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 5.4

Recognition of Cyber Threats and Strategies to Prevent Exposure to Inappropriate Content

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 5.4

Recognition of Cyber Threats and Strategies to Prevent Exposure to Inappropriate Content

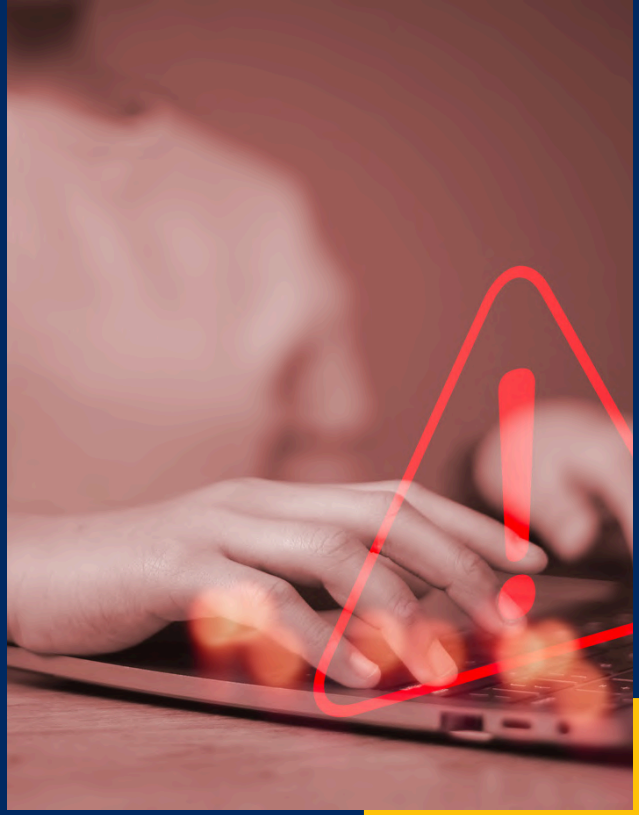
Objectives:

- To develop awareness of prevalent online risks, such as exposure to inappropriate content, cyberbullying, and grooming, particularly targeting vulnerable users like children and teenagers.
- To empower learners with critical skills to recognize warning signs of cyber threats, such as suspicious links, predatory online behavior, and manipulative content.
- To encourage proactive habits in managing online interactions by fostering critical thinking, identifying safe digital spaces, and maintaining open communication about online experiences.

Key Message(s):

- Online threats often hide behind innocent-looking platforms or interactions. Recognizing the signs is key to staying safe.
- Simple practices like using content filters and maintaining strong communication can help prevent exposure to harmful content and cyber threats.

TYPE OF LESSON:



Lesson Overview

Within today's hyper-connected digital environment, exposure to inappropriate content and cyber threats is an ever-present risk. This lesson is designed to provide a comprehensive understanding of the nature and risks of these threats, practical tools to mitigate them, and strategies to foster safer online interactions. Through engaging exercises and practical advice, you will leave the session better prepared to navigate the digital world safely and responsibly.

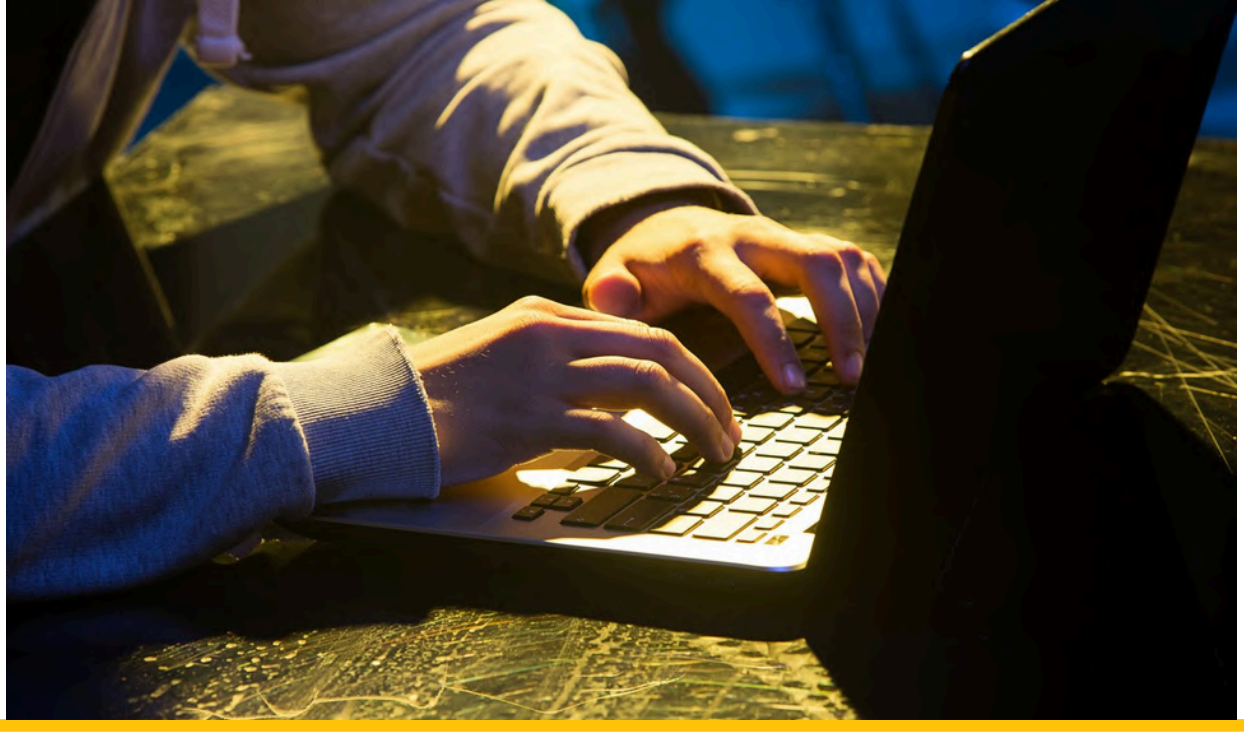
The workshop is organized into 4 steps:

1: Essentials of cyber threats and inappropriate content (10min)

2: Recognizing warning signs and risks (15 min)

3: Approaches for prevention and mitigation (10 min)

4: Reflection and application (5 min)



Step 1

Essentials of cyber threats and inappropriate content

Have you ever come across something online that made you feel uncomfortable or unsafe?
Cyber threats are harmful activities that target individuals or systems online, aiming to steal information, cause harm, or exploit vulnerabilities. Examples include:

- Cyberbullying: Using online platforms to harass or intimidate.
- Phishing: Sending deceptive messages to trick people into revealing personal information.
- Grooming: Building a relationship with someone online to exploit them later, often inappropriately.

What constitutes **inappropriate content**?
Content that is harmful, explicit, or unsuitable for certain age groups, such as:

- Explicit images or videos.
- Manipulative or predatory messages.
- Violent or hateful material.

Step 1

Essentials of cyber threats and inappropriate content

Exposure to such content can cause emotional distress, harm relationships, and lead to long-term consequences like identity theft or exploitation.

Activity

Now, we will divide into small teams. Each group will be given one scenario to analyze:

Scenario 1: You receive an email from a stranger who asks you for personal information

Scenario 2: You see a suspicious link in an email

Scenario 3: You come across an inappropriate comment on social media

Your task is to answer the questions in your group:

- What is risky about this situation?
- How can you respond safely?

Once the groups are finished, share conclusions together.

Step 2

Recognizing warning signs and risks

Take a look at the examples below and consider whether you've ever seen anything similar on the Internet. While brainstorming, discuss as a group, which of these warning signs are most common and how you can respond to them.

1.Unknown or suspicious sender

- You receive a message from someone you don’t know, asking for personal information or prompting you to click a link.
- The email address looks unusual, such as "bank123random@mail.com" instead of an official address.
- *Discussion question*: “What do you do when you get a message from someone you don’t recognize?”

2. Spelling or grammar errors

- The message is full of spelling mistakes or odd phrasing.
- Example: "Your acount is blokced! Click here to reactive"
- *Discussion question*: “Do errors in a message make you suspicious? Why or why not?”

Step 2

Recognizing warning signs and risks

3. Urgent requests or threats

- Messages like: "If you don’t pay within 24 hours, your account will be deactivated!"
- The content tries to scare you or pressure you into acting quickly.
- *Discussion question*: “How can you tell the difference between a real warning and a scam?”

4. Too good to be true offers

- Ads promising incredible rewards: "You’ve won a brand-new iPhone! Click here to claim your prize"
- Websites offering unrealistic benefits with little effort.
- *Discussion question*: “Why are these kinds of offers dangerous?”

Step 2 Recognizing warning signs and risks

5. Unknown links or attachments

- You receive a link that doesn’t look trustworthy, such as "www.freegift.now".
- Attachments from unknown senders that could contain viruses.
- *Discussion question*: “How can you check if a link or attachment is safe?”

In your group, pick one of these warning signs and discuss how you would handle the situation.

At the end, each group will share their insights and ideas on how to avoid these risks in everyday online activities.

Step 3

Approaches for prevention and mitigation

The best way to stay safe online is to take proactive steps that protect your data and prevent risks before they happen. Let's explore simple strategies you can start using right away.

Let's stay in the same groups. Read the following list of simple actions you can take to reduce risks online:

- **Use strong, unique passwords** and update them regularly.
- **Enable multi-factor authentication (MFA)** for important accounts.
- **Avoid suspicious links and attachments** - always verify the source.
- **Review privacy settings** on social media and apps to control who sees your information.
- **Keep software updated** to patch security vulnerabilities.

In your group, discuss which of these actions you already practice and which you might find challenging to implement.
Answer these questions together:

- "Which strategy do you think is most effective in staying safe online?"

Step 3

Approaches for prevention and mitigation

“How can you remind yourself to build better habits, like checking privacy settings or avoiding risky links?”
After brainstorming, each group shares one **new** strategy which plans to adopt and explains in few words why it’s important.

As a final reflection, take a moment to think about one specific habit or tool you will commit to using immediately to improve your online safety. Write it down on a post-it note, and consider how you can help others adopt the same habits. By sharing your knowledge, you can create a safer online environment not only for yourself but for your friends, family, and community.

Step 4

Reflection and application

Now that we've explored online risks and prevention strategies, it's time to reflect on what you've learned and think about how you can apply it in your everyday digital life.

Take a moment to answer the question silently:

- "What is one habit you currently have that might put you at risk online?"

Write down your answer on a post-it note.

As the next step, pair up with a partner and share your reflections:

- Explain the risky habit you identified and why it might be a problem.
- Share the action or tool you plan to adopt to mitigate this risk.
- Offer each other feedback or additional ideas to strengthen your plans.
- Discuss how these strategies can be applied in different situations, such as using public Wi-Fi, sharing personal information, or avoiding grooming and phishing.

Key Takeaway Summary

- **Awareness is the first step toward protection.**
- **Warning signs are everywhere, but once you learn to recognize them and respond appropriately, you can significantly enhance your online safety!**
- **Understanding cyber threats and inappropriate content empowers you to identify potential risks and respond confidently.**
- **Recognizing risks in everyday online situations allows you to act quickly and avoid dangers.**
- **By spreading consciousness, you’re helping to create a safer online community for everyone.**

Instructions for youth workers, educators, and teachers

Objective:
This lesson is designed to raise awareness about online risks, including cyber threats and inappropriate content, and equip participants with practical strategies to foster safer online interactions. By analyzing real-world scenarios, participants will learn to identify risks, recognize warning signs, and adopt preventive measures.

Materials Needed:

- Flipchart or digital presentation tool for outlining key concepts
- Pens and markers
- Blank sheets of paper for note-taking or completing activities
- Access to tools like *CyberWise* or *Malwarebytes Browser Guard* (in case of presenting them to participants)
- Colorful post-it notes for brainstorming

Step 1: Essentials of cyber threats and inappropriate content (10 min)

1. Start by asking participants: “Have you ever encountered something online that felt unsafe or suspicious?”. Encourage a few to share their experiences or provide a brief example, such as receiving a suspicious email or seeing an offensive comment. Use this to emphasize the importance of understanding and addressing online risks.
2. Mini lecture - explain key cyber threats: phishing, grooming, etc. Define inappropriate content, including:

- Explicit material - Harmful or graphic images and videos.
- Predatory messages - Manipulative or harmful communication.
- Age-inappropriate content - Material unsuitable for certain age groups.

3. Activity: Divide participants into groups of 3-5 and assign one of three different scenarios to each group.

Instructions for groups:

1. Analyze the risk: Discuss what makes the scenario risky (e.g. unknown sender, urgent tone, or suspicious link).
2. Suggest safe actions: Brainstorm practical responses:

- For emails: Avoid clicking links, verify the sender through official channels, or report as spam.
- For inappropriate comments: Block the user, report the comment, and avoid responding.
- For suspicious links: Hover to check the URL, don’t click if unsure, and consult a trusted source.

3. Share findings: Groups summarize their analysis and share with the class. Highlight common strategies and discuss their effectiveness.

4. Wrap up by reinforcing key points, linking the activity to broader strategies for online safety to be explored in subsequent steps.

Step 2: Recognizing warning signs and risks (15 min)

1. Introduce participants to common warning signs of cyber threats using clear examples:

- Suspicious links or unknown senders: Messages from unfamiliar contacts with links or attachments (e.g., "www.freeprizes.xyz").
- Spelling errors or urgent demands: Messages like “Your account is blocked! Reactivate now”, often poorly written to create urgency.
- Too-good-to-be-true offers: Promises of rewards or deals, such as “You’ve won a free iPhone!”

You can also use visuals, like screenshots of phishing attempts, and encourage participants to share examples for better engagement.

2. The next step is to conduct a group exercise. Divide participants into small groups and assign each group a specific warning sign to analyze (e.g., urgent messages or suspicious links). Provide these steps:

1. Analyze the warning: Discuss what makes the threat convincing (e.g., urgency or deception).
2. Propose solutions: Brainstorm responses, such as verifying sources, avoiding suspicious links, or reporting scams.
3. Summarize findings: Prepare practical tips for avoiding the assigned threat.

3. At the end, each group presents its insights and strategies. Summarize them in a consolidated list of best practices on a whiteboard or flipchart. Conclude by emphasizing the value of caution, verification and critical thinking in staying safe online.

Step 3: Approaches for prevention and mitigation (10 min)

1. Begin by emphasizing the importance of proactive steps to safeguard personal data and reduce risks online. Introduce a list of simple actions participants can adopt immediately, such as:

- Using strong, unique passwords and updating them regularly.
- Enabling multi-factor authentication (MFA) for critical accounts.
- Avoiding suspicious links and attachments by verifying their sources.
- Reviewing privacy settings on social media and apps.
- Keeping software updated to address security vulnerabilities.

Explain how these actions can effectively mitigate common online risks.

2. Keep participants in their existing groups and provide the list of actions. Ask them to discuss and complete the following tasks:

1. Group discussion:

- Identify which actions they already practice and which they find challenging.
- Discuss why certain strategies might be harder to implement and brainstorm ways to overcome these challenges.

2. Answer key questions:

- “Which strategy do you think is the most effective in staying safe online?”
- “How can you remind yourself to build better habits, such as regularly checking privacy settings or avoiding risky links?”

3. Share new strategies:

- Each group selects one new strategy they plan to adopt, explains why it’s important, and shares it with others.

Step 3: Approaches for prevention and mitigation (10 min)

3. Conclude the activity by asking each participant to reflect individually on one habit or tool they will commit to using immediately to improve their online safety. Have them write it on a post-it note. Encourage participants to think about how they can share this habit with friends, family, or colleagues to promote a safer online environment collectively.

Step 4: Reflection and application (5 min)

1. Individual reflection:
   - Ask learners: “What is one online habit you can change to improve safety?”
   - Participants write their responses on post-it notes.
2. Peer discussion:
   - Pair participants to share their goals and suggest actionable steps.
3. Wrap-up:
   - Conclude with a motivational takeaway. It could be, for example: “Small changes in your online behavior can make a big difference in your safety and that of your community”.

Key Takeaways:

Participants should leave the session with a clear understanding of how to identify cyber threats and inappropriate content, such as phishing attempts, manipulative messages, or suspicious links. Highlight the importance of practical safety strategies, like using strong passwords, enabling multi-factor authentication, and customizing privacy settings to safeguard personal information.

Invite participants to adopt a proactive mindset by fostering critical thinking and maintaining open discussions about online risks. Reinforce these principles through regular practice and by sharing knowledge with others, creating a ripple effect that promotes safer online habits within their communities.

Follow-Up and At-Home Activities:

Ask participants to:

- Review their personal social media settings.
- Test tools like Malwarebytes Browser Guard or content filters.
- Share one learned strategy with a friend or family member.

Tips for Teachers:

Make lessons engaging by using real-world examples and clear visuals to explain online risks and practical safety strategies. Encourage interactive discussions to help participants connect with the material. Hands-on activities, like creating safety guides, help solidify concepts. Maintain a supportive and open environment where questions are welcomed, and emphasize the long-term benefits of safe online habits. Reinforce key lessons through follow-up tasks or group reflections to ensure participants retain and apply what they've learned.

Follow-Up and At-Home Activities:

Ask participants to:

- Review their personal social media settings.
- Test tools like Malwarebytes Browser Guard or content filters.
- Share one learned strategy with a friend or family member.

Tips for Teachers:

Make lessons engaging by using real-world examples and clear visuals to explain online risks and practical safety strategies. Encourage interactive discussions to help participants connect with the material. Hands-on activities, like creating safety guides, help solidify concepts. Maintain a supportive and open environment where questions are welcomed, and emphasize the long-term benefits of safe online habits. Reinforce key lessons through follow-up tasks or group reflections to ensure participants retain and apply what they've learned.

Tools

CyberWise

CyberWise is an educational platform that offers tools, resources, and guides to help individuals, particularly parents, educators, and students, understand online safety. It provides modules on recognizing cyber threats like phishing, cyberbullying, and inappropriate content, along with strategies to mitigate risks.

www.cyberwise.org

Malwarebytes Browser Guard

This is a free browser extension that protects users from phishing, scams, malware, and inappropriate content. It actively blocks harmful websites and ads, ensuring safer browsing for all users, not just children.

www.malwarebytes.com

References

- CyberWise. (n.d.). Retrieved from https://www.cyberwise.org
- Dalby, J. (2021, January 15). How to Avoid Inappropriate Content. Gabb Now. Retrieved from https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (2023, September 25). Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. Retrieved from https://figshare.com/ndownloader/files/42443952
- Lynch, M. (2024, April 5). 19 simple ways to block inappropriate content. The Tech Edvocate. Retrieved from https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (2024, February 21). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Retrieved from https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Retrieved from https://www.malwarebytes.com/browserguard
- Roy, R. (2021, August 23). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Retrieved from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 Types of Cyber Security Threats and Solutions. Retrieved from https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

QUIZ

1. What is a key sign of a phishing attempt?
A. Receiving a message from a previously unknown but verified account
B. An email with no links, images or attachments
C. An email urging you to act immediately, often with poor grammar
D. A message from a known sender requesting routine information

2. Which behavior could increase the risk of cyber threats?
A. Regularly updating your devices and apps
B. Clicking on links in emails without verifying the sender
C. Using two-factor authentication for online accounts
D. Reviewing privacy settings on social media once a month

3. Which habit helps avoid falling victim to cyber threats?
A. Using a password manager to create and store unique passwords
B. Accepting all permissions when installing apps for convenience
C. Sharing passwords with trusted friends or family members to have a fallback in case you forget them
D. Disregarding security warnings from your browser

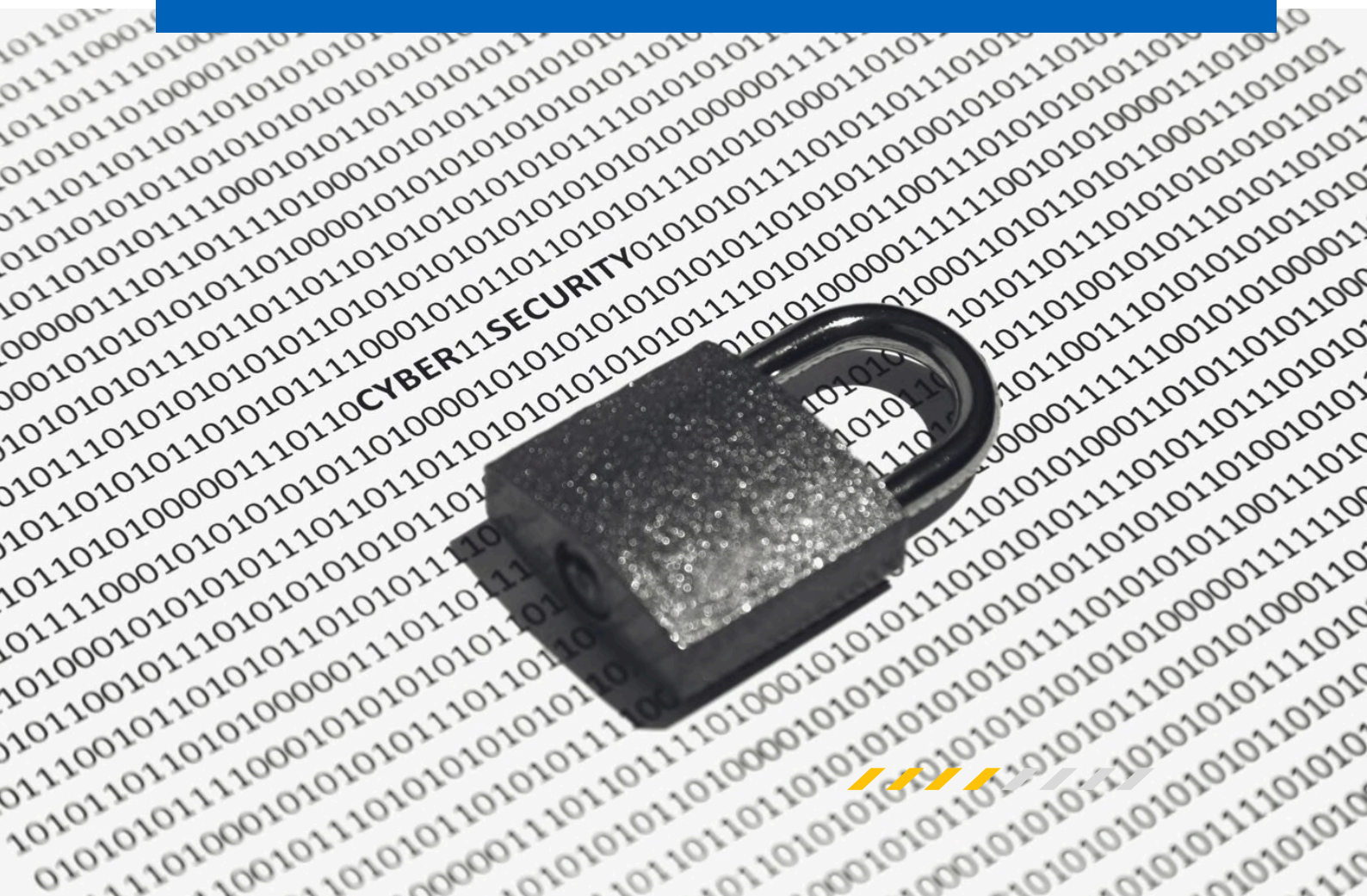
QUIZ

4. What makes a link suspicious and potentially harmful?
A. It uses HTTPS encryption
B. It redirects to another website
C. It contains unusual characters or domains
D. It is shared by a friend in a direct message

5. Which strategy is the most effective for preventing exposure to inappropriate content?
A. Keeping any online interaction to a minimum
B. Turning off all notifications on your devices
C. Relying on antivirus software alone
D. Using content filters and adjusting privacy settings

Solutions

Question 1: C
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

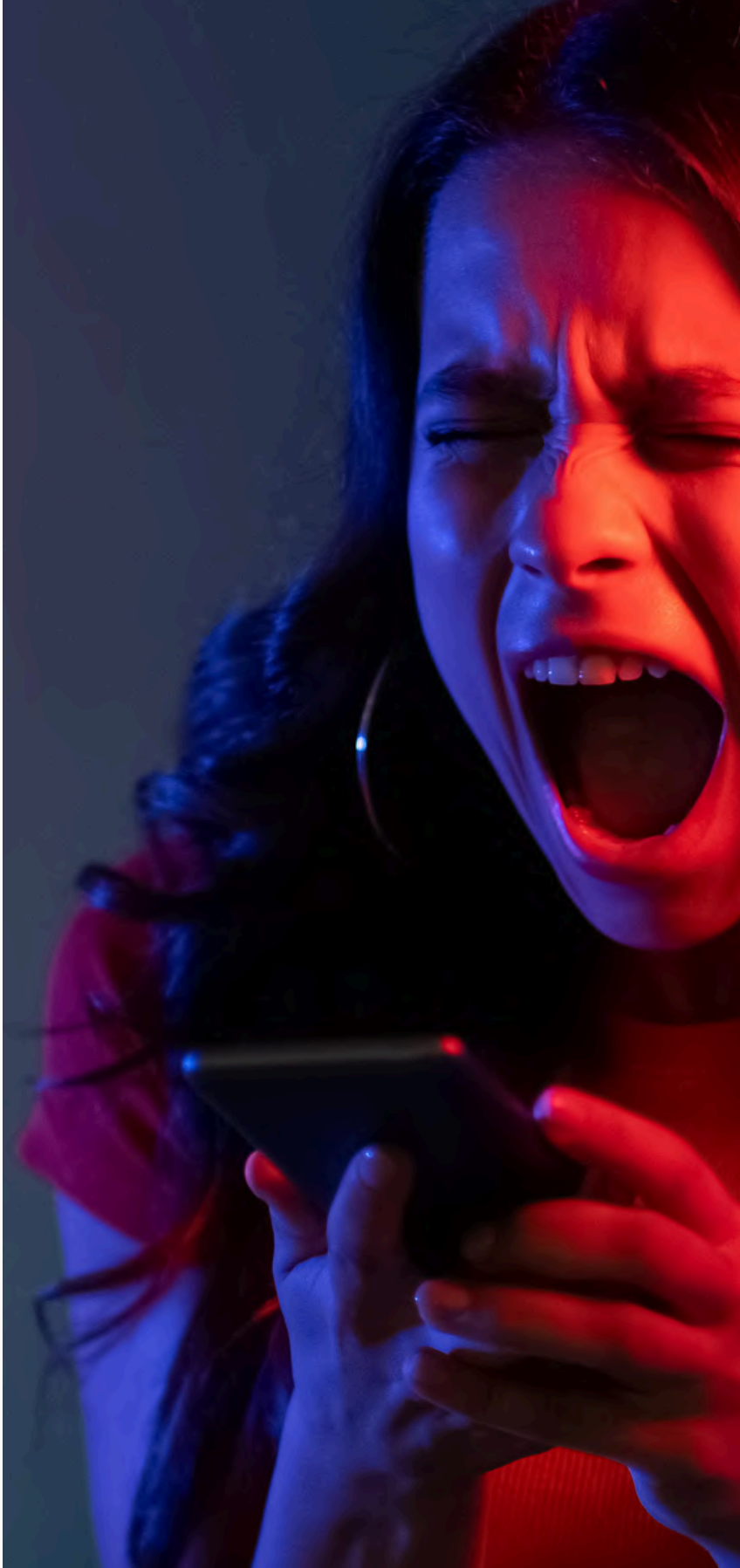
LABC

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.