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 5.2

Protecting Personal Information and Privacy Online

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 5.2

Protecting Personal Information and Privacy Online

Objectives:

- To raise awareness of the risks of sharing personal information online and how it can be misused.
- To equip learners with practical strategies to control their digital footprint, including data privacy settings, secure communication, and avoiding oversharing.
- To explore examples of privacy breaches, demonstrating their impact on individuals and how they could have been prevented.
- To inspire proactive behavior by building habits such as reviewing app permissions, understanding terms of service, and using privacy tools.

Key Message(s):

- Every piece of information you share online – from photos and likes to location data – can be exploited by cybercriminals or companies. Knowing how to limit access is your first line of defense.
- Protecting your privacy isn't about avoiding the internet; it's about being smart and intentional. Simple tools and decisions can keep your data safe without sacrificing your digital life.

TYPE OF LESSON:

Lesson Overview

With so much of our lives happening online, keeping personal information safe has never been more important. This lesson highlights why protecting your privacy matters. We'll explore how simple habits, like oversharing on social media or accepting app permissions without thinking, can leave your data exposed. By recognizing these risks and adopting practical strategies, you'll gain the tools to safeguard your digital identity and take control of your online safety.

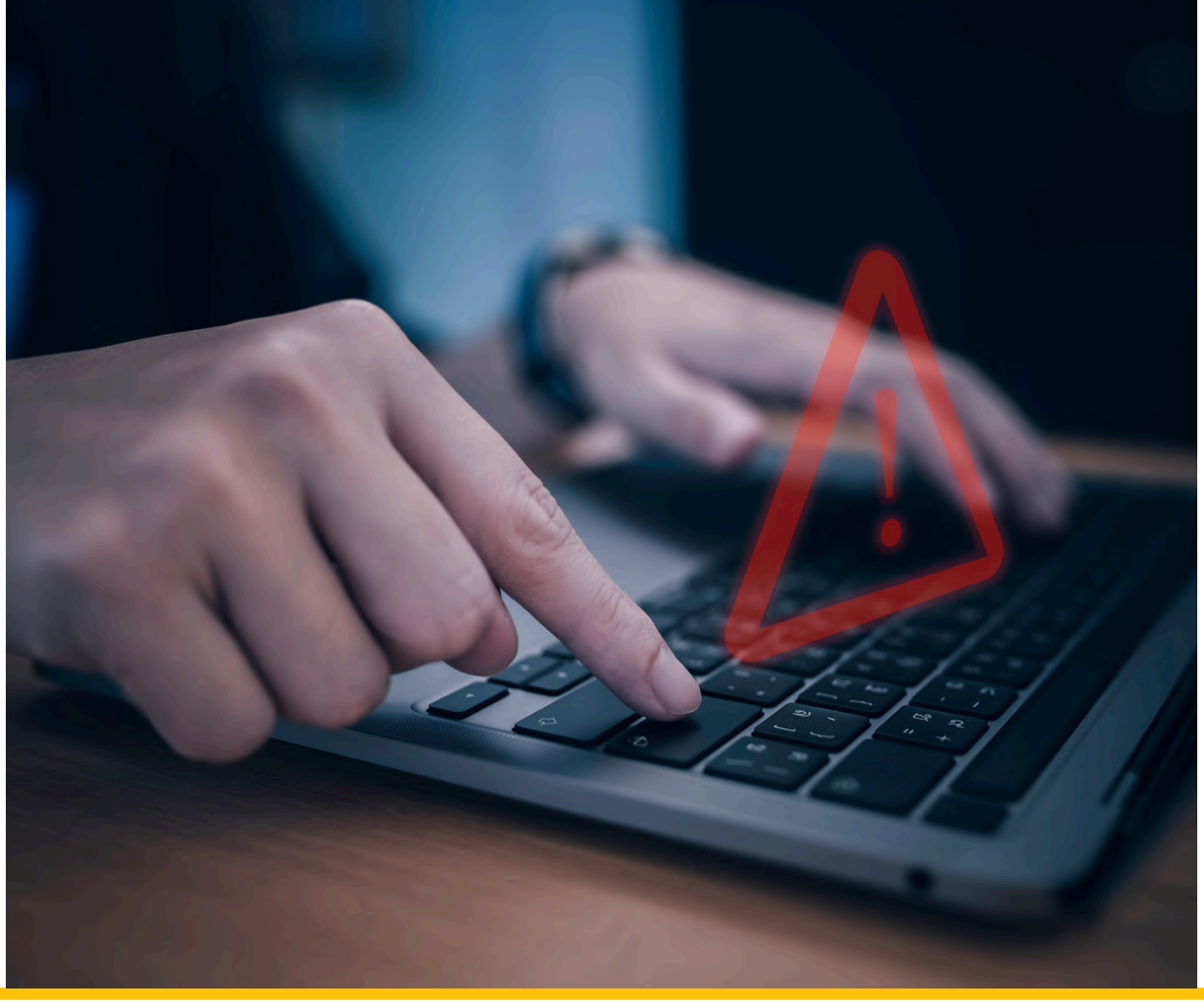
The workshop is organized into 4 steps:

1: Introduction to privacy risks online (15 min)

2: Exploring real-world privacy breaches (10 min)

3: Practical strategies for protecting personal information (10 min)

4: Closing reflection and key takeaways (5 min)



Step 1

Introduction to privacy risks online

Have you ever downloaded a new app, accepted its permissions, and never stopped to think what information it's collecting?
When we use the Internet, our personal data - like location, passwords, and browsing habits - can easily become exposed. Now, we'll explore what privacy risks exist and how they might affect you.

As a first step, **read the section "Common Online Privacy Threats" from this article**: **builtin.com/articles**

While reading, write down in a few words on a piece of paper:

- The privacy threat you find most disturbing and why this threat stands out to you or seems dangerous.

Step 1

Introduction to privacy risks online

Once you've finished reading, let's discuss:

- Which privacy threat surprised you the most, and why?
- How do you think these threats affect our everyday lives?
- What could happen if we ignore them?

Feel free to share a quick example from your experience - whether it's about weak passwords, data tracking, or something else you've seen or heard. If you're unsure, just listening to others will give you ideas!

Step 2

Exploring real-world privacy breaches

Let’s dive into a real-world example of what happens when we’re not careful with our personal information online.

Imagine this: Sarah loves sharing her life on social media. She posts photos of her new apartment, talks about her daily routines, and even shares her location when she’s at her favorite coffee shop. One day, Sarah discovers her bank account has been drained. How? A cybercriminal pieced together her personal information from her public posts - her location, lifestyle habits, and even hints about her passwords - to access her accounts. All because of oversharing!

Now, think about the following questions:

- What went wrong? What actions or habits led to the privacy breach?
- How could this situation have been prevented? What simple changes would have made a difference?

Write down your answers and be ready to share them with the group.

Step 2

Exploring real-world privacy breaches

Let’s talk about it together:

- What do you think went wrong in Sarah’s situation?
- Why do you think privacy breaches like this happen so easily?

At the end, take a moment to think:

- Have you or someone you know ever faced a privacy issue online? It could be a suspicious email, a hacked account, or an incident of oversharing on social media.
- How did it happen, and what was the outcome?

If you feel comfortable, share your story with the group. If not, that’s okay - just listening will give you valuable insight.

Step 3

Practical strategies for protecting personal information

Now that we've explored privacy risks and real-world example, let's focus on practical steps to protect ourselves (our data) online.

We'll start with a quick video: https://youtu.be/6WQzMAd6mJs

Pay attention to the key tips shared.

After watching, write down **three specific actions** you can take to improve your online privacy. Think about:

- Adjusting privacy settings on your social media accounts.
- Reviewing app permissions on your phone.
- Being cautious about what personal information you share online, especially on public platforms.

Step 3

Practical strategies for protecting personal information

Now, let's share **one strategy** you plan to implement. For example:

- "I'm going to review all the apps on my phone tonight and remove the ones I don't use"
- "I'll limit who can see my Facebook/Instagram posts and turn off public visibility for my profile"

Let's discuss:

1. What makes these privacy habits seem easy or difficult to adopt?
- Are we too comfortable sharing information online?
- Do we think privacy settings and permissions are confusing or time-consuming?

2. Why do so many people ignore simple privacy practices, even when they know the risks?
- Is it because they don't think a breach will happen to them?
- Do you think it's because people aren't aware of the tools or habits they should use?

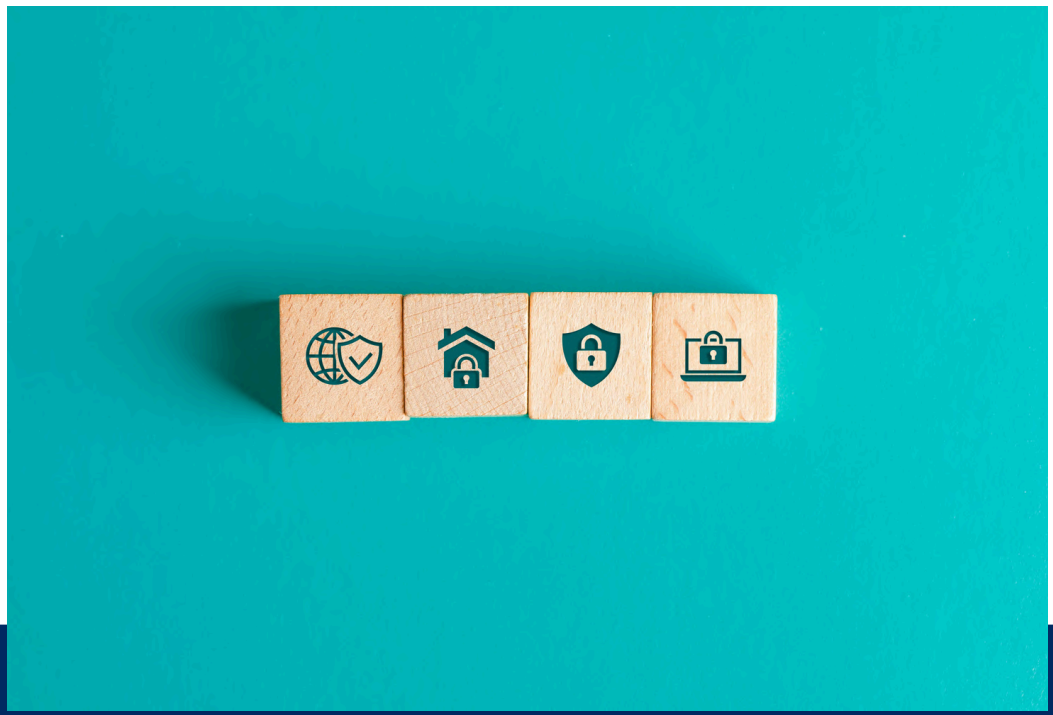
3. How can you stay motivated to stick with these habits?
- For example, setting reminders to update passwords or regularly reviewing social media settings.

Step 4

Closing reflection and key takeaways

To wrap up this workshop, let's take a moment to reflect on what we've learned and think about how we can apply it in our daily lives.

Ask yourself: *What is one habit you can change today to improve your online privacy?* It could be something simple, like turning off location sharing, checking your social media privacy settings, or being more cautious about what you post. Now, think about how you can help others: *How will you share what you've learned today with a friend, family member, or colleague?* Even small tips, like explaining why strong passwords matter or showing someone how to check app permissions, can make a big difference.



Key Takeaway Summary

- **Be mindful of what you share online: Small details, like locations or habits, can be misused if they fall into the wrong hands.**
- **Review and adjust privacy settings: Regularly check your social media, app permissions, and account settings to limit unnecessary data sharing.**
- **Limit what personal information you post publicly: Avoid sharing sensitive details like addresses, routines, or personal identifiers on social media or other platforms.**
- **Stay cautious with apps and links: Think before clicking on links, downloading apps, or granting permissions - trust only verified sources.**
- **Start with small steps: Simple habits, like turning off location tracking or limiting public posts, can make a big impact on protecting your privacy.**

Instructions for youth workers, educators, and teachers

Objective:
The goal of this lesson is to provide participants with practical skills and knowledge to protect their personal information and maintain online privacy. Through interactive activities, real-life examples, and reflective discussions, participants will identify common online privacy risks, gain insight into the impact of privacy breaches, and develop actionable strategies to safeguard their data. By the end of the session, learners will feel more aware, prepared, and committed to adopting habits that enhance their digital security.

Materials Needed:

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

Step 1: Introduction to privacy risks online (15 min)

1.Begin with a relatable question: “When was the last time you downloaded an app, accepted its permissions, or shared a post online? Did you stop to think about what personal information you might be giving away?”. Explain that these small, everyday actions can unintentionally expose private details like location, browsing habits, or personal routines to third parties or cybercriminals.

2. Emphasize that protecting personal data is essential in today’s digital world. Highlight that seemingly harmless behaviors - like sharing a photo or allowing apps access to your contacts - can have unintended consequences. Use a simple analogy: “Your personal information is like pieces of a puzzle. One piece alone may seem harmless, but when combined with others, it can reveal a lot about you”.

3. Activity – article reading and reflection
Distribute or share the section “Common Online Privacy Threats” from the article: What Is Online Privacy?.

Ask participants to:

- Identify the privacy threat they find most concerning.
- Reflect on why this threat feels especially dangerous or surprising.

Encourage them to jot down brief thoughts to prepare for the group discussion.

Step 1: Introduction to privacy risks online (15 min)

4. Facilitate a short discussion using these prompts:

- “Which privacy threat stood out to you the most, and why?”
- “How do these risks affect your online behavior or habits?”

Invite a few participants to share their reflections, reinforcing that awareness of these risks is the first step to better protecting personal information.

5. Wrap-up - summarize the key point of the discussion (for example: By recognizing these privacy risks, you are taking control of your online presence. Awareness allows you to make smarter decisions about what you share and how you interact online).

Step 2: Exploring real-world privacy breaches (10 min)

1. Start by sharing a relatable and impactful scenario to illustrate how oversharing online can lead to serious privacy breaches. Explain to participants that this story is not unique. Many people unknowingly share personal details that cybercriminals or malicious individuals can use to track them, hack into their accounts, or even steal their identity. Emphasize that privacy breaches often start with small, seemingly harmless pieces of information.

2. Show a short written scenario to participants, either based on the story of Sarah or a similar hypothetical situation:

Example of another scenario:

“Alex downloaded a free mobile app without reading the permissions. The app had access to his location, contacts, and media files. Shortly after, he noticed strange messages being sent to his friends. It turned out the app was collecting his data and sending spam messages using his account”.

Step 2: Exploring real-world privacy breaches (10 min)

3. Give participants instructions:
Work individually or in small groups to analyze the situation.

- What went wrong? What actions or behaviors caused the breach?
- How could this have been prevented? Identify simple steps or habits to protect personal information.

Write down your thoughts briefly.

4. Let participants share their reflections, as follows:

- “Have you or someone you know faced a similar issue, like phishing, hacking, or oversharing?”
- “Why do people share so much personal information without considering the risks?”
- Possible reasons:
  - Trusting apps or platforms.
  - Not realizing the consequences.
  - Confusing privacy settings.

Encourage open, supportive sharing of experiences or insights.

Step 3: Practical strategies for protecting personal information (10 min)

1. Video screening
Show the video How to Protect Your Personal Data Online. Encourage participants to pay close attention to practical, actionable strategies shared in the video. Emphasize that these tips are easy to implement but can significantly improve online privacy.
2. Activity – "Personal privacy plan"
Ask participants to write down three actions they will take to protect their privacy online.
Encourage them to consider:

- Adjusting social media privacy settings.
- Reviewing app permissions on their devices.
- Being mindful of what they post publicly.

3. Sharing within the group
Invite participants to share one action they plan to implement with the group. Use the following prompts to guide the discussion:

- "Which strategy feels easiest for you to start today, and why?"
- "What challenges might you face while trying to adopt these habits?"
- "How can we overcome common barriers, like forgetting to adjust settings or finding privacy tools confusing?"

Encourage the group to provide practical tips or share personal experiences on how they overcame similar challenges. Emphasize that taking small steps consistently can lead to significant improvements in online privacy.
4. Additionally, you can ask participants to think about how they can share these strategies with friends or family.

Step 4 Closing reflection and key takeaways:

1. Ask participants to reflect on:
   - “What is one habit you will change to improve your online privacy starting today?”
   - “How will you share what you’ve learned with friends or family?”
2. Reinforce the lesson’s main points:
   - Small changes, like adjusting settings or limiting what you share, make a big impact.
   - Protecting your data gives you control over your digital identity.
3. End the session with a concluding sentence. For example: “Your personal information is valuable. Take small, smart steps to protect it, and you’ll stay safer online”.

Key Takeaways:

At the end of the lesson, participants should clearly understand that online privacy starts with awareness and small, actionable steps. Simple changes, such as adjusting app permissions, reviewing privacy settings on social media, and being mindful of what is shared publicly, can significantly reduce risks. Encourage participants to take control of their digital behavior by developing habits like checking who has access to their data and staying cautious about suspicious links or messages. Reinforce the idea that protecting personal information empowers individuals to maintain control over their digital identities and safety.

Follow-Up and At-Home Activities

Ask participants to spend the next days implementing at least one privacy action they identified during the session. This could include reviewing privacy settings on one social media platform, deleting unused apps, or sharing privacy tips with friends or family members. Suggest they document their progress and reflect on how these changes make them feel more secure online. Additionally, encourage participants to explore tools like DuckDuckGo (a private search engine) or Google Privacy Checkup to see how easily they can improve their online safety. Consider organizing a follow-up session where participants can share their experiences and discuss challenges they faced.

Tips for Teachers:

It is recommended to include real-life examples in the discussion to make the concept of online privacy understandable. Use scenarios involving excessive social media sharing, data breaches or app permissions to show how small habits can have big consequences. Create a supportive space for participants to share their experiences without judgment. To ensure continued engagement, incorporate short, hands-on tasks into lessons, such as showing how to adjust privacy settings or recognize suspicious links. Revisit the topic regularly to maintain privacy awareness and encourage students to see protecting their information as a lifelong habit.

Tools

DuckDuckGo

DuckDuckGo is a privacy-focused search engine that does not track your search history or collect personal data. It ensures your searches remain private and helps minimize the digital footprint you leave while browsing.

duckduckgo.com

Google Privacy Checkup

Google Privacy Checkup is a built-in tool that helps you manage your Google account settings. It allows you to review and adjust what personal data is collected, who can see your activity, and which apps have access to your information.

myaccount.google.com/privacycheckup

References

- DuckDuckGo (n.d.). Retrieved from https://duckduckgo.com
- Farrier, E. (2024, August 21). A guide to protecting your personal information. Retrieved from https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online
- Glover, E. (2024, January 24). What Is Online Privacy?. Built In. Retrieved from https://builtin.com/articles/what-is-online-privacy
- Google Privacy Checkup (n.d.). Retrieved from https://myaccount.google.com/privacycheckup
- Negrean, R. (n.d.). 10 Tips for Protecting Online Privacy: Strategies for Digital Security. Privacy Tutor. Retrieved from https://privacytutor.net/10-tips-for-protecting-online-privacy
- Tech Implement Infra Pvt Ltd. (2024, December 8). Essential Tips on Protecting Personal and Professional Data Online. [Video]. YouTube. https://youtu.be/6WQzMAd6mJs?si=cq1NFnjxu7i8NRk5
- Webb, M. (2023, November 26). How to Protect Your Online Privacy: 7 Best Practices to Implement Today. Techopedia. Retrieved from https://www.techopedia.com/how-to/how-to-protect-your-privacy-online

QUIZ

1. What is one simple action you can take to limit the misuse of personal data online?
A. Avoid creating social media accounts altogether
B. Turn off all notifications on your devices
C. Accept app permissions without reviewing them
D. Adjust your social media privacy settings regularly

2. Which of the following is an example of oversharing that could lead to identity theft?
A. Sharing a vacation photo with close friends only
B. Posting your location and daily routines publicly
C. Sending photos of your pets via private message
D. Using emojis to describe your mood online

3. How can reviewing app permissions improve your online privacy?
A. It allows you to restrict apps from accessing unnecessary personal data
B. It helps you download apps faster by skipping permission checks
C. It ensures all apps on your device are automatically updated
D. It allows apps to run more smoothly on your device

QUIZ

4. Why do many people fail to protect their personal information online?

A. Privacy tools are unavailable for regular users

B. People trust companies to keep their data secure

C. Privacy settings and tools are often overlooked or seen as confusing

D. Most people believe they have no personal data worth protecting

5. What is a good habit to develop for protecting personal information?

A. Using the same password for convenience

B. Allowing apps to track your location at all times

C. Ignoring terms of service agreements

D. Being cautious about sharing sensitive information on public platforms

Solutions

Question 1: D
Question 2: B
Question 3: A
Question 4: C
Question 5: D

ERASMEDIAH

Educational Reinforcement Against the Social Media Hyperconnectivity

Lélekben Otthon Közhasznú Alapítvány

AdM Archivio della Memoria

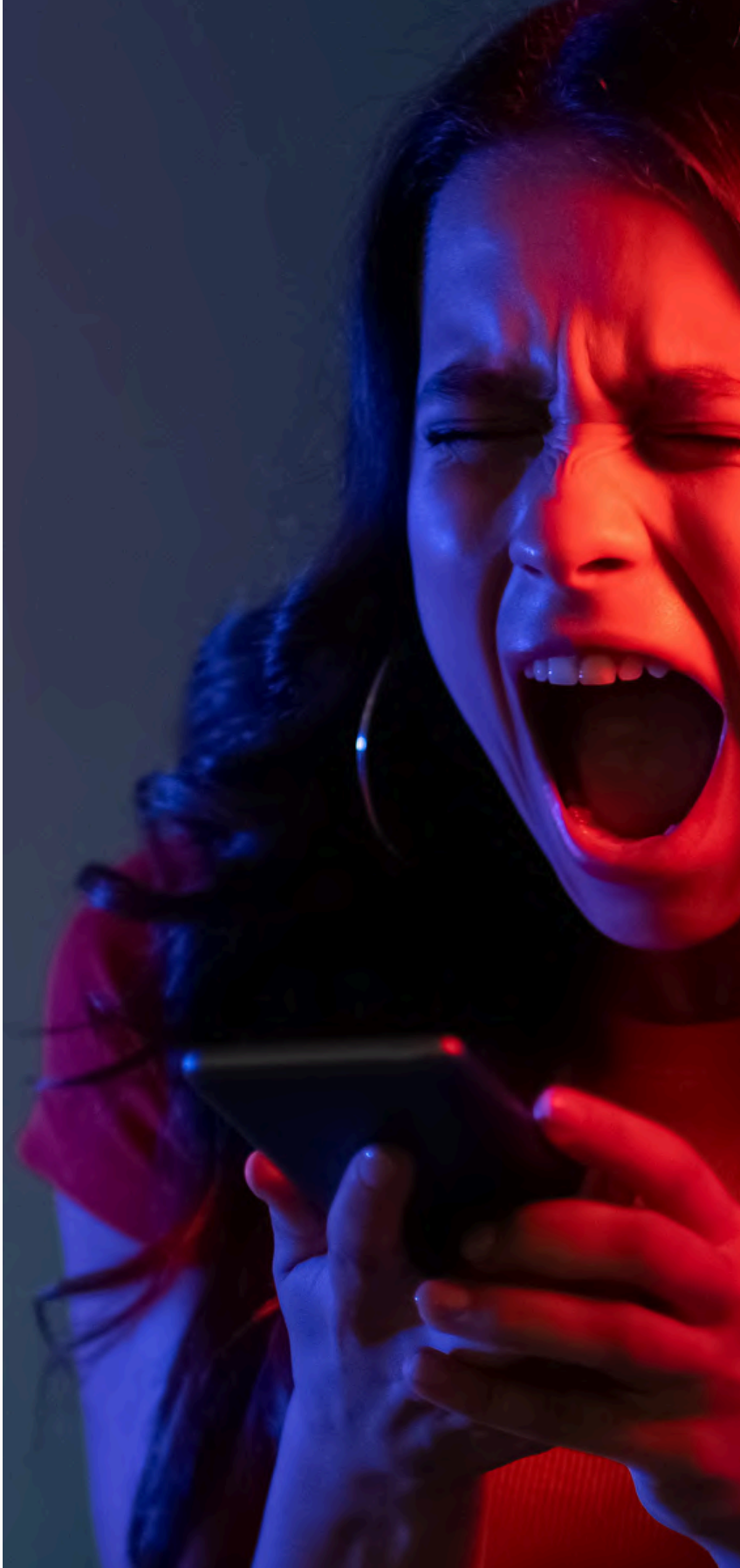
LABC

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.