



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

Budapest Engineering Vocational Training Centre
Öveges József Technical Secondary Grammar and Vocational School
Building 1: H-1117 Budapest Fehérvári út 10.
Building 2: H-1118 Budapest, Beregszász út 10.
www.oveges.hu
Tel/fax: +36 1 246 15 78



“New Generation Promoting Sustainable Development Goals”
2024-2-FI01-KA210-SCH-000294712
Small-scale partnerships in school education
“New Generation Promoting e-Safety” LTTA
04th – 08th May 2026, Budapest, Hungary

Role-plays, discussion topics and games for Promoting eSafety

1. Role-plays

1.1 Role-play

Topic: Phishing

Roles:

- user
- hacker
- IT security expert

Situation: The user receives an email that appears to come from a bank. The hacker tries to convince them to click the link. The IT expert helps identify the danger.

Questions for the user role:

- Who sent this email? Is it really the bank?
- Why are they asking me to click the link immediately?
- What happens if I provide my banking details?
- How can I check whether the email is real or fake?
- What should I do if the message seems suspicious?

Questions for the hacker role:

- How can I make the user believe the email is from the bank?
- What urgent message can I use to get the user to click?
- What data am I trying to obtain?
- What happens if the user provides their password or bank card details?
- How do I make the fake website look authentic?

Questions for the IT security expert role:

- What signs indicate a phishing email?

- What should be checked in a suspicious message?
- What should the user do if they receive such an email?
- How can banking data be protected?
- Why is clicking on the link dangerous?

Discussion questions:

- What signs help identify a fake email?
- What should the user have done?
- How can such attacks be prevented?
- What did the user learn from this situation?
- Why is online security important?
- How can an IT security expert help in such cases?

1.2 Role-play

Topic: Uploading a photo without permission

Related topic: Right to privacy

Roles:

- student who uploads a photo
- person appearing in the photo
- teacher or moderator

Situation: Someone uploads a group photo to a social media site without asking others.

Questions for the student uploading the photo:

- Why did you upload this photo to social media?
- Did you ask the people in the photo for permission?
- Did you know this could violate others' right to privacy?
- What would you do if someone uploaded a photo of you without permission?
- What do you think you should do now?

Questions for the person in the photo:

- How did you feel when you saw the photo online?
- Did anyone ask for your consent before uploading it?
- Why is it important for you to decide what images of you appear online?
- What would you like to happen to this photo?
- What advice would you give others in a similar situation?

Questions for the teacher or moderator:

- Why is permission important when sharing images?
- What rules apply to publishing photos of others?
- How can such situations be prevented in school or online communities?
- What should someone do if they upload a photo without permission?
- How does this relate to the right to privacy?

Group discussion questions:

- Why is it important to respect others' privacy online?
- What consequences can sharing a photo without permission have?
- What should always be asked before uploading a photo?
- How can social media (e.g., Instagram or Facebook) be used responsibly?

1.3 Role-play

Topic: Cyberbullying in a class group chat

Roles:

- bully
- victim
- classmate
- teacher

Situation: A student is being mocked in a group chat.

Questions for the bully:

- Why did you post the offensive message?
- Did you know it could hurt the victim?
- How do you think the victim feels?
- What could you do differently to avoid hurting someone online?
- Do you know the consequences of cyberbullying?

Questions for the victim:

- How did you feel when you saw the messages?
- Did you have someone you trusted to ask for help?
- What would you like to happen regarding the bullying?
- What could help you feel less alone?
- What advice would you give to others in a similar situation?

Questions for the classmate:

- What did you see in the chat, and how did you feel?
- What can you do if you witness cyberbullying?
- How can you support the victim?
- How can you report the situation to a teacher or parents?
- Why is it important not to participate, even if it seems funny?

Questions for the teacher:

- How can you recognize signs of cyberbullying?
- What can you do if a student becomes a victim?
- How can such situations be prevented in class groups?
- How can respectful online communication be taught?
- What rules should be introduced in the group?

Group discussion questions:

- What did you learn from the victim's perspective?
- How can we communicate safely and respectfully online?

- What can be done to prevent group chats from becoming harmful?
- What roles do teachers and classmates play in prevention?
- How does cyberbullying relate to digital rights and data protection?

1.4 Role-play

Topic: Password cracking – Strong passwords

Roles:

- user
- hacker
- security expert

Situation:

The user uses a weak password (e.g., birth date), which the hacker easily guesses.

Questions for the user:

- Why did you choose your birth date as a password?
- Did you know weak passwords are easy to crack?
- What could happen if someone accesses your account?
- What could you do to create a stronger password?
- How do you remember more complex passwords?

Questions for the hacker:

- Why are weak passwords easy to crack?
- How do you find weak passwords?
- What consequences can password cracking have for the victim?
- How are stolen passwords used in real life?
- What advice would you give users to avoid attacks?

Questions for the security expert:

- What makes a password strong and secure?
- What rules do you recommend for creating passwords?
 - o Example: uppercase, lowercase, numbers, special characters
- How does multi-factor authentication help protect accounts?
- What should a user do if they suspect their password has been leaked?
- What tools can be used for secure password management?

Group discussion questions:

- Why is it important to use strong passwords for all accounts?
- What is a “weak password” and why is it dangerous?
- How can you remember multiple strong passwords without writing them down?
- What did you learn about risks from the hacker role?
- How does password protection relate to digital rights and data protection?

2. Discussion topic: Digital footprint

Questions for the group:

- What does the information we leave online reveal about us?
- Can anything be completely deleted from the internet?
- How can this affect our future careers?

Basic questions:

- What does “digital footprint” mean?
- What online activities leave traces?
- What is the difference between active and passive digital footprints?

Social media and digital footprint:

- What data do you share on social media (e.g., Instagram, Facebook)?
- How can your digital footprint affect your reputation?
- What should you consider before posting a photo or comment?

Security and data protection:

- Why is it dangerous to share too much personal information?
- How can you reduce your digital footprint?
- What role do multi-factor authentication and strong passwords play?

Practical examples:

- If you upload a photo, what information remains about you?
- What do IP addresses and cookies reveal about your habits?
- What can you do to “clean up” your digital footprint?

Thought-provoking questions:

- How can your digital footprint affect job or university applications?
- How can you be present online safely without disappearing completely?
- How does digital footprint relate to your right to privacy?

3. Quick game – “Safe or Dangerous?”

- “My password is my birth date.”
- “I click on unknown links in emails.”
- “I ask my friend before uploading their photo.”
- “I use the same password for all accounts.”
- “My password includes uppercase, lowercase, numbers, and symbols.”
- “I make all my social media data public, including my address and phone number.”
- “I only share photos with friends and adjust privacy settings.”
- “I open an email claiming to be from my bank and click the link.”
- “I double-check URLs before clicking.”
- “I give my real name and address in an online game.”
- “I use strong passwords and enable two-factor authentication.”
- “Someone sends an offensive message, and I reply offensively.”
- “I don’t share others’ photos without permission.”

- “I enter all my data on public Wi-Fi, including banking details.”
- “I update my computer and phone security software.”
- “I upload a group photo without permission.”
- “I think before commenting to avoid hurting others online.”