a warning sign that this email might be fake?

3. If Ana thinks this email is suspicious, what should she do?
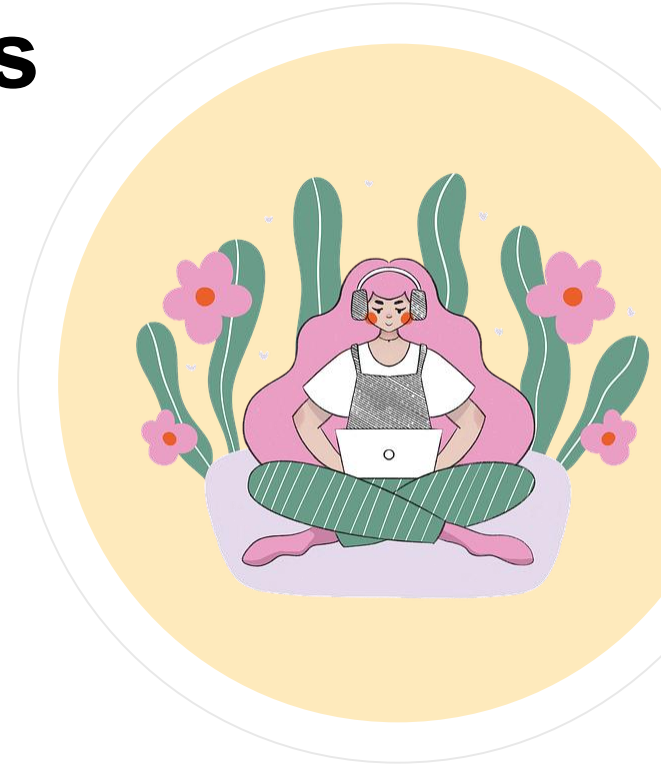
Activity: risk spotting

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

- ✅ Decide if the situation is risky or safe.
- ✅ Say why you think it is risky.
- ✅ Explain what you would do to stay safe.

Example

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?
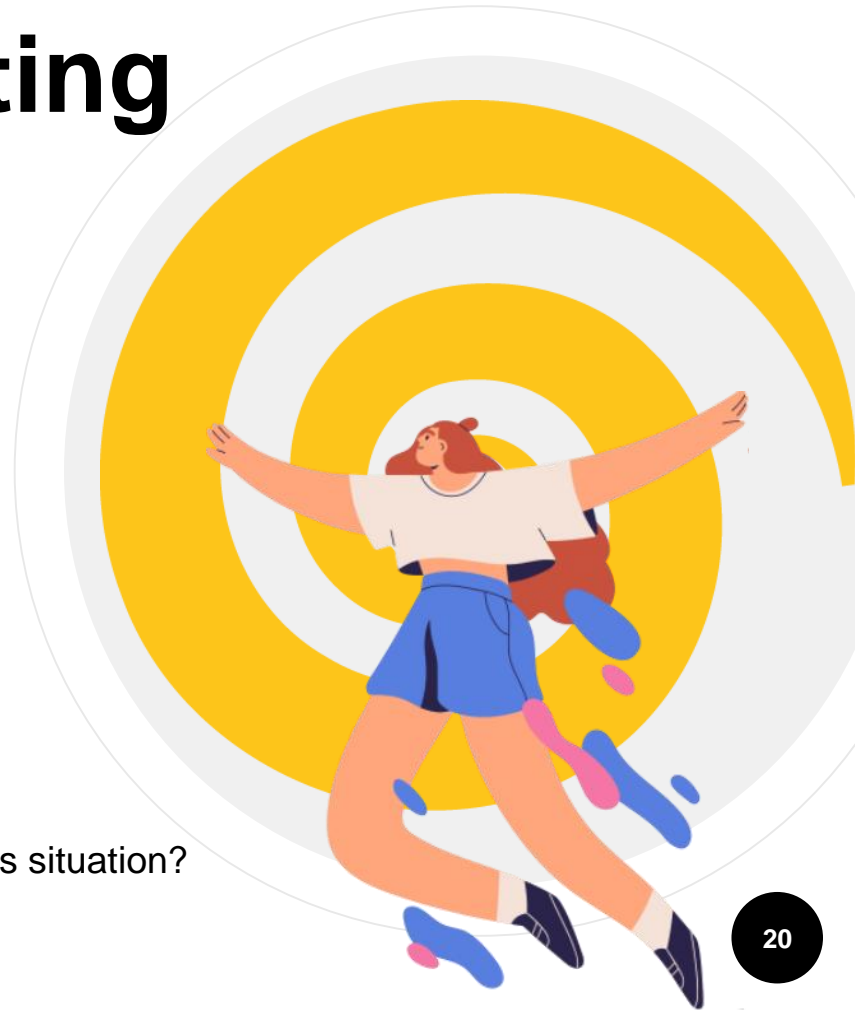
Risk spotting Scenarios

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?"
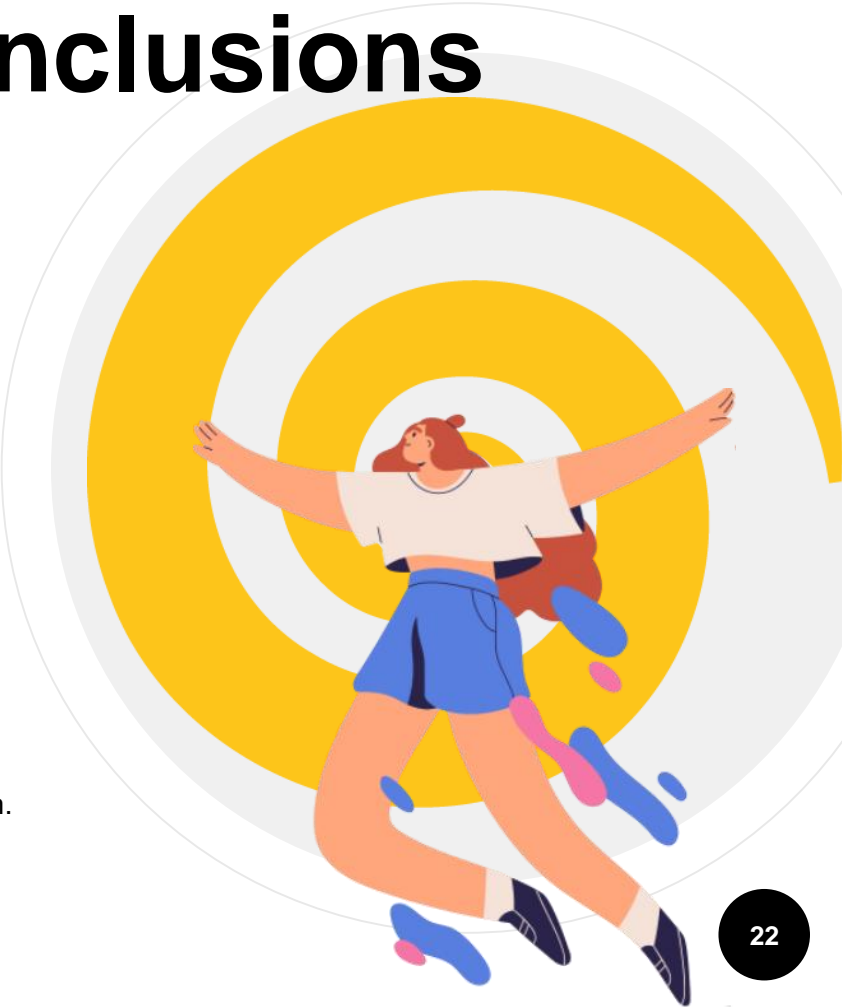
Reflections and conclusions

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.

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.

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

Co-funded by
the European Union

Role-playing

In this activity you will practice how to respond to different online risks by acting out situations in small groups. It will help you feel more confident about what to do if you face these risks in real life.

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

Situation: 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 a trusted adult about what happened.

Scenario 2

Situation: 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 3

Situation: 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 on the link.
- Delete the email and report it as spam.
- Talk to a trusted adult if you're unsure.

Discussion and Conclusion

Discussion

After having acted out the scenario, let's 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.
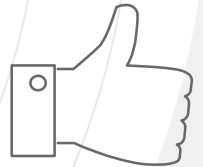
Risk Sorting Game

We will practice identifying safe and risky online behaviors by sorting examples into "Safe" or "Risky" categories.

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".

We will 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.

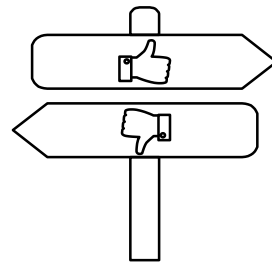After sorting the cards, we'll discuss our choices as a group.
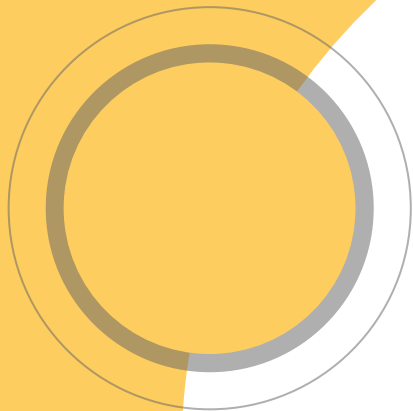
Risk Sorting Game

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!

ThankYOU