ERASMEDIAH – EDUCATIONAL REINFORCEMENT
AGAINST THE SOCIAL MEDIA HYPERCONNECTIVITY
PROJECT NUMBER: 2023-1-HU01-KA220-YOU-000161173

MODULE 5

CYBERSECURITY AND ONLINE SAFETY

ERASMEDIAH
Educational Reinforcement Against
the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Lesson 5.1

Introduction to Cybersecurity Fundamentals

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Duration: 40 minutes

Lesson 5.1

Introduction to Cybersecurity Fundamentals

Objectives:

- To develop a clear understanding of the core concepts of cybersecurity, including key terms like threats, vulnerabilities, and risks.
- To identify prevalent online threats such as phishing, malware, ransomware, and social engineering attacks, and understand their impact.
- To foster a proactive mindset toward identifying and responding to potential cybersecurity incidents.

Key Message(s):

- Whether you're an individual, a small business, or a global enterprise, understanding basic cybersecurity practices is essential to protect your digital footprint.
- Implementing simple preventative steps can save significant time, money, and stress compared to recovering from a cyberattack.

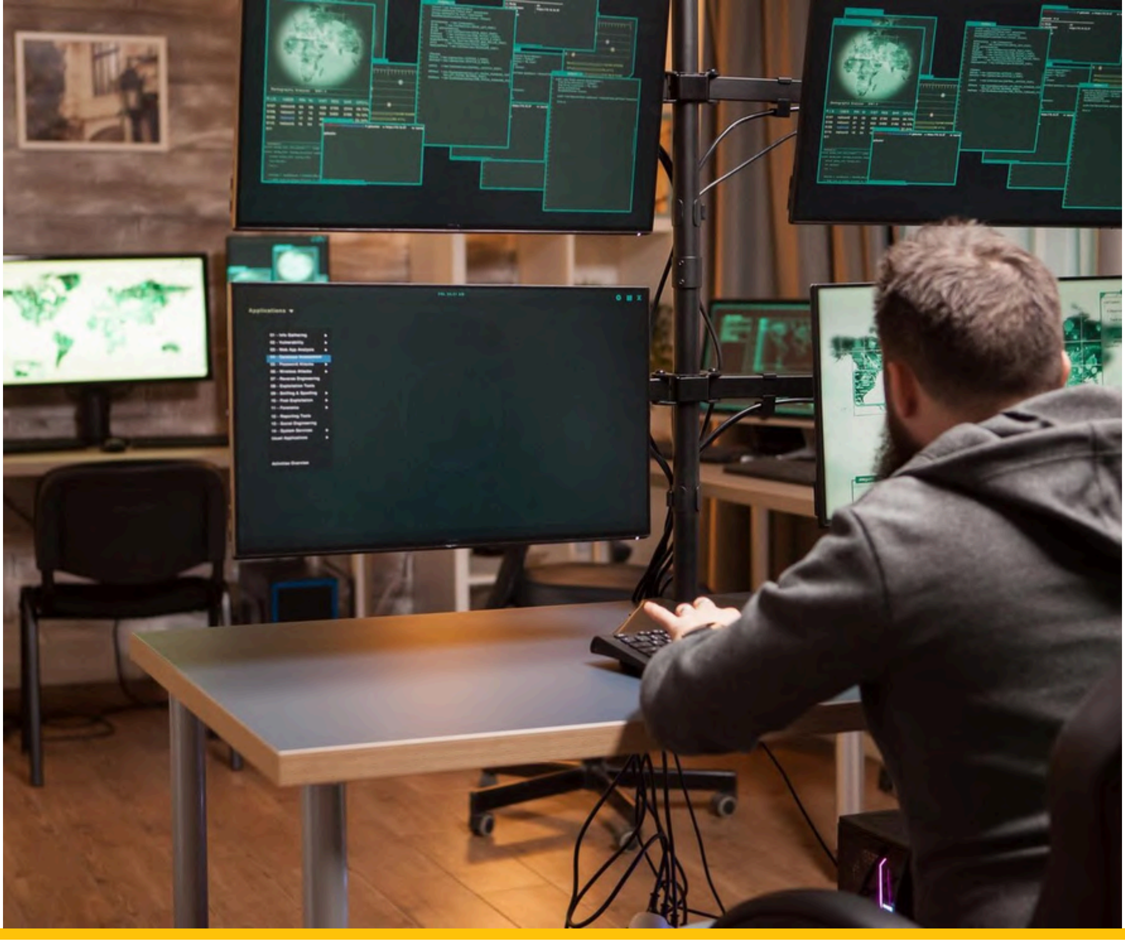
TYPE OF LESSON:

Lesson Overview

In today's digital world, understanding the fundamentals of cybersecurity is no longer optional - it's a necessity. This lesson introduces you to the core principles of cybersecurity, common threats, and practical ways to enhance online safety. Together, we'll explore how to safeguard personal and professional digital assets, fostering a culture of cyber-awareness and resilience.

The workshop is organized into 4 steps:

1: Introduction to cybersecurity basics (15 min)
2: Identifying common cyber threats (10 min)
3: Strategies for cybersecurity best practices (10 min)
4: Closing reflection and key takeaways (5 min)



Step 1 Introduction to cybersecurity basics

Let’s begin with a short video that introduces the concept of cybersecurity. In our daily lives, we constantly use digital tools, but how often do we stop to consider their security? Cybersecurity is essential for keeping ourselves and our personal information safe in the digital world. Today, we’ll dive into the fundamentals of cybersecurity and explore why it’s so important.

Let’s watch this video together:
https://youtu.be/inWWhr5tnEA?si=Pxp1YyvjrFdLoo38

Now that we’ve watched the video, let’s discuss:

1. What stood out to you about cybersecurity from the video?
2. Why do you think cybersecurity is important in our daily lives?

Step 1 Introduction to cybersecurity basics

Cybersecurity isn’t just about protecting systems; it’s also about understanding our own behaviors online. The way we interact with digital tools can either strengthen our security or leave us vulnerable to threats.

Now it's time to take a moment to reflect on your digital life.

Write down answers to the following questions:

1. How often do you think about the safety of your online activities?
2. Can you identify any habits that might put your personal information at risk?

Be ready to share your thoughts!

Step 2

Identifying common cyber threats

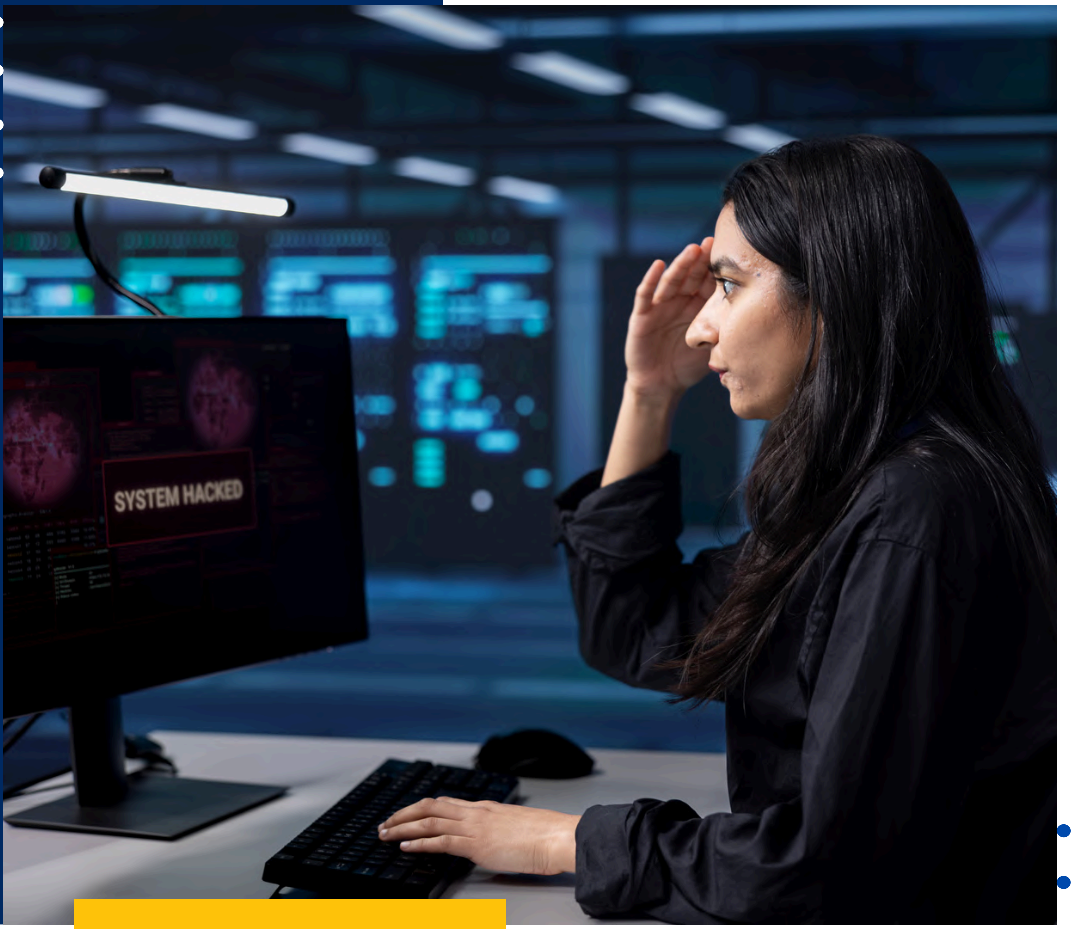
Let’s take a closer look at the types of cyber threats we might encounter.

The internet is a vast space filled with opportunities, but it also comes with risks. Cyber threats can target anyone, anywhere, making it crucial to understand their nature and impact. In this step, we’ll explore various types of threats and how they can affect us.

Read the article: IBM: Types of Cyber Threats

The article highlights:

- The different types of cyber threats, including phishing, ransomware, and malware.
- How these threats operate and who they target.
- Examples of the damage they can cause.



Step 2

Identifying common cyber threats

After reading the article, consider the following:

1. Which type of cyber threat did you find most concerning, and why?
2. Have you or someone you know experienced any of these threats?
3. How do you think understanding these threats can help in preventing them?

After that, write down one real-life example or scenario (it can be hypothetical) where one of these cyber threats mentioned in the article could occur.

Be prepared to share your example and discuss it with the group!

Step 3

Strategies for cybersecurity best practices

Now, let’s focus on protecting ourselves online.

While cyber threats are constantly evolving, there are simple and effective steps we can take to safeguard our information and maintain security. By adopting cybersecurity best practices, we can minimize risks and stay safer in our digital lives.

Cybersecurity doesn’t require advanced technical skills - small, intentional actions can make a big difference in protecting yourself and your data.

Step 3

Strategies for cybersecurity best practices

Here are a few key practices to consider:

- Create strong, unique passwords and change them regularly.
- Enable multi-factor authentication (MFA) for added security.
- Be cautious with links and attachments, especially from unknown sources.
- Keep software and devices updated to patch vulnerabilities.
- Use secure Wi-Fi connections, avoiding public networks whenever possible.

Activity: Cybersecurity best practices checklist

Step 1: Evaluate your current habits

- Reflect on your current online behaviors and habits. Are there areas where you might be putting yourself at risk?

Example: “I use the same password across multiple accounts”

Step 2: Create a plan

- Write down one actionable step for each key concept listed above. For example:

Strong passwords: “I will install a password manager to generate and store secure passwords” etc.

Step 3

Strategies for cybersecurity best practices

Step 3: Group share

- Share one of your planned actions with a partner or the group.
- Discuss how these steps might help improve your digital safety.
- Offer tips or suggestions for additional measures others can take.

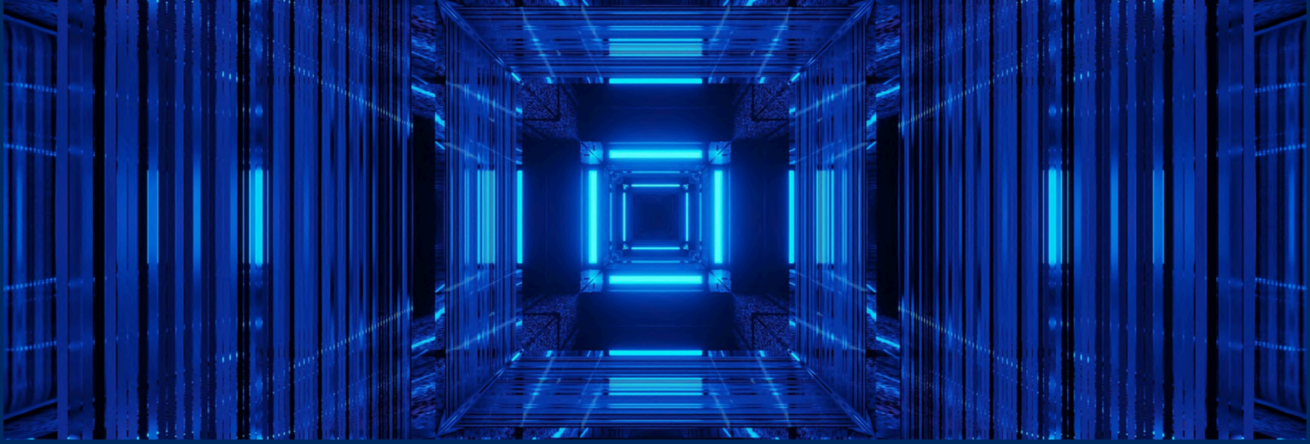
At the very end, answer the **key reflection question** thoughtfully in your mind:
What is one habit or strategy you can start practicing today to immediately improve your online security?

Step 4 Closing reflection and key takeaways

As we wrap up, let's take a moment to reflect on everything we've covered in this lesson and how we can use this knowledge moving forward.

Think about your online habits - are there any changes you feel inspired to make after today's discussion? If so, what's one step you'll take first to enhance your cybersecurity?
Now consider how we can help others. What's a simple tip or habit from this workshop that you could share with a friend or colleague to help them stay safe online?

Thank you all for your active participation and thoughtful contributions today!



Key Takeaway Summary

- Cybersecurity is for everyone. Understanding threats and adopting best practices helps us stay safe online.
- Small steps make a big difference. Tools like password managers and regular updates can significantly enhance your security.
- Stay informed. Cyber threats evolve constantly, so keeping up with the latest tips and tools is essential for long-term safety.
- Be proactive. The more you engage in secure habits, the safer you - and those around you - will be.

Instructions for youth workers, educators, and teachers

Objective:
This lesson aims to help youth workers, educators, and teachers equip young people with essential cybersecurity knowledge. Through engaging discussions, activities, and reflection, participants will understand common cyber threats, learn best practices for online safety, and create actionable plans to protect themselves in the digital world.

Materials Needed:

- Internet connection for video playback or articles
- Projector and screen
- Speakers
- Access to recommended cybersecurity tools
- Chart paper or whiteboard markers
- Pens or pencils
- Paper sheets

Step 1: Introduction to cybersecurity basics (15 min)

1.Begin by engaging participants with a relatable example: "Think about the last time you used a new app or visited a website. Did you stop to think about how secure your data is?"

2. Highlight the relevance of cybersecurity: Explain that cybersecurity isn't just for IT professionals; it's a critical skill for everyone in today's digital age. Emphasize how cybersecurity helps protect personal, professional, and organizational information.

3. Clearly outline the session's goals.

4. Activity: Video screening and discussion:

- Play the video: "What is Cybersecurity?" (watch here).
- Provide participants with guiding questions after watching.

5. After the video, lead a discussion:

- "What surprised you the most about cybersecurity?"
- "Do you think cybersecurity is important for everyone? Why or why not?"
- "What are the risks of not paying attention to online security?"

Step 1: Introduction to cybersecurity basics (15 min)

6. Personal reflection: Ask participants to take a few minutes to write down their thoughts:

- “How often do you consider the security of your online activities?”
- “Can you identify one or two habits that might put your personal information at risk?”
- “What changes do you think you could make to improve your online safety?”

7. Encourage sharing in pairs or small groups:

- Option 1: Share one habit you think is risky and get advice from your group on how to improve it.
- Option 2: Discuss whether you’ve ever experienced or heard about a cyber threat and how it was handled.

8. If participants prefer not to share in groups, allow them to write down one change they commit to making and submit it anonymously to the facilitator for later discussion.

Step 2: Identifying common cyber threats (10 min)

1. Share the article IBM: Types of Cyber Threats or a printed summary of its key points.
2. Allow participants 5 minutes to read and note the threats they find most concerning, focusing on their operation and potential impact.
3. Discussion:
Facilitate a group conversation:
- “Which cyber threat do you find most concerning, and why?”
- “Have you or someone you know experienced any of these threats? What happened?”

4. Add insights if needed:
Highlight statistics or examples to enrich the discussion, like phishing emails or ransomware attacks.
5. Scenario activity:
Ask participants to write a short example, real or hypothetical, involving one cyber threat, such as:
- Phishing: “A fraudulent email tricked someone into sharing their account login”
- Malware: “Clicking a suspicious link downloaded a virus, locking their files”

6. Share scenarios in the group and facilitate a discussion around:
- “What went wrong in the scenario?”
- “How could the situation have been avoided?”
- “What preventative measures would have helped?”

7. Optionally, you can add to the discussion by highlighting real-world preventative strategies for each type of threat.

Step 3: Strategies for cybersecurity best practices (10 min)

1. Overview of best practices:
    - Present simple, effective strategies:
    - Use strong, unique passwords.
    - Enable multi-factor authentication (MFA).
    - Avoid suspicious links and attachments.
    - Keep software and devices updated.
    - Use secure Wi-Fi or a VPN.
  - Use real-life examples or brief demonstrations to show the impact of each strategy.

2. If possible, demonstrate or explain the setup of one tool (included in the section "Tools" to make it relatable.

3. Activity: cybersecurity checklist:
  - Distribute a simple checklist template with the strategies listed.
  - Ask participants to write one actionable step for each.
  - Example: "I will enable MFA on my email."
  - Encourage participants to focus on simple, immediate actions and help clarify steps if needed.

4. Group sharing:
  - Participants share one step they plan to take.
  - Offer quick feedback and encourage discussion about the benefits of these changes.
  - Encourage participants to revisit their checklist regularly to update their habits.

Step 4 Closing reflection and key takeaways (5 min)

1. Reinforce learning and motivate participants to apply what they’ve learned.
2. Ask participants:
    - “What is one habit you plan to change or adopt starting today?”
    - “How will you share what you’ve learned with others?”
3. Group sharing:
    - Invite volunteers to share their reflections or a key takeaway.

4.Closing message:

- Remind participants: “Cybersecurity is everyone’s responsibility. Small, intentional steps can make a big difference in staying safe online”.
- Thank everyone for their active participation and encourage them to take action immediately.

Key Takeaways:

Emphasize to participants that cybersecurity is a skill everyone needs, regardless of their technical expertise. Use the lesson’s key points to highlight how understanding common threats and adopting preventative measures, like using strong passwords or enabling MFA, can dramatically reduce online risks. Encourage participants to adopt a proactive mindset by setting simple, achievable goals for improving their online habits. Reinforce these takeaways through follow-up discussions or activities that revisit these concepts, ensuring participants remain vigilant and motivated to maintain strong cybersecurity practices.

Follow-Up and At-Home Activities

Encourage participants to practice what they’ve learned by tracking their online activities over the next week. They can identify areas where they feel most vulnerable and implement one new cybersecurity strategy each day. Additionally, suggest trying tools like LastPass or Bitdefender at home and sharing their experiences with the group in a follow-up session.

Tips for Teachers:

Integrate cybersecurity topics into daily conversations or lessons by using real-life examples that relate to students' experiences, such as social media security or common scams. Use interactive methods like group discussions or role-playing scenarios to make the topic engaging and practical. Regularly check in on progress and provide support to reinforce the importance of building strong cybersecurity habits.

Tools

LastPass

LastPass is a powerful password management tool designed to enhance cybersecurity by generating and securely storing strong, unique passwords for all online accounts. It eliminates the need to remember multiple complex passwords by storing them in an encrypted digital vault, accessible only with a master password.

www.lastpass.com

Bitdefender

Bitdefender is an advanced cybersecurity tool that offers comprehensive protection against malware, phishing, ransomware, and other online threats. It combines robust antivirus software with intelligent anti-phishing measures to provide multi-layered security for personal and professional use.

www.bitdefender.com

References

- Bitdefender. (n.d.). Retrieved from https://www.bitdefender.com
- Cisco Networking Academy. (n.d.). Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More. Retrieved from https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US
- IBM. (2024, March 25). Types of cyberthreats. Retrieved from https://www.ibm.com/think/topics/cyberthreats-types
- Lakhwani, S. (2024, June 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Retrieved from https://www.knowledgehut.com/blog/security/cyber-security-fundamentals
- LastPass. (n.d.). Retrieved from https://www.lastpass.com
- Simplilearn. (2020, June 10). What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn. [Video]. YouTube. https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo

QUIZ

1. What is one of the main objectives of cybersecurity?

A. Ensuring that no one can access the internet without permission

B. Allowing businesses to monitor user activity

C. Protecting digital assets by managing risks and vulnerabilities

D. Blocking all emails from unknown senders

2. Which of the following demonstrates the use of multi-factor authentication (MFA)?

A. Logging in by answering a security question

B. Using your email password and a backup email for recovery

C. Combining a password with a temporary code sent to your phone

D. Saving passwords in an encrypted file on your computer

3. What makes phishing different from other online threats?

A. It involves directly hacking into systems without user interaction

B. It uses deceptive tactics to trick users into sharing sensitive information

C. It spreads through physical devices like USB drives

D. It works exclusively by installing malware on a computer

QUIZ

4. How does updating your software improve cybersecurity?
A. It enhances the design and usability of your applications
B. It reduces the chances of bugs interfering with your tasks
C. It closes security loopholes that attackers could exploit
D. It enables better compatibility with older hardware

5. Why is using a password manager beneficial?
A. It ensures all your passwords are backed up on a shared server
B. It automatically logs you out of accounts after a set time
C. It creates and securely stores complex passwords for each account
D. It alerts you when someone accesses your email without permission

Solutions

Question 1: C

Question 2: A

Question 3: B

Question 4: B

Question 5: A

ERASMEDIAH
Educational Reinforcement Against
the Social Media Hyperconnectivity

Lélekben Otthon
Közhasznú Alapítvány

AdM
ArchiviodellaMemoria

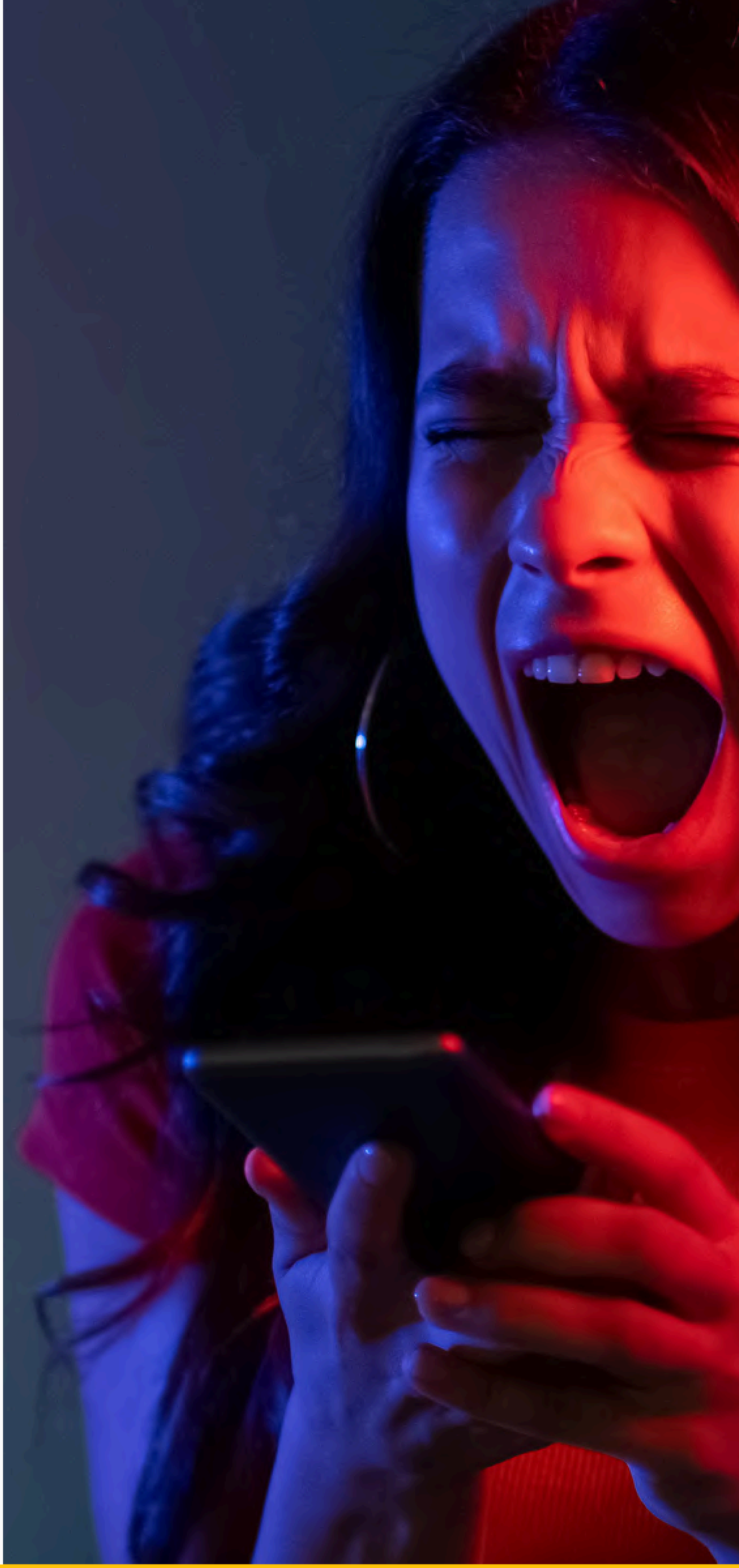
LABC

CWEP Centrum Wspierania
Edukacji
i Przedsiębiorczości

EDU
yayıncılık

ASSERTED KNOWLEDGE
THE ICT EQUALISERS

Inno Hub
Valencia



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.