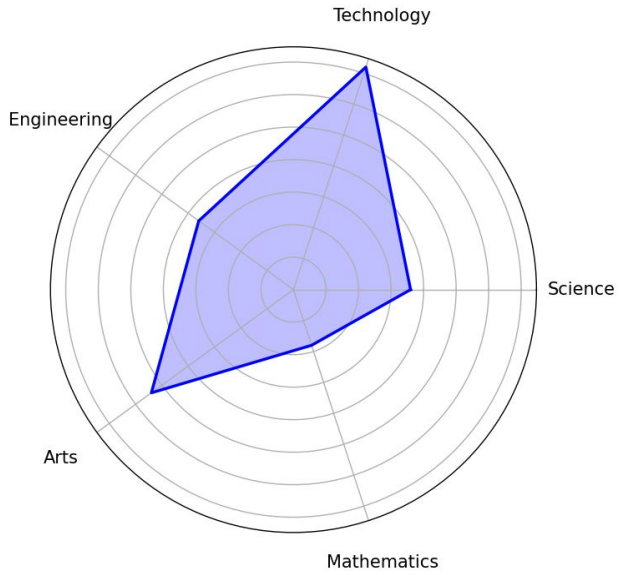
Curricular



Digital Risk Map

Duration	Age	Difficulty
45 min	17-18	Medium
#VISUALCREATIVITY #TECHNOLOGY #DIGITALCITIZENSHIP		

DESCRIPTION

In this curricular activity, students will identify and analyze common digital risks, such as phishing, malware, ransomware, and identity theft, visually representing them in groups.
Students are encouraged to critically reflect on their digital lives, explore prevention solutions, and communicate these ideas to the school community through creative visual maps.
The final product will be physically displayed at the school and, optionally, disseminated digitally. Students are also invited to reflect on the influence of traditional advice on digital security, and may incorporate popular proverbs into their representations.

ACTIVITY OBJECTIVES

- **Understand the concept of digital risks and its consequences.**
- **Work on digital citizenship and visual thinking skills.**
- **Visually represent digital threats and prevention strategies.**
- **Encourage female participation and leadership in technological activities.**
- **Communicate solutions clearly, inclusively and culturally contextualized for the entire school community.**

KEY COMPETENCES (EU)

- Digital competence
- Social and civic competence
- Cultural awareness and expression
- Competence to learn how to learn

Funded by the European Union

MATERIALS

Cardboards or A3 sheets

Support sheetswith examples of digital risks

Video

Colored pens

- Provided by students
- Provided by the teacher/institution
- Downloadable Elements

PREVIOUS PREPARATION

- Showing a short video with examples of real online frauds (MB Way scams, email phishing, etc.)
  Formation of groups of 4 to 6 students ensuring diversity and gender balance
- Delivery of tokens with visual vocabulary (e.g. “phishing”, “malware”, “social engineering”)
- Provocative question: “Have you ever felt like your data was at risk?”

CONTEXTUALIZATION AND ADAPTATION

Today we use the internet for everything: talking to friends, studying, shopping. But... are we really safe online?

The teacher starts with a video (https://www.youtube.com/watch?v=mxOcGFRXVLY) to present a real case of digital fraud.

Then the students reflect on questions such as:

1. Have you ever received strange messages on social media?
2. Can you identify?an attempt to steal data?
3. Have you ever thought, "That won't happen to me"?

The goal is to link the topic to the students' reality, show that these risks are current and close, and prepare the ground for them to create a visual map with the main cybersecurity risks and solutions, designed to inform and protect the school. Traditional proverbs about precaution and security (e.g.: "Prevention is better than cure") can be included as a starting point for the connection between popular knowledge and modern cybersecurity.

Funded by the European Union

Watch video 📽️ - ""What is Phishing and how to protect yourself"

★ *Link: https://www.youtube.com/watch?v=mxOcGFRXVLY*

Watch video 📽️ - "Rasomware work"

★ *Link: https://www.youtube.com/watch?v=Vu3xhTMFXmc*

Classroom activity 💡

In small groups, students analyze simulated suspicious messages (e.g., SMS, emails, social media messages) and discuss:
"How can we identify that this is a digital fraud?"
Each group presents an example to the class and explains the warning signs they found.

Note for the teacher 📝

Ensure that all students, especially girls, actively participate in both technical tasks and leadership roles. This approach promotes inclusion, combats stereotypes, and reinforces gender equity in STEAM activities.

Funded by the European Union

ACTIVITY

Introduction (10 min)

1. The professor shares a short video about real digital scams (https://www.youtube.com/watch?v=mxOcGFRXVLY).

2. Based on the video, an informal conversation is promoted with open questions:
   - ✓ Have you ever received a suspicious message?
   - ✓ Do you know what "phishing" is? How did you identify it?
   - ✓ How do you manage and protect your passwords?
   - ✓ Do you think all social groups are equally protected online?

Objective: activate prior knowledge, promote critical thinking and create an emotional connection with the topic.

Risk selection and planning (5 min)

Each group chooses (or is given) 1-2 digital risks to explore.

They use tokens to define:

- What is the risk?
- A practical example (real or invented)
- How can it be prevented?

Funded by the European Union

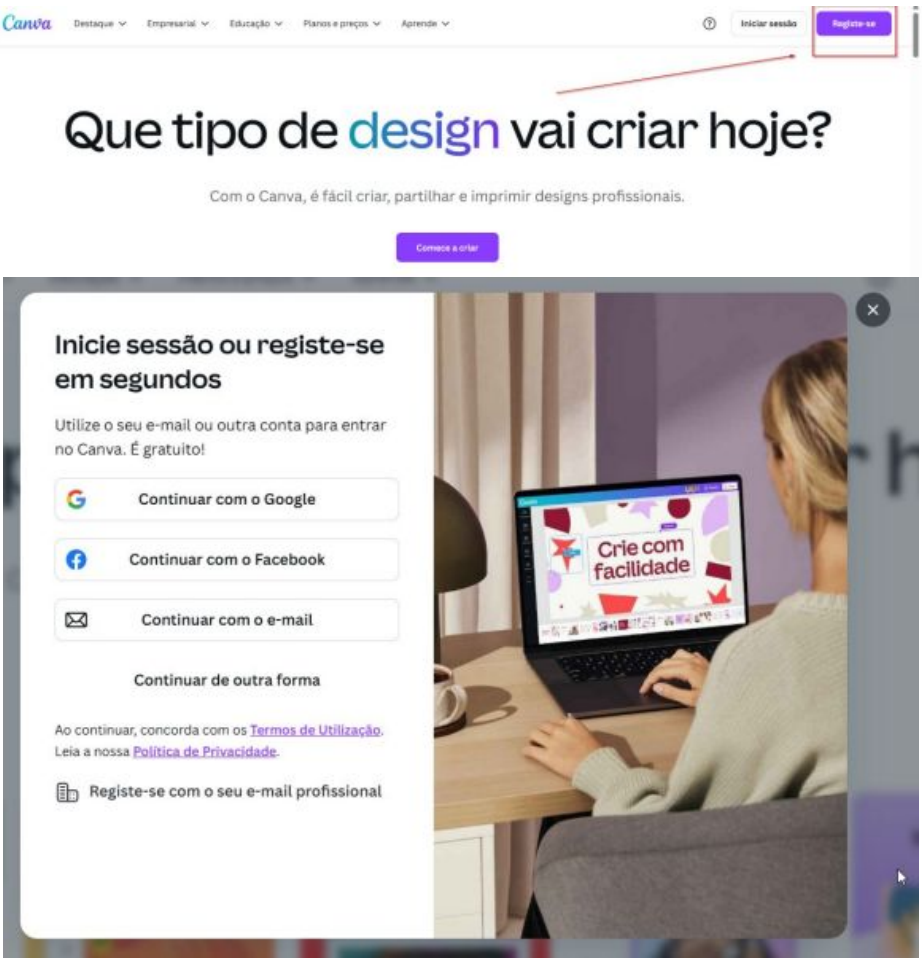
Construction of the visual map (15 min)

Using the CANVA platform, they aim to create an infographic about one of the risks they have identified. They should take into account:

- Name
- Icons or illustrations (representing different genders and cultures)
- Clear and short explanation
- Prevention tip(s)
- Awareness message

CANVA REGISTRATION

1. Access to: https://www.canva.com/pt_pt/
2. Click on “Register” (top right corner).

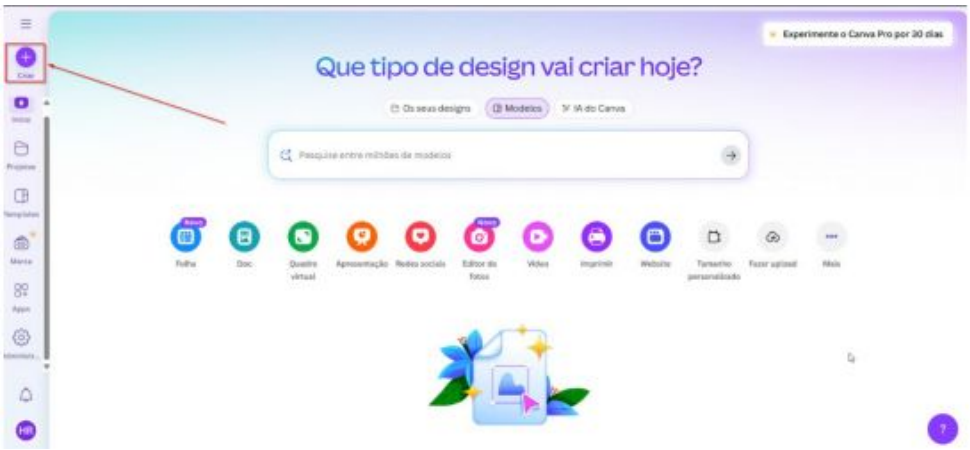


3. You can use in the registration:
   - Google account (e.g. school account)
   - Email and password

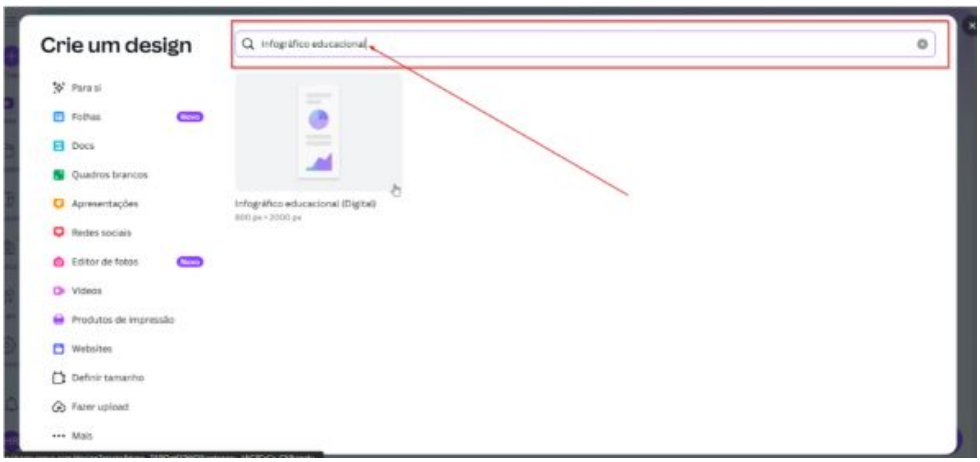
4. Check your email to confirm your account.

CREATE A DESIGN

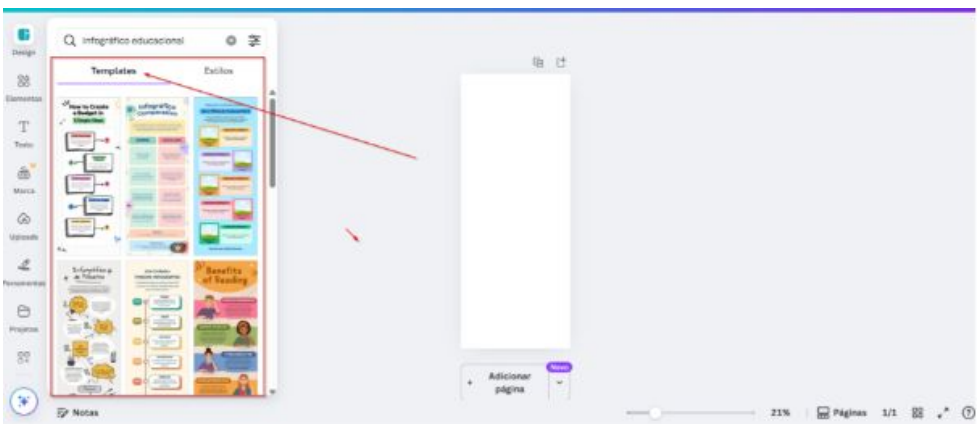
1. After logging into your account, click on “Create a design”



2. You will have several options, search for “Educational infographic”.

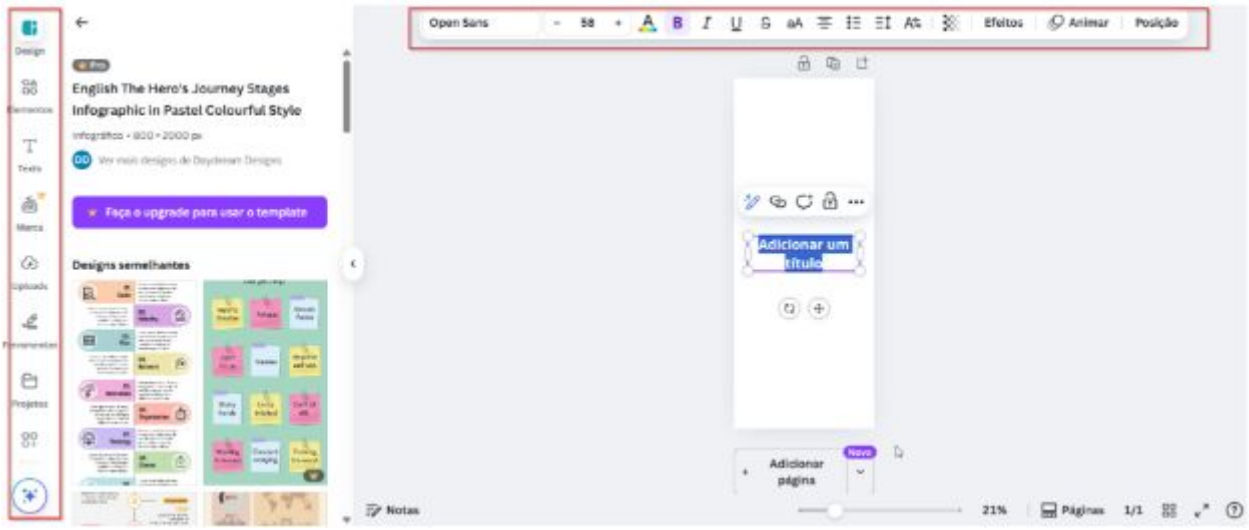


3. You will have several templates that you can choose and edit, choose a template to use in a group



4. You can use existing templates but you will need to activate the 30-day free trial option:

5. Or create your template from scratch using the tools found on the platform:



6. You must present the following content in a clear and attractive manner:

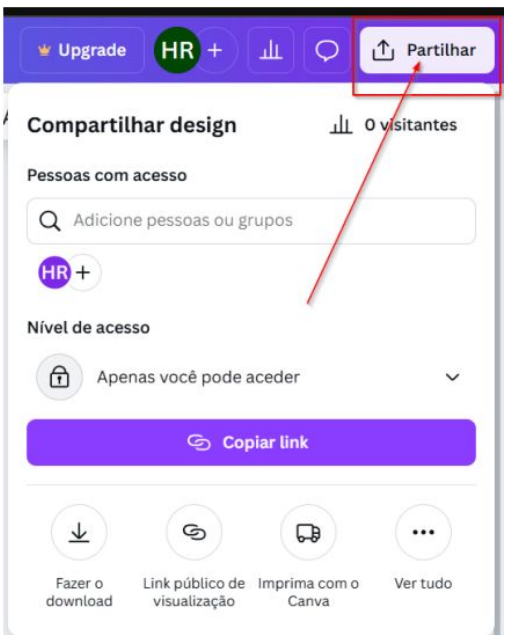
- ✓ Name
- ✓ Icons or illustrations (representing different genders and cultures)
- ✓ Clear and short explanation
- ✓ Prevention tip(s)
- ✓ Awareness message

Funded by the European Union

Example card:

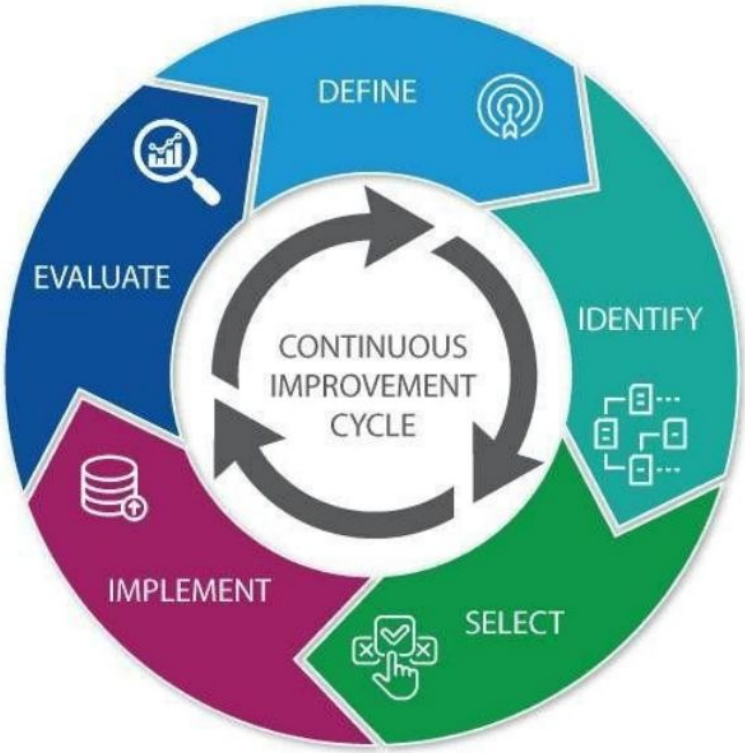
Presentation and sharing (10 min)

1. Exchange the map with another group to get structured feedback

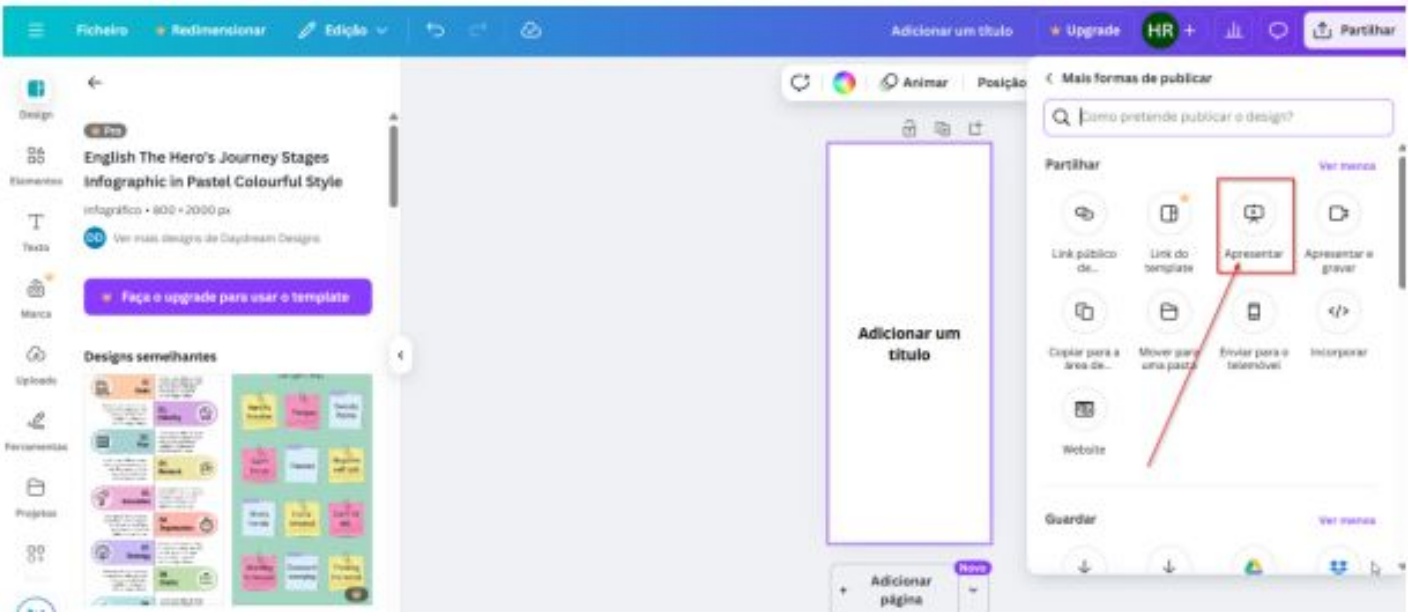


Funded by the European Union

2. Based on feedback, implement opportunities for improvement in design or content.



2. Use the “Present” function to present your work in class.



CONCLUSION AND SHARING

1. After presenting the maps, lead a final reflection with the whole class:
   - What was the most surprising or unknown risk for you?
   - How can you apply what you've learned to your digital life?
   - What advice would you give to a younger family member or colleague now?

2. Then, it promotes the sharing of work:
   - Infographics can be posted on school bulletin boards (corridors, library, ICT room)

Optionally, students can create a short awareness message (slogan) to accompany the infographic, such as: “Don’t fall into the net: think before you click.”

Don’t forget to take a photo of your experience and share it with us!

LinkedIn Instagram X

Funded by the European Union

PROJECT EVALUATION

Activity Objectives	Key Competences (EU)	Evaluation Criteria
Understand the concept of digital risks and their consequences	Digital competence and competence in science and technology	The student correctly identifies at least two types of digital risks and describes their consequences clearly.
Develop visual thinking and communicate solutions creatively	Cultural awareness and expression	The map created features a clear, creative visual design with relevant and accessible messages for the school audience.
Represent threats and prevention strategies collaboratively and inclusively	Social and civic competence	The student actively participates in the group, respects different opinions and contributes to the creation of the content and visual aspect of the map.
Promote female leadership and participation in technological and creative tasks	Social and civic competence	Girls and boys participate in all roles in the group, including technical, creative and presentation tasks.
Linking traditional knowledge to digital literacy	Sense of initiative and entrepreneurship	The group includes cultural/traditional references (e.g. proverbs) and explains how they relate to modern digital security.

BIBLIOGRAPHY AND REFERENCES

- CERT.pt – National Cybersecurity Center —https://www.cncs.gov.pt
- YouTube: https://www.youtube.com/watch?v=mxOcGFRXVLY
- STEAMbrace Instagram: https://www.instagram.com/steambrace_eu/

Funded by the European Union